

Brayan Allen, Brendon Bapst,
Terri Allan Xiks

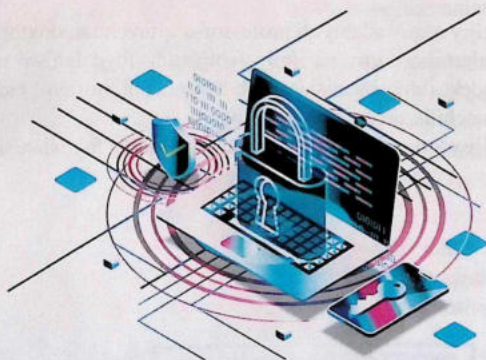


KIBERTAHDIDLARNI BOSHQARISH DASTURINI YARATISH

Brayan Allen, Brendon Bapst, Terri Allan Xiks

KIBERTAHDIDLARNI BOSHQARISH DASTURINI YARATISH

Raqamli texnologiyalar asrida xavfsizlik tizimini takomillashtirish



Toshkent – “Donishmand ziyosi” – 2025

UO'K 004.056.55(075.8)
KBK 32.811.4ya73
A 45

00.2
A 51

**O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi
huzuridagi Oliy ta'limni rivojlantirish tadqiqotlari markazining
buyurtmasiga asosan nashrga tayyorlandi va chop etildi.**

Ingliz tilidan **Dilnoza Radjabova** tarjimai

Brayan Allen, Brendon Bapst, Terri Allan Xiks.

Kibertahdidlarni boshqarish dasturini yaratish [Matn]: qo'llanma / Brayan
Allen va boshq. – Toshkent: Donishmand ziyosi, 2025. – 232 b.

Mazkur kitobda kibertahdidlarni boshqarish dasturini loyihalash, ishlab chiqish va tatbiq etishga doir batafsil ma'lumotlar keltirilgan bo'lib, bu dastur tashkilotning muayyan ehtiyojlariga qaratilgan. Ushbu qo'llanmada taklif qilingan strategik tushuncha va taktik ko'rsatmalar korporativ tashkilot direktorlari, ishboshqaruvchilar, xavfsizlik bo'yicha mutaxassislar, auditorlar uchun mo'ljallangan.

Mazkur xorijiy o'quv adabiyoti professor-o'qituvchilar, doktorantlar, magistrantlar va talabalarning o'quv va ilmiy faoliyatida foydalanishi uchun mo'ljallangan. Shuningdek, ilmiy izlanishlar olib borayotgan mustaqil tadqiqotchilar va keng ilmiy jamoatchilik uchun tavsiya qilinadi.

Ushbu xorijiy o'quv adabiyotidan tijorat maqsadida foydalanish qat'iyan man etiladi.



Kibertahdidlarni boshqarish dasturining yaratilishi

Kibertahdidlarni boshqarish bugungi kunda tashkilotlar duch keladigan eng jiddiy muammolardan biridir. Kitob kibertahdidlarni boshqarishning barqaror va ishonchli dasturini aniqlash va uni amaliyotda qo'llashni, shuningdek, uni amaliyotda to'g'ri qo'llashning afzalliklarini ham izohlaydi. Mazkur kitobda kibertahdidlarni boshqarish bo'yicha mutaxassislar Brayan Allen, Brendon Bapst va yozuvchi Terri Allan Xiks tomonidan tahdidlarni boshqarish va boshqa bir qator masalalar bo'yicha tavsiyalari ham berilgan.

Qo'llanmada xalqaro standartlar, qonun-qoidalar va direktorlar maslahat kengashining ko'rsatmalariga muvofiq tashkilotning nazorat majburiyatlarini bajarish usullari keltirilgan.

Mazkur kitob:

- Raqamlashtirish olib kiradigan transformatsion o'zgarishlar va kibertahdidlarni tushunishga;
- asosiy qonunchilik va tartibga solish asoslarini tushunishga, "kibertahdidlarni boshqarish" – tashkilotning eng ustuvor vazifalaridan biri ekanligini anglashga;
- kibertahdidlarni boshqarishning rasmiy dasturini tashkil etuvchi to'rt komponent haqida to'liq tasavvurga ega bo'lishga;
- tashkilotda CRMP bo'yicha berilgan ko'rsatmalarni amalda tatbiq etishga yordam beradi.

"Men, dunyodagi eng katta iqtisodiy texnologiyalar (Fintech¹) kompaniyasida kibertahdidlarni boshqarish dasturini ishlab chiqqan va takomillashtirgan kiberxavfsizlik bo'yicha mutaxassis sifatida shuni ayta olamanki, ishbu kitobda keltirilgan dasturning tuzilishi va g'oyalari turli sanoat hamda kompaniyalarda ishlayotgan kiberxavfsizlik mutaxassislariga foydali bo'ladi".

Greg Montana

Ishonchli milliy axborot xizmatlari (FIS²)
kompaniyasining sobiq ijrochi direktori
va boshqaruvning mustaqil a'zosi

¹ Fintech (financial technologies) – bank va moliyaviy xizmatlarni qo'llab-quvvatlash yoki taqdim etish uchun ishlatiladigan kompyuter dasturlari va boshqa texnologiyalar.

² FIS (Fidelity National Information Services) – Ishonchli milliy axborot xizmatlari.

Brayan Allen – Bank siyosati instituti kiberxavfsizlik va texnologik tahdidlarni boshqarish vitse-prezidenti bo'lib, bank rahbarlari bilan faoliyat yuritadi va sanoat manfaatlarini qonun chiqaruvchilar, huquqni muhofaza qiluvchi organlar, maxfiy xizmat jamoalari oldida himoya qiladi.

Brendon Bapst – EY³ kompaniyasining kiberxavfsizlik bo'limida tahdidlar bo'yicha maslahatchi. U kibertahdidlarga qarshi kurashda strategik rivojlanish dasturlarini ishlab chiqish jarayonida rahbarlar, fuqarolik jamiyati tashkilotlari va axborot xavfsizligi bo'yicha bosh mutaxassislar (CISO⁴) bilan yaqindan hamkorlik qiladi.

Terri Allan Xiks biznes va texnologiyalar sohasi yozuvchisi sifatida 30 yildan ko'proq tajribaga ega. Shuningdek, Allan Xiks Gartnerda 20 yildan ortiq faoliyat yuritib, moliyaviy xizmatlar, axborot xavfsizligi, normativ talablarga rioya qilish va korporativ boshqaruvga ko'proq e'tibor qaratgan.

³ EY (Ernst & Young Global Limited) – dunyoning eng yirik malakaviy xizmatlar tarmoqlaridan biri.

⁴ CISO (Chief Information Security Officer) – axborot xavfsizligi bo'yicha bosh mutaxassis.

KIRISH

Kasbiy faoliyatimizda biz ba'zan muhim burilish nuqtalarini boshdan kechiramiz: ish joyimizning o'zgarishi, boshqa kasbni tanlashimiz yoki yangicha qarashlarni qabul qilishimiz – bularning barchasi bizning hayot yo'limizni sezilarli tarzda o'zgartiradi. Bizning kuchli istak va maqsadli qiziqishimiz ham ko'plab kognitiv munozaralarga sabab bo'ladi. Ushbu munozaralar esa xavfsizlikka tahdidni boshqarish uchun muhim hisoblangan tamoyil hamda faol va qiymatga asoslangan yondashuv yaratishimizga asos bo'ldi. G'oyalar va strategiyalar evolyutsiyasi strukturali va keng qamrovli kibertahdidlarni boshqarish dasturi (keyingi o'rinlarda CRMP⁵)ning yaratilishiga olib keldi.

Brayanning hikoyasi

Bir necha yillar oldin ta'til paytida ayolim bilan Kaliforniyaga uchayotganimizda, men o'zimga oddiy bir savol berdim va bu savol men uchun haqiqiy kashfiyot bo'ldi. CRMP nima? O'sha paytda bu oddiy narsa bo'lib tuyuldi. Men bu savolga darhol javob topishga harakat qildim, ammo 30 ming futlik masofada Internet sekin ishlaganligi sabab, bu savolimga aniq javob topish qiyin bo'ldi. Savolning paydo bo'lishiga men o'qigan bir hujjat sabab bo'ldi. Bu Qimmatli qog'ozlar va birjalar komissiyasi (SEC⁶)ning 2018-yildagi kiberxavfsizlikni nazorat qilish bo'yicha korxona direktorlar kengashi va mansabdor shaxslar uchun ko'rsatmalari edi. SECning ushbu qo'llanmasida, direktorlar kengashi va korxona mansabdor shaxslari CRMPni nazorat qilishlari lozimligi alohida ta'kidlab o'tilgan. Biroq men savolimga na bu ko'rsatmadan va na boshqa manbalardan qoniqarli javob topdim. Kompaniyalarning bu savolga javobi borligiga SEC ishonar edi, biroq bu javobi yo'q muhim savol edi.

Ta'til paytida men nima sababdan SEC qo'llanmasini o'qiganimni tushuntirib berishimga ijozat bering. Men o'n yildan ko'proq vaqt davomida "Fortune 130" (Amerikaning eng yirik kompaniyalari ro'yxati kiritiladigan jurnal) ro'yxatiga kiritilgan muhim infratuzilma, telefon va Internet xizmatlari provayderi bo'lgan Time Warner Cable⁷da xavfsizlik bo'limi boshlig'i (CSO⁸) bo'lib ishlaganman. Men tajribamga tayanib, o'zimning uzoq yillik hamkasbim Rashel Leyer (Rachelle Leyer) bilan birgalikda "Tashkilotning favqulodda vaziyatlarda xavfsizlik

⁵ CRMP (Cyber risk management program) – kibertahdidlarni boshqarish dasturi.

⁶ SEC (Securities and Exchange Commission) – Qimmatli qog'ozlar va birjalar komissiyasi, Amerikaning qimmatli qog'ozlar bozorini nazorat qiluvchi va tartibga soluvchi asosiy organi.

⁷ Time Warner Cable – Amerika kabel televideniyesi kompaniyasi.

⁸ CSO (Chief security officer) – xavfsizlik bo'limi boshlig'i.

boshqaruvi: tushunchalar va ilovalar” nomli kitobimni yozgan edim. Tashkilotning favqulodda vaziyatlarda xavfsizlik boshqaruvi konsepsiyasi muhim tushunchaga asoslanadi. O‘z mohiyatiga ko‘ra, xavfsizlik bu tahdid bilan bog‘liq funksiyadir va xavfsizlik bo‘yicha mutaxassis bajaradigan har bir vazifa tahdidning besh asosiy tamoyillari orqali ko‘rib chiqilishi lozim: 1) Sizning mol-mulkingiz nima? 2) U bilan bog‘liq tahdidlar nimalardan iborat? 3) Bu tahdidlarning ta‘sirini qanday kamaytirishingiz mumkin? 4) Noxush voqealarga qanday munosabatda bo‘lishingiz mumkin? 5) Sharoit va atrof-muhitingiz haqida qanday doimiy ta‘lim olishingiz mumkin? Siz kiberxavfsizlik, jismoniy xavfsizlik, biznesning uzluk-sizligini ta‘minlash, firibgarlikka qarshi kurash yoki xavfsizlik sohasidagi boshqa yo‘nalishlar bilan shug‘ullanishingiz mumkin, bu muhim emas. Har bir yo‘nalishdagi taktika ushbu besh asosiy prinsipning biriga mos keladi. Ushbu kitobda keltirilgan tushunchalarni amalda qo‘llash hamda direktorlar kengashi va kompaniya rahbarlari bilan ishlash maqsadida men EY konsalting firmasiga murojaat qildim. Faoliyatimning aynan shu davrida favqulodda vaziyatlarda xavfsizlik boshqaruvida rahbarlarning roli nimadan iborat ekanligi meni qiziqtirdi. SEC hujjati zerikarli bo‘lib tuyulsa-da, u mening kasbimni o‘zgartirgan bir kashfiyot bo‘ldi. Qiziquvchanlik meni yana o‘z domiga tortdi.

Keyingi bir necha yil ichida Brandon va men bu masalani sinchkovlik bilan o‘rganib chiqdik va boshqa hamkasblarimiz bilan ko‘plab suhbatlar o‘tkazdik. Natijada esa yanayam ko‘proq savollar tug‘ila boshladi. Ikkalamiz ham yirik tashkilotlarda kibertahdidlarni boshqarish dasturlarini baholash va ishlab chiqish bo‘yicha katta tajribaga ega bo‘ldik. EY kompaniyasini tark etganimdan so‘ng, biz tahdid bilan bog‘liq keng qamrovli standartlar to‘plamini ishlab chiqishga harakat qildik. Biz direktorlar kengashi qabul qilgan tavsiyalarni tahlil qilib, boshqaruvchilarning javobgarligini belgilaydigan sud amaliyotlarini o‘rganib chiqdik va umuman, taktik zaruriyatdan tashqari, xavfsizlikning strategik funktsiya sifatidagi ahamiyati va vazifasini tahlil qildik.

Quyida esa izlanishlarimiz natijalarining ba‘zilarini keltirib o‘tamiz:

- Xavfsizlik – bu tahdid bilan bog‘liq funksiyadir (biz buni bilardik).
- Tahdidlarni boshqarish – bu yetuk amaliyot (xavfsizlik sohasida tahdidlarni boshqarish amaliyoti yetarli darajada rivojlanmagan).
- Xavfsizlik sohasidagi ko‘pgina tashkilotlar va mutaxassislar maxsus yondashuvga ega (qonunchilik, tartibga soluvchi organlar va o‘zgaruvchan iqtisodiyot korxonaning xavfsizlikni ta‘minlash metodlaridan yangicha umid qilmoqda, bularning barchasi tahdidlarni boshqarish funksiyasining kuchaytirilishi – oldinga siljish yo‘li ekanligini ko‘rsatadi).

• CRMP alohida dastur sifatida aniq izohlanishi mumkin, ochig‘ini aytganda, hozirgi bosqichda bu dastur ixtiyoriy emas.

CRMPni yaratish haqiqatan ham ahamiyatlidir, ammo rasmiy dastur sifatida tahdidlarni boshqarishni amalga oshirish tuzilma va majburiyatni talab qiladi.

Brendon bilan sayohatimiz ajoyib bo'ldi va u hali ham davom etmoqda. Biz bir-birimizni juda hurmat qilamiz va doimo bir-birimizni izlanishga undaymiz. Har safar suhbatlashganimizda men undan yangi narsani o'rganaman. Men Brendonni hamkasbim va yaqin do'stim sifatida qadrlayman.

Brendonning hikoyasi

EY kompaniyasi kiberxavfsizlik bo'limi maslahatchisi sifatida men bosh me-nejlar, fuqarolik jamiyati tashkilotlari, CSO, CISCO va turli sohalaridagi eng yirik kompaniyalarning xavfsizlik bo'yicha mutaxassislari bilan hamkorlik qilish sharafiga muayassar bo'ldim. Bu davrda kompaniyalar xavfsizlikni ta'minlash maqsadida taktik metodlardan tahdidlarni boshqarishda kompleks metodlarga o'tdi, bu esa eng qiyin muammolarni hal qilishda muhim qadam bo'ldi.

Bu yo'ldagi muvaffaqiyatim bebaho tajribalarim va ayniqsa hayotimdagi ba'zi insonlarning ta'siri bilan bog'liq edi. Kiberxavfsizlik dunyosiga kirib kelishim 15 yil oldin, amakim Jim Mazotasning tavsiyasi bilan boshlangan. U tadbirkor va bir nechta kiberxavfsizlik kompaniyalar asoschisidir. So'ng Malon universitetida ta'lim olib, sertifikatlarga ega bo'ldim. EY kompaniyasidagi faoliyatim davomida bir nechta rahbar va hamkasblarimning maslahatlari mening hayot yo'limni yana-da boyitdi.

Mijozlar bilan ishlash davomida men har bir kompaniyaning kiberxavfsizlik yo'nalishi takrorlanmas, yagona ekanligini angladim. Ulardan ba'zilari o'zgarish-larning dastlabki bosqichida bo'lib, fundamental muammolarga duch kelishadi va rahbariyat tomonidan turli darajada qo'llab-quvvatlanadi. Boshqalari esa, ayniq-sa moliyaviy xizmatlar va sog'liqni saqlash kabi sohalar, favqulodda vaziyatlar-da kiberxavfsizlik boshqaruvi bo'yicha yanada rivojlangan tajribaga ega. Ammo hamma narsada umumiy xususiyat mavjud: biznes faoliyatlarining tez sur'atlarda raqamlashtirilishi va tartibga soluvchi organlar tomonidan bosimning ortib bora-yotganligi shuni anglatadiki, xavfsizlikni ta'minlashda korporativ yondashuv yana rivojlanishda davom etishi lozim.

Bu kitob men va do'stim Brayan yillar davomida to'plagan g'oyalar, tajri-balar va eng yaxshi amaliyotlarning umumlashmasidir. Mazkur kitob xavfsizlik bo'yicha mutaxassislar, tahdidlarni boshqarish bilan shug'ullanuvchi boshqa in-sonlarga nazariya bilan bir qatorda kasbiy o'sish rejasi, ish joyida kuchaytirilgan xavfsizlik, shaxsiy hayotda va kasbiy faoliyatda qoniqishni oshirish kabi ma'lumotlarni taqdim etadi. Mazkur kitob tez sur'atlarda o'zgarayotgan dunyo uchun qo'llanmadir, chunki texnologiya va tahdidlar doimo rivojlanib borayotgan bo'lsa-da, bizning tahdidlarni oqilona boshqarish tamoyillari haqidagi ma'lumotlari-miz o'zgarmaydi.

Men Brayanni ustoz sifatida juda ham qadrlayman, u bilan hamkorlik qilish men uchun ajoyib tajriba bo'ldi. Ushbu kitob ustida ishlayotganda, men "nima uchun biz professional e'tiqodlarimizga sodiqmiz" degan savolga yanada oydin-

lik kiritdim. Mening maslahatchi sifatidagi tajribam hamda Brayanning xavfsizlik bo'limi boshlig'i va maslahatchi sifatidagi bebaho tajribasi shuni anglatadiki, ushbu kitob CRMPni yaratish bo'yicha yaxlit nuqtayi nazarni taqdim etadi.

Umumlashtirish

Biz, Brayan va Brendon, bir necha yildan buyon CRMPni takomillashtirish ustida ishlab kelmoqdamiz. Ushbu sohada faoliyat boshlashimizga bizning qiziquvchanligimiz va sohada mavjud bo'lgan tushunchalarga qarshi kurashishga urinishimiz sabab bo'lgan. Umid qilamizki, bu kitob sizni ham ilhomlantiradi, shuningdek, tajribangizni, korxona bo'limingizni yoki shaxsiy martabangizni rivojlantirishga bo'lgan qiziqishingizni oshiradi. Ushbu kitob nafaqat tahdidlarni boshqarishga ta'rif beradi, balki shaxsiy CRMPingizni qanday yaratishingizni ham aniq ko'rsatadi. Bu dastur mavjud standartlar, qonunlar va avtoritar yo'riqnoma tomonidan qo'llab-quvvatlansa maqsadga muvofiq bo'lar edi. Dastur mustaqil bo'lishi va xavfsizlik amaliyotining strategik elementlari uchun ishonchli asos bo'lib xizmat qilishi kerak. Shuningdek, u kutilgan natijalarga ega va himoyalangan. Raqamli texnologiyalar sharoitida bu dastur xavfsizlikni ta'minlashda yordam berishi, shuningdek, strategik qarorlar qabul qilishga, javobgarlikdan himoyalashga va xavfsizlikning strategik sherik sifatidagi ahamiyati to'g'risida ma'lumot berishga hissa qo'shadi.

CRMP haqidagi ta'rifimizni asoslash uchun SEC ko'rsatmalarini tahlil qila boshlaganimizda, biz yanada ko'proq narsalarni aniqladik. SEC majburiyatlarni rasmiylashtirishdan tashqari, sudlarda korxona rasmiylari, shu jumladan, axborot xavfsizligi bo'yicha bosh direktorlarning javobgarlik masalalarini ham ko'rib chiqayotgan edi. Bundan tashqari, doimiy ravishda yangi tahdidlarning paydo bo'lishi va ma'lumotlarning sizib chiqishi sababli har bir sanoat sohasi raqamli riskka duch keldi. Xavfsizlik bilan shug'ullanadigan tashkilotlar o'zlarining sa'y-harakatlarini jamoatchilikka yetkazish uchun bor kuchlarini sarfladilar va biror nojo'ya voqea sodir bo'lgan taqdirda ayb ularga yuklanmasligi uchun harakat qila boshlashdi. Bu kabi tashkilotlar "byudjetlar tasdiqlanganligi sababli hamma narsa xavfsiz" degan afsonani yo'qqa chiqarish uchun tinimsiz kurashdilar.

Bugungi kunda bu muammolarning ko'lamini va murakkabligi o'sib bormoqda. Barcha tashkilotlar raqamli texnologiyalarga o'tmoqda va bu zarur bo'lgan tahdid muvozanati masalalarini muhokama qilmasdan turib risk zonalarining shiddat bilan o'sishiga olib kelmoqda. Shu bilan birga, tadbirkorlar byudjet mablag'lari yetishmovchiligini boshdan kechira boshlayaptilar, ular yangi iqtisodiyotga tez moslashmasa, yanayam jiddiyroq xavf – raqobat va uning jiddiy oqibatlariga duch kelishadi, bu esa xavfsizlik bo'yicha tashkilotlarga yanada ko'proq bosim o'tkazadi.

Faoliyatimiz davomida biz vakolatli organlar bilan tanishdik va bu bizga CRMPni aniq izohlashga yordam berdi. Ma'lum bo'lishicha, foyda olish uchun

juda ko'p narsa mavjud. Bu shunchaki hali shakllantirilmagan xolos. Biz CRMP tuzilmasini SEC tavsiyalari, risklarni boshqarishning xalqaro standartlari, tartibga soluvchi organlarning yondashuvlari, sud amaliyoti va korxona direktorlari milliy uyushmasi (NACD⁹) tavsiyalari asosida shakllantirdik.

Bu tuzilma rasmiy dasturni tashkil etuvchi to'rt asosiy komponentni o'z ichiga oladi, shuningdek, uni amalga oshirish bo'yicha batafsil ko'rsatma beruvchi yordamchi tamoyillardan ham iborat. Tuzilma ushbu kitobda keltirilgan g'oyalarni qo'llab-quvvatlaydi va ularni *CRMP.info* manzilidan topish mumkin. Amaliyotda joriy etilgandan so'ng, u alohida rasmiy dastur yaratilishiga olib kelishi kerak va bu dastur barcha savollarga javob berishi lozim.

Ushbu kitob haqidagi umumiy tasavvurimiz aniq: sizga tizimlashtirilgan va aniq izohlangan CRMPni hamda uni amalga oshirishga yordam beradigan g'oyalar va tavsiyalarni taqdim etish.

Kitob kimlar uchun mo'ljallangan

Biz ushbu kitobni iloji boricha ko'pchilikka foydali bo'lishi uchun nashr etdik, shu bilan birga, har bir bosqichda kitobdagi ma'lum bir kontent aynan kim uchun foydali bo'lishi aniq ko'rsatilgan. Bizning fikrimizcha, quyidagi shaxslar kitobdan eng ko'p manfaatdor bo'lishi mumkin:

Turli darajadagi xavfsizlik bo'yicha mutaxassislar

Tahdidlarni boshqarish – ko'p yillar davomida ishlab chiqilgan, amaliyotda qo'llanilgan va takomillashtirilgan bo'lsa-da, u odatda keng qamrovli, rasmiylashtirilgan xavfsizlik dasturi sifatida qaralmaydi. Dasturni ishlab chiqish – ushbu amaliyotning yetuklik darajasi, niyat va maqsadini aniqlashga yordam beradi.

Turli faoliyat sohasidagi xavfsizlik bo'yicha mutaxassislar

Ushbu kitobning asosiy qismi kiberxavfsizlikka bag'ishlangan bo'lsa-da, undagi asosiy tushunchalar jismoniy xavfsizlik, firibgarlikka qarshi kurash, biznes uzluksizligi, barqarorlikni ta'minlashda tahdidlarni dasturiy boshqarishda qo'llanilishi mumkin.

Direktorlar kengashi

Ushbu kitob direktorlarga CRMPni nazorat qilishda ularning vazifasi va mas'uliyati haqida to'liq tushuncha berish uchun mo'ljallangan. Qo'llanmada dasturni yaratishda rahbariyatning vazifasi to'g'risida ma'lumotlar ham mavjud. Asosiy tamoyillar kiberxavfsizlikni biznes tahdid sifatida ko'rib chiqish muhimligini ta'kidlaydi, bu esa direktorlar kengashiga ko'proq dolzarb savollar va boshqaruvga oid aniqroq ko'rsatmalar berish imkoniyatini beradi. Direktorlar o'z e'tiborlarini kiberxavfsizlik usullaridagi texnik detallardan ko'ra, tahdidlarni boshqarishning strategik vazifasiga ko'proq qaratmalar, kiberxavfsizlikni boshqarish dasturining

⁹ NACD (National Association of Corporate Directors) – Korxona direktorlari milliy uyushmasi.

samaradorligini oshirishlari va o'sib borayotgan huquqiy va me'yoriy majburiyatlardan o'zlarini himoya qilishlari mumkin.

Mijozlar bilan ishlash bo'lim boshlig'i (CxO¹⁰) va biznes yo'nalish rahbarlari

Ushbu shaxslar yuqori darajadagi qaror qabul qiluvchilar bo'lib, ular tahdidlarni boshqarish amaliyotida xavfsizlikni ta'minlashning zarurligi to'g'risida aniq tasavvurga ega bo'ladilar, bu ularga ortib borayotgan javobgarlikni tushunish va ulardan himoyalanişga yordam beradi. Xavfsizlikka tahdid borasida to'g'ri va asosli qaror qabul qilishlari uchun bu shaxslarga xavfsizlik choralari ham o'rgatiladi.

Tartibga soluvchi organlar

Tartibga soluvchi organlar ushbu kitobda keltirilgan ko'rsatmalardan mantiqiy, ishonchli va takrorlanadigan maqsadlarga asoslangan qonun-qoidalarni ishlab chiqishda foydalanishlari mumkin. Umumiy taksonomiya va umumiy maqsad ularning harakatini yanada unumli, samarali va kuchli qiladi.

Auditorlar

Audit mutaxassislari odatda eng yaxshi tajribalarga e'tibor qaratishadi, mavjud siyosat, standartlar, asoslar va qonun hujjatlariga nisbatan korxona yoki tashkilotning xavfsizlik jarayonlari samaradorligini baholashadi. Ushbu kitob auditorlarga favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturlarini baholashda foydalanishi mumkin bo'lgan keng qamrovli tuzilmani taqdim etadi, chunki unda biznesning tahdidga moyilligi va unga chidamliligiga nisbatan xavfsizlikni ta'minlashga alohida e'tibor qaratiladi.

Raqamli texnologiyalar sabab yuzaga kelgan tahdidlar tadbirkorlar va kasb egalari ish faoliyatiga ta'sir qilishi mumkin

Raqamli texnologiyalarning ta'siri keng qamrovli, murakkab bo'lib, uni oldindan taxmin qilib bo'lmaydi. Natijada, turli soha mutaxassislari, aksariyat tadbirkorlar va ko'pgina kompaniyalarning qaror qabul qiluvchi shaxslari, raqamlashtirish yuzaga keltirgan tahdidlarni qanday aniqlash, tahdid va mukofot muvozanatiga oid asosli qarorlar qabul qilishga doir ma'lumotlarni o'rganib, juda katta foyda olishadi.

Yakuniy xulosa

Bu shubhasiz, ajoyib sayohatdir. Bu muammoning tezkor yechimi mavjud emas, uning nozik tomonlari cheksiz bo'lib, ular hali o'rganilishi kerak va bu shunga arziydi. Buning uchun biz o'z fikr va g'oyalarimizni: hozirgi kunda nimalar mavjudligi, o'tmishda qanday shug'ullanganimizni qayta ko'rib, yangi narsalarni o'rganishga ishtiyoqmand bo'lishimiz kifoya.

¹⁰ CxO (Chief experience officer) – mijozlar bilan ishlash bo'lim boshlig'i.

Mazkur kitob kiberxavfsizlik yo‘nalishi mutaxassislari uchun maxsus yozilgan, CRMP konsepsiyasi xavfsizlikka oid tahdidlar bilan bog‘liq turli amaliyotlarda ham qo‘llanilishi mumkin.

Ishonchimiz komilki, olgan bilimingiz sizning kasbiy faoliyatingizga yordam beradi.

Fikr-mulohaza bildirish, savollar berish uchun *CRMP.info* manziliga tashrif buyurishingiz mumkin.

Kitobda qo‘llanilgan shartli belgilar

Ushbu kitobda quyidagi tipografik belgilar qo‘llanilgan:

Kursiv (italics)

Yangi atamalar, URL manzillar, elektron pochta manzillari, fayl nomlari va fayl kengaytmalarini ko‘rsatadi.



Ushbu element umumiy eslatmani anglatadi.

Minnatdorchilik

Kasbiy faoliyatimizga va bu kitobni yozishimizda bizni qo‘llab-quvvatlagan va yo‘l ko‘rsatgan ko‘p insonlarga minnatdorchilik bildirishimiz lozim. Bizni doimo qo‘llab-quvvatlaydigan oilamizga, ayniqsa mehribon ayollarimiz Mariya va Saraga, hayotimiz davomida qiziquvchan bo‘lishimizga poydevor yaratgan va doimo ruhlantirgan ota-onamizga alohida minnatdorchilik bildiramiz. Shuningdek, yozuvchi va mulohazali do‘stimiz Terri Allan Xiksga; ushbu kitobni yozish jarayonida bizga yordam bergan O‘Rayli kompaniyasidagi Sara Hanterga; mayda detallarga ham sinchkovlik bilan e‘tibor qaratgan muharririmiz Adam Lourensga, fidoyi taqrizchilarga o‘z minnatdorchiligimizni bildiramiz.

1 BOB. RAQAMLI TEXNOLOGIYALAR ASRIDA KIBERXAVFSIZLIK: DUNYO TAHDID OSTIDA

Butun jahonda hukm surgan pandemiya Xitoy korxonalari faoliyatini to'xtatdi va bu bilan AQSHdagi Detroit shtatidan tortib, Yaponiyaning Yokogamasi-ga qadar mavjud zavodlardagi ishlab chiqarish jarayonining keskin susayishiga sabab bo'ldi, shuningdek, pandemiya ta'minot borasidagi muammolarni ham keltirib chiqardi. Amerika samolyoti parvozdan bir necha daqiqa o'tgach, sirli ravishda pastga qulab tushadi va natijada bortdagi barcha odamlar halok bo'ladi; olti oydan kamroq vaqt o'tgach esa, dunyoning narigi tomonida xuddi shu marka va modeldagi samolyot ham deyarli xuddi shu tarzda yerga qulab tushadi. Yoki Floridadagi suv ta'minoti stansiyasidagi boshqaruv tizimlariga ta'sir ko'rsatgan noma'lum shaxsni olaylik: uning suvni tozalash uchun ishlatiladigan kimyoviy moddalar miqdorini 100 marotaba oshirishi natijasida o'lim holatlari yuzaga ke-ladi. Yana bir tovlamachi shaxs esa odam o'g'irlashni soxtalashtirish maqsadi-da sun'iy intellektidan foydalanib, o'sha odamning yolg'on ovozini yaratadi, bu holat butun dunyo saylov vakillarini xavotirga soladi, chunki bu kabi "chuqur soxtalashtirish"lar demokratik saylovlarga putur yetkazishi mumkin. Boshqa bir misol: Ukraina harbiylari tomonidan ishlatilgan Rossiyaning sun'iy yo'ldosh navigatsiya tizimiga qarshi kiberhujumi shamol turbinalarini Germaniyagacha olib boradi; tajovuzkor shaxs pul undirib olish maqsadida katta quvur tizimini egallab oladi, bu esa vaqtinchalik AQSHning sharqiy qirg'og'ida katta yoqilg'i tanqisligini keltirib chiqaradi.

Ushbu fojiaiy voqealar bugungi kunda bizning kundalik hayotimiz hamda unga bog'liq bo'lgan tizim va jarayonlar qanchalik nozik ekanligidan dalolat beradi. Dunyo aloqa va hamkorlik maqsadida tobora ko'proq raqamli texno-logiyalarga tayanganligi sayin, ushbu murakkab munosabatlar majmuyi paydo bo'lmoqda. Raqamli texnologiyalar sabab juda tez sur'atlarda paydo bo'layot-gan tahdidlar tufayli bunday murakkab munosabatlar yuzaga kelmoqda. Hozirda butun dunyo bo'ylab korxonalar tahdidlarga duch kelmoqda, bu haqda biz bir necha yil oldin hatto tasavvur ham qila olmas edik. Bunday tahdidlar moliyaviy manfaatlariga jiddiy zarar yetkazishi va ba'zi hollarda kompaniyalarning biznes-dan chiqib ketishiga ham olib kelishi mumkin. Buning sababi nafaqat kibertah-didga qarshi kurashdagi muvaffaqiyatsizliklar, balki raqobat hamdir, ya'ni bir kompaniyaning tavakkal qilish qobiliyati va raqobatchisiga qaraganda tezroq harakat qilishidir.

Xavfsizlik tashkilotlari bu kabi tahdidlar keltirib chiqarayotgan muammolar-ni hal qilishda qiynalishmoqda va ko'pincha muvaffaqiyatsizlikka uchrashmoqda.

Ushbu kitob tubdan farq qiladigan yangi biznes va texnologiya sharoitida oldinga siljish yo'lini taqdim etadi. Mualliflarning ushbu sohadagi ko'p yillik tajribasiga asoslangan yondashuvga ko'ra, tashkilot o'zini bugun va kelajakda himoya qila olishi uchun keng miqyosda CRMPni kompleks tarzda ishlab chiqishi lozim. Kitobda ko'plab masalalar ko'rib chiqilgan. Nafaqat xavfsizlik bo'yicha mutaxassislar, balki korxonaning manfaatdor tomonlari ham korxonada ishlash parametrlari va strategik qarorlarni qabul qilishlari lozim. Asosiy masala – bu CRMPni aniqlash, uni ishlab chiqish va hayotga tatbiq etishdir.

Butunjahon nazorat qiluvchi organlari tashkilotlarning kibertahdidlarni qanday yo'llar bilan hal qilishayotganini, tahdidlarga bardoshlilik usulini qay tarzda yo'lga qo'ygani, uning amalga oshirilishi, ushbu dasturiy yondashuv ustidan tegishli nazorat amalga oshiriladimi yoki yo'qmi degan savollarga to'g'ri ko'proq e'tibor qaratmoqdalar. Sudlar kibertahdidlarni boshqarishga bevosita mas'ul bo'lgan kompaniya rahbarlari maslahat kengashi, kompaniya boshliqlari va tashkilotning boshqa mas'ul shaxslari: axborot xavfsizligi xizmati boshliqlarining shaxsiy javobgarligiga ko'proq ahamiyat bermoqdalar. Dasturning mavjud emasligi hamda dastur natijalarining o'zi bunday javobgarlik uchun asos bo'lishi mumkin.

Ko'pgina kitobxonlar, ayniqsa tajribali xavfsizlik mutaxassislari, biz taqdim etayotgan CRMPning ba'zilar yoki barcha komponentlarini bilishlari mumkin, ehtimol ular hech bo'lmaganda qisman ularning ba'zilarini allaqachon amalda qo'llashgan. Xavfsizlik bo'yicha mutaxassislar – bu tahdidlarni boshqarish bo'yicha mutaxassislardir (bu biz qayta takror va takror ko'rib chiqadigan muhim tushuncha). CRMPni ishlab chiqish va amalga oshirishda bu mutaxassislarning tahdidlarni boshqarish bo'yicha tajribasi bebahodir. Bu yondashuvning boshqalardan farqi shundaki, bunda barcha komponentlar bitta yaxlit, mukammal, rasmiy dasturda birlashtiriladi, bu butun tashkilot va sarmoyadorlarni hozirgi va kelajakdagi barcha tahdidlardan himoya qilish uchun mo'ljallangan keng qamrovli dasturdir.

Ushbu kitobda rasmiy CRMPning ta'rifi turli ishonchli manbalar asosida batafsil ko'rib chiqiladi, ishlab chiqilgan dasturning asosiy elementlarini isbotlash maqsadida global standartlar, qoidalar, sud ishlari va nufuzli manbalardan asoslar keltiriladi. Kitobda tahdidlarni boshqarish usulining amaliy yondashuvi tasvirlanmasa-da, unda ko'plab tahdidlarni boshqarish usullariga havolalar beriladi va dasturga kiritilishi mumkin bo'lgan misollar keltiriladi.

Hozirda CRMP nima uchun kerak? Raqamli texnologiyalar xavfsizlikning har bir sohasiga kiberelement olib kirdi va so'nggi yillarda kiberoxavfsizlik butun dunyo bo'ylab korxonalarning eng dolzarb muammolaridan biriga aylandi.

To'rtinchi sanoat inqilobi

Ba'zan "Sanoat 4.01" deb ataladigan "To'rtinchi sanoat inqilobi"¹¹ atamasi 2010-yillarda Jahon iqtisodiy forumi (WEF¹²) asoschisi, iqtisodchi Klaus Shvab tomonidan ommalashtirilgan. Mazkur konsepsiyaga odatda o'zaro bog'liq va avtomatlashtirilgan texnologiyalar natijasida yuzaga keladigan tizim va jarayonlardagi tez sur'atlardagi o'zgarishlar deb izoh beriladi va bu jarayon o'z navbatida jismoniy va raqamli dunyo o'rtasidagi farqlarni mavhumlashtiradi. Ushbu texnologiyalar orasida sun'iy intellekt, ilg'or robototexnika, mashina-mashina (M2M¹³) aloqa, Buyumlar interneti (IoT¹⁴)ni tashkil etuvchi avtonom qurilmalar tarmoqlari va boshqa ko'plab narsalar mavjud. Bu texnologiyalar yangi, kutilmagan tarzda ta'sir qilar ekan, ular insoniyat tarixida oldin hech qachon kuzatilmagan ijtimoiy, siyosiy, iqtisodiy va madaniy o'zgarishlarni keltirib chiqarmoqda.



Jahon iqtisodiy forumining 2016-yildagi "To'rtinchi sanoat inqilobi" haqidagi hisobotida shunday deyilgan: "Hozirgi o'sish tezligi ilgari hech qachon kuzatilmagan. Oldingi sanoat inqiloblari bilan solishtirganda, to'rtinchi inqilob chiziqli (tizilgan) emas, balki jadal tarzda rivojlanayotgan inqilobdir. Bundan tashqari, u har bir mamlakatdagi deyarli barcha sanoat sohasiga muammo tug'dirmoqda. Bu o'zgarishlarning kengligi va chuqurligi esa butun ishlab chiqarish, boshqaruv va boshqaruv tizimlarining o'zgarishidan darak beradi"¹⁵.

Biz hozir boshimizdan kechirayotgan keskin o'zgarishlarni tushunishimiz uchun, avvalambor, bir qadam ortga qaytib, tarixiy o'zgarishlarni qarab chiqishimiz muhim:

- Birinchi sanoat inqilobi sanoat ishlab chiqarishi (po'lat va to'qimachilik zavodlari) va transportni (poyezdlar va kemalar) ishga tushirish uchun – suv va daryolar (tegrimon g'ildiraklarini aylantirish maqsadida) hamda bug' qozonlarini quvvatlaydigan ko'mir qozonlardan foydalangan.
- Ikkinchi sanoat inqilobi bu jarayonlarni elektrlashtirib, haqiqiy ommaviy ishlab chiqarishga imkoniyat yaratdi.

¹¹ Ushbu nemis atamasi davlatning ishlab chiqarish va boshqa sanoatlardagi ahamiyatini ifodalaydi.

¹² WEF (World Economic Forum) – Jahon iqtisodiy forumi.

¹³ M2M (Machine-to-machine communication) – har qanday aloqa kanalidan foydalanadigan qurilmalar o'rtasida to'g'ridan to'g'ri aloqa.

¹⁴ IoT (Internet of Things) – Internet orqali boshqa qurilmalar va tizimlar bilan ma'lumotlarni ulash va almashish uchun sensorlar, dasturiy ta'minot va boshqa texnologiyalar bilan o'rnatilgan jismoniy obyektlar tarmog'ini ifodalaydi.

¹⁵ Klaus Schwab, "To'rtinchi sanoat inqilobi: Bu nimani anglatadi, unga qanday javob berish lozim" Jahon iqtisodiyot forumi, 2016-yil, 14-yanvar.

▪ Uchinchi sanoat inqilobi elektronikaga, avtomatlashtirishdan foydalanishga va operatsion samaradorlikni oshirish uchun ma'lumot almashishga asoslangan va bu hozir ham davom etmoqda.

▪ To'rtinchi sanoat inqilobi bir necha yil oldin hatto tasavvur ham qilinmagan operatsion samaradorlik va innovatsiyalar tezligini ta'minladi. Bu, birinchi navbatda, mavjud tizimlar, ilovalar, qurilmalar va jarayonlarni raqamlashtirish va eng muhimi, yangi raqamli texnologiyalarni uzluksiz, doimiy va tezkor yaratish bilan bog'liq.

Kelajakda dunyo "To'rtinchi sanoat inqilobi"ga o'zidan oldingi boshqa inqiloblarga nisbatan ancha radikal, keskin va muhim o'zgarish sifatida qaraydi. "To'rtinchi sanoat inqilobi" asosan uchinchi sanoat inqilobiga asoslanadi. Asosiy texnologik ishlanmalar shu davrga to'g'ri keladi: lampochka, mashina, radio, televizor va hokazolarning paydo bo'lishi.

Tashkilotlar va ular duch keladigan tahdidlarga ta'sir ko'rsatadigan beshta asosiy ko'rsatkich mavjud:

Sanoat kesishuvi

Sanoatlar o'zgarimoqda va o'zgarishlar davri doimiy ravishda tezlashmoqda. Yangi ekotizimlar, biznes modellari va iste'molchilarning xatti-harakatlari bozorining barcha segmentlarida sanoat chegarasini mavhumlashtirmoqda. Sanoat ekotizimlarida uchinchi shaxslar bilan, ba'zan hatto raqobatchilar bilan ham hamkorlik qiladigan korxonalar ilgari noma'lum bo'lgan tahdidlarga duch kelishmoqda, chunki ular muqarrar ravishda ma'lum darajada nazoratni boshqa tomonga berib qo'yadi.

Globallashuv

Qiymat zanjirida ishtirok etuvchi shaxslar va tashkilotlar, ya'ni ishlab chiqaruvchilar, ta'minotchilar, hamkorlar, mijozlar butun dunyo bo'ylab tarqalgan bir paytda, korxonalar o'zlari duch keladigan tahdidlar xilma-xil, oldindan taxmin qilib bo'lmaydigan va bu kabi tahdidlarga ular oldin hech qachon duch kelmaganliklarini anglashlari lozim.

Nazoratdan umidlar

Hozirda tashkilotlar qonun chiqaruvchi va tartibga soluvchi organlar, sanoat va iste'molchi tashkilotlari, shuningdek, boshqa manfaatdor tomonlar tarafidan har qachongidan ham ko'proq nazorat qilinmoqda. Manfaatdor tomonlarning barchasi korxonalarning biznes amaliyoti ustidan nazoratning kuchaytirilishini kutmoqda va ko'p hollarda buni talab qilmoqda.

Da'volar bilan bog'liq muammolar

Ko'pincha korxona harakatlari va harakatdagi muvaffaqiyatsizliklar, masalan, kiberxavfsizlikda ma'lumotlarning tarqalishi kabi hodisalar halokatli da'volarga olib keladi.

Normativ-huquqiy bazaning o'zgarishi

Normativ talablar tobora murakkab, qat'iy va ko'pincha munozarali bo'lib bormoqda. Bu esa qoidaga rioya qilmaslik xavfini hamda bu xavflarni boshqarish mashaqqati va xarajatlarini oshiradi.

Bu ko'rsatkichlarning barchasi ikki buzuvchi omil bilan tavsiflanadi: tezlik va hajm. Barcha narsalar keskin sur'atlarda sodir bo'lmoqda, bozor, siyosat, iste'molchilarning xatti-harakatlari shiddatli tus olmoqda, bu esa hamma narsaning yanada murakkabroq, o'zgaruvchan, bashorat qilish va boshqarishning qiyinlashuviga olib kelmoqda. Natijada, korxonalar har qachongidan ham tezkor bo'lishi va tahdidga oid qarorlar qabul qilishda shu tezkorlikni yanayam takomillashtirishi lozim.

Raqamli texnologiyalar ishlab chiqaruvchilarga operatsion tizim va logistika samaradorlikka erishishga imkon berdi, bu o'zgarishlarni bir necha yil oldin hattoki tasavvur qilish qiyin edi. Keling, uning qanday ishlashini oddiy: elektr transport vositasida foydalanish uchun mo'ljallangan yarimo'tkazgichning dizayni, sinovdan o'tkazilishi, ishlab chiqarilishi, yukning yetkazib berilishi va uning o'rnatilishi misolida ko'rib chiqamiz. Avvalo, Kaliforniya shtatidagi dizayn jamoasi chipning texnik xususiyatlarni Xitoydagi zavodga yuborishadi, zavodda uning prototipi ishlab chiqiladi. Prototip tayyor bo'lgach, u sinov uchun Michigan shtatidagi avtomobil ishlab chiqaruvchi kompaniyaga yuboriladi. Agar prototip talablarga javob bersa, texnik xususiyatlar Xitoyning boshqa hududida joylashgan zavodga jo'natiladi, u yerda ishlab chiqaruvchi chipning bir qismi bo'lgan noyob tuproq elementlari va boshqa materiallarni sotib olishni boshlaydi va ishlab chiqarish jadvalini rejalashtiradi. Bunday muhim jihat shundaki, jarayondagi turli bosqichlar har xil mutaxassislar tomonidan amalga oshirilishi mumkin. Bu mutaxassislar bir tashkiliy tuzilma yoki bir kompaniyaning xodimi bo'lishi shart emas va aksariyat hollarda bunday bo'lmaydi. Biroq, ularning barchasi raqamli dunyoning bir qismiga aylanadi, bu esa barcha ishtirokchilarni bu yo'lda yuzaga keladigan raqamli tahdidlarni hisobga olgan holda jarayonlar va o'zaro ta'sirlarni qayta ko'rib chiqishga majbur qiladi.

Aytaylik, ishlab chiqarish jarayoni muammosiz o'tdi va yarimo'tkazgichlarning birinchi partiyasi jo'natishga tayyor. Raqamli texnologiyalar ushbu jo'natmani batafsil kuzatish imkonini beradi. Ishlab chiqaruvchi har qanday vaqtda yarimo'tkazgichning qaysi yuk tashish konteynerida, qaysi ushlagichda, qaysi kemada va qaysi portda ekanligini aniq biladi. Bu nima uchun muhim? Bu ishlab chiqaruvchiga ishlab chiqarish jadvalini mutlaq aniqlik bilan rejalashtirishga imkon beradi. Chip asboblari elektr transport paneliga o'rnatilishi uchun o'z vaqtida yetkazib beriladi. Ishlab chiqarish kechiktirilmaydi va ishlab chiqaruvchi ham keraksiz zaxiralarni saqlash bilan bog'liq xarajatlar va xatarlardan xoli bo'ladi. Bu samaradorlik raqamli ulanish yordamida amalga oshiriladi va u "o'z vaqtida tejash" hamda real vaqtda aloqa va ma'lumot almashish imkonini beradi.

Ushbu tendensiyalar qanchalik tez o'zgarib bormoqda? O'zgarish tezligining ajoyib ko'rsatkichlaridan biri Standard & Poor's 500 indeksi¹⁶ bo'lib, u AQSHdagi eng qadimgi va eng muhim fond indekslaridan biridir. Taxminan yarim asr oldin, 1969-yilda, an'anaviy sanoat kompaniyalari, asosan ishlab chiqarish konsernlari, ro'yxatga kiritilgan 500 ta kompaniyaning uchdan bir qismini tashkil etgan. Bugungi kunda ro'yxatda faqat 68 ta sanoat korxonalari mavjud, birinchi o'rinni axborot texnologiyalari bilan shug'ullanadigan kompaniyalar egallaydi. S & P birjasida ro'yxatga olingan kompaniyalarning umr ko'rish davomiyligidagi o'zgarishlar bundan ham hayratlanarli. Innosight¹⁷ agentligining ma'lumotlariga ko'ra, 1964-yilda kompaniyalarning S & P ro'yxatidagi o'rtacha muddati 33 yilni tashkil etgan, S&P bashoratiga ko'ra, 2027-yilga kelib bu ko'rsatkich 12 yilga qisqaradi.

Bu nimani anglatadi? Tashkilotlar tezroq harakat qilishlari lozim. Tez harakat qilish tavakkal qilishni anglatadi. "Tavakkal-mukofot" dialogidagi muvozanat qisman turli tahdidlar o'rtasidagi muvozanatni saqlash bilan bog'liq. Bunday holda, kibertahdidlar boshqa loyihalarning samaradorligi va moliyalashtirilishiga ta'sir qilishi, shuningdek, ko'proq tavakkal qilishga tayyor yoki qodir bo'lgan raqobatchilardan ortda qolishiga olib kelishi mumkin. Yaxshi CRMP tahdid haqida ishonchli ma'lumotlarni o'z vaqtida taqdim etishi va kompaniyalarga ularni yaqin kelajakda nima kutayotganini bilishga va tezroq harakat qilishga imkon berishi kerak. Bunday hollarda, kompaniyalar tahdidlarni tezroq aniqlab olishadi, misol uchun, ishlatilishi kerak bo'lgan tormozlarning kechikishi haqida ko'proq ma'lumotga ega bo'ladi. Shubhasiz, bu narsa raqamli muhitda strategik ustunlikni anglatadi.

To'rtinchi sanoat inqilobi natijasida yuzaga kelgan tub o'zgarishlar (yangi texnologiya va yangi biznes modellarining paydo bo'lishi hamda eskilarining yo'qolishi) jarayonning keskin namunalari taqdim etdi, avstriyalik iqtisodchi Jozef Shumpeter uni "ijodiy vayronagarchilik" ("creative destruction") deb nomlagan. Jahon iqtisodiyoti raqamli texnologiya sabab yuzaga kelgan ijodiy vayronagarchilikning keskin davrini oldin hech qachon boshdan kechirmagan. Raqamli texnologiyalar innovatsiyani yetarlicha tez yoki umuman tatbiq qila olmaydigan kompaniyalarni tom ma'noda vayron qilsa-da, u yangicha fikrlaydigan va uzoqni ko'zlaydigan istiqbolli kompaniyalar uchun ijodiy imkoniyatlar eshigini ochmoqda. Ushbu kitobni o'qiyotgan xavfsizlik bo'yicha qaror qabul qiluvchilar uchun eng muhim jihat shundaki, raqamli texnologiyalar korxonalar, ularning faoliyati va jarayonlarni har qachongidan ham zaifroq qildi. Bu zaiflik va noziklik tiriklar xotirasida tom ma'noda misli ko'rilmagan voqea tufayli og'riqli tarzda namoyon bo'ldi va biz buni mazkur bobda batafsil muhokama qilamiz: COVID-19 pandemiyasi.

¹⁶ Standard and Poor's 500 yoki S & P 500 – bu AQSH fond birjalarida ro'yxatga olingan 500 ta eng yirik kompaniyalarning aksiyalar dinamikasini kuzatuvchi fond bozori indeksi.

¹⁷ Innosight Huron Consulting Group tarkibidagi strategik konsalting agentligi bo'lib, global korxonalarga biznes strategiyasi, innovatsiyalar va o'sishni o'zgartirish bo'yicha maslahat beradi.

Hozirgi kunda raqamli texnologiyalar professional va shaxsiy hayotimizning har bir jabhasida shu darajada chuqur kirib kelganki, ko'pchiligimiz buni oddiy hol deb qabul qilamiz. Bu esa ko'p hollarda, raqamli texnologiyalar olib keladigan tub o'zgarishlarni, uning professional hayotimizdagi keskin ta'sirini va eng avvalo, biz ushbu texnologiyalarga qanchalik bog'liqligimizni tushunmasligimizni anglatadi. Buni tan olmasdan turib, biz raqamlashtirish bilan bog'liq tobora ortib borayotgan tahdidlardan o'zimizni to'g'ri himoya qila olmaymiz, hatto ularni aniqlay olmaymiz. Albatta, endi bu nafaqat korxonaga, balki uchinchi tomonga ham tegishli.

Raqamli texnologiyalar dunyoni butunlay o'zgartirdi, raqamlashtirish sabab yuzaga keladigan korxona muhitidagi doimiy o'zgarishlar bilan teng qadam tashlash uchun favqulodda vaziyatlarda xavfsizlik boshqaruvi tamoman o'zgarishi kerak.

Kiberxavfsizlik – tahdid bilan bog'liq amaliyot

Murakkab, tez sur'atlarda o'zgarayotgan, bir-biriga chambarchas bog'liq bo'lgan bu dunyoda tahdiddan xoli muhit mavjud emas. Rivojlanishning dastabki bosqichidan buyon qanchadan qancha kemalar cho'kib ketgan, ekinlar nobud bo'lgan, Yevropa va Osiyoni bog'laydigan Buyuk ipak yo'lidagi karvonlar bosqinchilar tomonidan hujumga uchragan (bularning barchasi hozirgi "ta'minot zanjiri"ning dastlabki misollaridir). Korxonalar moslashishi, yangilik kiritishi, rivojlanishi va omon qolishi uchun har doim tavakkal qilishi kerak bo'lgan. Biznesning har bir yo'nalishi, u yoki bu tarzda, tahdidlarni boshqarish bilan bog'liq (bu har doim to'g'ri bo'lgan. Uch ming yil oldin qadimgi Misr savdogarlari o'z yuklarini sug'urta qilishgan). Mana yana bir amaldagi misol: moliya direktorining byudjet qarorlari tahdidlarni boshqarish jarayonini ifodalaydi, chunki u resurslarni qay tarzda ishlab chiqarish, tadqiqot, marketing, aksiyalarni qayta sotib olish va xavfsizlikka taqsimlanishini qaror qiladi. Bir sohaga ajratilgan har bir dollar, yevro, rupiy yoki iyen boshqa sohadan olinishiga to'g'ri keladi va moliya direktori xarajat va tahdid o'rtasidagi juda nozik muvozanatni saqlab qolishi kerak.

Tahdiddan xoli muhit mavjud emas.

Favqulodda vaziyatlarda kiberxavfsizlik boshqaruvi dasturining vazifasi – bu tashkilotlardagi qaror qabul qiluvchi shaxslarga ular duch kelishi mumkin bo'lgan tahdidlarni tushunishga va tahdidlarni inobatga olgan holda qaror qabul qilish jarayoniga yordam berishdir.

Bu nafaqat moliya direktori, balki xavfsizlik bo'yicha mutaxassislar uchun ham amal qiladi. Xavfsizlik bo'yicha mutaxassislar korxonadagi roli va mavqeyidan qat'i nazar, barcha tahdidlarni bartaraf etishga harakat qilmasliklari kerak, bu ilojisiz ish bo'libgina qolmasdan, qimmatli vaqt va resurslarning asossiz isrof qilinishi hamdir. (Bu nazariyani ko'pchilik intuitiv (ichki hissiyotlar bilan) tushunadi, chunki hammamiz kundalik hayotimizda tavakkalga asoslangan qarorlar qabul qilamiz. Bir oddiy misol: biznes uchrashuvga kechikayotgan odam tezlikni oshirgani uchun jarima qog'ozi olishi yoki yangi mijozni yo'qotishi mumkin, u tavakkal va mukofot orasidagi to'g'ri muvozanatni aniqlashi lozim bo'ladi.) Buning o'rniga, ular korxonaning manfaatdor tomonlari bilan birga tavakkal va mukofot o'rtasidagi to'g'ri muvozanatni aniqlashlari, tahdidning maqbul darajasini belgilashlari hamda mos keladigan xavfsizlik va tahdidlarni boshqarish choralari ishlab chiqishlari kerak.

Xavfsizlik bo'yicha mutaxassis – bu tahdidlarni boshqarish mutaxassisidir.

Xavfsizlik bo'yicha mutaxassislar har doim tahdidlarni boshqarish bilan shug'ullanishgan. Lekin ular odatda tahdid yoki zaifliklar aniqlangandagina tahdidlarni bir martalik yondashuv asosida bartaraf etishgan. Bu tabiiy hol, chunki tahdidlarni oldindan taxmin qilish va ularga tayyorgarlik ko'rish har doim qiyin masala bo'lgan, ammo hozirgi raqamlashtirish asrida, bu strategiya talabga javob bermaydi. Xavfsizlik bo'yicha mutaxassislarning ko'pchiligi buni allaqachon anglashgan va o'z tajribalarini oshirish uchun harakat qilmoqdalar, shunga qaramasdan hali qilinishi kerak bo'lgan ishlar juda ko'p. Bizning fikrimizcha, xavfsizlik va tahdidlarni boshqarish kasbiy fanlar sifatida yuqori darajada rivojlanishi lozim, xavfsizlik tashkilotlari esa bunga faqat qonunlashtirilgan favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturini tatbiq etish orqaligina erishishlari mumkin.

Yuzaga kelayotgan tahdidlarni tezlikda bartaraf etish hamda korxonaning o'zgaruvchan talablarini qondirish maqsadida xavfsizlik tizimi yetarli darajada rivojlangan bo'lishi lozim, bunga esa mukammal CRMP orqaligina erishsa bo'ladi.

Bu xavfsizlik tizimida bir qator tub o'zgarishlarni anglatgani bois, ko'pgina xavfsizlik mutaxassislari uchun bu masala qiyin bo'lishi shubhasiz. O'zgarishlar har doim qiyinchilik tig'dirgan, raqamli texnologiyalar sababli yuzaga kelgan tub o'zgarishlar ayniqsa qiyin bo'lishi aniq. Ushbu kitobni o'qiyotgan xavfsizlik bo'yicha mutaxassislar raqamli texnologiyalar tufayli vujudga kelgan tahdidga

asoslangan xavfsizlik yondashuvlari faqatgina qiyin emas, balki ular kasbiy hamda shaxsiy aloqalar va rivojlanishga imkoniyatlar berishini tushunishlari juda muhim. Xavfsizlik bo'yicha mutaxassislar o'zlarining asosiy vazifasi sifatida tavakkal va mukofot o'rtasidagi to'g'ri muvozanatni aniqlash va unga erishish uchun asosiy manfaatdor tomonlar bilan ishlashni tushunishadi va korxonani yaxshiroq himoya qilishga yordam berishadi. Shuningdek, xavfsizlik bo'yicha mutaxassislar, manfaatdor tomonlar ularni faqatgina antivirus dasturlarini o'rnatish bilan shug'ullanadigan yoki virtual tarmoqlarni joriy etadigan texnik xodimlar sifatida emas, balki strategik qaror qabul qiluvchi hamkasb sifatida qabul qilishlariga yordam beradi. Qisqasi, xavfsizlik masalalari boshqa muhim qarorlar singari muhim o'rin egallashi lozim, biroq bu ish oson emas. Bunda xavfsizlik bo'yicha mutaxassislardan o'zlarining keng qamrovli texnologik bilim va ko'nikmalarini yanada kengaytirish va rivojlantirish talab etiladi. Ular, shuningdek, ilgari "xavfsizlik" yoki "texnologiya" deb hisoblanmagan sohalarda ham o'z ko'nikmalarni rivojlantirishlari kerak bo'ladi. Misol uchun, biznes rahbarlari uchun tushunarli tillarda muloqot qilishni o'rganish kabi ko'nikmalarni rivojlantirish. Xavfsizlik bo'yicha mutaxassislardan dunyo va korxonani o'zgartirayotgan o'zgarishlar, tahdidlarni boshqarishning qonun-qoidalarini chuqurroq tushunish talab qilinadi.

Kibertahdidlarni boshqarish nazorati va javobgarligi

Shubhasiz, o'zgarayotgan narsa texnologiya emas, balki sizni o'zgartirayotgan texnologiyadir.

Janna Ros, Massachusetts texnologiya instituti,
Sloun axborot tizimlari tadqiqot markazi

Bugungi o'zgaruvchan davrda qayta ixtiro qilishdan boshqa yo'l yo'q. Siz boshqalardan ustun bo'lishingiz mumkin bo'lgan yagona barqaror jihatingiz – bu tezkorlik yoki epchillikdir. Boshqa hech narsa barqaror emas, siz yaratgan hamma narsaning nusxasini boshqalar ham yaratadi.

Jeff Bezos, "Raqamli texnologiya va tezkor biznesni shakllantirish"¹⁸

("Digital Transformation and Becoming an Agile Business")

Tahdidlarni boshqarish amaliyoti va nazorati tartibga soluvchi organlar va sudlarning e'tiborini tortdi. Masalan, SEC tomonidan taqdim etilgan yangi qoidalar to'plamiga ko'ra, jamoat kompaniyalari belgilangan vaqt ichida kiberxavfsizlik bilan bog'liq muhim noxush hodisalar to'g'risida xabar berishlari, kiberxavfsizlik hamda tahdidlarni boshqarish va strategiyalar bo'yicha hisobot berishlari lozim. Raqamli texnologiya har bir "zararli" hodisani kiberhodisaga aylantirib,

¹⁸ Jeff Bezos, "Digital Transformation and Becoming an Agile Business". 2023-y.

korxona xavfsizligi va korxona miqyosida tahdidlar to'g'risida qaror qabul qilishda kiberxavfsizlikning markaziy o'rinni egallashini anglatadi. Sanoatni tartibga soluvchi organlar ham kibertahdidlarni boshqarish va ularni nazorat qilishga ko'proq e'tibor qaratmoqdalar.

Sudlar ham endi korxonalarda tahdidlarni boshqarish bo'yicha kimlar mas'ul ekanligiga o'z e'tiborlarini qaratmoqdalar. Buni 2-bobda batafsil muhokama qilamiz. Direktorlar kengashi va kompaniya xodimlari, shu jumladan CISO ham, endilikda taktik ijro majburiyatlaridan tashqari, tahdidlarni boshqarishga ham mas'uldirlar.

“Nimaga aynan hozir” degan savol ham ushbu nazorat mas'uliyati bilan bog'liq. CRMP mavjud standartlar, sud amaliyoti va direktorlar kengashi darajasidagi kibertahdidlarni boshqarish ta'lim provayderlari tavsiyalariga, xususan, NACD va Jahon iqtisodiy forumi taqdim etgan tavsiyalarga asoslangan oqilona dasturni ishlab chiqishda yordam berishi mumkin.

Raqamli texnologiyalar va CRMPni takomillashtirish

So'nggi yillarda kiberhujumlarning hajm, jiddiyligi va murakkablik jihatidan hayratlanarli darajada o'sib borayotganligini kuzatish mumkin. Buning sabablari juda ko'p: masofaviy ish hajmining keskin o'sishi, xodimlarga tegishli qurilmalardan foydalanish, internetga qaramlikning kuchayishi va boshqa holatlarni misol qilish mumkin. Shubhasiz, ularning barchasining ta'siri sezilmoqda. 2021-yil noyabr oyida e'lon qilingan tadqiqotga ko'ra, dunyo bo'ylab 81% tashkilotlar o'sib borayotgan kibertahdidni boshdan o'tkazishgan va favqulodda vaziyatlarda kiberxavfsizlik tufayli ishlashdan to'xtashgan. Dunyo bo'ylab kiberjinoyatlardan olingan daromad 2022-yilda 8,4 trillion dollarga baholangan.

Yangi texnologiyalarning juda tez sur'atlarda doimiy ravishda yaratilishi korxonalarda tahdid turlarining ham o'zgarishiga olib keladi. Bu kiberxavfsizlikning vazifasi faqatgina tizimlar va ma'lumotlarni himoya qilishdan iborat emasligini anglatadi va bu faqatgina xavfsizlik tashkilotining muammosi emas.

Kiberxavfsizlik shunchaki “xavfsizlik” muammosi emas

Garchi kiberxavfsizlik – korxona xavfsizligi mutaxassislarining asosiy faoliyat sohasi bo'lsa-da, u korxonadagi vazifalarning katta qismiga ta'sir qiladi. Shu sababli, bu kitob nafaqat xavfsizlik mutaxassislariga, balki tashkilotlarda qarorlar qabul qilishda ishtirok etuvchi shaxslarga ham manfaatli bo'ladi deb umid qilamiz. Quyida bu shaxslarning ba'zilarini ko'rib chiqamiz va nima sababdan aynan ularga kiberxavfsizlik muammolarini hal qilishda zarur choralarni ko'rish muhim ekanligi haqida to'xtalib o'tamiz (1.1-jadvalga qarang).

**Turli lavozim egalari uchun CRMPning
afzalliklari**

Lavozim	Tahdid bilan bog'liq vazifa va majburiyatlar	CRMPning afzalliklari
Direktor (Kengash a'zosi)	Kompaniya amaliyotini nazorat qiladi va mustaqillikni ta'minlaydi.	Korxona uchun muhim tahdidlarni bilgan holda kibertahdidlarni boshqarish bo'yicha nazorat majburiyatlarini amalga oshirish uchun ishonchli tizim.
Kompaniya xodimi (CxO)	Nazoratni amalga oshiradi va korxona uchun muhim bo'lgan tahdidlar haqida kengashni xabardor qiladi. Tahdidlarni kamaytirishga oid tavsiya etilgan rejalarni ko'rib chiqadi va tasdiqlaydi.	Bozorda raqobatbardoshlik va dolzarblikni saqlab qotishda tahdidga oid zarur analitik ma'lumotlarga ega bo'lish – butun korxonada ma'lum tolerantlikka muvofiq tahdidni to'g'ri amalga oshirishga doir strategik ko'rsatmani taqdim etadi.
Korxona bo'limi rahbari	Korxona bo'linmalari va korxona funksiyasiga xos bo'lgan tahdidlar haqida tushuncha beradi.	Korxona bo'linmalari tomonidan qaror qabul qilishda zarur bo'lgan tahdidlar to'g'risida ma'lumot beradi.
Axborot xavfsizligi bo'yicha bosh mutaxassis	Tahdid muhitini kuzatishga imkon beradi, korxonani tahdidning maqbul darajasini o'rnatishga yo'naltiradi va tahdidlarni kamaytirish strategiyasining belgilangan talablarga mos ekanligiga ishonch hosil qiladi.	Tashkilotning tahdidga moyilligini hisobga olgan holda davomiy byudjet biznes asoslarini talif qiladi.
Komplaens ¹⁹ yoki tahdidlar bo'yicha menejer	Asosiy tahdidlarni aniqlash va ularni kamaytirish bo'yicha tavsiyalar beradi.	Korxona samaradorligini oshirishda ishonchli vosita sifatida xizmat qiladi.
Bosh yuriskonsult	Tashkilotning yuridik strategiyasi va kiberxavfsizlikka yondashuv (normativ talablarni tahlil qilish, kiberxavfsizlik bilan bog'liq yuridik tahdidni boshqarish, tashkilotning kiberxavfsizlik bilan bog'liq har qanday hodisalarga munosabatini huquqiy nuqtayi nazardan nazorat qilish) bo'yicha ko'rsatma beradi.	Yuridik guruhga tashkilotdagi kiberxavf darajasi haqida aniq ma'lumot beradi, bu esa ularga o'z vaqtida ma'lumot olish va potensial huquqiy muammolarni hal qilish imkonini beradi. Bu aniqlik ularga to'g'ri va asosli huquqiy maslahatlarni taqdim etadi.

¹⁹ Komplaens – bu qonun hujjatlariga, ichki hujjatlariga, xalqaro standartlarga rioya qilmaslik natijasi, shuningdek, nazorat qiluvchi organlar tomonidan sanksiyalar va (yoki) boshqa ta'sir choralari qo'llash natijasida yuzaga keladigan xavflar, zararlar va reputatsiyaviy yo'qotishlarning oldini olishga qaratilgan chora-tadbirlar tizimi.

Kiberfunksiya egasi (Cyber function owner) yoki amaliyotchi	Xavfsizlik bilan bog'liq sohalardan tahdid haqida ma'lumot beradi. Tahdidlarni kamaytirish bo'yicha kelishilgan strategiyani amalga oshiradi va uning samaradorligini kuzatib boradi.	Tashkiliy maqsadlar bilan kundalik taktik ishlarni birlashtiradi (ushbu vazifaga katta ahamiyat bergan holda).
Auditor	CRMPning dizayni va ishlashini mustaqil ravishda sinab ko'radi.	Dizaynli, aniq tushuntirilgan dastur.

Kiberxavfsizlik butun korxona, sanoat va tashkilotlarga ta'sir qiluvchi juda muhim omildir. Quyida sanoat sohalarning eng muhimlarini ko'rib chiqamiz (1.2-jadvalga qarang).

1.2-jadval

Har bir sanoat sohasining CRMPga ehtiyoji

Soha (Sector a ²⁰)	Texnologiyani qo'llashning tasviriy misollari	Nimalar tahdid ostida ekanligiga misollar
Energiya ishlab chiqarish va taqsimlash	AT va operatsion tizim (OT ²¹) manbalari unumdorlik va operatsion samaradorlikni oshirish maqsadida internetga ulangan.	Hamma narsa. Barcha tarmoqlar energiya ta'minoti barqarorligiga bog'liq. Energiya ta'minotsiz iqtisodiyot o'z vazifasini bajara olmaydi hamda odamlar salomatligi va farovonligi tahdid ostida qoladi.
Moliyaviy xizmatlar	Blokcheyn (Blockchain) ²² , robototexnika va AI / mashinali o'qitish (machine learning (ML) ²³) kabi raqamli texnologiyalar yaxshiroq xizmat ko'rsatish maqsadida moliyaviy tizimni optimalashtiradi.	Kapital bozorida ishonchsizlik bo'lsa va pul qiymatlarini saqlash hamda uzatish qobiliyati mavjud bo'lmasa jamiyat o'z vazifasini bajara olmaydi.

²⁰ "Muhim infratuzilma sektorlari", 2023-yil 10-oktyabr.

²¹ OT (Operational technology) – Operatsion tizim. Operatsion tizim – bu kompyuter texnikasi va foydalanuvchi o'rtasidagi interfeys bo'lib, uning asosiy vazifasi texnik ta'minot va dasturiy ta'minot o'rtasidagi aloqani ta'minlash hisoblanadi.

²² Blockchain (Blokcheyn) – bu markazlashtirilmagan ma'lumotlar bazasi bo'lib, u o'zida undan ro'yxatdan o'tgan barcha ishtirokchilar ma'lumotlari (o'tkazmalari) haqida ma'lumotlarni alohida "zanjir" shaklida saqlash imkonini beradi

²³ ML (machine learning) – Mashinali o'qitish – bu sun'iy intellekt nazariyasining bir bo'limi, kompyuter sun'iy intellekt yordamida hal qilish jarayoni va usullarini izlashdan iborat.

Transport va logistika²⁴	Bir-biriga yaqin transport vositalari va infrastruktura bilan real vaqtda ma'lumot almashadigan ulangan transport vositalari yangi avlod aloqa texnologiyalariga misol bo'lib, ular sayohatning xavfsizroq, samaraliroq bo'lishi va atrof-muhitga kamroq zarar keltirishi uchun loyihalashtirilgan.	Transport tizimlariga noqonuniy kirish haydovchilarning shaxsiy ma'lumotlarining yo'qolishiga yoki avtomobil funksiyalarini boshqarishga olib kelishi mumkin, bu esa baxtsiz hodisalar yoki o'limga sabab bo'lishi mumkin.
Sanoat	Avtomatlashtirish, sun'iy intellekt, 3D modellash (qo'shimchalar ishlab chiqarish) kabi raqamli texnologiyalar samaradorlik va hajmi oshiradi hamda mahsulotni bozorga olib chiqarish jarayonini tezlashtiradi.	Hozirda ushbu texnologiyalarning huquqiy javobgarligi, shuningdek, xavfsizlik va atrof-muhitni muhofaza qilish javobgarligi hali ham shakllanish bosqichida, internet xakerlari ishlab chiqarish chizmalari yoki rejalarini har qachongidan ko'ra osonroq qo'lga kiritadilar, bu esa yo'qotishlar xavfini oshiradi va hujum qilish uchun ko'proq imkoniyatlarni ochadi.
Sog'liqni saqlash	Tutash muhitlar, taqib yuriladigan qurilmalar (elektron qurilmalar), robotlashtirilgan jarrohlik amaliyotlari haqida ma'lumotlarni ishlab chiqaradigan kognitiv tizimlar sanoatni markazlashtirib rivojlantirmoqda, bu sog'liqni saqlash tizimining yaxshilanishiga va xarajatlarning kamayishiga yordam beradi.	Malakali tajovuzkorlar (masalan, pul miqdori to'lanmaguncha kompyuter tizimiga kirishni blokirovka qiladigan dasturdan foydalanadigan kiberjinyatchilar)ning maqsadli hujumlari himoyalangan tibbiy ma'lumotlarning buzilishiga va hatto muhim bo'lgan tibbiy xizmatlarning ishlashiga xalal berilishi.
Ta'lim	Bilim va axborot almashinuvi bir zunda va keng miqyosda amalga oshirilib, ta'limning aholining kengroq qatlami-ga yetib borishiga imkon beradi.	Tahdid darajasining o'sishi va maxfiylikning mavjud bo'lmashligi, shuningdek, noto'g'ri ma'lumotlarning yuqori tezlikda tarqalishi.
Davlat sektori	Ma'lumotlarni tez to'plash va ularni tahlil qilish, fuqarolar ishtirokini oshirish va ko'proq sifatli xizmatlar bilan ta'minlash.	Texnologik taraqqiyot natijasida hosil bo'lgan tahdidning umumiy murakabligi butun dunyo hukumatlar uchun sinov bo'ladi, bunda muammolarni samarali hal qilishda malaka va imkoniyatlarning yetishmasligi seziladi.

²⁴ "AQSH transport vazirligi ulangan transport tizimini kibertahdidlardan qanday himoya qilmoqda", AQSH transport departamenti, 2023-yil, oktyabr.

Aloqa	5G ²⁵ , AI/ML, IoT va ma'lumotlarga asoslangan tahlillar mijozlar tajribasini o'zgartirmoqda, mijozlarning xizmatlardan umidlarini (tezlik, ulanish va barqarorlik) yanada oshirmoqda.	Milliardlab ulangan qurilmalarning mavjudligi hujum sathini kengaytirdi, natijada katta va xavfliroq hujumlar amalga oshirilishiga imkon yaratildi.
Kimyo	Har qachongidan ham murakkabroq bo'lgan global ta'minot zanjiri butun dunyo bo'ylab olingan xomashyoni zamonaviy hayot uchun muhim bo'lgan 70,000 dan ortiq turli mahsulotlarga aylantirish imkonini beradi.	Kimyoviy moddalar xavfli bo'lganligi va boshqa muhim infratuzilmalar unga tayanishi sababli, ularni tobora o'sib borayotgan va rivojlanayotgan tahdidlardan himoya qilish zarur.

CRMP: Korxonaning dolzarb muammosi

Favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturining maqsadi – bu korxonani, uning yetakchilarini va boshqa asosiy manfaatdor tomonlarni xavfsizlik tahdidlari bo'yicha qaror qabul qilish jarayonida to'g'ri yo'naltirishdir. Xavfsizlik xizmati qaror qabul qilmaydi, biroq o'z tajriba va bilimlaridan kelib chiqqan holda ularga ma'lumot beradi. Natija esa, tahdid va foydani o'zaro muvozanatlashtiradigan, tahdidlarni baholashga asoslangan qarorlar to'plami vujudga keladi.

Raqamli asrda muvaffaqiyatga erishish uchun zarur bo'lgan muhim shartlardan biri – bu korxonaning favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturiga ega bo'lishidir.

Butun tashkilot – xavfsizlik tashkiloti, biznes bo'linmalari va xodimlar – favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturini doimiy ravishda rivojlantirish jarayonida ishtirok etishlari kerak. Nega? Chunki bu harakat taktik emas, strategik bo'lishi lozim. Bu dasturning muvaffaqiyatli bo'lishi uchun muhim omil bo'lib, shu bilan birga, xavfsizlik mutaxassislari uchun professional va shaxsiy rivojlanish uchun ham ahamiyatlidir. Har bir xodim muhim qarorlarni qabul qilish jarayonida ishtirok etishni xohlaydi. Rahbarlar bu jarayonga strategik fikr yurituvchilarni ko'proq jalb qilishadi; taktik jihatdan yondashadigan shaxslar esa odatda bunday imkoniyatga ega bo'lmaydi.

Soha duch keladigan eng muhim muammolardan biri – bu xavfsizlikni asosan taktik funksiya yoki faqat xarajat markazi sifatida ko'rish. Tabiiyki, bunday qarashlardan voz kechish oson bo'lmaydi va u vaqt talab etadi, lekin bu amalga oshirilishikerak bo'lgan muhim jihat. Tahdidlarni strategik boshqarishni muntazam ravishda amalga oshirish o'ta muhim.

CRMPni shakllantirish uchun biz global miqyosda tasdiqlangan va qabul qilingan tahdid standartlari, mavjud qonun-qoidalar, boshqaruvchilar hamda ken-

²⁵ 5G – mobil aloqaning beshinchi avlodi.

gashlarning tahdidni nazorat qilish uchun javobgar ekanligini ifodalaydigan sud amaliyoti bo'yicha qarorlari asosida tuzilgan bir tizimni ishlab chiqdik. Ushbu tamoyil CRMP nima va uni qabul qilishda qaysi komponentlarni hisobga olish kerakligini ifodalash orqali xavfsizlik yoki tahdid bo'yicha mutaxassis, auditor yoki nazoratchiga to'rtta asosiy komponent va qo'llab-quvvatlovchi tamoyillarni belgilab beradi. Dastur turli rivojlanish darajasidagi tashkilotlar uchun moslashtirilishi mumkin. Har qanday dastur barqarorlik va izchillik uchun qandaydir tuzilmani talab qiladi. Tadqiqot davomida barcha tahdidlarni boshqarish dasturlari izchil yondashuvga ega ekanligi aniqlandi. Ularni ta'riflash uchun turli dasturlarhar xil so'zva jarayonlardan foydalansa-da, biroq asosiy tamoyillar dastur uchun asos hisoblanadi.

CRMP to'rt muhim komponentdan iborat bo'lib, ular xalqaro standart tashkilotlari, sud qarorlari, tartibga solish tizimlari vaboshqaruv darajasidagi nizomlar orqali belgilangan:

- 3-bob, "Moslashuvchan boshqaruv"
- 4-bob, "Tahdidlar haqidagi ma'lumotlarga asoslangan tizim"
- 5-bob, "Tahdidlarga asoslangan strategiya va uning ijrosi"
- 6-bob, "Tahdidlar eskalatsiyasi²⁶ va ma'lumotlarning oshkor qilinishi"

Tizim ichida siz har bir komponent qo'llab-quvvatlovchi tamoyillar va ular haqida ma'lumot beruvchi manbalarni topasiz.

Kitobning yo'l xaritasi

Mazkur kitobda asosan CRMPni qanday aniqlash va rivojlantirish, shuningdek, uning qiymatini qanday baholash haqida gapirib o'tiladi. 2-bobda dastur nima dan tarkib topgani aniq belgilanadi. 3–6-boblarda to'rt asosiy komponent va yo'naltiruvchi tamoyillar batafsil muhokama qilinadi. 7-bobda korxonaning rivojlanish darajasiga, operatsion muhit, sanoat talablariga mos keluvchi dasturni tatbiq etish bo'yicha yo'riqnomalar taqdim etiladi. 8-bobda dastur boshqa operatsion tahdid amaliyotlari (masalan, fizik xavfsizlik, ta'minot zanjiri va uchinchi tomon xavfsizligi, biznesni davomiyli boshqaruvi va favqulodda vaziyatlardan tiklanish) bilan hamkorlik qilgan holda, butun korxonaning tahdid holatini rivojlantirishga yordam berishi mumkinligi muhokama qilinadi. 9-bobda esa yangi texnologiyalar ko'rib chiqilib, tahdidlarni boshqarish qanday qilib yetakchi amaliyot bo'lib qolishi tahlil qilinadi; shuningdek, sun'iy intellekt yanada chuqurroq tahlil qilinadi. Kitobdagi barcha misollar sof kibertexnologiyalar bilan bog'liq emas; ba'zi misollar har qanday turdagi tahdidlarni boshqarishga oid.

²⁶ Tahdid eskalatsiyasi (Risk escalation) – Tahdidning kuchayishi – bu tahdid uchun javobgarlikni tashkilot ichidagi vakolatli shaxslarga o'tkazish.

Yakuniy xulosa

Birinchi bobda korxonaning tahdid darajalarini o'zgartirayotgan keskin (transformatsion, disruptiv, qiziqarli va bir vaqtning o'zida qiyin bo'lgan) o'zgarishlar muhokama qilindi. Keyingi bobda esa, korxonalar nima uchun rasmiy va tizimli kibertahdidlarni boshqarish dasturini yaratishlari kerakligi chuqurroq tahlil qilinadi. Ushbu dastur aniq belgilangan va himoya qilingan bo'lishi, mustaqil ravishda ishlashga qodir bo'lishi va raqamli texnologiyalar asrida zarur strategik yo'riqnomani taqdim etishi kerak.

II BOB. KIBERTAHDIDLARNI BOSHQARISH DASTURI (CRMP)

Oldingi bobda biz tahdid muhitida doimiy va jadal o'zgarishlarni keltirib chiqaradigan ko'plab omillarni – ijtimoiy, siyosiy, iqtisodiy va ayniqsa texnologik omillarni ko'rib chiqdik. Ushbu bobda esa biz CRMPni batafsil ifodalab beramiz. Aniq belgilangan dastur bilan ifodalangan rasmiy yondashuv orqaligina korxonalar o'zlari duch keladigan tahdidlarning tezligi va jiddiyligi bilan bog'liq masalalarni hal qilishlari va buni izchil, ishonchli natijalar bilan amalga oshirishlari mumkin. Butunjahon tartibga soluvchi organlari bundan buyon talabga javob bermaydigan yoki umuman mavjud bo'lmagan CRMPni qabul qilmasliklarini ma'lum qilishmoqda.

SEC gapiradi – butun dunyo tinglaydi

2023-yil 26-iyuldagi tartibga soluvchi organlarning bir e'loni biznes olamini larzaga keltirdi: SEC yirik kiberhodisalar haqida xabar berish, kiberxavfsizlik tahdidlarini boshqarish, strategiya va boshqaruv bilan bog'liq ma'lumotlarni oshkor qilishga oid yangi qoidalar to'plamini joriy qildi. Kompaniyalarning oshkor qilish amaliyotini standartlashtirish va takomillashtirishga qaratilgan yangi qoidalar AQSHda faoliyat yurituvchi barcha davlat kompaniyalariga hamda ko'plab kichik va xorijiy kompaniyalarga nisbatan qo'llaniladi. SEC butun jahon miqyosida normativ standartlarni ishlab chiqish va qabul qilish bo'yicha katta nufuzga ega, chunki boshqa mamlakatlar va yurisdiksiyalardagi tartibga soluvchilar ko'pincha SECning ko'rsatmalariga ergashadilar, bu korxonaning manfaatdor tomonlari SECning yangi qoidalari va ularning ehtimoliy ta'siridan xabardor bo'lishlari lozimligini anglatadi.

SEC ushbu harakatlarni jismoniy shaxslar va korxonalarni investitsiya qarorlarini qabul qilishlarida “yanada izchil, taqqoslanadigan va qaror qabul qilishda foydali ma'lumotlar”²⁷ bilan ta'minlash uchun amalga oshirdi. Sodda qilib aytganda, bu “sezilarli darajada ahamiyatli” ma'lumotdir. SEC tomonidan berilgan ko'pyillik ta'rifga ko'ra, ahamiyatli ma'lumotlar – bu “ro'yxatdan o'tkazilgan qimmatli qog'ozni sotib olishdan oldin sarmoyador xabardor qilinishi kerak bo'lgan masalalarga oid ma'lumotlardir”²⁸. Bu umume'tirof etilgan tamoyil bo'lib, yangi qoidalar uni o'zgartirmaydi. Bundan tashqari, SEC “ahamiatlilik” kibermakonga

²⁷ Gerbrand Haverkamp, Gari Genslerga maktub, 2022-yil 19-may, Butunjahon benchmarking ittifoqi.

²⁸ Roberta S. Karmel, “Investorlar bilan aloqalar milliy instituti uchun nutq Nyu York bo'limi, Nyu York, 2-aprel, 1978-yil”, SEC, 26-aprel, 1978-yil.

ham tatbiq etilishini aniq ko'rsatmoqda, chunki SEC o'z e'lonida ta'kidlaganidek, "iqtisodiy faoliyatning tobora ortib borayotgan ulushi elektron tizimlarga shu darajada bog'liqlik, bu tizimlardagi uzilishlar [kompaniyalarga] sezilarli ta'sir ko'rsatishi va keng ko'lamli hujumlar bo'lgan taqdirda, butun iqtisodiyotga tizimli ta'sir ko'rsatishi mumkin"²⁹. SEC shunday deb ta'kidlaydi: "Dalillar shuni ko'rsatadiki, kompaniyalar kiberxavfsizlik hodisalari haqida yetarlicha xabar bermasligi mumkin" va "sarmoyadorlar asoslangan investitsiya qarorlarini qabul qilishlari uchun kiberxavfsizlik bo'yicha ma'lumotlar o'z vaqtida va izchil oshkor qilinishi zarur"³⁰.

SECning yangi qoidalarida oshkor qilishning ikkita asosiy turi ko'rsatiladi, biz ularni keyingi bo'limlarda muhokama qilamiz.

Noxush hodisalarning oshkor qilinishi ("Amaldagi ma'lumotlarning oshkor qilinishi")

SEC kiberhujumlar, ma'lumotlardan ruxsatsiz erkin foydalanish va boshqa nosozliklarni o'z ichiga oluvchi axborot xavfsizligi bo'yicha noxush hodisalarni oshkor qilish talablariga tub o'zgartirishlar kiritdi. Bu quyidagilarni o'z ichiga oladi:

- "Kiberxavfsizlik hodisasi" ta'rif kengaytirilib, "bir qator ruxsatsiz amalga oshirilgan hodisalar"ni ham o'z ichiga oldi. Bu kiberhujumlar va boshqa xavfsizlik tizimining nosozliklari yakka tartibda bo'lishi shart emasligi va uzoq vaqt davomida sodir bo'lishi mumkinligi haqidagi haqiqatni aks ettiradi.

- Kiberxavfsizlik hodisasini oshkor qilishda talab qilinadigan ma'lumotlar endi yanada aniqroq izohlangan bo'lib, noxush hodisa qachon aniqlangan va u uzluksizmi; noxush hodisaning tabiati va ko'lamining qisqacha tavsifi; ma'lumot o'g'irlanganmi, o'zgartirilganmi yoki ruxsatsiz maqsadlarda foydalanilganmi; noxush hodisaning kompaniya faoliyatiga ta'siri kabi bir qator ma'lumotlarni o'z ichiga qamrab oladi.

- Qoidalarga muvofiq, endi kompaniyalar muhim kiberxavfsizlik hodisasini aniqlaganidan so'ng, to'rt ish kuni ichida uni oshkor qilishlari shart (hukumatning oshkor qilish milliy xavfsizlik yoki jamoat xavfsizligiga zarar yetkazishi mumkinligi haqidagi qaroriga asoslangan ba'zi istisnolar mavjud). SEC, shuningdek, kompaniyalar o'zlarining muhim qarorlarini "kechiktirishlarsiz" qabul qilishlari zarurligini ta'kidlaydi.

- Noxush hodisalarni oshkor qilishda birinchi navbatda hodisaning tafsilotlariga emas, balki uning jiddiy ta'siriga, ya'ni u olib kelishi mumkin bo'lgan har qanday zararga e'tibor qaratilishi lozim. SEC, kompaniyalar jiddiyligni aniqlashda

²⁹ SEC, "Kiberxavfsizlik risklarini boshqarish, strategiya, boshqaruv va insidentlarni oshkor qilish", 2023-yil 5-sentyabr.

³⁰ SEC, "Kiberxavfsizlik risklarini boshqarish, strategiya, boshqaruv va insidentlarni oshkor qilish".

nafaqat miqdoriy omillarni, balki obro'ga putur yetkazish va mijozlar yoki sheriklarning ishonchini yo'qotish kabi sifat omillarini ham hisobga olishlari zarurligini alohida qayd etadi. Yana bir bor, asosiy mezon – ma'lumotlar sarmoyadorning qaror qabul qilishiga ta'sir qilish yoki qilmasligidan iboratdir.

**Tahdidlarni boshqarish, strategiya va boshqaruvga
oid ma'lumotlarning oshkor qilinishi
("Ma'lumotlarning davriy oshkor qilinishi")**

Bizning ishonchimiz komilki, kompaniyaning favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturi haqidagi ma'lumotlarning va direktorlar kengashining kiberxavfsizlik masalalari bo'yicha rahbariyat bilan qanday aloqada ekanligi haqidagi ma'lumotlarning oshkor qilinishi sarmoyadorlarga direktorlar kengashi tahdidlarni nazorat qilish bo'yicha o'z majburiyatini qay darajada bajarayotganini ko'rish hamda ularni baholash imkonini beradi.

SEC, "Davlat korxonalarining kiberxavfsizlikka oid ma'lumotlarni oshkor qilishlari bo'yicha komissiya bayonoti va yo'riqnomasi", 2018-yil.

SECning yangi qoidalari faqatgina noxush hodisalarnigina qamrab olmasdan, balki kompaniyaning kiberxavfsizlik amaliyotlarining butun ko'lamini hisobga oladi. Ushbu sohalaridagi asosiy o'zgarishlar quyidagilardan iborat:

- Kompaniyalardan favqulodda vaziyatlarda kiberxavfsizlikni baholash, aniqlash va boshqarish bo'yicha o'zlarida mavjud bo'lgan jarayonlarni davriy ravishda oshkor qilishlari talab qilinadi. Bu, xususan, kiberxavfsizlik jarayonlari kompaniyaning umumiy tahdidlarni boshqarish amaliyotiga kiritilganmi hamda qanday qilib kiritilganligini; maslahatchilar, auditorlar yoki boshqa uchinchi tomonlar jalb etilganligini hamda uchinchi tomonning sezilarli darajadagi muhim tahdidlarini aniqlash uchun jarayonlar mavjud yoki yo'qligini ko'zda tutadi.

- Kompaniyalar direktorlar kengashining kiberxavfsizlik tahdidlari bilan bog'liq risklarni nazorat qilishdagi vazifalari haqidagi ma'lumotlarni, xususan, ushbu tahdidlarni nazorat qiluvchi har qanday boshqaruv a'zosi yoki qo'mitaga tahdid haqidagi ma'lumotlarni oshkor qilishlari kerak (Eslatma: SEC, kiberxavfsizlik jarayonlari rahbariyat darajasida samarali amalga oshirilishi ehtimoli ko'proq degan fikrda bo'lib, kengash a'zolarining kiberxavfsizlik bo'yicha tajribasini oshkor etishni talab qilish to'g'risidagi taklifini qabul qilmadi).

- Shuningdek, kiberxavfsizlik tahdidlaridan kelib chiqadigan jiddiy xavflarni baholash va boshqarishda rahbarlik vazifasi talab etiladi.

Yangi SEC qoidalari va butunjahon tartibga soluvchi organlariga tegishli e'lonlarning tub mohiyati ayondir: kiberxavfsizlik va kibertahdid juda murakkab, keng qamrovli bo'lib, zarur bo'lgan hollarda, improvizatsiya va voqea-hodisaga asoslanib chora ko'rilishi muhimdir. Ushbu masalalar nafaqat kiberxavfsizlikni, balki kibertahdidning umumiy boshqaruvini va uning korxona miqyosidagi ta'siri-

ni ham hisobga oladigan rasmiy, tizimli yondashuvni talab qiladi. Bu esa faqatgina CRMP doirasida ro'y berishi mumkin.

CRMP tamoyillari

2018-yilda SEC davlat kompaniyalariga favqulodda vaziyatlarda kiberxavfsizlikka oid ma'lumotlarni oshkor qilish bo'yicha ko'rsatmalarni, shu jumladan, kompaniya o'z kibertahdidlarini qanday boshqarishi bo'yicha kengashlar va korxona mansabdor shaxslarining kutilayotgan nazoratga oid sharhlarini taqdim etdi. SEC o'z bayonotida, davlat kompaniyalari investorlarni favqulodda vaziyatlarda kiberxavfsizlik hodisalari to'g'risida xabardor qilish uchun tezkor choralar ko'rishi zarurligini alohida uqtirib o'tadi. Bu favqulodda vaziyatlarda kiberxavfsizlikni boshqarish dasturi yordamida kengashning nazorat majburiyatlarini bajarishdagi vazifasi haqidagi qat'iy eslatmani o'z ichiga oladi.

SECning bayonotidan navbatdagi savol tug'iladi: "favqulodda vaziyatlarda kiberxavfsizlik boshqaruvi dasturi nima?" Keyingi bo'lim CRMP, ya'ni CRMPni har tomonlama aniqlash va joriy qilish uchun mo'ljallangan. Hokimiyat va nazorat qiluvchi organlar tashkilotlarga manfaatdor tomonlar bilan kibertahdidlar haqida suhbatlar o'tkazishga ehtiyoj sezilayotganini ta'kidlashdi. Kengashlar va rahbarlar dasturiy yondashuv orqali kibertahdid muhitini to'g'ri nazorat qilish imkoniyatiga ega bo'lishi zarur. Amaldagi ko'pgina standartlar va ma'lumotnomalar alohida ko'rib chiqilsa, biznesga chindan xizmat qiladigan kompleks dastur talablariga mutlaqo mos kelmasligini kuzatish mumkin. Bu esa, korxonalarining kibertahdidlarni to'g'ri boshqarishi va nazorat qilishi uchun rasmiy ko'rsatmalar, qoidalar va standartlarni uyg'unlashtiradigan va talqin qiladigan yagona tizimga bo'lgan zaruratini ifodalaydi.

CRMP tamoyillari yetakchi amaliyot va standartlardan olingan tushunchalarni umumlashtirib, kibertahdidlarni boshqarishda tizimli va kompleks yondashuvni ta'minlaydi. Bu prinsiplar yakka tartibdagi korxonaning individual ehtiyojlari va normativ-huquqiy muhitiga moslashtirilishi mumkin. Bu prinsiplar korxonalarining tahdidga oid asoslangan qarorlar qabul qilishida, raqamli asrda muvaffaqiyat qozonishlarini ta'minlash maqsadida o'zlarining xavfsizlik strategiyalarini ishlab chiqishlari uchun o'z CRMPlarini amaliyotga joriy qilishlarida qo'llanma sifatida ham xizmat qiladi.

CRMP to'rtta asosiy tarkibiy qismga bo'linadi (2.1-jadvalga qarang): Moslashuvchan boshqaruv; Tahdidlar haqidagi ma'lumotlarga asoslangan tizim; Tahdidlarni baholashga asoslangan strategiya va uning ijrosi; Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilinishi.

Ushbu tarkibiy qismlarning har biri ijroni amalga oshirish bo'yicha yana bir necha qo'shimcha tamoyillarga bo'linadi. Keyingi to'rt bobning har birida biz ushbu tarkibiy qismlarning har birini, ularga tegishli prinsiplar va ma'lumot manbalarini chuqur tahlil qilib o'tamiz. CRMP tamoyillari haqida har tomonlama tu-

shunchaga ega bo'lish uchun Ilovaga qarang. CRMP tamoyillari onlayn rejimda ham mavjud.

2.1-jadval

CRMP tamoyillari

CRMP tarkibiy qismlari	Tamoyillar	Ma'lumot manbalari
Moslashuvchan boshqaruv	70-betda “Moslashuvchan boshqaruvning yetti tamoyili”ga qarang	• SECning yakuniy kiberqoidasi • NIST CSF 2.0³¹ • 2023-yilgi NACD³²ning direktorlar qo'llanmasi • ISO 27001:2022³³ • NIST 8286 • IIA³⁴ning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • ISO 31000:2018 • AICPA³⁵ning CRMP
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	90-betda “Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili”ga qarang	• SECning yakuniy kiberqoidasi • NIST CSF 2.02.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	115-betda “Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili”ga qarang	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIA³⁶ning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	146-betda “Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili”ga qarang	• SECning Yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • AICPAning CRMP

³¹ NIST CSF (Cybersecurity Framework of National Institute of Standards and Technology) – Standartlar va texnologiyalar milliy instituti kiberxavfsizlik asoslari.

³² NACD (National Association of Corporate Directors) – Korxona rahbarlari milliy uyushmasi

³³ ISO (International Organization for Standardization) – Xalqaro standartlashtirish tashkiloti.

³⁴ IIA (The Institute of Internal Auditors) – Ichki auditorlar instituti.

³⁵ AICPA (The American Institute of Certified Public Accountants) – Amerika sertifikatlangan jamoat buxgalterlari instituti.

³⁶ IIA (The Institute of Internal Auditors) – Ichki auditorlar instituti.

Ko'pgina xavfsizlik va tahdidlar bo'yicha mutaxassislar o'zlarida favqulodda vaziyatlarda xavfsizlikni boshqarish dasturi allaqachon mavjud deya hisoblashadi va ehtimol haqiqatan ham ularda dasturning hech bo'lmaganda ba'zi zarur komponentlari mavjud bo'lishi mumkin. Bular boshqaruv modeli, tahdidlar reyestri va noxush oqibatlarini yumshatish bo'yicha chora-tadbirlar to'plamini o'z ichiga olishi mumkin. Ushbu yumshatish bo'yicha chora-tadbirlar xodimlar va pudrat-chilar uchun ko'p faktorli autentifikatsiyadan (MFA³⁷) tortib, AT zaifliklarini aniqlash uchun Pentest (penetration testing³⁸), korxona obyektlarida fizik xavfsizlikni ta'minlash uchun standartlar va amaliyotlarga bo'lgan har qanday narsalarni qamrab olishi mumkin. Aslida, bularning barchasi foydali va zarur bo'lgan shunchaki vositalar, texnologiyalar, texnikalar va jarayonlardir, biroq ular tahdidlarni boshqarish bo'yicha haqiqiy amaliyotni amalga oshirish maqsadida qonuniylashtirilgan avtonom dasturda birlashtirilmasa, ular talablarga javob bermaydi.

CRMP: Asosiy harakatlantiruvchi omillar

Shuni anglash muhimki, ushbu to'rt komponent mavhum tushuncha yoki faoliyatning asossiz yo'nalishlari emas. Aslida, ularning har biri juda muhim va ko'p hollarda ushbu to'rt komponent korxona qarorlarini qabul qiluvchilari o'z e'tiboridan chetda qoldira olmaydigan murakkab va tez o'sib borayotgan huquqiy, tartibga soluvchi, siyosiy va ekologik omillar bilan bog'liq. Keling, ushbu harakatlantiruvchi omillarning eng muhimlarini ko'rib chiqaylik:

Amaldagi qonunchilikka muvofiqlik asoslari

Mintaqaviy, milliy, davlat va hatto mahalliy miqyosdagi hukumatlar tegishli xavfsizlik qoidalariga rioya qilishdan tashqari, tahdidli hududlarni qamrab oluvchi va tahdidlarni nazorat qilish hamda ularni boshqarish uchun mo'ljallangan rasmiylashtirilgan jarayonlarga ko'proq e'tibor qaratuvchi qoidalar to'plamini o'rnatdilar. Hukumat idoralari va ushbu qoidalarni tatbiq etish uchun tashkil etilgan boshqa organlar, qoidalarining amal qilinishini ta'minlash uchun jiddiy choralar ko'rishga va qoidalarga rioya qilmagan taqdirda, korxonalarni ham, mas'ul shaxslarni ham jazolashga tayyor ekanliklarini ko'rsatdilar. SEC ko'rsatmalariga rioya qilmaslik (misol uchun, jiddiy ahamiyatga ega moliyaviy ma'lumotlarni to'g'ri taqdim etmaslik) kompaniyaning eng yuqori darajadagi qaror qabul qiluvchilari: direktorlar kengashi, korxonaning rahbar xodimlari, shu jumladan, CISolar uchun jiddiy oqibatlarga olib kelishi mumkin. Kiberxavfsizlikning uchta asosiy tamoyilini ko'rish uchun 2.2-jadvalga qarang.

³⁷ MFA (multifactor authentication) – Ko'p faktorli autentifikatsiya, ushbu autentifikatsiya ikki bosqichli tekshirish jarayonini talab qiladi, bu nafaqat foydalanuvchi nomi va parolni, balki faqat foydalanuvchi biladigan ma'lumotni ham talab qiladi.

³⁸ Pen (penetration) testing – Pentest, tarmoq yoki dasturga xakerlik hujumiga o'xshash jarayonlarni amalga oshiruvchi test tizimi hisoblanadi. Pentestning maqsadi tizim yoki dasturning qanday himoyalanganini o'rganishdir.

Qonuniy javobgarlik

So'nggi yillarda, bir qator sud qarorlari (ulardan bir nechtasini biz ushbu bobda ko'rib chiqamiz) korxonalar va ularni boshqaradigan shaxslardan talab qilindigan favqulodda vaziyatlarda xavfsizlik amaliyotlariga aniqlik kiritdilar. Sudlar mukammallikni talab qilmayaptilar, lekin ular tahdidlarni baholash, ularni boshqarish va hisobot berishda vijdonan yondashishni kutishmoqda. Sudlar vijdonan harakat qilmagan tashkilotlar va shaxslar jarimalar va fuqarolik sudlovlari kabi jazo va hatto qamoq muddati bilan javobgarlikka tortilishini ta'kidlashmoqda.

Direktorlar kengashi a'zolari va yuqori darajadagi rahbarlarga kibertahdidlar bo'yicha ko'rsatmalar beradigan nufuzli organlar

Ko'pgina nodavlat idoralari (ba'zilar muayyan sanoat tarmoqlariga, ba'zilar ma'lum hududlarga, ba'zilar esa butun dunyo bo'ylab yo'naltirilgan bo'lib) korxonalarga kibertahdid masalalarini hal qilish bo'yicha amaliy ko'rsatmalar beradi. Bunga NACDning Qo'shma shtatlardagi ochiq savdo kompaniyalari direktorlari uchun nashr etgan "Kibertahdidlarni nazorat qilish bo'yicha qo'llanma"si hamda Jahon iqtisodiy forumining xalqaro yo'riqnomasi misol bo'la oladi.

Sanoat tomonidan tan olingan standart va dasturlarni ishlab chiqaruvchi tashkilotlar

Tashkilotlarga o'zlarining kiberxavfsizlik dasturlarini yaratishi va kiberxavfsizlikning samaradorligi to'g'risida hisobot berishlariga ko'maklashish maqsadida bir nechta kiberxavfsizlik asoslari ishlab chiqilgan bo'lib, bular jumlasiga NISTning kiberxavfsizlik asoslari 2.0, xalqaro standartlashtirish tashkilotining va AICPAning kiberxavfsizlikka tahdidlarni boshqarish bo'yicha hisobot berish asoslari kiradi. NISTning kiberxavfsizlik asoslari 2.0, 2024-yil boshida ommaga taqdim etilib, u texnik xavfsizlik nazoratlari bilan chegaralanib qolmasdan, strategik tahdidlarni boshqarish va tahdidlarni boshqarish amaliyoti bo'yicha ko'proq yo'l-yo'riqlarni ham o'z ichiga oladi. Ba'zi tamoyillar deyarli barcha korxonaga qo'llanilsa, boshqalari esa faqatgina ma'lum bir sanoat yoki ma'lum bir mintaqaga xosdir.

Kiberxavfsizlikning asosiy tamoyillari

Tashkilot	Prinsiplar	Tavsif
NIST	Milliy standartlar va texnologiyalar institutining “Kiberxavfsizlik asoslari 2.0” (ommaga taqdim etilishi rejalashtirilgan muddat 2024-yilning boshi)	NISTning 2.0 kiberxavfsizlik asoslari sanoat, hukumat idoralari va boshqa tashkilotlarga kiberxavfsizlik tahdidlarini kamaytirish bo'yicha ko'rsatmalar beradi. U kiberxavfsizlik bo'yicha sa'y-harakatlarni yaxshiroq tushunish, baholash, ustuvorliklarni belgilash va ma'lum qilish uchun har qanday tashkilot tomonidan, hajmi, sektori yoki yetukligidan qat'i nazar, foydalanishi mumkin bo'lgan yuqori darajadagi kiberxavfsizlik natijalarini sistemalashtirishni taklif etadi ³⁹ .
ISO	ISO/IEC 27001:2022	ISO/IEC 27001 axborot xavfsizligini boshqarish tizimlari (ISMS ⁴⁰) uchun dunyodagi eng mashhur standart hisoblanadi. U ISMSni amalga oshirishi kerak bo'lgan talablarni belgilaydi. ISO/IEC 27001 standarti har qanday o'lchamdagi va faoliyatning barcha sohalaridagi kompaniyalarga axborot xavfsizligini boshqarish tizimini yaratish, joriy etish, saqlash va doimiy ravishda takomillashtirish bo'yicha ko'rsatmalarni taqdim etadi. ISO/IEC 27001 ga muvofiqlik – tashkilot yoki korxona kompaniyaga tegishli yoki boshqariladigan ma'lumotlar xavfsizligi bilan bog'liq tahdidlarni boshqarish tizimini joriy qilganligini anglatadi ⁴¹ .
AICPA	Favqulodda vaziyatlarda kiberxavfsizlikni boshqarish bo'yicha hisobot berish asoslari	AICPA tashkilotlarga favqulodda vaziyatlarda kiberxavfsizlikni boshqarish dasturlarining samaradorligi to'g'risida tegishli va foydali ma'lumotlarni yetkazishda yordam beradigan kiberxavfsizlik risklarini boshqarish bo'yicha hisobot berish asoslarini ishlab chiqdi. Ushbu asoslar kiberxavfsizlikni ta'minlovchi Tizimli va tashkiliy nazoratning (SOC ⁴²) asosiy tarkibiy qismi bo'lib, uning yordamida sertifikatlangan buxgalterlar korxona miqyosida favqulodda vaziyatlarda kiberxavfsizlikni boshqarish dasturi haqida hisobot beradi ⁴³ .

Tahdidlarni boshqarishning keng qamrovli dasturi – dasturni loyihalash va joriy qilish uchun kiritilishi kerak bo'lgan keng ko'lamdagi qonunlar, me'yoriy-huquqiy hujjatlarga muvofiqlik talablari va sanoat protokollariga asoslanadi.

³⁹ Milliy standartlar va texnologiyalar institutining “Kiberxavfsizlik asoslari 2.0” Milliy standartlar va texnologiyalar instituti, 2023-yil, 8-avgust.

⁴⁰ ISMS (information security management systems) – Axborot xavfsizligini boshqarish tizimlari.

⁴¹ “ISO/IEC 27001 Axborot xavfsizligini boshqarish tizimlari”, ISO, 2022-yil oktyabr.

⁴² SOC (System and Organization Controls) – Tizimli va tashkiliy nazorat.

⁴³ “Kiberxavfsizlik uchun tizimli va tashkiliy nazorat”, AICPA va CIMA, 2023-yil 10-oktyabr.

Vazifa va majburiyatlarni bajarish

Korxona qarorlarini qabul qiluvchilar CRMPning ushbu to'rt asosiy tarkibiy qismini o'zlarining korxona muhitlari va talablariga moslashtirishlari mumkin (Ilovaga qarang). Kitobimizda ushbu harakatlantiruvchi omillar ko'rib chiqiladi, shuningdek, ularning xavfsizlik va tahdidning muayyan sohalariga, jumladan kibernetik xavfsizlikka ta'siri o'rganiladi. Muayyan harakatlantiruvchi omillar qay tarzda sizning vazifangiz, korxonangiz va sanoatingiz talablariga javob berishi ko'rsatib o'tiladi. Quyida eng muhim harakatlantiruvchi omillardan bir nechtasini va ularning dasturning to'rt tarkibiy qismlari bilan qanday bog'liqligini ko'rib chiqamiz.

Moslashuvchan boshqaruv

Boshqaruvning eng muhim harakatlantiruvchi omillaridan biri SECning ko'rsatmalari bo'lib, u eng yuqori darajadagi ko'pgina muhim va majburiy sud qarorlari bilan tasdiqlangan. SEC ko'rsatmalariga amal qilmaslik kompaniyaning eng yuqori darajadagi qaror qabul qiluvchilari, shu jumladan korporativ mansabdor shaxslar va direktorlar kengashi uchun jiddiy oqibatlariga olib kelishi mumkin.

Tahdidlar haqidagi ma'lumotlarga asoslangan tizim

Ushbu bobda muhokama etiladigan bir qator sud ishlari shuni ko'rsatadiki, direktorlar kengashi vijdonan ishlashi va shaxsiy javobgarlikdan qochishi uchun Tahdidlar haqidagi ma'lumotlarga asoslangan tizimga ega bo'lishlari kerak va bu tizim topshiriqni bajarish uchun muhim bo'lgan barcha narsaga qo'llanilishi lozim.

Tahdidlarni baholashga asoslangan strategiya va uning ijrosi

Tabiiyki, tahdid hamisha moliyaviy ta'sirga ega bo'ladi, shuning uchun bu holat moliyaviy rahbarlar va tashkilotlarning moliyaviy farovonligi uchun mas'ul bo'lgan boshqa xodimlarni xavotirga soladi. Ko'pincha tartibga soluvchi organlar va sudlar tashkilotlar o'zlarining tahdid muhitlarini yaxshi tushunishlari zarurligini ta'kidlaydi, talab va chidamlilikni amalga oshirish uchun zarur bo'lgan resurslarni aniqlashdan oldin talab va chidamliliklarini aniqlaydigan qarorlar qabul qilishlarini ta'kidlaydilar.

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilinishi

Ushbu bobda keltirib o'tiladigan hayotiy misollardan shuni anglash mumkin, ki, sudlar doimo ishlar yomonlashganda korxona ichidagi va tashqarisidagi tegishli odamlar bundan xabardor qilinishi zarurligi haqida ogohlantirishgan. AICPA, NIST va SEC kabi organlarning barchasi tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish bo'yicha ko'rsatmalarni taqdim etganligi bu masalaning naqadar muhimligini ko'rsatadi.

Shuni ta'kidlash joizki, ushbu harakatlantiruvchi omillar va ularni hal qilish uchun ishlab chiqilgan ko'rsatmalar faqatgina tahdid, qiyinchilik yoki muammo sifatida qaralmasligi lozim. Bu harakatlantiruvchi omillar birma-bir muvofiq-

lashtirish uchun mo'ljallanmagan, aksincha, harakatlantiruvchi omillar yaxlit holda qanday qilib ushbu omillarni hal qilish maqsadida yaxlit va muvofiqlashtirilgan CRMPni talab qilayotganligini o'rganish uchun mo'ljallangan. Ehtimol, biz bajarilishi lozim bo'lgan ishlarni bajarmaslikning salbiy oqibatlari haqida gapirayotgandek tuyulishimiz mumkin, ammo bu juda muhim. Biroq xavfsizlik mutaxassislari uchun mavjud bo'lgan tartibga soluvchi, huquqiy va sanoat yo'riqnomalari tahdidlar bo'yicha qaror qabul qilishda ishtirok etuvchi har bir inson uchun qimmatli himoyani taklif qiladi (agar tegishli tavsiyalarga amal qilinsa).

Tahdidlar uchun javobgarlik va mas'uliyat: Xalqaro hodisa

Yuqori darajadagi javobgarlik, mas'uliyat va majburiyatga bo'lgan zaruriyat faqatgina AQSH bilan chegaralanib qolmaydi. Bu xalqaro hodisa, chunki raqamlashtirish deyarli har bir korxonani "xalqaro korxonaga" aylantirdi. Misol uchun, butun dunyoda davlat/xususiy hamkorlikni targ'ib qiluvchi tashkilot WEF o'n yildan ortiq vaqt mobaynida kiberxavfsizlik masalalari bilan shug'ullanib kelmoqda. 2017-yilda WEF Bostonning yirik konsalting firmasi (Boston Consulting Group) va axborot texnologiyalari sohasidagi Amerikaning ko'p millatli kompaniyasi Hewlett Packard Enterprise bilan birgalikda kibermuammolarni hal qilishda ishtirok etadigan direktorlar kengashi uchun amaliy asos bo'lib xizmat qiladigan *"Direktorlar kengashi uchun kiberchidamlilikni oshirish tamoyillari va vositalari"*ni nashr etdi. Hujjatda tahdidlar qanchalik yuqori ekanligi aniq ko'rsatilgan: "Kiberbardoshlilik va kibertahdidlarni boshqarish bugungi kunda aksariyat tashkilotlar uchun juda muhim masalalardan biridir. Rahbarlar ushbu tahdidlarning jiddiyligini yanada ko'proq anglashmoqda hamda tahdidlarni boshqarish mas'uliyati boshqaruv kengashi va yuqori darajadagi ijroiya guruhlarida ekanligini tan olishmoqda".

Turli milliy va xalqaro tashkilotlar tomonidan yaratilgan ko'plab tamoyillar va standartlar mavjud bo'lib, ularning barchasini mazkur kitobda batafsil muhokama qilish imkonsiz. Albatta, ular o'rtasida mintaqaviy, yurisdiksiyaviy va boshqa farqlarni aks ettiruvchi ko'plab talqinlar mavjud va ularda ko'pgina bo'shliqlarni kuzatish mumkin. Shunga qaramay, ular birgalikda kibertahdidlarni boshqarishning eng dolzarb tarkibiy qismlari va muammolarini ko'rsatadi.

Tahdidlarni boshqarish to'liq muvaffaqiyatsizlikka uchraganda: Boeing 737 MAX samolyoti halokatlari

Ushbu kitobning asosiy g'oyasi shundan iboratki, biz ta'riflagan to'rt tarkibiy qismga ega hamda o'rnatilgan qoidalar, standartlar va protokollarga asoslangan rasmiy CRMP raqamli asrda muhim ahamiyatga egadir. Buni isbotlashning eng samarali usuli – dastur mavjud bo'lmaganda nimalar sodir bo'lishi mumkinligini ko'rsatishdir. Biz dunyodagi eng yirik, eng muhim va yaqin vaqtgacha eng obro'li transmilliy korporatsiyalardan biri bo'lgan Boeingdagi halokatli muvaffaqiyatsizlikka e'tibor qaratishni ma'qul ko'rdik. Bu kiberxavfsizlikka misol bo'lmasa-da, biroq u raqamlashtirish korxona ichidagi tahdidlarni qay darajada o'zgartirishi mumkinligini ko'rsatadi.

Ishlab chiqaruvchi liniyasiga endigina taqdim etilgan Boeing 737 MAX samolyoti 2018-yilning 29-oktyabr kuni Indoneziyaning Jakarta shahridan havo-ga ko'tarilganidan ko'p vaqt o'tmay yerga qulab tushadi va bortda bo'lgan 189 yo'lovchining hammasi halok bo'ladi. Olti oydan kamroq vaqt o'tgach, Efiopiya-da yana xuddi shu rusumdagi 737 MAX samolyoti shunga o'xshash sharoitlarda halokatga uchraydi, bu baxtsiz hodisada esa 157 ta yo'lovchi halok bo'ladi.

Butun dunyo bo'ylab tartibga soluvchi organlar tomonidan o'tkazilgan tezkor tekshiruvlar shuni ko'rsatadiki, ikkala halokat ham samolyotni boshqarish tizimi-dagi muhim raqamli komponentning ishlamay qolganligi sababli sodir bo'lgan. Bundan ko'rinadiki, Boeing kompaniyasining tahdidni to'g'ri boshqara olmagan-ligi kompaniyadagi asosiy qaror qabul qiluvchi shaxslariga uzoq muddatli jinoiy firibgarlikni amalga oshirishga imkon bergan.

Bu falokatning oqibatlari Boeing kompaniyasi uchun shafqatsiz bo'ldi. 346 yo'lovchining halok bo'lishi har qanday holatda ham dahshatli ekani o'z-o'zidan ayon. Bundan tashqari, Boeing biznesi uchun oqibatlar halokatli bo'ldi. Dunyo bo'ylab aviakompaniyalar o'zlarining 737 MAX samolyotlari parvozlarini to'x-tatdilar, aviatashuvchi kompaniyalar esa bu turdagi samolyotlarga buyurtmalarini bekor qilishdi. Amerika Qo'shma Shtatlari Milliy aviatsiya ma'muriyati (FAA⁴⁴) dastlab butun dunyo bo'ylab samolyotni yerga qo'ndirish haqidagi chaqiriqlariga qarshilik ko'rsatganiga qaramay, 2019-yilning mart oyida nihoyat taslim bo'ladi va 2020-yilning noyabr oyigacha hech qanday 737 MAX samolyotlari parvoz qil-madi. Boeing kompaniyasining hech ham dog' tushmagan obro'siga putur yetgan edi. Ba'zi onlayn sayohat agentlari hatto sayohatchilarga 737 MAX samolyotla-rida uchmaslikni maslahat bera boshlashdi. Boeing hatto o'zining juda mashhur 7 seriyali brendini to'xtatishni o'ylayotganligi haqida xabar tarqaldi, bu samolyot 1950-yillarning oxirida "havo qatnovlari asri"ni boshlab bergan samolyot sifatida tanilgan edi.

Kompaniyaning pul xarajatlari juda ko'payib ketdi, bu nafaqat mijozlarni yo'qotish bilan bog'liq edi, balki xarajatlar kelgusi yillar davomida ham o'sishda davom etishini anglatar edi. 2023-yil yanvar oyi holatiga ko'ra, Boeing kompa-niyasi halokat qurbonlarining oilalariga 500 million dollardan ko'proq va avia-kompaniyalarga zararni qoplash uchun yana 1,7 milliard dollar tovon puli to'la-gan. Ammo kompaniyaga yetkazilgan moliyaviy zarar shu bilan tugab qolmadi. Boeing kompaniyasi nazorat qiluvchilar va boshqalar oldidagi vakolatlari uchun firibgarlikda ayblangan hamda kompaniya 2,5 milliard dollardan ortiq jarima to'lab, jinoiy javobgarlikdan qochib qutulgan. Barcha sud ishlari va atrofdagi vaziyat yumshagach, Boeing kompaniyasining xarajatlari 20 milliard dollardan oshdi. Bu har qanday kompaniya uchun, hatto Boeing kabi badavlat kompaniya

⁴⁴ FAA (The Federal Aviation Administration) – Amerika Qo'shma Shtatlari Milliy aviatsiya ma'muriyati.

uchun ham dahshatli zarba bo'ldi. Shubhasiz, bunday xarajatlarga kompaniyaning vijdotsizligi sabab bo'ldi:

Boeing xodimlari tomonidan FAAga yetkazilgan chalg'ituvchi ma'lumotlar, yarim haqiqatlar va xaspo'shlash sabab, hukumat parvoz qilayotgan xalq xavfsizligini ta'minlay olmadi.

AQSHlik advokat Erin Nili Koks⁴⁵

Boeing kompaniyasining muammolari dizayndagi asosiy nuqsondan boshlandi: muhandislik o'zgarishlaridan kelib chiqqan holda parvoz buzilishlarini tuzatishga yordam beradigan raqamli sensor va unga tegishli dasturiy ta'minotning ishlamay qolishidan boshlandi. 737 MAX samolyoti dvigatellarining joylashuvi samolyotning muvozanatsiz va beqaror bo'lishiga olib keldi va muammoni tuzatish uchun ishlab chiqilgan texnologiya (samolyotni raqamlashtirish) samolyotning to'satdan yerga qulashiga olib kelishi mumkinligini ko'rsatdi. Boeing kompaniyasining turli darajadagi xodimlari ushbu muammodan xabardor bo'lishgan va bu halokatli natijalarga olib kelishi mumkinligini bilishgan. Ba'zilar bu muammo haqida rahbariyatni ogohlantirgan bo'lsa, boshqalari uni e'tiborsiz qoldirishgan. Yana boshqalari esa FAA kabi nazorat qiluvchi organlardan, samolyotlarni sotib olgan aviakompaniyalardan, hatto uchuvchilardan haqiqatni yashirishga urinishgan, hatto o'quv qo'llanmalaridan nosoz tizim haqidagi muhim ma'lumotlar o'chirilgan.

Tahdidlarni boshqarish tizimi mavjud bo'lgan taqdirda ham, Boeing muammolarni aniqlab, ularga kerakli chora ko'rishga harakat qilgan bo'lishi aniq emas. Ehtimol, kompaniyaning yuqori rahbariyati tegishli ravishda xabardor qilinganida, ular muammolarni bartaraf etishga million dollar yoki ehtimol yuz million dollar sarflab, yuzaga kelishi mumkin bo'lgan tahdidning oldini olgan bo'lardi, ammo ortga nazar soladigan bo'lsak, bu ehtimoldan yiroqdek tuyuladi. Birinchi halokat sodir bo'lganidan so'ng, kompaniya mas'uliyat va javobgarlikni his etgan holda, muammoni tezda aniqlab, chora ko'rganida ikkinchi halokatning oldi olingan bo'lar edi. Hech bo'lmaganda, kompaniya va 737 MAX samolyoti loyihasi va ishlab chiqarish jarayoni bilan shug'ullanadigan ko'plab xodimlar qonuniy javobgarlikdan himoyalangan bo'lar edi. Sababi, ular ushbu muhim tahdidlarni to'g'ri aniqlash va ularni boshqarish uchun harakat qilganliklarini namoyon eta olishar edi, hatto bu harakatlar muvaffaqiyatsizlikka uchragan taqdirda ham.

⁴⁵ "Boeing 737 Max firibgarlikda ayblandi va 2,5 milliard dollardan ortiq pul to'lashga rozi bo'ldi", AQSH Adliya vazirligining jamoatchilik bilan aloqalar boshqarmasi, 2021-yil 7-yanvar.

Boeing samolyoti halokatlarida qo'llanilgan tahdidlarni boshqarish dasturi

Keling, Boeing samolyoti halokatlarini tahdidlarni boshqarish dasturining to'rt tarkibiy qismi obyektivi orqali ko'rib chiqamiz:

Moslashuvchan boshqaruv

Har qanday korxona tahdidlarni boshqarish dasturi doirasida umumiy tahdidlarni boshqarishni ta'minlash uchun, dasturning ko'lamini, chuqurligi, natijalari aniq belgilangan hamda aniq o'rnatilgan vakolat va javobgarlikni qamrab olgan strukturaga ega bo'lishi kerak. Bu struktura o'zgaruvchan sharoitlarga tezkor munosabat bildiradigan va moslashuvchan bo'lishi lozim. Agar kompaniyaning boshqaruv organi loyihalash va ishlab chiqarish jarayonida boshidan ishtirok etganida va parvozlarni boshqarish tizimi bilan bog'liq tahdidlar nomaqbul ekanligini aniqlaganida, butun Boeing falokatining oldini olish mumkin edi. Muammolar ko'payib, tahdidlar oydinlashgan sari (ayniqsa birinchi halokatdan so'ng), tezkor va moslashuvchan boshqaruv organi ikkinchi halokatning oldini olish uchun Boeing kompaniyasidan ko'ra jiddiyroq choralar ko'rishi tabiiy edi. Boshqaruv asosan madaniyatni belgilaydi: korxona nimani qadrlaydi va uning ustuvorliklari nimadan iborat. Shuni ta'kidlash joizki, 737 MAX samolyotning ba'zi loyihachilari va muhandislari Boeing korporativ madaniyati o'z'garganini, ayniqsa kompaniyaning 1997-yilda McDonnell Douglas⁴⁶ kompaniyasi bilan birlashganidan keyin o'z'garganini sezishgan, natijada xavfsizlikdan ko'ra foyda ustunlik qilgan.

Yaxshi dastur hech bo'lmaganda birinchi halokatdan so'ng, 737 MAX samolyot parvozlarni to'xtatgan va ikkinchi halokatda vafot etgan 157 kishining hayotini saqlab qolgan bo'lardi deya taxmin qilish adolatli bo'lar edi.

Tahdidlar haqidagi ma'lumotlarga asoslangan tizim

Bu butun korxona bo'ylab va tobora murakkablashib borayotgan raqamli muhitda barcha tahdid turlarini aniqlash, ularni qabul qilish, boshqarish va yengillashtirishda tizimli, korxona miqyosidagi yondashuvni anglatadi. Shuni yodda tutish lozimki, mutlaqo tahdiddan xoli muhit mavjud emas va bunday muhitni yaratishga harakat qilish befoyda va ba'zan hatto samarasizdir. Barcha korxonalar ma'lum bir tahdidlarni qabul qilishadi va dunyodagi eng raqobatbardosh sanoatlarda faoliyat olib borayotgan Boeing kompaniyasi ham bundan mustasno emas. (Ta'kidlash joizki, ba'zi sanoat tarmoqlaridan imkon qadar tahdidlarda xoli bo'lish talab etiladi, jumladan, aviatsiya sanoati, chunki undagi nosozlik halokat-

⁴⁶ McDonnell Douglas Corporation – Amerikaning yirik aerokosmik muhandislik korporatsiyasi va mudofaa pudratchisi.

li oqibatlariga olib kelishi mumkin.) Boeing kompaniyasi samolyotlarda parvoz-larni boshqarish tizimi bilan bog'liq muammolar paydo bo'la boshlaganidan beri duch kelgan tahdidlardan biri shunda ediki, nosozliklarni ta'mirlash kompaniya uchun juda qimmatga tushishi mumkin edi. Bunday miqdordagi qo'shimcha xarajat Boeing kompaniyasining foydasini keskin pasaytirgan bo'lar edi, ammo bu kompaniyaning halokatdan so'ng sarflagan umumiy xarajatlari kabi ko'p bo'lmas edi. Shu bilan birga, u qaror qabul qiluvchilarni javobgarlikdan himoya qilish-ga yordam berishi mumkin edi, chunki Boeing kompaniyasi hech bo'lmaganda tahdidlarni aniqlab, unga nisbatan tizimli sa'y-harakatlarni amalga oshirganligini ko'rsata olar edi.

Tahdidlarni baholashga asoslangan strategiya va uning ijrosi

Bu ma'lum bir ishtiyoq va chidamlilikni mos ravishda aniqlash va amalga oshirishdir. Yana bir bor ta'kidlash joizki, mutlaq tahdiddan xoli muhitga erishish mumkin emas va tahdidlarni baholash va qabul qilish bo'yicha korxona miqyosi-dagi strategiya Boeing kompaniyasining to'g'ri qarorlar qabul qilishini kafolatla-maydi. Shunga qaramay, bu strategiya turli darajadagi Boeing xodimlari tomoni-dan qabul qilingan noto'g'ri qarorlarning hech bo'lmaganda ayrimlarining oldini olgan bo'lar edi. Tahdidlarga nisbatan aniq belgilangan pozitsiya korxona xodim-lariga va ichki tashkilotlarga (loyihalash, ishlab chiqarish, xavfsizlik, huquqiy va boshqalar) tahdidlarga chidamli biznes strategiyalarni ishlab chiqish va amalga oshirish imkonini beradi. Kompaniya faoliyatining barcha jihatlarini, mahsulotni loyihalashtirishdan tortib resurslarning taqsimlanishigacha, ishlab chiqarishdan tortib tartibga soluvchi organlar bilan hamkorlikka va hokazolar ushbu chi-damlilikni hisobga olgan holda ishlab chiqilishi zarur.

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilinishi

Ehtimol, aynan shu sohada Boeing kompaniyasi yaxshi ishlaydigan tahdid-larni boshqarish dasturidan ko'proq foyda ko'rishi mumkin edi. 737 MAX sa-molyoti halokati bo'yicha olib borilgan tergov ishlari shuni ko'rsatadiki, Boeing kompaniyasidagi turli vazifalarda ishlaydigan xodimlar samolyot bilan bog'liq muammolar va ularning jiddiyligini bilishgan. Fojia sodir bo'lganidan so'ng, bu kabi halokatli muammoni e'tiborsiz qoldirish mumkin emasdek tuyular edi, ammo haqiqat shundaki, ko'pchilik buni e'tiborsiz qoldirdi.

Ehtimol, Boeing kompaniyasida tahdidlar haqidagi ma'lumotlarni shaffoflik bilan tegishli shaxsga rasmiy ravishda yetkazib beradigan tizim mavjud bo'l-magan. To'g'ri eskalatsiya va ma'lumotlarning oshkor qilinishi samolyot bilan bog'liq barcha tahdidlarni bartaraf etmasa-da, u Efiopiya Airlines samolyotida halok bo'lgan kamida 157 kishining hayotini qutqarib qolgan bo'lar edi. Agar Boeing kompaniyasining eng yuqori darajadagi rahbarlari birinchi halokatdan so'ng ochiq va halol bo'lganlarida, FAA va dunyoning boshqa tartibga soluvchi organlari shubhasiz 737 MAX samolyoti parvozini to'xtatgan bo'lar edi.

Boeingning muvaffaqiyatsizliklari texnologiyaga haddan ziyod suyanish natijasidir. Boeing kompaniyasi bo'limlari va xodimlari ishlab chiqarish maqsadlariga erishish uchun shunchalik bosim ostida bo'lganki, ular maqsadga erishish uchun qisqaroq, ammo xavfliroq yo'lni tanlashgan, kompaniya boshqaruv organlari muammolar aniqlanganda ularga ko'z yumishgan yoki kompaniya pul ishlashda davom etishi uchun odamlar barcha narsaga, hattoki qonunni buzish va odamlarning hayotini xavf ostiga qo'yishga tayyor bo'lgan.

“Jiddiy va o'ta muhim”: Boeing ishi

Boeing kompaniyasi “xavfsizlikni nazorat qilish”ni tashkilot piramidasining eng ustuvor vazifasi sifatida belgilamagan. “Boeing” boshqaruv qo'mitalarining hech biriga samolyot xavfsizligini nazorat qilish vazifasi yuklanmagan va hech bir qo'mita nizomida samolyot xavfsizligi haqida yozilmagan.

Delaver shtati Kansler sudi, “In Re Boeing Co. Derivative Litig”

Boeing muvaffaqiyatsizligi kompaniyaga, uning xodimlariga, aviakompaniya mijozlariga va eng muhimi, uning yo'lovchilariga ta'siri shubhasiz muhimdir. Lekin 737 MAX samolyoti halokatinin oqibatlarini Boeing va aviatsiya sanoati bilan chegaralanmaydi. Bu fojia nima sababdan har bir korxona va har bir sanoat segmenti uchun samarali xavfsizlikni boshqarish dasturi zarurligini tushunishga yordam beradi. Eng tezkor oqibat – bu sudning Boeingni tizimdagi nosozliklar uchun javobgar deb topishi bo'ldi. Boeing kompaniyasiga qarshi aksiyadorlar da'vosi bo'yicha sudda, samolyot xavfsizligi uning faoliyati uchun “jiddiy va o'ta muhim”⁴⁷ ekanligi e'tirof etildi. Shu sababli, Boeing boshqaruv kengashi xavfsizlik masalalari ustidan nazoratni kuchaytirishlari lozim edi. Boshqaruv kengashida samolyot xavfsizligini nazorat qilish, muhokama qilish yoki muntazam ravishda hisobot berish tizimi mavjud emas edi. (Kompaniya tahdidlarni nazorat qilish funksiyasiga ega edi, ammo kompaniya asosan moliyaviy tahdidlarga ko'proq e'tibor qaratdi.) Direktorlar rahbariyatdan maxsus hisobotlarni olishar, lekin bu hisobotlar tahdidlarga asoslangan jarayonni ifodalash uchun yetarlicha tizimli yoki shaffof emas edi. Garchi “qizil bayroqlar” (tahdid belgilari) rahbariyatga taqdim etilgan bo'lsa-da, tegishli eskalatsiya tuzilmasi mavjud bo'lmaganligi sababli ular haqida kengashga xabar qilinmagan.

Nima uchun ushbu masala aviatsiya sanoatidan tashqari boshqa korxonalar uchun ham muhim va uni kibertahdidni boshqarish nuqtayi nazaridan nima muhim qiladi? Bularning barchasi oddiy, ammo kuchli ibora – “jiddiy va o'ta muhim”ga borib taqaladi. Biz ta'kidlaganimizdek, raqamli dunyoda barcha tahdidlar raqamli tahdidlardir va barcha raqamli tahdidlar kibertahdidlarni keltirib chiqaradi. Muqarrar xulosa shuki, kibertahdidlar, boshqa har qanday turdagi tahdidlar

⁴⁷ In re C. A. 2019-0907-MTZ (Del. Ch. 7-sentyabr, 2021), <https://oreil.ly/gihKI>.

singari, “jiddiy va muhim ahamiyatga ega”. Bu shuni anglatadiki, kompaniyalar, direktorlar kengashi va yuqori lavozimli rahbarlar, har qanday boshqa muhim tahdidlar kabi, kibertahdidlar uchun ham bir xil mas’uliyat va javobgarlikka ega.

Kiber va raqamli: Ahamiyatli farq

Tahdidlarni boshqarish haqida gapirar ekanmiz, “kiber” muhit va “raqamlashtirish” tushunchalarini farqlash muhimdir. Kibermuhitni alohida, mustaqil muhit deya hisoblash foydali bo‘lishi mumkin. Mamlakatda mahalliy, xalqaro, ichki, tashqi va moddiy muhitlar bo‘lgani kabi, kibermuhit ham mavjud. Bu elektron ma’lumotlar tarmoqlar orqali uzatiladigan, korxonalar aloqa, ma’lumotlar almashinuvi va boshqa amaliyotlarni amalga oshiradigan raqamli sohani ifodalaydi. Dastlab, bu sohaga kiritilgan asosiy resurs axborot edi. Ammo texnologiya rivojlanishi bilan kibermuhitdagi resurslarning turlari va miqdori ham o‘zgarib bordi. Raqamlashtirish an’anaviy yoki jismoniy tizimlar, jarayonlar va ma’lumotlarni raqamli formatga aylantirish jarayonini belgilaydi.

Asosiy maqsad nima? Ishlash, samaradorlikni oshirish va biznes operatsiyalari va kommunikatsiyalarida mumkin bo‘lgan imkoniyatlar doirasini kengaytirish. Moddiy hujjatlardan bulutli ma’lumotlar bazalariga yoki an’anaviy majlislardan virtual konferensiyalardan foydalanib, kompaniyalar bevosita raqamlashtirishda ishtirok etmoqdalar. Xo’sh, bularning ikkisi bir biri bilan qanday bog‘liq? Raqamlashtirish kibermuhitga potensial zaifliklarni olib kiradi. Jarayonlar qanchalik ko‘p raqamli formatlarga aylantirilsa va ularni qo‘llab-quvvatlasa, ehtimoliy hujumlar maydoni keskin kengayadi. Ushbu zaifliklar, tahdid qiluvchi shaxslarning niyatlari bilan uyg‘unlashganda esa, jiddiy tahdidlarni keltirib chiqarishi mumkin – bu kibertahdidlardir. Ulardan biznesga, jismoniy shaxslarga va kengroq jamiyatga jiddiy zarar yetkazish maqsadida foydalanish mumkin, shuning uchun CRMPga bo‘lgan ehtiyoj juda zarur.

Favqulodda vaziyatlarda xavfsizlik dasturining afzalliklari

Favqulodda vaziyatlarda xavfsizlik dasturining afzalliklari korxona duch keladigan tahdidlarga strategik yondashuvni ifodalaydi. Tahdidlarni boshqarish dasturi bo‘lmasa, xavfsizlik asosan taktik funksiya sifatida qaraladi. Idrok masalasi xavfsizlik amaliyotchilari duch keladigan eng katta muammolardan biridir. Odamlar xavfsizlik tashkiloti bilan “bir martalik” o‘zaro munosabatlarga ega. Masalan, rahbardan parolni o‘zgartirish so‘raladi, boshqa insonga maxfiy ilovaga kirish uchun virtual xususiy tarmoq (VPN⁴⁸) kerak bo‘lishi yoki biror-bir obyektga tashrif buyurgan mehmon xavfsizlik xodimiga ID taqdim etishi kerak. Ammo bu nazorat choralari ortida hech qanday mantiq yo‘q. Insonlar xavfsizlik tashkiloti bilan ba‘zan to‘qnash kelganda, “xavfsizlik”ni nomaqbul to‘qnashuv, o‘z maqsadlariga erishish yo‘lidagi yana bir bezovta qiluvchi to‘siq sifatida ko‘rishlari mumkin.

⁴⁸ VPN (virtual private network) – virtual xususiy tarmoq.

Xavfsizlik bo'yicha mutaxassislar o'zlarini nafaqat texnik xodimlar, balki strategik biznes sheriklar sifatida tan olinishlarini istashadi. Agar ular muhim qarorlar qabul qilinadigan muzokaralarda ishtirok etmoqchi bo'lsalar, ular nima qilishlari va nimalar qilishga qodir ekanliklari haqidagi tasavvurlarini o'zgartirishlari kerak bo'ladi.

Tahdidlarni boshqarish bo'yicha sa'y-harakatlar va maqsadlar o'zgarishi lozim. Rasmiy ishlab chiqilgan dastur yordamida tahdidlarni boshqarish samaradorli bo'lishini rahbariyat aniq tushunishi lozim. Biznes rahbarlari tahdidlarni hisobga olgan holda, biznes qarorlarini qabul qilishlari uchun tahdid haqida izchil va shaffof ma'lumotlarga ega bo'lishlari kerak. Ular xavfsizlik xodimlarini strategik biznes hamkorlar sifatida ko'rishlari va ular bilan hamkorlik qilishlari lozim. Xavfsizlikni idrok etishdagi ushbu tub o'zgarishlarni bartaraf etish uchun vaqt kerak bo'ladi, shunga qaramasdan u amalga oshishi zarur.

CRMP: Asosiy afzalliklari

Mustahkam CRMPni amalga oshirish bugungi raqamli muhitda muhim ahamiyatga ega va u ko'plab afzalliklarni taqdim etadi:

Kengash va ijroiya darajasidagi himoya:

Qaror qabul qiluvchi yuqori mansabdor shaxslar kibertahdidlarni boshqarish faoliyatini nazorat qilishlari shart, tahdid haqida yetarli va to'g'ri ma'lumot olishlariga ishonch hosil qilishlari lozim. Bu shuni anglatadiki, ular o'rnatilgan tahdid funksiyasini va qabul qilingan tahdidga oid qarorlarni zarur paytda tushuntirishlari va kerak bo'lganda himoya qilishlari mumkin.

Xavfsizlikning taktik funksiyadan strategik tahdid vazifasi sifatida qabul qilinishi:

Tahdidlarni boshqarishning tezkor modeli yordamida tez qaror qabul qilish va ustuvorliklarni belgilash korxonaga kibertahdidlar haqida qaror qabul qilish, rivojlanayotgan muhitlardan xabardor bo'lish va umumiy biznes strategiyasiga muvofiq harakat qilish va raqobatchilardan aniq strategik ustunlikni ta'minlash imkonini beradi. Natijada, xavfsizlik va tahdidlar bo'yicha tashkilotlar strategik suhbatlar bilan shug'ullanadi va ular faqatgina xarajatlar markazining taktik funksiyasi emas, balki biznesni faollashtiruvchi sifatida ham namoyon bo'ladi.

Oqlangan byudjet

Kuchli istak va bag'rikenglikka, shuningdek, tahdid va mukofotning muvozanatiga asoslangan favqulodda vaziyatlarda xavfsizlik boshqaruvi xodimlar va boshqa resurslar xarajatlarni asoslashni osonlashtiradi.

Xavfsizlik bo'yicha mutaxassisning ish faoliyatidan qoniqishi va himoyasi

O'rnatilgan dastur CISO yoki boshqa yuqori darajadagi xavfsizlik bo'yicha mutaxassislarga muhim muzokaralarda qatnashib, qarorlar qabul qilishga imkon beradi, noxush hodisalardan keyingi oqibatlardan va keraksiz ta'na va ayblovlardan himoya qiladi.

Ushbu afzalliklarning ba'zilar korxonalarning kundalik faoliyatiga va xususan xavfsizlik tashkilotlariga qanday tatbiq etilishini quyida ko'rib chiqamiz:

1-AFZALLIK: XAVFSIZLIKKA TAHDID FUNKSIYASINING STRATEGIK TAN OLINISHI

Aniq belgilangan favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturining eng muhim afzalliklaridan biri shundaki, u xavfsizlik tashkiloti va uning faoliyati-ga muhim strategik korxona maqomini beradi.

Yuqorida aytib o'tganimizdek, ta'riflangan favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturi *izchil*, *kutilgan* va *ishonchli* natijalarga olib keladi. Keling, ushbu uchta so'z nimani anglatishini va nima uchun ular muhim ekanligini batafsil ko'rib chiqamiz:

Izchil

Har qanday korxona dasturining muvaffaqiyatli bo'lishida izchillik juda muhim o'rin tutadi. Tahdidlarni boshqarish asosan kutilmagan hodisalarni oldindan ko'rish, boshqarish va ularning noxush oqibatlarini kamaytirish bilan bog'liq bo'lib, shu sababli izchillik tahdidlarni boshqarish dasturida o'ta muhimdir. Tahdidlarni boshqarishda doimo improvizatsiya elementlari mavjud bo'ladi, chunki yangi va kutilmagan tahdidlar va zaifliklarni doimiy tarzda bartaraf etish kerak. Sizda ishonchli natijalarga olib keladigan, izchil jarayonlar va umidlar bilan aniq belgilangan dastur mavjud bo'lsa, tezkor qarorlar qabul qilish yanada osonroq va samaraliroq bo'ladi.

Kutilgan

Favqulodda vaziyatlarda xavfsizlik boshqaruvi dasturida barcha manfaatdor tomonlar, direktorlar kengashidan tortib bosh direktor hamda biznes yo'nalishlari rahbarlarigacha o'zlarining talablariga mos keladigan va o'z vaqtida yetkazib beriladigan tahdidlar haqidagi ma'lumotlarini o'z vaqtida olish imkoniyatiga ega bo'lishlari lozim. "*O'z vaqtida*" deganda, masalan, dasturiy ta'minotni joriy etishning boshida yoki yangi mahsulotni loyihalash jarayonining boshida taqdim etiladigan tahdidlar to'g'risidagi ma'lumotlarni tushunish mumkin. Biroq manfaatdor tomonlar dasturdan ko'proq narsani kutish huquqiga ega. Ular dasturni o'z xizmat vazifalariga to'sqinlik qilmaydigan, taktik vazifa emas, balki strategik vazifa sifatida ko'rishlari kerak. Manfaatdor tomonlar yangi loyihaning boshidan oxirigacha to'liq ishtirok etishlari lozim, shunda ular xavfsizlik tashkiloti bilan birgalikda qaror qabul qilishda ko'rsatmalar berishlari hamda tahdid va foydaning to'g'ri muvozanatini topishlari mumkin.

Ishonchli

Aniq belgilangan dasturning joriy etilishi uning natijalariga to'liq ishonish mumkinligini anglatadi. Dastur taqdim etayotgan tahdidlarni baholash va ope-ratsion ko'rsatmalar o'nlab yillar davomida takomillashib kelayotgan tahdidlar-ni boshqarish bo'yicha asosiy usullarga asoslanadi. Manfaatdor tomonlar o'zlari tayanadigan narsaga ishonishlari mumkin, chunki bu belgilangan, tasdiqlangan,

e'lon qilingan va eng muhimi, boshqaruv organi tomonidan nazorat qilinadigan dastur natijasidir. (Boshqaruvning muhim ahamiyati haqida 3-bobda to'xtalib o'tamiz.)

Agar yuqoridagi uch asosiy komponent tatbiq etilsa, ularning ijobiy ta'siri butun korxona bo'ylab sezila boshlanadi va muvaffaqiyat o'z-o'zidan mustahkamlanadi. Masalan, korxonalarining tahdidlarga moyilligi va chidamliligini aniqlash – butun korxona miqyosida amalga oshiriladigan xavfsizlik strategiyasini ishlab chiqishga va resurslarga bo'lgan talablarni asoslashga imkon beradi.

2-AFZALLIK: KIBERTAHDIDLARGA QARSHI KURASH BO'LINMASINING SAMARALI BYUDJETINI TA'MINLASH

Byudjet masalalari batafsil ko'rib chiqilishi lozim. Axborot texnologiyalari sohasida byudjet mablag'lari har doim juda cheklangan bo'lib, xavfsizlik sohasida byudjet mablag'lari yanada ko'proq cheklangan, chunki tarixan xavfsizlik xizmati strategik hamkorlar sifatida emas, balki xarajat markazi sifatida, hattoki biznesni samarali yuritish yo'lidagi to'siq sifatida qaralgan. Xavfsizlik sohasiga byudjet ko'pincha korxona byudjeti yoki axborot texnologiya byudjetidan ajratiladi, yangi tahdid aniqlanganda yoki bundan ham yomon, noxush hodisa sodir bo'lgandan so'ngina yangi resurslar maxsus asosda ajratiladi. Tezkor, maxsus yondashuv ayniqsa xavfli, chunki raqamli texnologiyalar har qachongidan ham xavfli tahdid muhitini keltirib chiqarmoqda, shu bilan birga hujumlar soni, ularning tezligi va biznesga salbiy ta'siri doimiy ravishda oshib bormoqda (Ajablanarli tomoni shundaki, byudjet talablarini jiddiy hodisa yuz bermagan, tinch davrda aniqlash qiyin). Natija esa – byudjet tanqisligi hamda biznesga real foyda olib kelmaydigan funksiyaga mablag' ajratishni istamaslik.

CRMP korxonaning byudjet qarorlarini qabul qiluvchilarga tahdidga moyillik va chidamlilikni aniqlashda yordam berish orqali ushbu muammoni hal qiladi, tahdiddan mutlaq xoli muhitini yaratish imkonsiz ekanligini tan oladi, bu esa pragmatik, real va harakatga asoslangan xavfsizlik strategiyasining asosini tashkil qilishi mumkin.

3-AFZALLIK: TAHDIDLAR BO'YICHA QAROR QABUL QILUVCHI SHAXSLAR UCHUN HIMOYA

Kibertahdid sodir bo'lganda, xavfsizlik dasturi oddiy, samarasiz va foydasiz harakatlardan qochishga imkon beradi. Agar tahdid aniqlangan va tasdiqlangan va tahdidlarga tolerantlik asosida choralar ko'rilgan bo'lsa, yuzaga kelgan noxush hodisalarda biror shaxsni yoki alohida bo'limni ayblash qiyinroq bo'ladi. Har qanday turdagi yirik noxush hodisadan keyin belgilangan tolerantlik qayta ko'rib chiqilishi kerak, unga o'zgartirishlar kiritishga ehtiyoj bo'lishi ham mumkin, ammo bu CRMP tomonidan o'rnatilgan jarayonlarga asoslanadi.

Aniq ishlab chiqilgan va jamoatchilik e'tiboriga to'g'ri yetkazilgan kiberxavfsizlik dasturi barcha korxonalarni ma'lum yuridik va me'yoriy majburiyatlardan himoya qiladi.

Yaxshi ishlab chiqilgan CRMP muammo yuzaga kelganda, nafaqat xavfsizlik bo'yicha mutaxassisi yoki butun xavfsizlik tashkilotini shunchaki himoya qilibgina qolmaydi. U butun korxonani, shu jumladan, biznes sohasi rahbarlarini, yuqori darajadagi rahbarlarni, bosh direktorni va hatto direktorlar kengashini har qanday noxush oqibatlardan, shu jumladan huquqiy va me'yoriy javobgarlikdan himoya qiladi.

Tizimli, ammo tahdiddan mutlaq xoli bo'lmagan CRMP

Sizda savol tug'ilishi mumkin: "Agar dastur barcha muammolarni hal qilmasa, qanday qilib u meni himoya qila oladi?" Ko'pgina sud jarayonlarida korxonalar va ularning asosiy rahbarlari tahdidlarni boshqarish uchun mas'uliyatni o'z zimmalariga olishlari kerakligi aniq ko'rsatiladi. Bu direktorlar kengashi har bir texnologiya qarorini nazorat qilishi yoki korxonani har qanday tahdiddan himoya qilishi kerakligini anglatmaydi. Sudlar tahdiddan mutlaq xoli muhit mavjud emasligini tan olishadi va korxona noxush hodisalardan xoli bo'lishi kerak deb hisoblashmaydi, ammo ular kutayotgan ba'zi muhim narsalar bor:

- Korxona maqbul standartlarga javob berishi va tegishli xavfsizlik qoidalariga rioya qilishi kerak.
- Rahbarlar CRMP tarkibiy qismlarini ishlab chiqishlari, ularni joriy etishlari hamda tegishli darajada nazorat qilishlari zarur, shu jumladan, tahdidlarni hisobga olgan holda qaror qabul qilish jarayoni va boshqaruv tuzilmasi, manfaatdor tomonlar bilan muloqot qilish va tahdidlar eskalatsiyasi bo'yicha tegishli tartib-taomillarni amalga oshirishlari kerak.
- Tahdidlarni boshqarish dasturi tizimli bo'lishi kerak. Bu tahdidlarni boshqarish tizimi butun korxona bo'ylab joriy etilishini va izchil boshqarilishini ta'minlaydi.

Tahdidlarni boshqarish bo'yicha qarorlar qabul qilish ko'proq ish, ko'proq tuzilma va manfaatdor tomonlardan mas'uliyatni talab qiladi. Nazorat yetishmovchiligiga asoslangan javobgarlikdan himoyalaniş uchun korxona va uning rahbarlari o'zlariga ba'zi asosiy savollarni berishganini va ularning javoblari asosida kibertahdidlarni boshqarishning ishonchli usullarini ishlab chiqqanliklarini ko'rsatishlari kerak. Biz aniqlagan eng muhim savollar quyidagicha:

- "Boshqaruv organi biznes qarorlarini qabul qiluvchi shaxslar nomidan vakillik qiladimi, u tegishli mustaqillikka va belgilangan nizomga egami, agar u tashkil etilgan bo'lsa, u korxona tahdidlarini boshqarish yoki taftish komissiyasiga muvofiqmi?"

• “Boshqaruv organi tahdidlarga moyillik va chidamlilik, shuningdek, biznesni uning oldida javobgarlikka tortish mexanizmini oʻrnatdimi? Xavfsizlik strategiyasi va byudjeti tahdidlarga moyillik va chidamlilikka mos keladimi?”

• Boshqaruv organi tomonidan tasdiqlangan muayyan biznes manfaatlari va chidamlilikni koʻrsatadigan tahdidlar toʻgʻrisida choraklik hisobot mavjudmi? Ular oʻz vaqtida yangilanadimi?”

• “Boshqaruv organi muntazam ravishda tizimli kibertahdidlar haqida gapiradimi?”

• “Kengash va ijroiya qoʻmitasi kiber hisobotlarida chidamlilikni ifodalovchi asosiy xavf koʻrsatkichlari (KRI⁴⁹)ni belgilaganmi va xavfsizlik guruhi ushbu chidamlilikka amal qilyaptimi?”

• “Belgilangan tahdid darajalariga mos keladigan rasmiy tahdidlar eskalatsiyasi jarayoni bormi?”

• “Audit masalalari boʻyicha boʻlinma CRMPning mavjudligi va maqsadga muvofiqligini tekshiradimi?”

• “Audit jarayonida faqatgina xavfsizlik boʻyicha operativ nazorat va xavfsizlik imkoniyatlari tekshirilmadan, balki biznes belgilangan talab va chidamlilik asosida ishlashi ham tekshirilyaptimi?”

• “Kibertahdidlarni boshqarish boʻyicha kengash oʻzining kibertahdidlarni boshqarish boʻyicha dasturi mavjudligiga, tashkil etilganiga va kibertahdidlarni nazorat qilish boʻyicha oʻz majburiyatlarini bajarishga ishonchi komilmi?”

• “Biznes uchun ahamiyatli boʻlgan kibertahdidlarni toʻgʻri aniqlash va oshkor qilish jarayoni mavjudmi?”

Agar sizda ushbu savollarga aniq javob boʻlmasa, demak sizda toʻgʻri belgilangan CRMP mavjud emas. Agar korxonangiz jamoat kompaniyasi boʻlsa, demak, boshqaruv kengashi va yuqori darajadagi rahbarlar kibertahdidlarni boshqarish boʻyicha nazorat majburiyatlarini bajarmayapti.

Kengashning masʼuliyati va yuridik javobgarligi

Boshqaruv darajasidagi huquqiy javobgarlik ham kengash nazorati majburiyatlari taʼrifini va CRMP nima ekanligini shakllantira boshladi. Buning sabablaridan biri shundaki, aksiyadorlarning daʼvolari boʻyicha sud qarorlari kengashlarning bir vaqtlar kuchli boʻlgan himoyasini zaiflashtira boshlaydi, masʼuliyat darajasini pasaytiradi va kengashning kibertahdidlarni nazorat qilish boʻyicha oʻz majburiyatlarini bajarish yondashuvlarini oʻzgartirishga undaydi. Kengash darajasidagi javobgarlikning “viجدonan qilingan xatti-harakat” tamoyilini oʻrnatgan voqea sogʻliqni saqlash xizmatlarining yirik taʼminotchisi Caremark International

⁴⁹ KRI (key risk indicators) – asosiy xavf koʻrsatkichlari, bu boshqaruvda xavf darajasini koʻrsatish uchun ishlatiladigan oʻlchovdir.

kompaniyasiga nisbatan chiqarilgan 1996-yildagi sud qarori edi. Bir guruh aksiyadorlar kompaniya o'z xodimlariga nisbatan tegishli tahdid nazoratini amalga oshira olmadi, bu esa ba'zi xodimlarga keng ko'lamli firibgarlikni amalga oshirishga yordam berdi deya da'vo qilib, Caremark kompaniyasi direktorlarini sudga berishdi. Ba'zi Caremark xodimlari shifokorlar bilan Caremark mahsulotlari va xizmatlarini bemorlarga tavsiya etish bo'yicha shartnomalar imzolashgan. Da'vo AQSH Sog'liqni saqlash va aholiga xizmat ko'rsatish departamenti hamda Adliya vazirligi tomonidan to'rt yillik tergovga olib keldi va natijada bir nechta jinoyiy ayblovlar qo'zg'atildi. Oxir-oqibat kompaniya bitta jinoyat ayblovi bo'yicha aybini tan oldi.

Caremark kompaniyasining xatosi unga qimmatga tushdi, sog'liqni saqlash sohasida o'ta muhim bo'lgan korporativ obro' va brendga yetkazilgan zararni hisobga olmaganda, jinoyiy va fuqarolik jarimalari va sudlanuvchilarga taxminan 250 million AQSH dollari miqdoridagi to'lovlar to'landi. Caremark ishining oqibatlari kompaniya va sog'liqni saqlash sohasi doirasidan tashqariga chiqadi. Sud qaroriga ko'ra, direktorlar kengashlari kompaniya harakatlari nisbatan tegishli tekshiruvni amalga oshirmaganligi, vijdonan harakat qilmagani uchun javobgarlikka tortilishi mumkin.

Vijdonan qilingan sa'y-harakatlar atamasi mas'uliyatning eng yuqori chegarasidir. Caremark ishi bo'yicha sud qarori shuni ko'rsatadiki, direktorlar kengashi kompaniyaning xodimi tomonidan amalga oshirilgan har bir xatti-harakat uchun javobgar emas, ular faqatgina nazorat va boshqaruvni ta'minlash uchun jiddiy harakat qilishlari kerak. Qaror aslida ularga qonuniy harakatlardan himoyalaniшни taklif qilish sifatida ko'rildi, ammo keyingi hollarda qarorlar bu himoyalarni bekor qila boshladi. Caremark kompaniyasi keyingi sud qarorlari uchun muhim pretsedent (o'xshash voqea) yaratdi, Marchand v. Barnhill⁵⁰ shular jumlasidandir:

Garchi Caremark ba'zi sharhlovchilar xohlaganchalik ko'p narsani talab qilmasa ham, u boshqaruv kengashidan nazorat qilishning oqilona tizimini o'rnatish va korxonaning asosiy tahdidlari haqida hisobot berishda vijdonan harakat qilishini talab qiladi.

Marchand v. Barnhill , 212 A.3d 805

"Vijdonan yondashish" nima degan savol boshqa bir sud ishining diqqat markazida bo'lib yig'ilish zallarini larzaga soldi. Bu sud ishi oziq-ovqat sanoati bilan bog'liq edi. 2015-yilda Kanzasda uch kishining o'limiga sabab bo'lgan oziq-ovqat zaharlanishi Oklahomadagi Blue Bell Creameries muzqaymoq ishlab chiqarish

⁵⁰ Marchand v. Barnhill – Marchand V. Barnhill sud ishi korporativ huquq sohasidagi muhim qarordir. Bu direktorlarning majburiyatlari va ularning aksiyadorlar oldidagi majburiyatlarini tushunish uchun muhim ish sanaladi. Ushbu sud ishida direktorlarning potensial tahdidlarni hisobga olmaganligi uchun javobgarligi ko'rib chiqilgan.

korxonasidan olingan muzqaymoq tarkibidagi listeria bakteriyalari bilan bog'liq edi.

Blue Bell korxonasi o'zining yuz yillik tarixida birinchi marta mahsulotni qaytarib olishga, Oklaxomadagi zavodni va yana boshqa obyektni uzoq muddatga yopishga hamda sakkiz million gallon⁵¹dan ortiq mahsulotni chiqindixonaga yuborishga majbur bo'ldi. Oziq-ovqat va farmatsevtika idorasi (FDA⁵²) tomondan olib borilgan tekshiruv shuni ko'rsatdiki, kompaniya o'z mahsulotlari aynishining oldini olish uchun standart sanoat amaliyotiga rioya qilmagan va halokatli epidemiyadan bir necha yillar oldin Oklahomadagi muassasadan listeriya izlari qayta-qayta topilgan.

Blue Bell epidemiyasining eng ayanchli jihati, shubhasiz, odamlarning fojiali o'limi edi. Bundan tashqari, kompaniya va direktorlar kengashlari uchun oqibatlar juda halokatli bo'ldi. Kompaniyaning ishlab chiqarish imkoniyatlari cheklandi, uning bir necha shtatlardagi faoliyati to'liq to'xtadi. Kompaniyaning minglab xodimlari doimiy yoki vaqtinchalik ishdan bo'shatildi, yana ko'pchilikning maoshi kamaytirildi (Blue Bell kompaniyasi bu holatlar listeria epidemiyasi natijasi ekanligini hech qachon aniq tasdiqlamagan). Kompaniya va uning bosh direktori/prezidenti fitna va firibgarlik kabi ayblovlar bilan jinoyat ishlarida ayblangan, natijada Adliya vazirligining da'vo qilishicha, bu epidemiyani yashirish holati bo'lgan. Kompaniya sifatsiz mahsulotlarini tarqatish bo'yicha aybini tan oldi (ushbu bandni yozish paytida sobiq prezidentning ishlari hali sudga topshirilmagan edi) va 19,5 million dollar miqdoridagi jinoiy jarimalar, ma'muriy jarimalar va kompensatsiya to'lashga rozi bo'ldi.

Blue Bell kompaniyasining listeria bilan bog'liq mojarosi bir asrlik kompaniyaning faoliyatini xavf ostiga qo'ydi. Kompaniyaning naqd pullari shu darajada kam ediki, u Blue Bell aksiyalarining qiymatini keskin pasaytiradigan yirik xususiy investitsiyalarni qabul qilishga majbur bo'ldi. Belgilangan xizmat ko'rsatish standartlariga rioya qilmaganligi uchun aksiyador kompaniyaning direktorlar kengashi, ikkita yuqori martabali rahbariga, shu jumladan sobiq bosh direktorga qarshi sudga da'vo ishini ochdi va 2019-yilda sudlar quyidagilarga kelishib oldilar:

Direktorlar kengashining "haqqoniy axborot va hisobot tizimini ta'minlashdagi vazifalarini to'liq bajarmasligi" kompaniyaning manfaatlarini ko'zlab harakat qilish majburiyatini buzgan holda vijdotsizlarcha qilingan harakatdir.

Marchand v. Barnhill, 212 A.3d 805 (Del. 2019)

Blue Bell ishi va bu masalani hal qilish to'g'risidagi sud qarorining muhim ahamiyati shundaki, "vijdonan" ish tutmaslik nimalarga olib kelishini anglashdir.

⁵¹ Gallon (G) – suyuqlik o'lchov birligi. 1G – 4,5 litr.

⁵² FDA (Food and Drug Administration) – Amerika oziq-ovqat va farmatsevtika idorasi.

Sudlar “vijdonan” yondashish uchun tahdidlar haqida ma’lumot va hisobot beruvchi tahdidlarga asoslangan tizimli dasturni joriy qilishni talab qila boshlashdi. Blue Bell sud ishida kompaniyaning kasodga uchrashi, uning vijdonan harakat qilmaganligi deb topildi. Sud quyidagilarni aniqladi:

- Oziq-ovqat xavfsizligi masalalarini hal qilish uchun kengash darajasidagi qo‘mita mavjud emas edi.

- Oziq-ovqat xavfsizligi qoidalariga rioya qilish amaliyotlari, tahdidlar yoki hisobotlardan kengash xabardor bo‘lishini talab qiladigan muntazam jarayon yoki bayonnomalar mavjud emas edi.

- Kengashda oziq-ovqat xavfsizligi risklarini muntazam ravishda (masalan, har chorakda yoki yilda ikki marta) ko‘rib chiqish jadvali mavjud emas edi.

- Uch nafar mijozning o‘limidan oldin Blue Bell kompaniyasi rahbariyati kompaniya mahsulotlari xavfsizligi yuzasidan jiddiy xavotir uyg‘otgan xabarlarini olgan, biroq boshqaruv kengashi yig‘ilishlari bayonnomalarida ular kengashga oshkor qilingani haqida hech qanday dalil ko‘rsatilmagan. Aslida, kengashga oziq-ovqat xavfsizligi to‘g‘risida ijobiy ma’lumotlar berilgan, ammo haqiqiy manzara umuman boshqacha edi.

O‘zaro bog‘liqlik: Caremark ishi boshqaruv kengashi javobgarlikning oldini olish uchun vijdonan harakat qilishi kerakligini ko‘rsatdi. Marchand ishi esa, vijdonan harakat qilish uchun CRMPning ikkinchi asosiy tarkibiy qismi bo‘lgan Tahdidlar haqidagi ma’lumotlarga asoslangan tizimga ega bo‘lish kerakligini, aks holda shaxsiy javobgarlik yuzaga kelishi mumkinligini isbotladi. Ushbu qaror kengash darajasida halollik va mas’uliyatning yangi standartlarini o‘rnatish orqali Caremark ishini sezilarli darajada kengaytirdi. Qarorda kompaniya direktorlar kengashi va uning har bir a‘zosi tizimli ravishda tahdidlarni boshqarish bo‘yicha qarorlar qabul qilishda mas’ul ekanligi va tahdidlarni boshqarish bo‘yicha mas’uliyatlarini to‘g‘ri bajarmagan taqdirda javobgarlikka tortilishi qayd etildi. Bu kibernetika bilan qanday bog‘liq? Mana shu joyda Boeing ishi yana yodga tushadi.

Boeing kompaniyasi ishi bo‘yicha sud qarori va kibertahdid nazorati bo‘yicha javobgarlik

Boshqaruv kengashi darajasidagi javobgarlikni belgilash jarayoni shu bilan tugab qolmaydi. Boeing kompaniyasining jamoaviy da’vosi, kengashning majburiyatlarini “o‘ta muhim” bo‘lgan barcha narsalarga dasturiy yondashuvni talab qilish sifatida belgilashni davom ettiradi va kengash darajasidagi javobgarlikni kibernetika nazorat javobgarligiga bir qadam yaqinlashtiradi. Boeing aksiyadorlari boshqaruv kengashini xavfsizlik masalalari bo‘yicha o‘z nazorat vazifalarini bajarmaganlikda ayblab, da’vo arizasi bilan chiqdi. Sud kompaniyaning da’voni ko‘rib chiqishni to‘xtatish to‘g‘risidagi iltimosini rad etdi hamda Caremark va Marchand ishlari bo‘yicha qarorlarga aniqlik kiritishda davom etdi, sud samolyot parvozi xavfsizligi “jiddiy va o‘ta muhim” deya ta’kidlab, boshqaruv kengashidan xavf-

sizlik tahdidlari bilan bog'liq masalalar bo'yicha o'z nazorat funksiyasini qat'iy bajarishi kerakligini talab qildi. Sud boshqaruv kengashi samolyot parvozi xavfsizligi tahdidlarini muntazam ravishda tekshirib borish uchun hech qanday hisobot yoki axborot tizimini yetarli darajada joriy etmaganligini aniqladi. Sud quyidagilarni aniqladi:

- Boshqaruv kengashida samolyot xavfsizligini muntazam ravishda tekshirib borish, muhokama qilish yoki muntazam ravishda hisobot berish uchun tizim mavjud emas edi.

- Boshqaruv kengashi tahdidlarni nazorat qilish funksiyasiga ega bo'lsa-da, uning nazorati birinchi navbatda moliyaviy tahdidlarga qaratilgan bo'lib, "jiddiy va o'ta muhim" bo'lgan samolyotlar xavfsizligini qamrab olmagan.

- Boshqaruv kengashi yetarli darajada shaffof bo'lmagan boshqaruv hisobotlarini olgan va qo'shimcha ma'lumot so'ramagan, batafsilroq yoki muntazam hisobot berish jarayonini talab qilmagan.

- Qizil bayroqlar, ya'ni tahdid belgilari rahbariyatga taqdim etilgan, ammo boshqaruv kengashiga tegishli ravishda yetkazilmagan, bu esa tegishli hisobot tizimi mavjud emasligini ko'rsatmoqda.

Boeing aksiyadorning da'vo ishini 237,5 million dollar to'lash evaziga hal qildi.

Sud qayta va qayta boshqaruv kengashi tahdidni boshqarish bo'yicha nazoratni dasturiy ravishda amalga oshirish kerakligini ta'kidladi. Boeing ishidan yana bir muhim xulosa chiqarish mumkin, u boshqaruv kengashi nazoratini ayniqsa "o'ta muhim" vazifalarga qo'llashga qaratilgan. Sudning xulosasida shunday deyilgan: "Boeing kompaniyasi "xavfsizlikni nazorat qilish"ni tashkilot piramidasi-ning eng ustuvor vazifasi sifatida belgilamagan. "Boeing" boshqaruv qo'mitalarining hech biriga samolyot xavfsizligini nazorat qilish vazifasi yuklanmagan va hech bir qo'mita nizomida samolyot xavfsizligi haqida yozilmagan"⁵³.

Unda yana davom etiladi: "Xavfsizlik masalalari muhim bo'lgan vaziyatda, boshqaruvning faqat umumiy hisobotlar bilan xavfsizlikni ko'rib chiqishining yetarli emasligi ta'kidlanadi. Xavfsizlik uchun ko'rsatilgan e'tibor yanada aniq va tizimli bo'lishi kerak. Bunday hisobotlar muhim xavfsizlik masalalarini to'liq qamrab ololmaydi. Boeing boshqaruv kengashi samolyot xavfsizligi bo'yicha talablarga rioya qilishni rahbariyat ixtiyoriga topshirib qo'ymasdan, balki aniq tuzilgan muvofiqlik tizimini joriy etishi va keyin uning ustidan nazorat olib borishi lozim"⁵⁴.

Nima uchun bu juda muhim? Birinchi bobda biz To'rtinchi sanoat inqilobining boshlanishi – raqamlashtirishni muhokama qilgan edik. Shu nuqtayi nazardan, raqamlashtirish va unga aloqador barcha biznes jarayonlari va tahdidlarni

⁵³ In re C. A. 2019-0907-MTZ (Del. Ch. Sep. 7, 2021), <https://oreil.ly/3rxul>

⁵⁴ In re C. A. 2019-0907-MTZ (Del. Ch. Sep. 7, 2021).

“o‘ta muhim” deb hisoblamaslikning iloji yo‘q. Raqamlashtirish va tahdid o‘rtasidagi bog‘liqlik ayondir, shuningdek, raqamli tahdidlarni nazorat qilish majburiyatlari nimalarga olib kelishi ham aniq. Nazorat “o‘ta muhim” hisoblangan vazifalarga qo‘llaniladigan aniq va tizimli CRMPni talab qiladi, shubhasiz, kiber-muhitdagi vazifalar shular jumlasidandir.

Axborot xavfsizligi boshqarmasi boshliqlari javobgarlik uchun tanqid ostida

Ushbu kitobni yozish jarayonida, SEC tomonidan kiberxavfsizlik hamjamiyatini hayratda qoldiradigan harakat bo‘ldi. Amerikaning axborot texnologiyasi sohasida faoliyat yuritadigan SolarWinds kompaniyasi ma‘lumotlar sizib chiqishi kabi noxush voqeani boshdan kechirdi va SEC bu kompaniyaning yuqori lavozimli rahbarlarini ularga qarshi qonuniy choralar ko‘rilishi haqida ogohlantirdi. Ayniqsa e‘tiborga molik tomoni shundaki, kompaniyaning axborot xavfsizligi boshqarmasi boshlig‘i bu xabarnomani olganlar orasida edi⁵⁵. Equifax kompaniyasi axborot xavfsizligi bo‘limi boshlig‘i Jamil Farshi, LinkedIn ijtimoiy tarmog‘i sahifasida, axborot xavfsizligi bo‘limi boshlig‘i bu kabi xabarnomani birinchi marta olayotganligini ta’kidladi.

SECning bu bildirishnomalari “Uels (Wells) bildirishnomalari” deb nomlanadi, bu komissiyaning SEC qoidalarini buzganlarga ayblovlar qo‘yishga mo‘ljallangan xabarnomasidir. SEC qoidabuzarliklari ularning asosiy faoliyatiga qaratilgan bo‘lib, kibertahdidlarni boshqarish nazorati, ijro etilishi va tahdid eskalatsiyasi orqali shaffof nazorat kabi masalalarini muhokama qilish bilan bevosita bog‘liq. SEC tomonidan e‘lon qilingan rasmiy qoidalar CISOlarni haqiqiy tashvishga solishi aniq. Uels bildirishnomalari juda ahamiyatli voqea bo‘lib, bu CISO endi kibertahdidlarni boshqarish nazorati va ularning ijrosi uchun yanada ko‘proq javobgar bo‘lishini ko‘rsatadi.

SECning bu kabi bildirishnomalari SolarWinds kompaniyasiga kiberhujum aniqlanganidan taxminan ikki yarim yil o‘tgach paydo bo‘ldi, bu federal hukumat va xususiy sektorga qarshi o‘tkazilan eng keng qamrovli va murakkab xakerlik chora-tadbirlari yig‘indisi edi. Buzg‘unchilik ko‘plab federal agentliklar va 100 dan ortiq kompaniyalarga ta’sir ko‘rsatdi. Xakerlar SolarWinds kompaniyasining Orion axborot texnologiyalari boshqaruv platformasi yangilanishidan foydalanib, zararlangan kompyuterlarga masofadan turib kirish imkoniyatiga ega bo‘lishdi. AQSH hukumati bu hujumga Rossiya tashqi razvedka xizmatini aybdor deb topdi.

Uber⁵⁶ kompaniyasining sobiq xavfsizlik xizmati rahbari Jozef Sallivanga 2016-yilda kompaniyaga qilingan kiberhujumni yashirgani uchun hukm o‘qil-

⁵⁵ Tim Starks (Devid DiMolfetta tomonidan olib borilgan tadqiqotlar bilan), “SEC kibernetika rahbarlarining xavotirga tushayotganini payqadi”, “Washington Post” gazetasi, 2023-yil 29-iyun.

⁵⁶ Uber – San-Fransiskoda joylashgan Amerika xalqaro jamoat kompaniyasi bo‘lib, taksi qidirish, chaqirish va oziq-ovqat yetkazib berish uchun xuddi shu nomdagi mobil ilovani yaratgan.

ganidan keyin CISO va boshqa kiberxavfsizlik rahbarlari ustidan kuchaytirilgan tekshiruvlar boshlandi (3-bobda bu haqida batafsilroq ma'lumot keltiriladi). Bunday harakatlar kompaniyalardagi kiberxavfsizlikdagi kamchiliklar uchun alohida shaxslarni javobgarlikka tortish ko'rsatkichlarining ortib borayotganini ko'rsatadi. Bu esa, kiberxavfsizlik sohasi yetakchilari CISOlarning yanada ko'proq javobgarlik nishoni ostida bo'lishini ifodalaydi.

Ushbu kitobni yozar ekanmiz, sodir bo'layotgon voqealar bu masalaning naqadar dolzarbligini ko'rsatadi. 2023-yil oktyabr oyida SEC SolarWinds korporatsiyasi va uning axborot xavfsizligi bo'yicha bosh direktori Timoti G. Braunni firibgarlik va ichki nazoratni bajarmaslikda aybladi. 2018-yilda kompaniya o'z aksiyalarini birjada birinchi marta ommaga taklif qilgan (IPO³⁷), 2020-yilda esa muhim kiberhujum fosh etilgan. Kompaniyaning kiberxavfsizlik amaliyotini noto'g'ri taqdim etgani, tahdid va kamchiliklarni oshkor etmagani kabi ayblovlar aynan shu davrda yuzaga kelgan.

Kompaniya xavfsizlikning zaif tomonlarini, yuzaga kelishi mumkin bo'lgan jiddiy moliyaviy zarar va obro'ga putur yetishi mumkinligini tan olinishiga qaramay, ma'lum bo'lgan maxsus kamchiliklar sarmoyadorlarga oshkor qilinmasdan, faqat umumiy tahdidlar haqida ma'lumot berilgan. SEC shikoyatida bayon etilishicha, Braun va boshqa xodimlar kompaniyaning zaif tomonlaridan xabardor bo'lishgan, ammo bu muammolarni to'g'ri bartaraf eta olmagan, bu esa muhim aktivlarni himoya qila olmaslik hamda SEC qoidalariga binoan muhim tahdidlar eskalatsiyasi va ularni oshkor qilish bo'yicha majburiyatlarini bajarmaslik holatlariga olib kelgan.

Bu holat tegishli xavfsizlik qoidalariga rioya qilishdan tashqari CISONing vazifasi va mas'uliyatidagi keskin o'zgarishlarni ko'rsatadi. SECning Braunga qarshi harakati axborot xavfsizligi bo'limi boshlig'i uchun kiberxavfsizlik xavf-xatarlarini boshqarishda yangi javobgarlik darajasini bildiradi. Endi axborot xavfsizligi bo'limi boshlig'i uchun faqat taktik chora-tadbirlarni amalga oshirish yetarli emas; ular, shuningdek, o'z kompaniyalarining investorlar uchun taqdim etgan ma'lumotlari kiberxavfsizlik tahdidlari va amaliyotlarining haqiqiy holatini o'z vaqtida va dasturiy tarzda aks ettirishini kafolatlashi lozim. SECning muvofiqlik haqidagi talabiga ko'ra, CISO va ularning kompaniyalari nafaqat o'zlarining tahdid muhitiga moslashtirilgan kiberxavfsizlik bo'yicha mustahkam chora-tadbirlarni amalga oshirishi, balki investorlar bilan ma'lum muammolar bo'yicha shaffoflikni ta'minlashi zarur. Ushbu yangi nazorat CISONi nafaqat nazoratni amalga oshirish, balki kiberxavfsizlik tahdidlarini strategik boshqarish uchun ham mas'ul etib qo'yadi.

³⁷ IPO (initial public offering) – birlamchi ommaviy taklif, bu – kompaniyaning o'z aksiyalarini birjada birinchi marta ommaga taklif qilish orqali ochiq kompaniyaga aylanish jarayoni.

Yakuniy xulosa

Ushbu kitobning dastlabki ikki bobida biz kibertahdidlarni boshqarishning keng qamrovli dasturi nima sababdan korxonalar uchun juda muhimligini muhokama qildik. Biz korxona tahdid muhitiga tub o'zgarishlarni olib keladigan ijtimoiy, siyosiy, iqtisodiy, madaniy va texnologik o'zgarishlarni, shuningdek, huquqiy qarorlar va me'yoriy muvofiqlik talablarining korxona manfaatdor tomonlari uchun kibertahdidlarni boshqarishni eng muhim vazifaga aylantirishdagi ahamiyati haqida batafsil ma'lumot berdik.

CRMPni shakllantirishda birgalikda ishlaydigan to'rt asosiy tarkibiy qismga e'tibor qarataylik: moslashuvchan boshqaruv, tahdidlar haqidagi ma'lumotlarga asoslangan tizim, tahdidlarni baholashga asoslangan strategiya va uning ijrosi, tahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilinishi. Keyingi to'rt bobda dasturning asosiy tarkibiy qismlari va ularning ishonarli yo'riqnomalar, jumladan, me'yoriy-huquqiy baza, sanoat standartlari va protokollar bilan qanday belgilanganligini batafsil muhokama qilamiz. Shuningdek, har bir asosiy komponentni asoslovchi tamoyillarni batafsilroq bayon qilamiz va korxonangiz uchun mos bo'lgan CRMPni yaratishda e'tiborga olinadigan prinsiplarni taqdim etamiz.

Keyingi bobda har qanday tahdidlarni boshqarish dasturining markazi bo'lgan moslashuvchan boshqaruv dasturini aniqlash, ishlab chiqish va amalga oshirish to'g'risida ma'lumot beriladi.

III BOB. MOSLASHUVCHAN BOSHQARUV

Oldingi bobda, ijtimoiy, siyosiy, iqtisodiy va madaniy o'zgarishlar sabab korxonalar keng qamrovli CRMPga ehtiyoji mavjudligini muhokama qildik. Shuningdek, dasturning to'rt asosiy qismlari haqida tushuncha berildi. Endi, dasturning birinchi tarkibiy qismi va biz CRMPning vakolatli ko'rsatmalariga moslashtirilgan poydevori deya ta'riflagan – *Moslashuvchan boshqaruv* haqida batafsil to'xtalib o'tamiz. Avvalambor, talabga javob beradigan tahdidlarni boshqarish usullari, jumladan, kibertahdidlarni boshqarish usullari mavjud bo'lmasa, nimalar sodir bo'lishi haqida ba'zi hayotiy misollarga to'xtalib o'tamiz. (Keng qamrovli tizim haqida ko'proq ma'lumot uchun ilovaga qarang. Maxsus moslashuvchan boshqaruvni amalda qo'llash haqida ko'proq ma'lumot olish uchun 7-bobga qarang.)

Xalqaro avtotransport vositalarini almashish xizmati (ride-sharing services) kompaniyasi katta miqdordagi ma'lumotlarning tarqalib ketishining oldini olish maqsadida xakerlarga pul to'laydi. Keyin kompaniya bu haqida yolg'on ma'lumotlar beraveradi, sirlar oshkor bo'lganda esa, kompaniya 150 million AQSH dollariga yaqin jarima pulini to'laydi, shu bilan birga kompaniyaning xavfsizlik bo'yicha bosh direktori federal jinoiy javobgarlikka tortiladi. Ijtimoiy tarmoqlarning yangi boshqaruv siyosati keskin o'zgargani, shuningdek, reklama agentlari brenzlari soxta akkauntlar tomonidan ko'p marotaba tahdid ostida qo'yilganligi bois ularning platformani tark etishi ijtimoiy tarmoq xizmatida tartibsizlikni keltirib chiqaradi.

Uber va Twitter – bu ikki yuqori profilli korxonalar batamom bir-biridan farq qiladi. Atigi 10 yil oldin bozorda paydo bo'lgan, biroq tez sur'atlarda o'sib borayotgan avtomobil almashish xizmatlari kompaniyasi bozordagi raqobatga bardosh berishi uchun moslashuvchan, tezkor va ulkan tahdidlarga tayyor bo'lishi kerak edi. Bundan farqli o'laroq, ijtimoiy media platformalari asosan foydalanuvchilar va reklama agentlarining ularning xizmatidan foydalanishga bo'lgan xohishiga tayanadi, beqaror va gavjum bozor sharoitida esa, ijtimoiy media platformalari tahdid va foyda o'rtasidagi muvozanatni topish bilan bog'liq juda ko'plab muammolarga duch keladi. Shunga qaramay, bir-biridan farq qiluvchi bu ikki korxonalarga katta zarar keltirgan inqirozlarning ikkita umumiy jihati mavjud.

Birinchisi, har ikki kompaniyaning muammolari raqamlashtirish jarayoni sababli yuzaga kelib, chuqurlashgan va tezlashgan. Ikkinchidan, tahdidlarni boshqarish dasturining tarkibiy qismlaridan biri bo'lgan – moslashuvchan boshqaruvning to'liq muvaffaqiyatsizlikka uchraganidir.

Tahdidlarni boshqarishning ba'zi sohaları tahdidlarni boshqarish modelini yaratishdan ko'ra ancha murakkabroq va mashaqqatliroq. Biroq bu sohalar kompaniyaning obro'sini, brendini, raqobatbardoshligini va ba'zi holatlarda omon qolishi uchun juda ham muhim. Samarali boshqaruv – korxona ish jarayonini tashkil qilishda muhim omil bo'lib, u jiddiy muammolarni hal qilishda, kelajakda sodir bo'ladigan muammolarning oldini olish va ularni to'g'ri hal qilishda ahamiyatlidir. Bu, shuningdek, korxonada ishlar noto'g'ri ketganda, korxonada qaror qabul qiluvchi shaxslar (direktorlar kengashidan tortib boshqalargacha)ni huquqiy va me'yoriy javobgarlikdan himoya qilishda juda zarurdir.

Korxonalardan tahdidlarning butunlay bartaraf etilishi kutilmaydi. Ta'kidlaganimizdek, har bir korxona muvaffaqiyatga erishish uchun tavakkal qilishi hamda tavakkal bilan mukofotning muvozanatini o'rnatishi lozim. Ammo ulkan va o'sib borayotgan hokimiyat organlari: hokimliklar, sud, tartibga soluvchi organlar, sanoat tashkilotlari va boshqalar korxonalarning tahdidlarni boshqarishning moslashuvchan usulini amaliyotda tatbiq etilishini kutishadi. Boshqaruvning moslashuvchan usuli korxonaning barcha faoliyatida o'z aksini topishi lozim. Bu usul juda zarur bo'lib, tahdid bilan bog'liq muammolar yuz berganda, manfaatdor tomonlarning bu muammolarni tez va samarali boshqarish va tahdid bilan bog'liq qarorlari uchun javobgar bo'lishini ta'minlaydi.

Shunihi muhimki, moslashuvchan boshqaruv usullari biz yuqorida muhokama qilgan Kibertahdidlarni boshqarishning rasmiy dasturini ifodalashi kerak. Haqiqat shundaki, tahdidlarni boshqarish dasturining markazi bo'lgan moslashuvchan boshqaruv mavjud bo'lmasa, korxonalar (yuqorida keltirib o'tilgan ikki misol kabi) tahdid bilan bog'liq qaror qabul qilish jarayonida to'g'ri harakat qila olmaydilar va juda jiddiy muammolarga duch kelishlari ehtimoldan xoli emas.

Mazkur bobda tahdidlarni boshqarishning moslashuvchan usulini batafsil ko'rib chiqamiz: u o'zi nima, nima sababdan muhim, CRMPning asosiy tarkibiy qismi sifatida qanday amalga oshiriladi va boshqariladi.

Moslashuvchan boshqaruv ta'rif

Moslashuvchan boshqaruv atamasining ko'plab ta'riflari mavjud. Quyida keng e'tirof etilgan, taniqli manbalardan olingan ikkita ta'rif berilgan bo'lib, ular bir-biriga va ushbu kitobda bayon etilgan tamoyillarga mos.

Jahon iqtisodiy forumi *moslashuvchan boshqaruvni* quyidagicha ta'riflaydi: "Moslashuvchan, insonga yo'naltirilgan, ko'p tomonlama va barqaror siyosat... foydalanuvchi uchun haqiqiy yoki idrok etilgan qiymatni yaratishga hissa qo'shgan holda o'zgarishlarni tezda amalga oshirishga, o'zgarishlarni faol yoki tezkor ravishda qabul qilishga va o'zgarishlardan o'rganishga doimiy tayyorlik".

Loyihani boshqarish instituti (PMI⁵⁸) Moslashuvchan jamoa boshqaruvini moslashuvchan va tejamkor ish usullarini aks ettiruvchi va qo'llab-quvvatlaydigan epchil yoki tejamkor jamoalarni boshqarish sifatida belgilaydi. Loyihani boshqarish instituti samarali moslashuvchan boshqaruv uchun quyidagi tamoyillarni belgilab bergan:

- Jamoalar bilan hamkorlik qilish ularni qoidalarga bo'ysunishga majburlashdan ko'ra samaraliroqdir.
- Jamoalarga "to'g'ri ish" qilishga imkon berish, hodisadan keyin tekshirish va talablarga rioya etilishini ta'minlashga harakat qilishdan ko'ra samaraliroqdir.
- Doimiy monitoring loyihaning muhim bosqichlardagi tekshiruvlardan ko'ra, ma'lumotning ko'proq o'z vaqtida berilishini ta'minlaydi.

Uber kompaniyasi tomonidan xakerlik hujumining yashirilishi

2014–2016-yillarda xakerlar butun dunyo bo'ylab 57 millionga yaqin Uber kompaniyasi haydovchilari va mijozlarining shaxsiy ma'lumotlarini o'g'irlashgan. Bu, hatto ma'lumotlar xavfsizligining buzilishi tom ma'noda kundalik hodisa bo'lgan dunyoda ham, axborot xavfsizligining hayratomuz xatosidir. Kompaniya bu xatolikni va uning oqibatlarini qay tarzda hal qilganligi korxona madaniyati bilan belgilanadi. Ammo shundan so'ng sodir bo'lgan voqealar, jiddiy, ammo nisbatan oddiy xavfsizlik muammosini ham dahshatli tushga aylantirdi.

Qonunga ko'ra, Uber kompaniyasi ma'lumotlar o'g'irlanganligi to'g'risida zudlik bilan tartibga soluvchi organlar va aksiyadorlarni xabardor qilishi lozim edi. Kompaniyaning ushbu majburiyatlaridan xabardorligi borasida hech qanday shubha yo'q edi: Uber kompaniyasining ma'lumotlar bilan ishlash amaliyoti, AQSH Federal savdo komissiyasi (FTC⁵⁹) bilan muzokaralar va Nyu York shtati tomonidan da'vo mavzusi bo'lib, allaqachon sinchkov tekshiruv ostida edi. Shunga qaramay, kompaniya rahbarlari, jumladan, CSO, sobiq federal prokuror Jozef Sallivan, nafaqat ma'lumotlar o'g'irlanganligi to'g'risidagi dalillarni oshkor qilmagan, balki yillar davomida uni yashirishga uringan. Uber kompaniyasi texnik xodimlari odil sudlovga to'sqinlik qilishda urindi, tergovchilarga kompaniya obro'siga putur yetkazuvchi ma'lumotlarni topishga yo'l qo'ymaslik uchun kamida oltita davlatda o'z serverlarida "favqulodda o'chirish tugmalarini" o'rnatdilar. Kompaniya, "bag baunti" ("bug bounty⁶⁰") dasturi bo'yicha xavfsizlik kamchiliklarini aniqlagan tadqiqotchilarga mukofot uchun mo'ljallangan 100 ming AQSH dollarini xakerlarga sukut saqlashlari uchun to'lab, buni tartibga soluvchi

⁵⁸ PMI (Project Management Institute) – Loyihani boshqarish instituti.

⁵⁹ FTC (Federal Trade Commission) – Federal savdo komissiyasi.

⁶⁰ Bug Bounty (Bag Baunti) – bu ba'zi veb-saytlar va dasturiy ta'minot ishlab chiquvchilari tomonidan taqdim etilgan dastur bo'lib, u orqali odamlar xatolarni, ayniqsa ekspluatatsiya va zaifliklarni topganliklari uchun mukofotlanadi.

organlardan va direktorlar kengashidan yashirgan. Oxir-oqibat, bu ish fosh bo'ldi va Uber uchun oqibatlar shafqatsiz bo'ldi. Shubhasiz, kompaniyaning obro'si va brendi zarar ko'rdi. Umumiy 50 shtat va Kolumbiya okrugining bosh prokurorlari kompaniyani sudga berishdi, natijada kompaniya da'volarni hal qilish uchun 148 million AQSH dollari to'ladi. Zarar shu bilan ham tugamadi. Bosh direktor va boshqaruv a'zosi lavozimidagi kompaniya asoschisi iste'foga chiqishga majbur bo'ldi, xavfsizlik xizmati rahbari ikki og'ir jinoyat bandi bo'yicha ayblanib, qamoq jazosidan zo'rg'a qutulib qoldi. Sallivanning hukmini e'lon qilishda sudya shunday deya ta'kidladi: "Do'stlaringiz, xavfsizlik xizmati rahbarlari bilan sayrga chiqib suhbatlashganingizda, ularga dam olayotganingizni ayting".

O'z-o'zidan savol tug'iladi: Uber kompaniyasida ma'lumotlar o'g'irlanishi kabi dahshatli voqea va uning oqibatlari qanday qilib sodir bo'lishi mumkin? Qanday qilib jiddiy, tajribali, zukko biznes rahbarlari va xavfsizlik mutaxassislari o'z kompaniyalari obro'sini, o'z martabalarini, ehtimol hatto o'z erkinliklarini bunday tahdid ostiga qo'yishlari mumkin? Javoblar ko'p. Bu odamlarni axloqsiz yoki hatto noqonuniy xatti-harakatlardan qochib qutulish mumkin deb o'ylashga olib keluvchi yomon ta'sirga ega korporativ madaniyat bo'lishi mumkin. Ehtimol, bu zaif nazorat masalasi bo'lib, yuqori darajadagi qaror qabul qiluvchilar o'zlaridan quyida nima sodir bo'layotganligini bilishmaydi. Yoki bu biznes ustuvorliklariga muvofiq kelmaydigan xavfsizlikni ta'minlash amaliyotlari bo'lishi mumkin.

Haqiqat shundaki, korxonalar va ularning xodimlari turli yo'llar bilan cheksiz muammoga duch kelishlari mumkin. (Shuningdek, ular turli yo'llar bilan ham muvaffaqiyatga erishishlari mumkin, shuning uchun ular tahdid va foyda o'rta-sida mos va maqbul muvozanatni o'rnatishlari juda muhim.) Muammolar paydo bo'lishining barcha yo'llarini oldindan bilish yoki ularning oqibatlarini butunlay hal etish imkonsizdir. Biroq, korxona uchun bashorat qilinadigan tahdidlarni ham, oldindan aytib bo'lmaydigan tahdidlarni ham samarali hal qilishga imkon beradigan moslashuvchan boshqaruv amaliyotlarini yaratish juda muhimdir. Ushbu amaliyotlar, CRMPning bir qismi sifatida samarali amalga oshirilganda, qarorlar qabul qilishning barcha darajalarida muntazam ravishda xabardor qiladi va yo'naltiradi, ma'lum tahdidlarga chidamlilik bilan ochiq madaniyatni targ'ib qiladi, korxona va uning xodimlarini huquqiy va me'yoriy javobgarlikdan va boshqa salbiy ta'sirlardan himoya qiladi.

Samarali boshqaruv qanday bo'ladi?

Boshqaruv turli shakllarda bo'lishi mumkin, ammo haqiqiy boshqaruvning asosiy maqsadi doimo bir xil bo'ladi: korxonalarni barcha sohalarida va turli darajalarda tahdidlarga asoslangan qaror qabul qilishda yo'l ko'rsatishdan iborat. Bu jarayon eng yuqori darajadagi rahbariyatdan korxona uchun umumiy muhitni belgilash hamda aniq jarayonlar, tizimlar, vazifalar va javobgarlikni o'rnatish orqa-

li amalga oshiriladi. Haqiqiy ma'noda, bu korxona madaniyati masalasi bo'lib, bunda korxona o'zi, xodimlari va boshqa manfaatdor tomonlar uchun standartlar o'rnatadi.

Boshqaruv va *boshqarish* o'rtasidagi farqni izohlasak. Boshqaruv atamasi tashkilotga rahbarlik qilish va uni yo'naltirish uchun o'rnatilgan tizimlar, jarayonlar va tuzilmalarni anglatadi. U qarorlar qanday qabul qilinishini shakllantiradigan qoidalar, qonunlar, vazifalar, mas'uliyat va siyosatlarini, shuningdek boshqaruv organiga berilgan vakolatlarni o'z ichiga oladi. Mohiyatan, boshqaruv korxona faoliyat yuritadigan va qarorlar qabul qiladigan strukturadir.

Boshqarish esa, boshqaruv doirasidagi qarorlar qabul qilish va siyosatni amalga oshirishning haqiqiy hodisasini anglatadi. Bu tashkilotni va tahdidlarni boshqarish uchun mavjud tizimlar va tuzilmalardan foydalanish jarayonidir. Boshqarish tahdid bilan shug'ullanadigan tashkilotning byudjeti va boshqa resurslarini belgilashni, o'z oldiga maqsad va vazifalarni qo'yishni, shuningdek, korxonaning belgilangan siyosat va tartiblarni amalga oshirishini ta'minlashni o'z ichiga oladi.

Ommaviy axborot vositalarida deyarli har kuni muvaffaqiyatsiz boshqaruvga misollar keltiriladi, ushbu bobda boshqaruvni noto'g'ri yo'lga qo'ygan va o'zlarining muvaffaqiyatsizliklari tufayli jiddiy oqibatlarga duch kelgan korxonalarga e'tibor qaratishimiz muqarrar. Ammo shuni ta'kidlash joizki, shunday kompaniyalar ham borki, ular tahdidni boshqarishning ushbu muhim sohasi haqida to'g'ri tushunchaga egadirlar. Bu shuni anglatadiki, ular jiddiy muammolarni hal qilish imkonini beradigan tahdidlarni boshqarish bo'yicha muvofiq amaliyotga ega va bu korxonani, uning qaror qabul qiluvchilarini va korxonaning barcha manfaatdor tomonlarni himoya qilish imkonini beradi.

1982-yilgi Taylenol dorisi bilan zaharlanish holati ushbu sohada oltin standart bo'lib qolmoqda. (Oltin standartga 40 yildan oshiq vaqt bo'lganligi korxonalarning boshqarish amaliyoti qanchalik yomon va ular qanchalik kam darajada takomillashtirilganligini ko'rsatadi.) Chikago shtati hududida yetti kishi qasddan soxtalashtirilgan Taylenol belgisi ostidagi preparat tarkibidagi atsetaminofenni qabul qilish natijasida vafot etdi, va bu jinoyat ortidan xuddi shunga o'xshash jinoyatlar ketma-ket sodir bo'ldi. Butun dunyoda Taylenol va uning ishlab chiqaruvchisi Johnson & Johnson kompaniyasining boshqa retsepsiz beriladigan dori vositalarining xavfsizligi haqida vahima va qo'rquv hukmron edi.

Agar kompaniya bu holat bo'yicha namunali yo'l tutmaganida, uning inqirozga uchrashi muqarrar edi. Kompaniya butun dunyo bo'ylab Taylenol preparatlarini darhol qaytarib olib, ishlab chiqarish muassasalarini tergovchilarga ochib, ruxsatsiz ochilishdan himoyalangan va pechatlangan qadoqlarni yaratdi, eng muhimi, tergovchilar, tartibga soluvchi organlar va jamoatchilik bilan to'la shaffof munosabatda bo'ldi. Ushbu chinakam tezkor javob reaksiyasi natijasida Jonson &

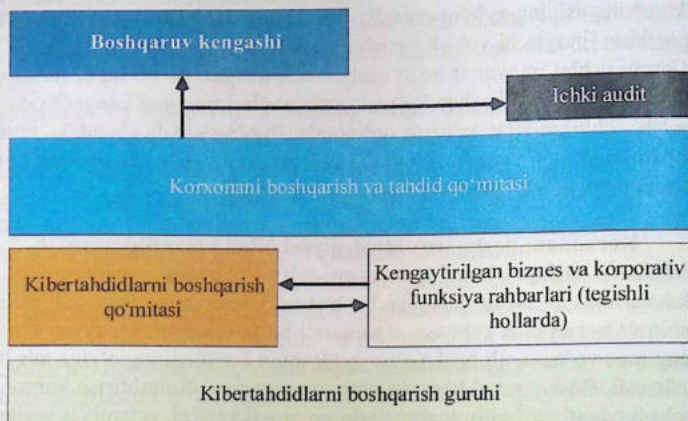
Jonson kompaniyasining aybdor emasligi va zaharlanishlar kompaniyaga aloqasi bo'lmagan bitta jinoyatchi yoki bir necha jinoyatchilarning ishi ekanligi ma'lum bo'ldi. Garchi ushbu jinoyatlar hech qachon ochilmagan bo'lsa ham, Johnson & Johnsonning Taylenol va boshqa ko'plab mahsulotlari bugungi kungacha dunyodagi eng ishonchli brendlar qatorida qolmoqda. Buning sababi shundaki, kompaniya jamoatchilikning ishonchiga loyiqligini aniq ko'rsatdi va buni sifatli korporativ madaniyatni namoyish etish orqali amalga oshirdi.

Korxonani boshqaruv strategiyasi bilan muvofiqlashtirish

Tahdidlarni boshqarishning qanday modeli yoki qanday yondashuv qo'llanilishidan qat'i nazar, moslashuvchan boshqaruv korxonaning maqsadli madaniyatiga aniq va aynan mos kelmasa, u samarali bo'la olmaydi. Muayyan korxona uchun eng mos va samarali boshqaruv yondashuvi korxonaning o'ziga xos holatiga asoslanadi. Boshqaruvni korxona ehtiyojlariga muvofiqlashtirish korxona va uning sohasi tabiati, tashkiliy tuzilmalarining murakkabligi, u faoliyat yuritayotgan tartibga solish muhiti va brend obro'sining ahamiyati kabi masalalarni aniq baholashni talab qiladi.

Korxonaning o'ziga xos holatini bunday baholash natijasida favqulodda holatlarda xavfsizlikni samarali nazorat qilish imkonini beruvchi operatsion tizim yaratiladi. Bu, aslida, madaniy baholash bo'lib, u korxona haqida umumiy tasavvurga ega bo'lish imkonini beradi: korxona qanday faoliyat ko'rsatadi, kimlar qanday qaror qabul qiladi, bu qarorlar nimaga asoslanadi va qarorlar uchun kim javobgar bo'ladi. Bu esa turli vaziyatlarda turlicha yondashuvlarni anglatadi. Misol uchun, asosan boshqaruvda improvizatsiya uslubiga ega bo'lgan tez rivojlanayotgan korxonalar (texnologik startap singari), tez qarorlar qabul qilish uchun kichikroq va moslashuvchan operatsion tuzimga muhtoj bo'lishi mumkin. Boshqa tomondan esa, uzoq vaqt davomida faoliyat yuritayotgan, rivojlangan hamda qattiq nazorat qilinadigan korxonalar o'zining ko'plab manfaatdor tomonlari bilan mustahkamlangan ishonchni buzmaslik uchun yaxshiroq o'rganib ishlab chiqilgan qarorlar qabul qilishi kerak.

Xo'sh, korxona tahdidlarini boshqarish strategiyasini muvofiqlashtirish yoki yaratish qayerdan boshlanadi? Boshqaruv yuqoridan boshlanadi (3.1-chizmaga qarang). Buning mohiyati shundaki, korxonaning eng yuqori darajadagi rahbariyati: direktorlar kengashi, bosh direktor va barcha rahbariyat boshqaruv jarayoniga jiddiy munosabatda bo'lishlari lozim. Ular majburiyatlarni aniq va ishonarli tarzda, butun tashkiliy tuzilma bo'ylab yetkazishlari zarur. Rahbariyatning faol ishtiroki korxonaning boshqaruv strategiyasi va uni amalga qo'llash uchun umumiy muhitni belgilaydi. Bu tegishli odamlar to'g'ri sabablarga ko'ra tegishli majburiyatlarni o'z bo'ynilariga olishlarini ta'minlaydi. Shuningdek, bu boshqaruv strategiyasini amalga oshirish uchun zarur resurslar: odamlar, jarayonlar va texnologiyalar bilan ta'minlashni kafolatlaydi.



3.1-chizma. Kibertahdidlarni boshqarishning tasviriy modeli

Bu yuqori darajadagi qarorlar bo'lib, ular xavfsizlik tashkiloti doirasida va undan tashqarida qabul qilinishi kerak. Qaror qabul qiluvchi yuqori lavozimli mansabdor shaxslar qarorlar uchun mas'ul va javobgar bo'lishi kerak, ammo xavfsizlik hali ham hal qiluvchi rol o'ynaydi. Eng yaqqol misolni ko'rib chiqadigan bo'lsak, xavfsizlik tashkiloti tahdid muhiti haqida teran tushunchaga ega va o'zining qarorlarini asoslash uchun ushbu tushunchani boshqaruv organiga yetkazishi mumkin. Shuningdek xavfsizlik xizmati ham o'zining atrof-muhit tahdidi haqidagi bilimlaridan foydalanib, boshqaruvning korxona uchun zarurligi haqidagi muhim xabarni yetkazishi mumkin.

Moslashuvchan boshqaruvni tatbiq etish uchun, tahdidlar to'g'risida qaror qabul qiluvchi shaxslar o'zlarining dasturlari korxonaning talablari va imkoniyatlariga mos kelishiga ishonch hosil qilishlari kerak. Bu jarayonga yordam berish uchun biz 2-bobda tavsiflangan CRMP tamoyillarini ishlab chiqdik, unda ishonchli ko'rsatmalarga asoslangan muhim asosiy tamoyillar va amaliyotlar to'plamlariga oydinlik kiritilgan. Ushbu prinsip dasturni ishga tushirish va kibertahdid strategiyalari va amaliyotlarini rivojlantirish uchun qo'llanma bo'lib xizmat qiladi. Prinsiplar tezkor, moslashuvchan va o'zgaruvchan bo'lishi kerak. Keng qamrovli prinsipning o'zi haqida batafsilroq ma'lumot uchun IIlovaga, moslashuvchan boshqaruv tamoyillari haqida ma'lumot olish uchun 3.1-jadvalga qarang.

CRMP tamoyillari – Moslashuvchan boshqaruv

CRMP tarkibiy qismlari	Tamoyillar	Ma'lumot manbalari
Moslashuvchan boshqaruv	75-betda "Moslashuvchan boshqaruvning yetti tamoyili"ga qarang	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACD⁶¹ning direktorlar qo'llanmasi • ISO 27001:2022 • NIST 8286 • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • ISO 31000:2018 • AICPAning CRMP
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	94-betda "Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	120-betda "Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	151-betda "Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • AICPAning CRMP

Moslashuvchan boshqaruv tizimi juda muhim bo'lib, uni loyihalash, yaratish va korxonangizga mos kelishiga ishonch hosil qilish oson ish emas. Boshqaruv prinsipi oldindan bashorat qilingan tahdidlarga qarshi turishi uchun yetarlicha keng qamrovli bo'lishi kerak, ammo haddan tashqari murakkablik boshqaruvni qiyinlashtiradi va odamlarni uni chetlab o'tish yo'llarini izlashga undaydi.

Boshqaruv tizimini ishlab chiqishda bir xil yondashuv hammaga ham mos kelavermaydi. Masalan, kuchli nazorat sohasida faoliyat ko'rsatadigan korxona muvofiqlik talablariga, shuningdek, sheriklar va mijozlar kabi uchinchi tomon-

⁶¹ NACD (National Association of Corporate Directors) – Korxona rahbarlari milliy uyushmasi.

larning talablariga javob berish uchun aniqroq belgilangan standartlarga muhtoj bo'ladi. Amaliyotda, bu shuni anglatadiki, transmilliy investitsiya banki texnologik startapga qaraganda butunlay boshqa standartlar to'plamiga ega bo'lishi kerak, shuningdek, texnologik startapga ham mashhur AT kompaniyasiga qaraganda, garchi har ikkala kompaniya bir xil sohada ishlasa-da, butunlay boshqa standartlar to'plami kerak bo'ladi.

Moslashuvchan boshqaruvning yetti tamoyili

Korxonaning talablari qanday bo'lishidan qat'i nazar, uning moslashuvchan boshqaruv tizimi va amaliyoti quyida ko'rsatilgan yetti asosiy tamoyilga amal qilishi kerak:

1-TAMOYIL: SIYOSAT VA JARAYONLARNI JORIY ETISH

CRMPni yaratish uchun butun korxona miqyosida siyosat va jarayonlar joriy etilishi kerak.

Tahdidlarni yoki boshqa narsalarni boshqarishga qaratilgan korxona siyosati, agar aniq belgilanmagan, rasmiylashtirilmagan va bu haqda bilishi kerak bo'lgan tegishli shaxslarga ma'lum qilinmagan bo'lsa, u hech qachon samarali bo'la olmaydi. Boshqaruv guruhi va uning ijrochi homiylari ushbu kitobda batafsil tavsiflangan CRMP ko'rinishida kibertahdidni rasmiy boshqarish uchun zarur siyosat va tartib-taomillarni yaratishni ta'minlashlari kerak.

Ushbu jarayonda muhim qadam – bu boshqaruv organi tomonidan korxona nima qilishni rejalashtirayotgani, uning sababi va buning korxonadagi manfaatdor tomonlarga qanday ta'sir qilishini belgilab beruvchi keng qamrovli siyosat bayonotini chiqarishi hisoblanadi. Bu boshqaruv sa'y-harakatlarining muhimligi va korxona tomonidan ularga bo'lgan munosabatning jiddiyligini ko'rsatadi.

Boshqaruv siyosati bayonoti, biznes aloqalarining har qanday shakli kabi, korxona madaniyatiga muvofiq kelishi kerak. U keraksiz yuridik, texnik yoki biznes jargonlarisiz aniq va barcha ishtirokchilar uchun tushunarli bo'lgan tilda taqdim etilishi lozim. Shuningdek, u siyosatning maqsadlarini, kutilayotgan natijalarini va biznes aloqalariga ta'sirini muhokama qilishi kerak. Eng muhimi, u javobgarlikni o'rnatishi va manfaatdor tomonlardan nima kutilayotganini aniq ifodalashi kerak. U tahdid shaffofligining asosiy tamoyillarini va nima uchun ular juda muhimligini tushuntirishi kerak. Barcha darajadagi korxona xodimlari korxonaning tahdidga moyillik darajasini va unga rioya qilish muhimligini tushunishlari zarur. Bu potensial tahdidlarni aniqlab, ularni e'tiborsiz qoldirmasdan yoki yashirmasdan tegishli shaxs yoki bo'limga yetkazishni anglatadi.

Har qanday korxonani boshqarish amaliyoti uning talablari va imkoniyatlariga muvofiq bo'lishi kerak.

Korxonalarga ushbu sa'y-harakatlarda yordam berish uchun keng turdagi sanoat standartlari mavjud, jumladan:

NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi (NIST CSF 2.0 GV.PO-01, 02)

NIST kibertahdidlarni boshqarish va dasturni belgilashda siyosat, jarayonlar va tartib-taomillarning muhimligini tan oladi. Ularga ega bo'lgan holda, tashkilot kibertahdidini strategik boshqarishda tizimli va izchil yondashuvni ta'minlashi mumkin (bu kiberxavflarni boshqarish dasturidir).

ISO/IEC 27001:2022 5.2

ISO 5.2 bandda yuqori rahbariyat tashkilotning biznes va tahdid sharoitlariga mos keladigan axborot xavfsizligi siyosatini o'rnatishi kerakligini ta'kidlaydi.

ISO 31000: 2018 6.1

ISONing ushbu yo'riqnomasi tahdidlarni boshqarish jarayonini tavsiflab, tahdidlarni yetkazish va maslahat berish, aloqa o'rnatish, shuningdek baholash, qayta ishlash, monitoring qilish, tahlil qilish, ro'yxatga olish va hisobot berish bo'yicha siyosat, tartib va amaliyotlarni tizimli ravishda qo'llashni o'z ichiga oladi.

2018-yilgi SEC komissiyasining bayonoti va jamoatchilik kompaniyalari uchun kiberxavfsizlik ma'lumotlarini oshkor qilish bo'yicha ko'rsatmalari

"Biz, kompaniyaning CRMP va direktorlar kengashi kiberxavfsizlik masalalari bo'yicha rahbarlik bilan qanday hamkorlik qilishi to'g'risidagi ma'lumotlarning oshkor qilinishi investorlarga direktorlar kengashi ushbu tobora muhimlashib borayotgan sohada tahdidlarni nazorat qilish bo'yicha o'z majburiyatlarini qay darajada bajarayotganligini baholash imkonini beradi, deb hisoblaymiz".

"Favqulodda vaziyatlarda kiberxavfsizlikni boshqarish siyosati va tartib-taomillari butun korxona miqyosida, shu jumladan qimmatli qog'ozlar bozori federal qonunlariga rioya qilish bo'yicha tahdidlarni boshqarishning asosiy elementlari hisoblanadi".

2-TAMOYIL: "UCH CHIZIQLI HIMOYA MODELII" DOIRASIDA BOSHQARUV, VAZIFALAR VA MAJBURIYATLARNI O'RNATISH

"Uch chiziqli himoya modeli" doirasida CRMP aniq belgilangan vazifalar, majburiyatlar va natijalar bilan o'rnatilishi kerak.

Boshqaruv mustaqil yoki yakka holda amalga oshirilmaydi. Yuqorida ta'kidlab o'tganimizdek, tahdidlarni samarali boshqarish uchun rasmiy dastur muhim ahamiyatga ega va har qanday korxonaning boshqaruv amaliyoti bunday dasturning bir qismi bo'lishi kerak. Biroq boshqaruv amaliyoti barcha korxonalar uchun bir xil bo'lmaydi. Butun dunyo bo'ylab faoliyat yuritadigan ishlab chiqaruvchi tashkilotga keng ko'lamli rasmiy boshqaruv organi kerak bo'ladi, yuqori menejment vakillari va boshqa yuqori darajadagi rahbarlardan iborat bunday rasmiy

boshqaruv organi muntazam ravishda yig'ilishlar o'tkazadi va direktorlar kengashi oldida qat'iy hisobot talablarini qo'yadi. Bundan farqli o'laroq, kichik texnologik startaplar shunchaki kichik bir guruh tashkil etib, ularga tahdidlar bilan bog'liq mas'uliyatlarni hamda boshqaruv standartlari va amaliyotlarini o'rnatish va amalga oshirish hamda yuzaga kelishi mumkin bo'lgan muammolarni tegishli tarzda yetkazish vazifalarini yuklashni yetarli deb topishi mumkin. Ko'pgina korxonalar ushbu ikki qarama-qarshilik orasidagi yondashuvni, muntazam ravishda yoki vaqti-vaqti bilan uchrashadigan va muammolar yoki tashvishlar bo'yicha yuqori rahbariyatga maslahat beradigan qo'mita bilan ishlashni tanlaydilar.

Korxona boshqaruv uchun qanday yondashuvni tanlamasin, u kutilayotgan natijalarni (ya'ni tahdid natijalarini), boshqaruv vazifalari hamda majburiyatini aniq belgilashi va ma'lum qilishi kerak. Natijalar, vazifalar va majburiyatlarni belgilashda juda foydali va keng qo'llaniladigan yondashuvlardan biri Ichki auditorlar instituti (IIA)ning Uch chiziqli himoya modelidir.

Tahdidlarni boshqarish dasturini loyihalashda foydali asoslardan biri – bu butun dunyo bo'ylab korporativ auditorlar uchun standartlar va sertifikatlashni o'rnatuvchi professional uyushma bo'lgan IIA'dir (3.2-rasmga qarang). IIAning Uch chiziqli himoya modeli (asl "Uch chiziqli himoya"ning yangilanishi) nafaqat auditorlar uchun, balki turli turdagi va hajmdagi korxonalar uchun keng qo'llanilishi mumkin. Sodda qilib aytganda, ushbu tizim tahdidlarni boshqarishning turli jihatlari uchun javob beradigan uch turdagi vazifalarni o'z ichiga oladi:

Birinchii chiziq.

Birinchisi, boshqaruv xodimlari bo'lib, ular korxona o'zining tashkiliy maqsadlariga erishishini ta'minlash, shu jumladan mijozlarga mahsulot va xizmatlar ko'rsatish va tahdidlarni boshqarish bo'yicha belgilangan maqsadlarga erishish uchun mas'uldirlar.

Ikkinchi chiziq.

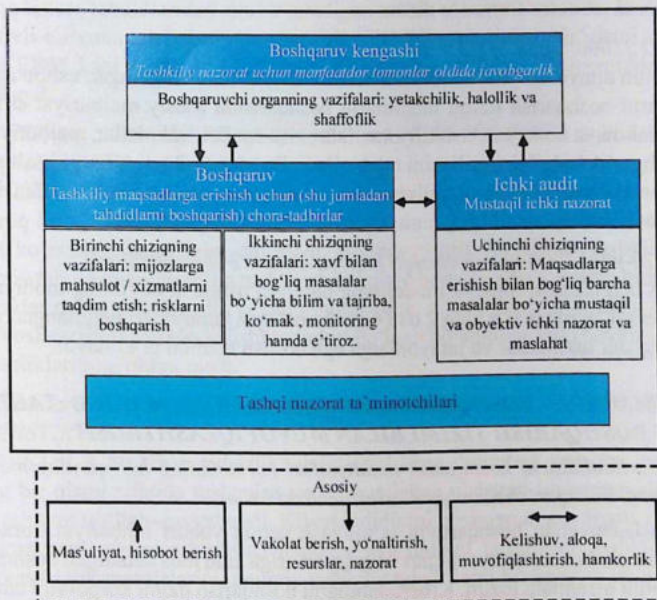
Ikkinchi chiziq tahdidlarni boshqarish bo'yicha tajribaga ega bo'lgan mutaxassislardan iborat bo'lib, ular birinchi chiziqdagilarning amaliyotlarini kuza-tib boradilar, yo'l-yo'riq va yordam taklif qiladilar va eng muhimi, korxonaning tahdidlarni boshqarish standartlariga javob bera olmaydigan amaliyotlarga e'tiroz bildiradilar.

Uchinchi chiziq.

Bu ichki audit tashkiloti bo'lib, u korxona maqsadlariga erishish bilan bog'liq barcha masalalar, shu jumladan, tahdidlar bo'yicha mustaqil va obyektiv ko'mak va ichki nazoratni ta'minlaydi.

Shuni ta'kidlash joizki, faqat uchinchi chiziq mustaqil tarzda faoliyat ko'rsatadi. Birinchi va ikkinchi chiziqlar tahdidlarni boshqarish tizimini yaratish uchun birgalikda hamkorlik qiladi, ikkinchi chiziq doimiy ravishda birinchi chiziqning

tahdidlar bilan bog‘liq natijasini nazorat qilib, ularni tahlil qiladi, uchinchi chiziq esa mustaqil auditni ta‘minlaydi. Uch chiziqlarning barchasi vakolatlarni topshirish, javobgarlikni o‘rnatish va halollikni ta‘minlash uchun mas‘ul bo‘lgan boshqaruv organi nomidan boshqariladi. Ichki audit, shuningdek, qo‘shimcha nazoratni ta‘minlaydigan tashqi provayderlar, ya‘ni tashqi mustaqil auditorlar yoki maslahatchilar tomonidan to‘ldirilishi mumkin.



3.2-chizma. IIAning Uch chiziqli himoya modeli

Ushbu tamoyil bilan bog‘liq bo‘lgan yo‘l-yo‘riqlar va istiqbollarni taqdim etadigan ba‘zi maxsus vakolatlarga e‘tibor qaratsak:

2023-yilgi SEC yo‘riqnomasining S-K106(c) bandi – Boshqaruv va 20-F shakl⁶²

Ushbu bandda kibertahdidlarni boshqarish bo‘yicha ko‘p qatlamli yondashuvga urg‘u beriladi. SEC kiberxavfsizlikni yuqori darajada (boshqaruv) va operativ darajada (rahbariyat) nazorat qilishning muhimligini ta‘kidlab, boshqaruv-

⁶² 2023 SEC Regulation S-K Item 106(c)–Governance and Form 20-F – 2023-yilgi SEC yo‘riqnomasining S-K106(c) bandi – Boshqaruv va shakl 20-F.

ning mustahkam bo'lishi kerakligini, shuningdek, aniq belgilangan vazifalar va majburiyatlar tashkilotning turli darajalariga yetib borishi kerakligini e'tirof etadi.

*NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi 2.0 GV.RR-01-04*⁶³

NISTning kiberxavfsizlik asoslari loyihasi butun ishchi kuchi uchun kiberxavfsizlik vazifalari va mas'uliyatlarini belgilashni va bu vazifa va mas'uliyatlar barcha manfaatdor tomonlar bilan moslashtirilishi va muvofiqlashtirilishini talab qiladi.

*ISO 31000: 2018 5.2, 5.4.3*⁶⁴

Butun dunyo bo'ylab sanoat korxonalari tomonidan tan olingan ushbu asosiy tahdidlarni boshqarish tizimi tahdidlarni boshqarishni asosiy majburiyat sifatida tan olinishini va muayyan tashkiliy vazifalar, risk egalari, vakolatlar, majburiyatlar va javobgarlik belgilab berilishini talab qiladi. Bundan tashqari, yuqori boshqaruv va nazorat organlari ushbu omillarni korxonaning barcha darajalariga yetkazishni ta'minlashi kerak.

*2020-yilgi II Aning uch chiziqli himoya modeli 2-4-tamoyillari*⁶⁵

IIA uch chiziqli himoya modelining barchasi ushbu tamoyilning mohiyatiga urg'u beradi, ayniqsa IIA ning 2 dan 4 gacha bo'lgan tamoyillari belgilangan vazifalar, tegishli tuzilmalar va jarayonlarga ega bo'lish talabini ta'kidlaydi.

3-TAMOYIL: BOSHQARUV AMALIYOTLARINI MAVJUD TAHDIDLARNI BOSHQARISH TIZIMI BILAN MUVOFIQLASHTIRISH

Kibertahdidlarni boshqarish amaliyotlari korxonaning har qanday mavjud tahdidlarni boshqarish tizimiga moslashtirilishi lozim.

Moslashuvchan boshqaruvni ta'minlash uchun yuqori rahbariyat korxonaning strategik biznes ustuvorliklari va maqsadlariga aniq mos keladigan boshqaruv amaliyotini o'rnatishi lozim. Kibertahdidlarni boshqarish tizimi korporativ tahdidlarni boshqarish, ta'minot zanjiri, uchinchi tomon va AT/OT tahdidlarini boshqarish tizimlari kabi korxonada mavjud bo'lishi mumkin bo'lgan boshqa har qanday tahdidlarni boshqarish tizimlari bilan mos kelishi kerak. Bunday muvofiqlashtirish muhim ahamiyatga ega, chunki u o'xshash tahdid klassifikatsiyasi singiri, o'xshash tahdid vositalaridan foydalangan holda tahdidlarni muvofiqlashtirish va tahdidlar haqida ma'lumot berishni yaxshilashga imkon beradi. Albatta, barcha korxonalarda ham tahdidlarni boshqarish dasturlari mavjud emas, agar CRMP

⁶³ 2023 Draft NIST CSF 2.0 GV.RR-01-04 – Standartlar va texnologiyalar milliy institutining 2023-yilgi kiberxavfsizlik asoslari loyihasi.

⁶⁴ ISO (International Organization for Standardization) 31000: 2018 5.2, 5.4.3 – Xalqaro standartlashtirish tashkilotining ushbu hujjati tashkilotlar duch keladigan tahdidlarni boshqarish bo'yicha ko'rsatmalar beradi.

⁶⁵ 2020 IIA Three Lines Model Principle 2-4 – 2020-yilgi Ichki auditorlar institutining uch chiziqli himoya modeli 2-4-tamoyillari.

mavjud bo'lsa, u har qanday tahdid funksiyalari va komponentlari bilan to'liq mos kelishi kerak. Ko'plab standartlar va bayonnomalar ushbu tamoyilning muhimligini ta'kidlaydi va qo'shimcha ko'rsatmalar beradi, shu jumladan:

2023-yilgi NACDning kibertahdidlarni nazorat qilish tamoyillari to'g'risidagi direktorlar qo'llanmasi 1,4⁶⁶

NACD kibertahdidlarni boshqarishning muhimligini nafaqat o'ziga xos va boshqa biznes tahdidlaridan ajralib turadigan texnik muammo sifatida, balki keng qamrovli korxona tahdidlarini boshqarish (ERM⁶⁷) dasturining bir qismi sifatida (ya'ni ERM kabi mavjud tahdid tizimlari bilan muvofiqlashtirish) muhimligini ta'kidlaydi.

NISTning 2023-yilgi kiberxavfsizlik asoslari 2.0 GV. RM-03 loyihasi (2023 Draft NIST CSF⁶⁸ 2.0 GV. RM-03)

NIST kibertahdidlarni boshqarish alohida amalga oshirilmasdan, balki kengroq bo'lgan korxona tahdidlarini boshqarishning ajralmas qismi sifatida faoliyat ko'rsatishi kerakligini tan oladi. Bunday yaxlit yondashuv tashkilotning umumiy tahdid muhitini to'liq tushunishga imkon beradi va bu o'z navbatida asosli qarorlar qabul qilishga olib keladi. Shuningdek, u izchillikni ta'minlab, tahdidlarni boshqarishda yuzaga kelishi mumkin bo'lgan bo'shliqlar yoki bir-biriga mos kelmasliklarining oldini oladi.

Standartlar va texnologiyalar milliy instituti idoralararo yoki ichki hisobotlari (NISTIR⁶⁹) 8286

NISTIR 8286 kiberxavfsizlik tahdidlarini keng doiradagi korxona tahdidlarining bir qismi sifatida tushunish va boshqarishga nisbatan integratsiyalashgan yondashuvni qo'llab-quvvatlaydi. Kibertahdidlarni boshqarish amaliyoti va mavjud korporativ tizimlar o'rtasida uzluksiz uyg'unlikni ta'minlash tashkilotlarga kiberxavfsizlik masalalarini umumiy tashkiliy tahdidlarni boshqarish jarayonlariga kiritadigan uyg'unlashtirilgan, yaxshi muvofiqlashtirilgan tushuncha va strategiyani yaratishini ta'minlaydi va shu bilan korxonaning barqarorligi va xavfsizlik holatini oshiradi.

Biz so'z yuritayotgan muvofiqlashtirish, asosan, kibertahdidlarni boshqarish bo'yicha boshqaruv amaliyotlari allaqachon mavjud bo'lgan har qanday tahdid amaliyoti yoki boshqaruv modeli bilan to'g'ri ishlashini ta'minlash masalasidir. Korxonaning kiberboshqaruv amaliyoti hech qachon o'zicha mavjud

⁶⁶ 2023 NACD Director's Handbook on Cyber-Risk Oversight Principles 1, 4 – 2023-yilgi Korxona direktorlari milliy uyushmasining kibertahdidlarni nazorat qilish tamoyillari to'g'risidagi direktorlar qo'llanmasi.

⁶⁷ ERM (enterprise risk management) – Korxona tahdidlarini boshqarish.

⁶⁸ NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) – Standartlar va texnologiyalar milliy instituti kiberxavfsizlik asoslari.

⁶⁹ NISTIR (National Institute of Standards and Technology Interagency or Internal Reports) – Standartlar va texnologiyalar milliy instituti idoralararo yoki ichki hisobotlari.

bo'lasligi lozim. Masalan, agar korxona boshqaruv kengashi audit qo'mitasi-ga hisobot beradigan ERM dasturiga ega bo'lsa, kiberxavfsizlikni boshqarish amaliyoti ushbu yuqori darajadagi boshqaruv tuzilmalariga mos kelishi va ulardan foydalanlik to'g'risida hisobot berishi zarur. Bu biznes va boshqaruv organiga tahdidlarni, tahdidlarning ehtimoli/ta'sir ko'lamini, korxona tahdidlari reyestrtdagi hisobotlarni va boshqa omillarni umumiy tushunish asosida qaror qabul qilish imkonini beradi.

NIST standartlari CRMP va ERM dasturi birgalikda qanday ishlashi kerakligini ta'riflash uchun yaratilgan. Asosiy omillardan biri shundaki: ikki dastur doirasida tahdidlarni baholash natijalari format va ma'lum atamalarni tushunish jihatidan o'zaro o'xshash bo'lishi kerak. Sodda qilib aytganda, "jiddiy tahdid" singari tushunchalar har ikkala dastur uchun ham bir xil ma'noni anglatishi lozim. (Bularning barchasi 8-bobda muhokama qilinadigan umumiy operatsion barqarorlikning [OpRes] funksiyasidir.)

4-TAMOYIL: DIREKTORLAR KENGASHI VA RAHBARIYAT QAMROV DOIRASINI BELGILAYDI

Korxonada kibertahdidlarga qarshi kurash amaliyotlarining qamrov doirasi direktorlar kengashi va yuqori rahbariyat tomonidan belgilanishi va tasdiqlanishi lozim.

Korxona tomonidan qamrab olinishi kerak bo'lgan tahdid sohalari biz allaqachon muhokama qilib o'tgan ko'plab omillarga (shu jumladan sanoat, geografiya va tartibga soluvchi muhit) qarab farq qilinishi mumkin. Ba'zilar uchun faqat AT va boshqa raqamli aktivlar (jumladan, operatsion aktivlar) bilan bog'liq tahdidlarni hal qilish yetarli bo'ladi. Boshqalar esa xavfsizlikning boshqa funksiyalari, jismoniy tahdidlar, firibgarlik, biznesning uzluksizligini boshqarish va favqulodda vaziyatlar oqibatlarini bartaraf etish va boshqalar bilan bog'liq tahdid amaliyotlarini amalga oshirishlari kerak bo'ladi.

Qamrov doirasi degani, aslida nima himoya qilinishi kerak va nima himoya qilinishi kerak emasligini anglatadi. Samarali va moslashuvchan boshqaruvda tahdidlarni boshqarish amaliyotlarining qamrov doirasi eng yuqori darajada aniqlanishi kerak va ushbu ko'lam doirasida muayyan tahdidlar bilan bog'liq qarorlar tahdidlarni boshqarishga mas'ul shaxs tomonidan qabul qilinishi juda muhimdir, bu mas'ul shaxs tahdidga oid qarorlar ta'sir qiladigan aktivlar uchun javobgardir.

Ushbu muammoni hal qiluvchi bir nechta prinsiplar va standartlar quyidagilardan iborat:

2023-yilgi NIST kiberxavfsizlik asoslari 2.0 GV.OC-01, GV.RR-01 loyihasi

Ushbu loyihaning "Tashkiliy muhit" bo'limida aynan rahbarlar tashkiliy vazifa haqida har tomonlama tushunchaga ega ekanligi ta'kidlanadi. Ular kiber-

tahdidlarni ustuvor qo'yish uchun tashkilotning vazifasi va biznes muhitiga mos keladigan tahdidlarni boshqarish amaliyotlarini qo'llash doirasini juda yaxshi ta'riflay oladi. "Vazifalar va majburiyatlar" bo'limida esa, rahbariyat tayinlanishi lozimligi hamda ular kibertahdidlar bilan bog'liq qarorlar uchun mas'uliyatni o'z zimmasiga olishi va tahdidlardan xabardorlik madaniyatini yaratishi kerakligi ta'kidlanadi. Tahdidlarni boshqarish bo'yicha qarorlarga javobgarlikni o'z zimmasiga olar ekan, rahbarlar nafaqat belgilangan qamrov doirasini tasdiqlaydilar, balki butun tashkilotda tahdidlardan xabardorlik madaniyatini joriy etishni qo'llab-quvvatlaydilar.

ISO 31000:2018 5.2

Ushbu standartga ko'ra, yuqori rahbariyat va ba'zi hollarda nazorat organlari tahdidlarni boshqarishning barcha korxona faoliyatiga integratsiyalashuvini ta'minlashi kerakligi va ular ushbu faoliyatga yetakchilik qilishi va majburiyatlarini namoyon etishi kerakligi ta'kidlanadi.

Buning ma'nosi shundaki, korxonaning boshqaruv tuzilmasida nimalar himoya qilinishi kerakligi eng yuqori darajalarda belgilanishi va tasdiqlanishi kerak. Masalan, CISO operatsion tizimlar uning xizmat vazifasiga kirmaydi deb o'ylashi va shu sababli bu sohadagi tahdidlar uchun javobgarlikni o'z zimmasiga olishdan bosh tortishi mumkin. Bu asosli positsiyasi bo'lishi mumkin va tahdidlar bo'yicha qarorlar CISO tomonidan emas, balki korxona boshqaruv organi yoki shunga o'xshash organ tomonidan qabul qilinishi kerak.

Qamrov doirasi va vazifalar aniqlangandan, tasdiqlanib, ma'lum qilingandan so'ng, aksariyat hollarda aniq taktik choralar ko'rish bo'yicha qarorlarni tahdidlar bo'yicha qaror chiqaruvchilar, ya'ni aktivni himoya qilish uchun mas'ul bo'lgan shaxslar qabul qilishi kerak. Masalan, Microsoft Teams ilovasi bilan bog'liq xavfsizlik muammolari yuz berganda, muhandislar yoki ma'muriy bo'lim menejrlari bilan maslahatlashish talab qilinmaydi.

5-TAMOYIL: DIREKTORLAR KENGASHI VA YUQORI BO'G'IN RAHBARLARI NAZORATNI AMALGA OSHIRADILAR

Direktorlar kengashi va yuqori darajadagi rahbarlar korxonaning kibertahdidlar bilan kurashida tegishli nazoratni ta'minlashi zarur.

Nazorat va javobgarlik har qanday tahdidlarni boshqarish dasturining muvaffaqiyati uchun juda muhim hisoblanadi va bu asosan boshqaruv amaliyotiga taalluqlidir. Nazorat va javobgarlik korxonaning eng yuqori darajalarida, hech bo'lmaganda yuqori bo'g'in rahbarlarida, direktorlar kengashida amalga oshirishi kerak. Buning sababi oddiy: aynan ular tahdidlarni boshqarish amaliyotlarini nazorat qilish bo'yicha huquqiy va normativ javobgarlikka mas'ul bo'lib, ular aksiyadorlar va iste'molchilarni himoya qiluvchi guruhlar hamda sudlar tomonidan javobgarlikka tortiladilar. 2-bobda keltirilgan sud qarorlaridan shu ayonki, tah-

ISOning mazkur standarti tahdidlarni boshqarish tizimi samaradorligini davriy baholashni va uning tashkilot maqsadlariga erishish uchun hali ham mos ekanligini aniqlashni talab qiladi.

7-TAMOYIL: RESURLARNI BELGILANGAN VAZIFA VA MAJBURIYATLARGA MUVOFIQLASHTIRISH

Tegishli resurslar va malakalar to'plami belgilangan vazifalar va majburiyatlarga muvofiq bo'lishi va doimiy mashg'ulotlar o'tkazilishi kerak.

CRMPning hech bir komponenti zarur majburiyatlarsiz, ustuvorliklar, resurslar va ayniqsa boshqaruvsiz samarali bo'la olmaydi. Ushbu vazifalarni amalga oshirishda, tahdidlarni boshqarish haqida to'liq ma'lumotga ega bo'lmagan operativ xodimlarga qo'shimcha vazifalarni yuklamasdan, tahdid bilan bog'liq zarur ko'nikmalarga ega bo'lgan mutaxassislarini jalb qilish muhimdir.

Boshqaruv organi korxonaning umumiy biznes strategiyasi va maqsadlarini hal qilish uchun ba'zan juda tezkor tarzda rivojlanishga va moslashishga tayyor bo'lishi lozim (bu ushbu bobda muhokama qilingan moslashuvchanlikning yana bir jihatidir). Raqamli texnologiyalar bu muammoni ayniqsa dolzarb masalaga aylantiradi. Misol uchun, korxona o'z mahsuloti va xizmatlarini yoki uning ichki jarayonini raqamlashtirayotgan bo'lsa, u tahdidlar bilan bog'liq qaror qabul qilishda haqqoniy ma'lumotlarga muhtoj. Bu, masalan, ma'lum bir aktiv muhim infratuzilmani yoki ta'minot zanjirining asosiy komponentini ifodalaydimi yoki yo'qligini aniqlashni anglatishi mumkin, shunda biznesga tegishli tahdidlar bo'yicha qarorlar qabul qilinadi va sharoitlar o'zgarganda o'zgartiriladi.

Ushbu talablarni harakatlantiruvchi omillarga quyidagilar kiradi:

NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi 2.0 GV. RM-03

U kiberxavfsizlik bilan bog'liq tahdidlar strategiyasi, vazifa, majburiyatlari va siyosatlariga mutanosib ravishda yetarli resurslar ajratilishiga urg'u beradi.

ISO/IEC 27001:2022 7.1

ISOning 27001 standarti 7.1-bo'limida tashkilot axborot xavfsizligini boshqarish tizimini yaratish, amalga oshirish, saqlash va doimiy ravishda takomillashtirish uchun zarur bo'lgan resurslarni aniqlashi va ta'minlashi kerakligi talab etiladi.

NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 3-tamoyil

NACDning 3-tamoyili, xususan, kengashning kibertahdidlarni boshqarish bo'yicha tajribaga ega bo'lishi zarurligini e'tirof etadi. Bu kengash a'zolarini to'g'ri ko'nikmalar va resurslar bilan ta'minlash – ularning samarali nazoratni

ta'minlash va kiberxavfsizlik bo'yicha ongli qarorlar qabul qilish qobiliyatini oshirishini ta'kidlaydi.

AICPAning CRMP tavsif mezonlari DC10⁷⁴

AICPA malakali mutaxassislarni yollash va ularni rivojlantirish hamda ularni kiberxavfsizlik bo'yicha majburiyatlari uchun javobgarlikka tortish jarayonini belgilaydi.

Yakuniy xulosa

Xulosa shuki, xavfsizlik tabiatan tahdid bilan bog'liq amaliyotdir va uning vazifasi xavfsizlikka oid tahdidlar bilan bog'liq qarorlar qabul qilishda asosli usullardan foydalanish orqali biznesni boshqarish. Asosiy vazifa – bu biznes rahbarlari (aktiv egalari va manfaatdor tomonlar) asosli biznes qarorlarini qabul qilishlarini ta'minlashdir. Tizimli moslashuvchan boshqaruv organini rasmiylashtirish orqali yuqori rahbarlarning ishtiroki korxonada boshqaruv va tahdidlarni inobatga olishga jiddiy yondashilishini ta'minlash uchun muhim ahamiyatga ega. Yana shuni muhimki, korxona faoliyatida to'liq va faol ishtirok etadigan yuqori bo'g'in-dagi qaror qabul qiluvchilar, umumiy boshqaruv sa'y-harakatlari uchun aniqlik kiritadilar. Shuningdek, ular samarali moslashuvchan boshqaruv uchun muhim bo'lgan nazorat va javobgarlikni o'rnatish va amalga oshirish uchun mas'uliyatni o'z zimmlariga oladilar.

Moslashuvchan boshqaruv to'g'ri vaqtda, to'g'ri sabablarga ko'ra, tegishli odamlar tomonidan tahdidlarni boshqarishga oid qarorlar qabul qilish uchun asos yaratadi. Ammo tahdidlar bilan bog'liq qarorlarning samaradorligi ular asoslangan ma'lumotlarga bog'liq bo'ladi. Ikkinchi asosiy komponent "Tahdidlar haqidagi ma'lumotlarga asoslangan tizim"ni kibertahdidlarni boshqarish bo'yicha har qanday dasturning markaziy komponenti sifatida o'rnatish zarurdir.

⁷⁴ 2017 AICPA CRMP Description Criteria DC13, DC16 – Amerika sertifikatlangan jamoat buxgalterlari institutining 2017-yilgi CRMP tavsif mezonlari DC10, DC16.

IV BOB. TAHDID HAQIDAGI MA'LUMOTLARGA ASOSLANGAN TIZIM

Ushbu kitobning boshida biz raqamli dunyoda korxonalar duch keladigan bir necha ko'z ko'rib, quloq eshitmagan hamda oldindan taxmin qilib bo'lmaydigan tahdidlarni muhokama qildik, shuningdek, rasmiy CRMP yordamida ushbu tahdidlarni bartaraf etishning muhimligini ta'kidlab o'tdik.

Raqamlashtirish va uning oqibatlariga qaratilayotgan barcha e'tiborga qaramay, CRMP raqamlashtirish bilan bog'liq muammolarni hal qilish uchun mo'ljallanmaganligini tushunish muhimdir. Aslini olganda, bu umuman muammo ham emas. Raqamlashtirish bir necha yil oldin tasavvur qilib bo'lmaydigan tahdidlarni keltirib chiqarsa-da, u yangi biznes imkoniyatlarini ham taqdim etdi. Ushbu kitobda o'rganilayotgan asosiy masala shundaki, xavfsizlikni ta'minlash va tahdidlarni boshqarishda amaldagi yondashuvlar va amaliyotlar yetarli darajada takomillashtirilmagan, buning natijasida esa korxonalar yuzaga kelayotgan tahdidlardan o'zini himoya qila olmayapti, shu bilan birga, yangi biznes imkoniyatlaridan tez va samarali foydalanishga yo'l ochadi. Bu to'rt asosiy tarkibiy qismga asoslangan, aniq belgilangan CRMPni talab qilinadi. Oldingi bobda ushbu tarkibiy qismlardan birinchisi, ya'ni moslashuvchan boshqaruv masalasi batafsil ko'rib chiqildi. Endi esa, ikkinchi asosiy komponent, ya'ni tahdidlar haqidagi ma'lumotlarga asoslangan tizim haqida to'xtalib o'tamiz.

TAHDIDMI YOKI IMKONIYAT? TOYOTA KOMPANIYASIDA ISHNING TO'XTATILISHI

2022-yilning mart oyi boshida dunyoning eng yirik avtomobil ishlab chiqaruvchi kompaniyasi Toyota Yaponiyadagi barcha 14 ta zavoddagi 28 ta ishlab chiqarish liniyasida faoliyatini bir kundan ko'proq muddatga to'xtatib qo'ydi, chunki avtomobil qismlarining asosiy vositachita'minotchisi tovlamachilik hujumiga (ransomware⁷⁵) uchragan edi. Rossiya Ukrainaga hujum boshlaganidan so'ng, Yaponiya hukumati Ukrainaga ko'rsatgan ko'magiga javoban davlat tomonidan homiylik qilingan deya gumon qilindi va hujum Toyota kompaniyasining bir-biriga chambarchas bog'langan umummilliy *Kanban* – o'z vaqtda yetkazib berish tizimining asosiy ishtirokchisi va elektron komponentlarning asosiy ta'minotchisi bo'lgan Kojima Industries kompaniyasiga qarshi qaratilgan edi.

Toyota kompaniyasi "o'z vaqtida" ishlab chiqarish tizimini birinchi bo'lib yo'lga qo'ydi, bu kerakli mahsulotni o'z vaqtida, kerak bo'lishidan bir necha daqiqa yoki hatto soniyalar oldin, kerakli miqdorda yetkazib berish texnikasidir. Bu mahsulotlarni omborxonada saqlash va inventarizatsiyani boshqarish kabi sohalarida xarajatlarni tejaydi, moliyaviy foyda keltiradi, shuningdek, maxsus buyurtmalarni tez va aniq yetkazib berish imkonini beradi.

⁷⁵ Ransomware – jabrlanuvchining kompyuterini ishlashga yaroqsiz holga keltiradigan troyan ot tipidagi zararli dastur hisoblanadi.

Toyota kompaniyasi ushbu operatsion modelni strategik ustunlik deb biladi. Shuning uchun Kojima kompaniyasining tovlamachilik dasturi hujumiga uchrashi hamda buning natijasi-da Toyota kompaniyasi ta'minot zanjiri uzilishi hodisasini muvaffaqiyatsizlik sifatida ko'rish mantiqan to'g'ri bo'lib tuyuladi. Ammo bu aslida muvaffaqiyatga erishganlik haqidagi hikoya, ya'ni Toyota kompaniyasiga tavakkal qilish va raqobatchilar oldidagi ustunlikka erishishga imkon bergan va hattoki ruhlantirgan tahdidlar haqidagi ma'lumotlarga asoslangan tizim haqidagi hikoya bo'lsa-chi? Bizda kompaniya ichidagi barcha tafsilotlar mavjud bo'lmasa-da, ammo biz ba'zi asosli farazlarni keltirishimiz mumkin: Toyota *kanban* tizimini o'z biznes modelining strategik komponenti, muhim infratuzilma sifatida ko'rgan va kompaniya rahbariyati bu tizim duch kelgan tahdidlar, jumladan, tovlamachilik dasturi va boshqa kiberhujumlarning ortib borayotganligi haqida xabardor qilingan bo'lardi. Ayniqsa, ta'minot zanjirida yuzlab mustaqil ta'minotchilar bilan bog'liq bo'lgan ko'plab zaifliklar hisobga olinsa, tovlamachilik dasturi xavf tug'dirishi shubhasiz. Albatta, Toyota kompaniyasi xavfsizlikni nazorat qilish, noxush hodisalarni kuzatish va unga qarshi chora ko'rish orqali kibertahdidlarni bartaraf etish bo'yicha sa'y-harakatlarni amalga oshirgan, tahdidlar ehtimoli hamda ularning ehtimoliy ta'sir jihatlari ishlab chiqqan bo'lar edi. Tahdidlarga qaramay, tahdid va foyda muvozanatidan qoniqqan Toyota kompaniyasi "o'z vaqtida" ishlab chiqish tizimini tatbiq etishda davom etdi. 2022-yilgi tovlamachilik dasturi bilan bog'liq hodisa bu qaror noto'g'ri bo'lganini anglatadimi? Balki. Agar salbiy ta'sirlar foydadan ustun bo'lsa, unda ha. Ammo bunday bo'lmagan degan xulosaga kelish uchun yetarli asos bor. Toyota kompaniyasi zavodlari deyarli 24 soatga yopildi, bu esa har yili ishlab chiqarilayotgan 10 milliondan ziyod avtomobillarning atigi 13 mingini ishlab chiqarishni kechiktirdi.

Xarajatlarni tejash va buyurtma asosida yetkazib berish imkoniyatlari nuqtayi nazaridan "o'z vaqtida" ishlab chiqarish tizimining foydalari hujumdan ko'rigan zarardan ko'ra ancha ko'proq. Yakuniy xulosa: Toyota kompaniyasi tahdid va foyda muvozanatini aniqlash uchun tahdidlarni hisobga olgan holda qaror qabul qilgani va natijalar bu to'g'ri qaror bo'lganligini ko'rsatmoqda.

Tahdid sharoitlari o'zgarishi mumkin, ba'zida ular to'satdan o'zgaradi va o'zgargan sharoitlar qarorlarning o'zgarishini talab qilishi mumkin. Raqobatchilardan oldinda bo'lish uchun tavakkalga boradigan kompaniya xoh u Toyota kabi mustahkam obro'ga ega bo'lgan ko'p millatli kompaniya bo'lsin yoxud tez rivojlanayotgan startap bo'lsin, u o'z faoliyati va aktivlariga potentsial ta'sir ko'rsatishi mumkin bo'lgan tahdid muhitidagi o'zgarishlar haqida doimiy ravishda xabardor bo'lishi kerak. Aniq va tasdiqlangan tahdidlar haqidagi ma'lumotlarga asoslangan tizim tahdidga oid qarorlarni qabul qilishda ishtirok etadigan manfaatdor shaxslarning ko'p qatlamlarini xabardor qilish jarayonini yaratadi.

Endi dasturning eng muhim tarkibiy qismini ko'rib chiqamiz: tahdidlarni boshqarish bo'yicha qarorlar qabul qilishda korxonalar foydalanadigan ma'lumotlar. Biz ushbu ma'lumotni qanday qilib tizimli jarayon bo'yicha qabul qilish, baholash, boshqarish va ma'lum qilish kerakligini batafsil tushuntiramiz, bu esa korxona rahbarlari tahdidlar to'g'risida o'z vaqtida asoslangan qarorlar qabul qilishlarini ta'minlaydi.

Nega tahdid haqidagi ma'lumotlar juda muhim?

Ko'pgina sud qarorlari, shu jumladan, biz muhokama qilgan holatlar, korxonalarning eng yuqori bo'g'indagi qaror qabul qiluvchilari tahdidlarga qarshi

kurashishda muvaffaqiyatsizlikka uchraganligi va undan ham muhimi, tahdidlar to'g'risida ma'lumot berilmaganligi uchun javobgar ekanligini ko'rsatadi. Bu tahdidga oid qarorlar qabul qiladigan yoki qabul qilishi kerak bo'lgan har bir shaxsga, shu jumladan direktorlar kengashi, CEO va yuqori lavozimli rahbarlarga tegishlidir. Sudlar "men bilmasdim" yoki ma'lumot tasodifiy bo'lgan degan da'volar, ishlar yomonlashganda yetarli bahona emasligini aniq ko'rsatdi. Tahdidga oid ma'lumotlarini yig'ish, baholash, taqdim etish va tahdidga oid ma'lumotlarni oshkor etishning samarali tizimi mavjud bo'lmasa, mas'ullarning barchasi jiddiy yuridik javobgarlikka, ham fuqarolik (Boeing kompaniyasi xavfsizlik xizmati boshlig'i sud ishi misolida ko'rganingizdek), ham jinoiy javobgarlikka tortiladi. Muammolar shu bilan tugab qolmaydi. Yakuniy xulosa: tahdid haqidagi ma'lumotni tegishli shaxslarga o'z vaqtida yetkazish uchun tizimli jarayonning o'rnatilmaganligi juda jiddiy tahdidlar majmuyini keltirib chiqaradi: ya'ni huquqiy, me'yoriy, moliyaviy va obro'ga ta'sir ko'rsatuvchi tahdidlar.



Boeing kompaniyasi ishi bo'yicha sud qaroridan olingan bir iqtibos shuni aniq ko'rsatadiki, muhim vazifalar, javobgarlik va majburiyat uchun risk mas'uliyati korxona qarorlarini qabul qilishning eng yuqori darajalarida o'rin topgan: "xavfsizlik masalalari muhim bo'lgan vaziyatda, boshqaruvning faqat umumiy hisobotlar bilan xavfsizlikni ko'rib chiqishining yetarli emasligi ta'kidlanadi. Xavfsizlik uchun ko'rsatilgan e'tibor yanada aniq va tizimli bo'lishi kerak. Bunday hisobotlar muhim xavfsizlik masalalarini to'liq qamrab ololmaydi. Boeing boshqaruv kengashi samolyot xavfsizligi bo'yicha talablarga rioya qilishni rahbariyat ixtiyoriga topshirib qo'ymasdan, balki aniq tuzilgan muvofiqlik tizimini joriy etishi va keyin uning ustidan nazorat olib borishi lozim"⁷⁶.

Tahdid va tahdid to'g'risidagi ma'lumotlar ta'rifi

Keling, ushbu atamalarni ta'riflab, tahdid to'g'risidagi ma'lumotlar nima ekanligiga oydinlik kiritsak. Milliy kiberxavfsizlik markazi tahdid to'g'risidagi ma'lumotni "qarorga ta'sir qilishi mumkin bo'lgan har qanday ma'lumot" deya ta'riflaydi.

Tahdidlarni boshqarish mas'uliyatiga ega bo'lgan korxona qaror qabul qiluvchilarning ko'pchiligi tahdid nima ekanligini bilamiz deb o'ylashadi, ammo ular tizimli, tasdiqlangan va rasmiylashtirilgan jarayondan foydalangan holda tahdidga oid xulosa chiqarmasalar, ularning tahdid haqidagi tushunchasi to'liq yoki izchil bo'lmasligi va ko'p hollarda shunchaki noto'g'ri bo'lishi mumkin. Bu, ayniqsa,

⁷⁶ In re C. A. 2019-0907-MTZ (Del. Ch. Sep. 7, 2021), https://oreil.ly/R_6fF.

xavfsizlik bo'yicha mutaxassislarga – hatto eng katta va tajribali mutaxassislarga ham tegishli.

Xavfsizlik bo'yicha mutaxassis tahdid deganda xavf-xatar va zaifliklarni hamda ularga qarshi kurashish uchun mavjud nazoratlar yoki imkoniyatlarni tushunishi mumkin: ya'ni zararli insayderlar (malicious insiders⁷⁷), tuzatilmagan dasturiy ta'minot zaifliklari va ma'lumotlarni himoya qilish. Shubhasiz, bu masalalar va ular to'g'risidagi ma'lumotlarning barchasi muhim va ahamiyatli, ammo bu tahdid haqidagi ma'lumot emas. Nima uchun? Chunki u biznes kontekstiga to'liq muvofiq tarzda o'rnatib qo'yilmagan.

Tahdid to'g'risidagi ma'lumotlarni chuqurroq o'rganishdan oldin, tahdidning o'zi nimani ekanligiga aniqlik kiritdik. Quyida oddiy tenglama shaklida taqdim etilgan juda sodda ta'rif keltirilgan:

$$\text{Tahdid} = \text{Ehtimollik} \times \text{Ta'sir}$$

Keling, uni biroz batafsilroq ko'rib chiqaylik:

$$\text{Tahdid} = \text{Ehtimollik (zaiflikdan foydalanadigan tahdid)} \times \text{Ta'sir (korxona jarayoni, aktivi yoki maqsadiga)}$$

Zaiflikdan foydalanadigan tahdidning ehtimolligi muhim, chunki korxona duch keladigan tahdidlarni va undan kelib chiqadigan kamchiliklarga (zaifliklarga) tamoman chora ko'rish u yoqda tursin, ularni hisoblashning iloji yo'q. Kibertahdid muhitining ko'lami haqida bir misol: Microsoft kompaniyasi faqat 2022-yilning o'zida o'z tizimlarida 1212 ta kamchilikni aniqladi. Aksariyat korxonalar murakkab va turli xildagi AT muhitlarida ishlaydi, ularning ko'pchiligi uchun o'zlarida mavjud tizimlar va ilovalar haqida aniq tasavvurga ega bo'lish tobora qiyinlashmoqda. Hujum qilingan taqdirda yuzaga kelishi mumkin bo'lgan potensial tahdidning yuzaga kelish ehtimoli va zaifliklarni tushunish uchun aktivni tushunish juda muhimdir. Ammo asosiy vositalarni tushunish hujum qilingan taqdirda yuzaga kelishi mumkin bo'lgan ta'sirni va potensial tahdid zaiflikdan foydalanishi mumkinligini tushunish uchun juda muhimdir. Mana oddiy misol. Microsoft SQL Serverga mo'ljallangan nol kunlik zaif nuqtadan foydalanish, bu platformadan muhim veb-ilovani qo'llab-quvvatlash uchun foydalanadigan korxona uchun jiddiy muammo hisoblanadi, ammo foydalanishdan chiqarilayotgan va ommabop bo'lmagan veb-ilovalar uchun bu ehtimol tashvish tug'dirmasligi mumkin.

Xavfning o'zi tahdid emas va xavf haqidagi ma'lumot ham tahdid haqidagi ma'lumot hisoblanmaydi.

Endi ta'sir masalasiga kelsak. Bu jarayon biznes uchun eng qimmatli bo'lgan aktivlarni ro'yxatga olishdan boshlanadi. Bu aktivlarga korxonaning tijorat sirlari va boshqa intellektual mulki, mijozlarning shaxsiy ma'lumotlari yoki elektron

⁷⁷ Malicious insiders – zararli insayder – bu kompaniyaning maxfiy ma'lumotlarini qasddan tarqatish yoki suiiste'mol qilish uchun imtiyozli kirish huquqidan foydalanadigan xodim, pudratchi yoki biznes sherik.

tijorat platformasining asosiy dasturiy kodi kirishi mumkin. Shundan kelib chiqib, tahdid yoki zaiflikning korxona tizimlari, ilovalari, operatsiyalari va jarayonlariga potensial ta'siri yanada aniqroq bo'ladi. Ta'sir qilingan aktivlar va natijada yuzaga keladigan oqibatlar yoki ta'sirlarni har tomonlama tushunmasdan turib, korxona duch keladigan tahdidlarni tushunish va tegishli choralarni belgilash hamda ularni amalga oshirish imkonsiz bo'ladi.

Tahdid ehtimoli va ta'siri o'rtasidagi bog'liqlikni aniqlash jarayoni, shubhasiz, tahdid haqidagi ma'lumotlarni shakllantirishda katta ahamiyatga ega, bu tahdid haqidagi ma'lumotlar nimani o'z ichiga olishini tushunishda muhim bosqich hisoblanadi. Buyuk Britaniya milliy kiberxavfsizlik markazi (NCSC⁷⁸) oddiy, ammo foydali ta'rif beradi: "Tahdid haqidagi ma'lumot qarorga ta'sir qilishi mumkin bo'lgan har qanday ma'lumotdir". NCSC qo'shimcha qiladi: "Ba'zi tashkilotlarda faqat ma'lum turdagi ma'lumotlarni qonuniy tahdid haqidagi ma'lumot sifatida qabul qilish tendensiyasi mavjud. Bunday cheklovlar muhim bir narsani o'tkazib yuborish ehtimolini oshiradi"⁷⁹. Asosiy ma'no shundaki, haqiqiy hayotdagi tahdidlarni boshqarish uchun biror-bir tahdid yoki zaiflikka tor e'tibor qaratishdan ko'ra, tahdid haqidagi ma'lumotlarga keng qamrovli yondashuv muhimdir.

Tahdidlarni hisobga olgan qarorlar tizimi ushbu tushunchalardan foydalanadi va ularni muntazam, takroriy va izchil ravishda amalga oshiradi. Ishonchli va tasdiqlangan metodologiyadan foydalanish orqali, korxona va uning rahbarlari tahdid natijalariga ishonch hosil qilib, tahdid va manfaat o'rtasidagi maqbul muvozanatni topish uchun asosli qarorlar qabul qilishlari mumkin.

Ushbu kitobda biz taqdim etayotgan CRMP tizimi, keng qamrovli CRMP ning bir qismi sifatida integratsiyalashgan samarali, tahdidga asoslangan tizimni yaratishda hisobga olinadigan asosiy tamoyillarni aniqlash uchun qo'llaniladi. Keng qamrovli tizimning o'zi haqida batafsil ma'lumot olish uchun ilovaga qarang. Muayyan amalga oshirish masalalari bo'yicha qo'shimcha ma'lumot olish uchun 7-bobga qarang. Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning o'ziga xos xususiyatlari uchun esa 4.1-jadvalga qarang.

⁷⁸ NCSC (National Cyber Security Centre) – Milliy kiberxavfsizlik markazi.

⁷⁹ "Tahdidlarni boshqarish", Kiberxavfsizlik milliy markazi, 2023-yil 10-oktyabr. 7-bet.

**CRMP tizimi – Tahdidlar haqidagi ma'lumotlarga
asoslangan tizim**

CRMP tarkibiy qismlari	Tamoyillar	Ma'lumot manbalari
Moslashuvchan boshqaruv	75-betda "Moslashuvchan boshqaruvning yetti tamoyili"ga qarang	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACD⁸⁰ning direktorlar qo'llanmasi • ISO 27001:2022 • NIST 8286 • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • ISO 31000:2018 • AICPAning CRMP
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	94-betda "Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	120-betda "Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	151-betda "Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • AICPAning CRMP

**Tahdid haqidagi ma'lumotlarga asoslangan tizimning
besh tamoyili**

Ushbu kitobda rasmiy, tizimli, kiber-maxsus amaliyotlar to'plami bo'lgan CRMP bayoni keltirilgan bo'lib, u tez o'zgaruvchan tahdid muhitining muammolari va imkoniyatlarini hal qilish uchun mo'ljallangan, ushbu amaliyotlar biz muhokama qilgan ishonchli manbalarning talablariga moslashtirilgan. Bu dastur

⁸⁰ NACD (National Association of Corporate Directors) – Korxona rahbarlari milliy uyushmasi.

o'z vaqtida, tegishli tahdid haqidagi ma'lumotlar bilan ta'minlanishini kafolatlash uchun, biz eng yaxshi amaliyotlarni tavsiflaymiz. Har qanday tahdidlarni hisobga olgan holda qaror qabul qilish jarayoni samarali bo'lishi va korxonaning o'ziga xos ehtiyojlariga mos kelishi uchun amal qilish kerak bo'lgan beshta asosiy tamoyil mavjud.

1-TAMOYIL: TAHDIDLARNI BAHOLASH TIZIMI VA METODOLOGIYASINI ANIQLASH

Tashkilotdada kibertahdidni aniqlash, baholash va o'lchash uchun tahdid asoslari va metodologiyasini aniqlash va uni amalga oshirish lozim.

Kibertahdidlarni aniqlash, baholash va o'lchashga tizimli yondashuv muhim ahamiyatga ega, chunki u oldingi bobda muhokama qilingan boshqaruv organiga tahdidga asoslangan tegishli qarorlar qabul qilish uchun zarur bo'lgan ishonchli va takrorlanadigan ma'lumotlarni taqdim etadi. Xavfsizlik tashkiloti ushbu sa'y-harakatlarning markazida bo'lib, boshqaruv organini va umuman korxonani tahdidga oid qarorlar qabul qilish uchun zarur bo'lgan ma'lumot bilan ta'minlaydi, lekin xavfsizlik tashkiloti qarorlar qabul qilmaydi va ular uchun mas'ul yoki javobgar emas.

Xavfsizlik tashkilotining vazifasi tahdidga oid qarorlar qabul qilish emas, balki korxonani tahdidlarni hisobga olgan holda qaror qabul qilish jarayoni orqali boshqarishdir.

Tashkilotning boshqa bo'limlari bilan hamkorlikda xavfsizlik tashkilotining taqdim etadigan ma'lumotlari – boshqaruv organi va biznes manfaatdor tomonlariga bilim beradigan va ularga yo'l-yo'riq ko'rsatadigan kibertahdidlar haqidagi ma'lumotlarni hisobga oluvchi tizimning bir qismi sifatida ko'rib chiqilishi kerak. Bu ma'lumotlarga korxonaning tahdidlar haqidagi axboroti, AT identifikatsiyasi, operatsion tizim, IoT aktivlari, tahdidlar haqida ma'lumotlar, aniqlangan korxonada tahdid darajasi, biznes ustuvorliklari, kelajakdagi biznes strategiyalari, mavjud tahdidni kamaytirish choralari va olingan saboqlarni o'z ichiga olishi mumkin.

Nega tizim va metodologiya mavjud bo'lishi kerak? Ko'pgina korxonalar va xavfsizlik tashkilotlari tahdidlarni aniqlash bo'yicha amaliyot va jarayonlarga ega bo'lsa-da, ammo ko'pincha alohida, tarqoq harakatlar sifatida yoki faqat uzoq vaqt oralig'ida amalga oshiriladi va keyinchalik deyarli unutilib ketiladi. Ular, shuningdek, ma'lumotlar buzilishi, viruslar tarqalishi yoki nazoratdagi xatoliklar singari o'tmishda bo'lib o'tgan voqealardan kelib chiqadi. (Raqamli asrning tez sur'atlardagi o'zgarishi bizga o'tmishga qarab kelajakni to'liq tushunib bo'lmashligini o'rgatdi.) Tahdid haqida ma'lumotlar va ularni aniqlash jarayoni qaror qabul qiluvchilar tomonidan belgilanadigan va tasdiqlanadigan muntazam tartibda

o'tkazilishi lozim, chunki tahdid haqida uzluksiz ma'lumot olmaslikning o'zi ham tahdid hisoblanadi.

Tasdiqlangan tizim va metodologiya bir martalik yoki reaktiv yondashuv o'rini egallaydi, bu tizimning maqsadi maqbul tahdid darajalarini aniqlash uchun ma'lumotlarni yig'ish, yuzaga keladigan va ehtimoliy tahdidlarni aniqlash hamda haqiqatan sodir bo'ladigan tahdidlarni boshqarish yoki uning oqibatlarini yumshatishdir. Shuni ta'kidlash joizki, ko'rsatkichlar ushbu jarayonda muhim rol o'ynaydi, ular operatsion yoki muvofiqlik ko'rsatkichlari emas, balki biznes kontekstiga mos keladigan tushunarli va foydali ma'lumotlarni taqdim etadigan *tahdid* ko'rsatkichlari bo'lishi lozim.

Korxonalar tahdidga asoslangan jarayonlarni amalga oshirish hamda ijro etishda eng ko'p uchraydigan muammolardan biri shundaki, korxonalar haddan ziyod ko'p yoki noto'g'ri ma'lumotlarga ega va ular ushbu ma'lumotlarni o'zlarining tahdidga oid qaror chiqarishlarida samarali va ahamiyatli bo'lishi uchun vaziyatga moslashtirishga harakat qilishadi. Yana bir muammo – bu ma'lumotlarni maqsadli auditoriya tomonidan aniq tushuniladigan atamalar va tillarga o'girib, ma'lumotlarning mo'ljallangan maqsadga muvofiqligini ta'minlash. Masalan, direktorlar kengashi va yuqori martabali rahbarlar eng dolzarb tahdidlar yoki ular bilan bog'liq biznes muammolari, korxonaning tahdidga moyilligi, tahdidning byudjetga ta'siri va boshqa biznes muammolari haqida yuqori darajadagi ma'lumotlarni olishga intilishadi. CIO⁸¹ yoki yirik firma rahbariga qarorlar qabul qilish uchun batafsilroq ma'lumotlar ko'proq qo'l kelishi mumkin. Tahdid haqidagi ma'lumotni hisobga oluvchi tizimning mufassalligi korxona tomonidan muhokama qilinishi, ishlab chiqilishi va tasdiqlanishi kerak bo'lgan tahdid haqidagi ma'lumotni hisobga oluvchi prinsiplarni aniqlashning bir qismidir. Bu zaruriy ravishda davom etadigan jarayon bo'lib, yangi paydo bo'layotgan tendensiyalarni aniqlash va ularga javob berish uchun doimiy tekshiruv va bazaviy natijalarga nisbatan hisobot berishni talab qiladi. (Hisobotlar byudjetlashtirish va ustuvorliklarni belgilash bo'yicha o'rnatilgan jarayonga muvofiq bo'lishi kerak, bu haqda keyingi bobda muhokama qilinadi.) Ushbu chora-tadbirlarning barchasi bitta umumiy maqsadga ega: kiberxavfsizlikni korxona miqyosida tahdidlarni boshqarishning keng qamrovli tizimiga samarali integratsiyalashuvini ta'minlash.

Quyida keltirilgan sohaga doir qo'llanmalar alohida ahamiyatga ega:

*SEC yo'riqnomasi S-K 106(b) bandi – Tahdidlarni boshqarish va strategiya*⁸²

Ushbu bandning mohiyati kompaniyalarning kiberxavfsizlik tahdidlaridan kelib chiqadigan moddiy tahdidlarni baholash va aniqlash uchun tizimli jarayonlarga ega bo'lishini ta'minlashdan iborat. U tashkilotlarga kiberxavf murakkab-

⁸¹ CIO (Chief Information Officer) – axborot texnologiyalari bo'yicha direktor.

⁸² SEC Regulation S-K Item 106(b)–Risk Management and Strategy – SEC yo'riqnomasi S-K 106(b) bandi – Tahdidlarni boshqarish va strategiya.

liklarini boshqarish uchun o'rnatilgan asosning zarurligini ta'kidlovchi tamoyilni mustahkamlaydi.

NACDning 2023-yilgi kibertahdidlarni nazorat qilish to'g'risidagi direktorlar qo'llanmasi, 1, 4, 5-tamoyillar⁸³

NACD ta'kidlaganidek, kiberxavfsizlikni "strategik tahdid" sifatida ko'rish uchun kibertahdidlarni nafaqat axborot texnologiyalari nuqtayi nazaridan, balki korxona nuqtayi nazaridan ko'rib chiqish kerak. Unda, shuningdek, oldinroq muhokama qilingan komponent "Moslashuvchan boshqaruv"ning muhimligi ta'kidlanadi va korxona miqyosida tahdidlarni aniqlash, baholash va o'lchash imkoniyatiga ega bo'lish uchun biznes bilan hamkorlikda ishlash zarurligini ta'kidlanadi.

NISTning 2023-yilgi kiberxavfsizlik asoslari 2.0 GVRM, ID, RA loyihasi⁸⁴

NIST ushbu kategoriyalar bo'yicha tushunchalarni taqdim etadi, ko'rsatmalar beradi va belgilangan asos va metodologiya zarurligini ta'kidlaydi.

ISO/IEC 27001:2022 6.1.2, 6.1.3 band

ISO/IEC 27001 tahdidga asoslangan yondashuvni qabul qiladi. Yuqori bo'g'indagi rahbariyat tashkilotning tahdidlarni aniqlash, baholash va tegishli tarzda tartibga solish uchun javobgardir, shu jumladan tashkilot doirasiga mos keladigan tahdidlarni baholash metodologiyasini aniqlash uchun javobgardir. 6.1.2 va 6.1.3-bandlar tahdidni baholash va uni tartibga solish jarayonlarini talab qiladi. Bundan tashqari, ISO/IEC 27005 axborot xavfsizligi tahdidlarini boshqarish bo'yicha batafsil ko'rsatmalar beradi.

AICPAning CRMP tavsif mezonlari DC11⁸⁵

Ushbu buxgalteriya bosharti kiberxavfsizlik tahdidlarini va tashkilotning kiberxavfsizlik tahdidlarini boshqarish dasturiga sezilarli ta'sir ko'rsatishi mumkin bo'lgan ekologik, texnologik, tashkiliy va boshqa o'zgarishlarni aniqlash va tashkilotning kiberxavfsizlik maqsadlariga erishish uchun tegishli tahdidlarni baholash jarayonini talab qiladi.

2-TAMOYIL: TAHDID DARAJALARINI ANIQLASH METODOLOGIYASINI ISHLAB CHIQLASH

Tahdidning maqbul darajalari uchun tasdiqlangan va takrorlanadigan metodologiya yaratilishi lozim.

Maqbul tahdid darajalarini aniqlash uchun bir necha metodologiyalar mavjud, ammo biz ulardan faqatgina uchtasini muhokama qilamiz. Qaysi metodologi-

⁸³ 2023 NACD Director's Handbook on Cyber-Risk Oversight Principle 1, 4, 5 – NACDning 2023-yilgi kibertahdidlarni nazorat qilish to'g'risidagi direktorlar qo'llanmasi, 1, 4, 5-tamoyillar.

⁸⁴ 2023 Draft NIST CSF 2.0 GVRM, ID, RA – Standartlar va texnologiyalar milliy institutining 2023-yilgi kiberxavfsizlik asoslari 2.0 GVRM, ID, RA loyihasi.

⁸⁵ 2017 AICPA CRMP tavsif mezonlari DC11 – Amerika sertifikatlangan jamoat buxgalterlari institutining 2017-yilgi CRMP tavsif mezonlari DC11.

yadan foydalanishdan qat'i nazar, ma'lum bir korxona muhiti uchun tahdidga moyillik va chidamlilikning maqbul darajalari aniqlanishi lozim, eng muhimi, ushbu tahdid darajalari tahdid uchun javobgar shaxslar va boshqa yuqori qaror qabul qiluvchilar tomonidan tasdiqlanganligini ta'minlash zarur. Qabul qilingan yoki ishlab chiqilgan metodologiya juda xilma-xil bo'lishi mumkin, ammo qaysi metodologiya qo'llanilishidan qat'i nazar, u quyidagi besh vazifani bajarishi lozim:

Joriy holatdagi tahdid darajasini aniqlash

Bu korxona hozirda duch kelayotgan tahdidlarni va amalga oshirilayotgan tahdidlarni kamaytirish choralarining samaradorligini baholashni anglatadi.

Kelajakda kutilayotgan tahdid darajalarini aniqlash va ular yuzasidan keli-shuvga erishish

Boshqaruv organi bilan hamkorlikda ishlab chiqilgan maqbul kelajakda yu-zaga kelishi mumkin bo'lgan tahdidlarni aniqlash – korxonaga o'zgaruvchan va yangi paydo bo'ladigan tahdidlarni boshqarish bo'yicha sa'y-harakatlarini birin-chi o'ringa qo'yish imkonini beradi.

Kelajak kutilayotgan maqbul tahdid darajalaridan foydalanib, umumiy tah-did strategiyasi va ijro modelini ishlab chiqish.

Bu nafaqat korxonaning tahdidga moyillik va chidamlilik darajasini uning umumiy biznes strategiyasiga moslashtirishi, balki tegishli byudjet mablag'larini ishlab chiqish va ularni asoslash imkonini bergani uchun ham juda muhimdir (bu masala keyingi bobda keng yoritiladi).

Tahdid strategiyasining amalga oshirilishini nazorat qilish

Bu samaradorlikni aniqlash va korxonaning maqbul tahdid doirasida qoli-shini ta'minlash uchun boshqaruv organi tomonidan nazorat qilinadigan uzluksiz jarayon bo'lishi kerak.

Kelishilgan vaqt oralig'i asosida uzluksiz nazorat

Belgilangan vaqt oralig'ida tahdidga moyillik va chidamlilikni ko'rib chiqish, baholash va nazorat qilish uchun tegishli tartibning mavjudligi tahdid muhitidagi o'zgarishlarni oldindan bilish va ularga moslashish imkonini beradi.

Tahdidga moyillik va chidamlilik: Muhim farq

Ko'pgina korxona qaror qabul qiluvchilari, hatto yuqori malakali xavfsizlik mutaxassislari ham, *tahdidga moyillik* va *tahdidga chidamlilik* atamalarini tushunmaydilar. Shu sababli, ke-ling, bu ikki tushuncha o'rtasidagi farqni oydinlashtirib olaylik. Tredvey komissiyasining homiy tashkilotlar qo'mitasi (COSO⁸⁶) tomonidan berilgan ta'riflar foydali ma'lumotni taqdim etadi:

- Tahdidga moyillik – bu keng miqyosda tashkilot biror-bir foydali sarmoyaga erishish uchun qabul qilishga tayyor bo'lgan tahdid miqdoridir. Har bir tashkilot daromadni oshirish uchun turli maqsadlarni ko'zlaydi va buning uchun o'z zimmasiga olishga tayyor bo'lgan tahdidlarni yaxshi tushunishi zarur.

⁸⁶ COSO (Committee of Sponsoring Organizations) – Homiy tashkilotlar qo'mitasi.

• Tahdidga chidamlilik ishlab chiqarish bo'linmalarini ular o'z faoliyat doirasida tahdidga moyillikni amalga oshirayotganlarida boshqaradi. Tahdidga chidamlilik moslashuvchanlik darajasini bildiradi, tahdidga moyillik esa tavakkal qilmaslik kerak bo'lgan chegarani belgilaydi.

Turli korxonalar turli xildagi tahdidga moyillik va tahdidga chidamlilik xususiyatiga ega va ularni aniqlash hamda ular o'rtasida maqbul muvozanatni o'rnatish uchun juda ko'plab yondashuvlar mavjud. Qanday yondashuv qo'llanilmasin, qaror qabul qilish va amalga oshirishni yaxshilash uchun maqbul tahdid nima ekanligi to'g'risida yakuniy qarorni aynan korxona qabul qilishi lozim. Korxonani xabardor qilish va uning roziligini olish uchun takrorlanadigan metodologiya mavjud bo'lishi zarur.

To'g'ri va samarali tahdid darajalarini aniqlash zarurati keng ko'lamli standartlar va bayonnomalar bilan qo'llab-quvvatlanadi, jumladan:

- *NISTning kiberxavfsizlik asoslari 2.0* da tahdidga moyillik va tahdidga chidamlilik tashkilotning biznes muhiti asosida aniqlanishi va yetkazilishi kerakligini ta'kidlaydi.

- *NACDning kibertahdidlarni nazorat qilish bo'yicha direktor qo'llanmasi, 1 va 5 tamoyillar.* 1-tamoyil strategik maqsadlar va biznes imkoniyatlariga mos kelishi uchun kibertahdidlar bo'yicha munozaralar zarurligini ta'kidlaydi. Buni amalga oshirish uchun mustahkam metodologiya zarur bo'lib, u tijorat korxonasi-ning rivojlanishi uchun asos bo'ladi va boshqaruv tomonidan belgilangan va direktorlar kengashi tomonidan tasdiqlangan tahdidga moyillik o'lchovini osonlashtiradi. Ushbu qo'llanmaning 5-tamoyilida tahdidga moyillik haqidagi bayonotlarni aniqlik, obyektivlik va o'lchash qobiliyati bilan qanday tuzish kerakligi haqida gap ketadi, shu bilan birga dastlabki aniqlash paytida mavjud bo'lgan iqtisodiy sharoit kabi subyektiv elementlari ham hisobga olinishi ta'kidlanadi.

Kiberxavfsizlik tahdidlarini baholashning qaysi metodologiyasi tanlanmasin, uning muayyan asosiy umumiy maqsadlari bo'ladi. U tahdid darajalarini belgilaydi, ularni turli manfaatdor tomonlar aniq tushuna oladigan atamalarga aylantiradi va tahdid darajalarini turli boshqaruv darajalari va korxonaning boshqa tahdidga oid vazifalari bilan muvofiqlashtiradi. Bu metodologiya, korxonaning tahdidlarni boshqarishda yetuklikka erishish uchun amalga oshirayotgan harakatlarini manfaatdor tomonlarga ma'lum qilish imkonini beradi. Shuningdek, u barcha darajadagi boshqaruv funksiyalarini o'z ichiga oladigan natijalarni taqdim etadi.

Shuni ta'kidlash joizki, tahdidni baholashning tegishli va to'g'ri darajasini aniqlash vaqt va kuch talab qiladi. Darhaqiqat, bu shunday jarayonki, u yetuklikni modellashtirishdan boshlanadi, keyin samaradorlik ko'rsatkichlari integratsiyalashadi, so'ngra avtomatlashtirilgan vositalardan foydalangan holda sifatli baholashga va nihoyat tahdid miqdorini aniqlashga o'tiladi. Ushbu tamoyilning yakuniy maqsadi korxona va uning tahdid bo'yicha qaror qabul qiluvchilar tanlangan doirada barcha mavjud ma'lumotlardan foydalanishini ta'minlashdan iborat. Ushbu tanlangan asos tahdidning maqbul darajalariga mos keladi va boshqaruv orga-

nini xabardor qilish uchun natijalardan foydalanadi. Ushbu tamoyilning asosiy maqsadi korxona va uning tahdidlari bo'yicha qaror qabul qiluvchilarga tanlangan doirada mavjud bo'lgan barcha ma'lumotlardan foydalanish imkonini beradigan tizimni yaratishdir. Keyinchalik bu ma'lumotlar qabul qilinadigan tahdid darajalarini kelishish va boshqaruv organini xabardor qiladigan tushunchalarni taqdim etish uchun ishlatiladi.

3-TAMOYIL: TAHDIDGA ASOSLANGAN EHTIYOJLAR TUSHUNCHASINI SHAKLLANTIRISH

Boshqaruv organi aniqlanib, o'zining kibertahdidlarga oid ma'lumotlarga asoslangan ehtiyojlarini har tomonlama tushunishni shakllantirish jarayoniga jalb qilinishi lozim.

Kiberxavfsizlik tahdidlarini boshqarish, xuddi boshqa turdagi tahdidlarni boshqarish kabi, keng doiradagi korxona manfaatdor tomonlari, shu jumladan yuqori boshqaruv darajadagi qaror qabul qiluvchi rahbarlar tomonidan majburiyat va ishtirokni talab qiladi (biz bu haqda o'tgan bobda batafsil to'xtalgan edik). Bu samarali muloqotni taqozo etadi. Muloqot turli shaxs va auditoriyaga mo'ljallangan, manfaatdor tomonlar osonlikcha tushuna oladigan hamda korxona boshqaruv organining talablariga muvofiq bo'lgan tarzda taqdim etilishi lozim.

Turli manfaatdor tomonlarning ehtiyojlari, tabiiyki, juda farq qiladi. Xavfsizlik mutaxassislari yuqori darajadagi texnik ma'lumotlarga ehtiyoj sezishi mumkin. Biznes bo'linmalari rahbarlari o'z sohalarining operatsion faoliyatiga oid ma'lumotlarni izlaydi, katta xodimlar va direktorlar kengashi esa faqat eng yuqori darajadagi ma'lumotlarga muhtoj bo'lishlari mumkin. Shuni ta'kidlash joizki, bu jarayon tahdid funksiyalaridan boshqa manfaatdor tomonlarga qaratilgan bir tomonlama axborot uzatish emas, balki o'zaro muloqot bo'lishi lozim. Bosh maqsad – barcha ishtirokchi tomonlarni tegishli va yetarli darajadagi tahdid ma'lumotlari hamda tahdidni baholash natijalari bilan ta'minlashdir. Bu ularga tahdidga asoslangan biznes qarorlarini qabul qilish va o'z tadbirkorlik faoliyatini belgilangan hamda o'rnatilgan tahid chegaralari doirasida amalga oshirish imkonini beradi.

NIST kiberxavfsizlik tahdidlarini aniqlash va baholash uchun kiberxavfsizlikka yo'naltirilgan foydali metodologiya ishlab chiqdi (4.1-rasmga qarang).

Tahdidga haqidagi ma'lumotlarga asoslangan tizimni rivojlantirishning muhim elementi tegishli manfaatdor tomonlar va zarur tahdid ma'lumotlari o'rta-sida samarali mehnat munosabatlarini o'rnatishdir. Bu aloqa tizimning maqsadi va tuzilmasini aniqlashga yordam beradi va uni shunchaki taqdim etilayotgan ma'lumotlarning natijasi emas, balki korxona rahbarlari tomonidan o'rnatilishi va rasmiy tasdiqlanishini ta'minlaydi.



4.1-chizma. Korxona tahdidlari va muvofiqlashtirish bo'yicha NIST tasviri⁸⁷

Quyida keltirilgan sohaga oid standartlar ushbu tamoyilni qo'llab-quvvatlaydigan qo'shimcha ma'lumotnomalardir:

NISTning 2023-yilgi CSF 2.0 0 GV.OC-02 loyihasi

Ushbu kichik turkum ichki va tashqi manfaatdor tomonlarni aniqlash va ularning kibertahdidlarni boshqarish bilan bog'liq bo'lgan kelajak rejalarini tushunish muhimligini ta'kidlaydi.

AICPAning 2017-yilgi CRMP tavsif mezonlari DC13

AICPA tashkilotning CRMPning ishlashini qo'llab-quvvatlash uchun zarur bo'lgan tegishli kiberxavfsizlik ma'lumotlarini ichki ravishda uzatish jarayonini, shu jumladan kiberxavfsizlik maqsadlari va majburiyatlarini, shuningdek aniqlangan xavfsizlik hodisalarini va ularning yechimlarini uzatish uchun chegaralarni bayon qiladi.

⁸⁷ Manba: NISTIR 8286A: Korxona tahdidlarini boshqarish uchun kiberxavfsizlik tahdidlarini aniqlash va baholash, NIST, 2021-yil, noyabr. <https://oreil.ly/jcUFj>.

IIAning 2020-yilgi uch chiziqli himoya modeli, 1-tamoyil

IIAning boshqaruv tamoyili manfaatdor tomonlar oldidagi mas'uliyatni va tahdidlar to'g'risidagi ma'lumotlarga asoslangan ehtiyojlarni tushunish, shaffoflik va muloqotni rag'batlantirish uchun manfaatdor tomonlarni aniqlash va jalb qilishga e'tibor qaratadi.

4-TAMOYIL: TAHDIDLARNI BAHOLASH MUDDATI BO'YICHA KELISHIB OLISH

Tahdidni baholash jarayoni kelishilgan vaqt oralig'ida amalga oshirilishi va uning natijalari muntazam ravishda baholanib turishi lozim.

Tahdid hech qachon turg'un bo'lmagan va raqamlashtirish ushbu haqiqatni har qachongidan ham aniqroq ko'rsatdi, bu o'z navbatida tahdidlarni boshqarish ham turg'un bo'lolmasligini anglatadi. Shuning uchun tahdid haqidagi ma'lumotlarga asoslangan tizim biznes o'zgarishi bilan tahdidlar ham o'zgarishini va aksincha ekanligini tan olishi lozim. Ushbu haqiqat tahdidlarni baholash hayot sikli va belgilangan vaqt oraliqlarida tahdidlarni hamda ularni nazorat qilish choralarining ta'sirini muntazam ravishda baholash uchun ketma-ket bosqichlarni joriy etishni talab qiladi.

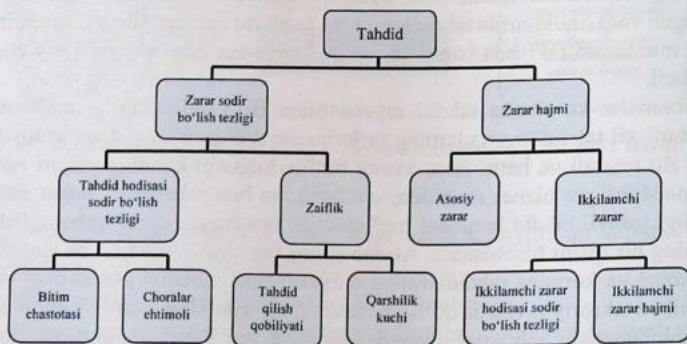
Korxonalar ko'pincha tahdid reyestlaridan (ro'yxatlaridan) – ma'lum bir vaqtda turli xil tahdidlar va ularning turlarini qayd etuvchi hujjatlardan foydalanadilar. Bu foydali va hatto zarur vosita bo'lib, bugungi kunning yuqori bosimli raqamlashtirilgan biznes muhitida, u odatda ma'lumot beruvchi hujjat sifatida foydaliligi tufayli tahdid haqidagi ma'lumotga asoslangan qaror qabul qilish jarayonining bir qismi hisoblanadi. Ammo shuni tan olish muhimki, bu shunchaki vosita xolos va korxona tahdidlarining o'zgaruvchan tabiatini aks ettirish uchun uni izchil va takroriy ravishda qo'llash zarur. Yangi tahdidlar, ularning ehtimoli va ta'siri aniqlanganda, tahdidlar reyestri doimiy ravishda yangilanib turishi lozim, bu boshqaruv organiga yangi xavflarga javob choralarini belgilash va ularni tahdidlar reyestriga kiritish imkonini beradi. Tahdidlar reyestridagi biror elementga yangi javob chorasi qo'llanilganda, bu tahdidlarni baholash jarayonining yangi joriy holatini aks ettiradi. Bu o'z vaqtida, muntazam va tizimli ravishda ma'lumotlarni qabul qilish, ko'rib chiqish va tahlil etish imkonini beradi.

Tahdidlarni baholash jarayoni sur'ati to'g'risida yana bir muhim masala shundaki, u har bir korxona uchun turlicha bo'lishi mumkin va korxona o'zi uchun qulay, ortiqcha vaqt talab qilmaydigan yoki faoliyatga xalaqit bermaydigan chastotani belgilashi lozim. Ba'zi korxonalar tahdidni baholashni yiliga bir marta yangilashni va yil davomida muhim o'zgarishlar uchun asosiy xavf ko'rsatkichlarini (KRI) kuzatib borishni yetarli deb hisoblashi mumkin. Boshqalar uchun esa (masalan, moliyaviy xizmatlar kabi yuqori tartibga solinadigan sohalaridagi korxonalar) doimiy ravishda yangilangan tahdid qiymatlarini taqdim etadigan avtomat-

lashtirilgan kibertahdidni miqdoriy baholash tizimiga ega bo'lish foydali bo'lishi mumkin.

AXBOROT TAHDIDLARINI OMILLI TAHLIL QILISH INSTITUTNING TAHDIDLAR MODELII

Ehtimollik va ta'sirni aniqlash uchun tahdidlarni baholashning turli xil modellari mavjud. Ulardan eng nufuzlilaridan biri tahdidni boshqarish bo'yicha eng yaxshi amaliyotlarni o'rnatish va targ'ib qilishga bag'ishlangan notijorat tashkilot bo'lgan Axborot tahdidlarni omilli tahlil qilish (FAIR⁸⁸) instituti tomonidan keltirilgan. Ushbu amaliyotlar tahdidlarni boshqarish bo'yicha mutaxassislarga o'zlarining biznes sheriklari bilan hamkorlik qilib, tashkilotni himoya qilish va biznesni boshqarish o'rtasida to'g'ri muvozanatni ta'minlash imkonini beradi (bu birinchi bobda ta'kidlangan xavf va mukofot o'rtasidagi muvozanatdir). Aslida, bu biz avvalroq taqdim etgan ehtimollik va ta'sir ko'paytmasi tenglamasining batafsilroq varianti bo'lib, u yillik moliyaviy yo'qotishlar yoki ta'sir ko'rsatkichlari bo'yicha ifodalangan. Ehtimollik komponentlari chap tomonda, ta'sirlar esa o'ng tomonda joylashgan bo'lib, ikkala qism ham tahdidni umumiy tushunishga xizmat qiladi (4.2-rasmga qarang).



4.2-rasm. Axborot xavfsizligi va operatsion tahdidlar uchun
FAIR institutining standart miqdoriy modeli⁸⁹

Quyidagi standartlarga rioya qilish uchun zarur shart sifatida tahdidlarni davriy baholash jarayonining muhimligi ta'kidlanadi:

SEC yo'riqnomasi S-K 106(b) bandi – tahdidlarni boshqarish va strategiya

Ushbu badda kibertahdidlar biznes faoliyati yoki moliyaviy sharoitlarga qanday ta'sir qilishi mumkinligiga e'tibor qaratilib, ushbu band tashkilotlarni o'zgaruvchan tahdidlar va biznes ustuvorliklari nuqtayi nazaridan tahdidga bo'lgan

⁸⁸ FAIR (Factor Analysis of Information Risk) – Axborot tahdidlarni omilli tahlil qilish.

⁸⁹ Manba: "Axborot tahdidlarini omilli tahlil qilish instituti modeli", /Tahdid obyektlari, 2017-yil.

munosabatlarini doimiy ravishda qayta ko'rib chiqishga undaydi. Bu tamoyilning takroriy tahdidlarni baholash jarayoniga e'tiborini kuchaytiradi.

NACDning kibertahdidni nazorat qilish bo'yicha direktorlar qo'llanmasi, 5-tamoyil.

NACDning kiberxavfsizlikni izchil o'lchash va hisobot berishga bo'lgan da'vati, muntazam, tizimli tahdidlarni baholash jarayonining muhimligini ta'kidlaydi.

NISTning 2023-yilgi CSF 2.0 ID. RA⁹⁰ (tahdidlarni baholashni aniqlash), ID.IM⁹¹ (ijobiy o'zgarishni aniqlash) 01-03 loyihasi

ID. RA tahdidlarni baholash muhimligini ta'kidlaydi, ID.IM esa tashkilotning tahdidlarni boshqarish jarayonlarini ular tashkilotning ehtiyojlariga javob berishini va aniqlangan tahdidlarni samarali hal qilishini ta'minlashi uchun muntazam ravishda qayta ko'rib chiqish va yangilab borish muhimligini ta'kidlaydi. Ikkalasi ham kiberxavfsizlikka proaktiv yondashish zarurligini ta'kidlab, o'zgaruvchan tahdid vaziyatiga asoslangan strategiyalarni doimiy ravishda tuzatishga urg'u beradi. Umuman olganda, NISTning ushbu loyihasi, samarali kibertahdidlarni boshqarish bir martalik yoki "xo'jako'rsinga" qilinadigan harakat emas, balki doimiy dastur sifatida ishlashi kerak degan fikrga muvofiq keladi.

5-TAMOYIL: HISOBOT JARAYONLARINI YO'LGA QO'YISH

Hisobot berish jarayonlari boshqaruv organiga kibertahdidlarning mavjud amaliyotlarga va strategik qarorlarga ta'siri to'g'risida ma'lumot berishi kerak.

Tahdidlarni hisobga olgan tizim – bu aniq belgilangan siyosat va o'rnatilgan jarayonlarga ega bo'lgan tizimdir, bu jarayonlar boshqaruv organiga va boshqa barcha tegishli manfaatdor tomonlarga hisobot berishni o'z ichiga olishi shart. Hisobot berish jarayoni boshqaruv organini va u orqali biznesni xavfsizlik hodisalari, ya'ni kelishilgan chegaralardan oshib ketadigan va chora ko'rishni, qabul qilishni yoki boshqa tahdidlarni bartaraf etishni talab qiladigan tahdidlar haqida ogohlantiradi. Bu ayniqsa muhimdir, chunki bu ogohlantirishlar hisobot darajasini va zarur bo'lganda eskalatsiyani, ya'ni keskinlashuvni rag'batlantiradi (tahdidlar eskalatsiyasi haqida keyingi bobda batafsil to'xtalamiz).

Hisobotlar muloqot shakli hisoblanadi va har qanday muloqot kabi, u ham maqsadli auditoriyaga mazmun va uslub jihatidan tushunarli, amaliy va aniq bo'lishi kerak. Direktorlar kengashining hisobot berishi samarali hisobot berish talablarining yaxshi namunasidir. Bu sizdan odatda texnik bilimga yoki chuqur texnik tushunchaga ega bo'lmagan kishilar bilan murakkab texnik mavzu haqida muloqot qilishingizni talab etishi mumkin. Direktorlarning majburiyatlari aslida

⁹⁰ ID: RA (Identify risk assessment) – tahdidlarni baholashni aniqlash.

⁹¹ ID: IM (Identify improvement) – ijobiy o'zgarishni aniqlash.

ishonchli, ya'ni butun korxonaning moliyaviy farovonligiga qaratilgan. Buning ma'nosi shundaki, kengash hisoboti kibertahdidni to'g'ridan to'g'ri asosiy biznes operatsiyalari va jarayonlari hamda ko'rsatkichlari bilan bog'liq bo'lgan biznes atamaları orqali ifodalashi kerak. Pirovard maqsad: boshqaruv kengashida kiberxavfning samarali boshqarilayotganiga ishonch uyg'otishdir.

Shuni yodda tutingki, hisobot berish – mavzu qanday bo'lmasin, auditoriya kim bo'lishidan qat'i nazar, aslida hikoya qilish san'atidir. Samarali hisobot berishning asosiy tarkibiy qismi – bu aniq, oson tushuniladigan hikoya yaratishdan iborat bo'lib, u maqsadli auditoriyani his qilish va o'ylashga undaydi. Ko'plab tadqiqotlar shuni ko'rsatadiki, ko'pchilik tinglovchilar, hatto eng ilg'or fikrlilari ham, qarorlarni hech bo'lmaganda his-tuyg'ularga asoslangan holda qabul qilishadi.

Biroq, tahdidlarni boshqarish jarayonlarida ishtirok etuvchilarning ko'pchiligi oddiygina ko'rsatkichlar va boshqa ma'lumotlarni yetkazishga ko'proq o'rganib qolishgan. Texnik mutaxassislar odatda o'zlari tushunadigan va o'z nuqtayi nazarlarini asoslaydigan ma'lumotlar to'plami bilan boshlashadi, ammo bu asosan texnik bo'lmagan auditoriya uchun tushunarsiz va undan ham yomon, ishonchsiz bo'lishi mumkin. Eng yaxshi yondashuv – bu hissiy ta'sirga ega bo'lgan hikoyadan boshlash, masalan, muvaffaqiyatli bartaraf etilgan xavfsizlik kamchiligidan boshlash va keyin qo'shimcha ma'lumotlarni taqdim etish bilan davom ettirishdir.

Boshqaruvga oid hisobot berish amaliyotlari uchun eng muhim bo'lgan soha-ga doir standartlar va protokollar quyidagilardir:

2023-yilgi NIST CSF 2.0 loyihasining GV.OV-01 dan GV.OV-03 gacha bo'lgan qismlari

Ushbu subkategoriyada tashkilot rahbarlari kiberxavfsizlik tahdidlarini boshqarish samaradorligini va uning natijalarini ko'rib chiqishlari va baholashlari kerakligi va bu faqat tizimli va shaffof hisobot berish jarayonlari orqali amalga oshirilishi mumkinligi ta'kidlanadi. Ushbu qayta aloqa zanjiri rahbarlarga strategiyalarni zaruratga qarab o'zgartirishga imkon beradi, bu esa tashkilotning kiberxavfsizlik holati mustahkam va o'zgarib borayotgan tahdidlar muhitiga moslashuvchan bo'lishini ta'minlaydi.

NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 5-tamoyil.

NACDning beshinchi tamoyili, ayniqsa, o'zgaruvchan biznes muhitiga javoban kibertahdidlar to'g'risida muntazam ravishda hisobot berish va ularni o'lchash zarurligini ta'kidlaydi. Ushbu amaliyot tashkilotlarga o'zlarining tahdid holatlari to'g'risida xabardor bo'lishga va asosli qarorlar qabul qilishga imkon beradi, bu esa samarali moslashuvchan boshqaruvni ta'minlashning asosiy qismidir.

Ushbu buxgalteriya standartiga ko'ra, tashkilotning kiberxavfsizlikni boshqarish dasturining samarali ishlashini ta'minlash uchun zarur bo'lgan tegishli kiberxavfsizlik to'g'risidagi ma'lumotlarni ichki aloqa orqali yetkazish jarayoni talab qilinadi. Bu jarayonga aniqlangan xavfsizlik hodisalarini tegishli manfaatdor tomonlarga, jumladan tegishli rahbariyat va kengashga yetkazish uchun zarur bo'lgan maqsadlar va chegaralarni belgilash ham kiradi.

Yakuniy xulosa

Ushbu bobda biz tahdidlar haqidagi ma'lumotga asoslangan tizimni shakllantirishga tizimli yondashishning dolzarbligini ta'kidladik – bu yondashuv ham dasturiy, ham u qo'llaniladigan muayyan vaziyatlarga moslashtirilgan. Ushbu yondashuv turg'un emas. Bu tahdidga moyillik va chidamlilikning aniq chegaralarini belgilash uchun tahdid haqida hisobot berish va tezkorlik kabi aniq natijalarni talab qiladi. Qaror topgan sud amaliyotlari tomonidan belgilab qo'yilganidek, missiya uchun hal qiluvchi ahamiyatga ega deb topilgan har qanday narsa bunday darajadagi sinchkovlik va strategik nazoratni talab qiladi.

Buning mohiyati shundaki, tahdidlar haqidagi ma'lumotlarga asoslangan tizim alohida faoliyat olib bormasligi lozim. U kibertahdidlarni boshqarishning kengroq dasturiga uzluksiz integratsiya qilinishi hamda boshqa asosiy komponentlar bilan hamkorlik va muvofiqlashtirishni rivojlantirishga yordam berishi kerak. Bu nafaqat ma'lumotlarga asoslangan boshqaruvni osonlashtiradi, balki bizning keyingi bobimizning asosiy mavzusi bo'lgan tahdidlarga asoslangan strategiyani shakllantirish va amalga oshirish uchun yo'l ochadi.

V BOB. TAHDIDGA ASOSLANGAN STRATEGIYA VA UNING IJROSI

Ushbu kitobda biz tahdid uchun mas'ul shaxslar, xavfsizlik bo'yicha muxassislar va boshqa manfaatdor tomonlarni tasodifiy hodisalarga asoslangan bir martalik yondashuvlar o'rnini bosadigan rasmiy, tizimli jarayonlar to'plamida bir-lashtiradigan CRMP zarurligini ta'kidlab o'tdik. Bu butun korxonaning tez o'z-garuvchan tahdid muhitining muammolarini hal qilishini ta'minlashning hamda o'zini javobgarlikdan himoya qilishga yordam berishning yagona yo'lidir. Ammo korxonaning o'ziga xos ehtiyojlariga mos keladigan dasturni ishlab chiqish va amalga oshirish oson ish emas. Bu aniq belgilangan strategiya va uni izchil amalga oshirishni talab qiladi. Ushbu bob aynan shu masalaga qaratilgan. Biz tahdidga asoslangan strategiya va uni amalga oshirishning oltita asosiy tamoyillarini batafsil ko'rib chiqamiz hamda ularga ta'sir ko'rsatuvchi me'yoriy-huquqiy asoslar va sohaga oid protokollarini bayon qilamiz.

Biz ushbu yuqori darajadagi hamkorlikka asoslangan uzluksiz takomil-lashtirish jarayonida asosiy manfaatdor tomonlarning, xususan, axborot xavfsizli-gi bo'yicha rahbarlarning va boshqa xavfsizlik xodimlarining, shuningdek, ichki va tashqi auditorlarning tutgan o'rnini aniqlaymiz. Bularning barchasini korxona-niing tahdid muhiti va uning tahdidlarni boshqarishdagi strategik ehtiyojlari qan-chalik tubdan va qanchalik tez o'zgarishi mumkinligini yaqinda bo'lib o'tgan ajo-yib misol orqali, ya'ni generativ sun'iy intellektning (AI⁹²) to'satdan jamoatchilik e'tiboriga taqdim etilishi misolida ko'rib chiqamiz.

Raqamli asrda tahdid va foydani muvozanatlash san'ati bo'lgan kibertahdid-larni boshqarish har qachongidan ham murakkablashib bormoqda. Ushbu muam-mo dolzarb va u doimiy ravishda o'sib bormoqda. Shuningdek, biznes muhiti ham, tahdid vaziyati ham doimiy ravishda o'zgarib bormoqda. Ammo haqiqat shundaki, aksariyat korxonalar o'zlarining kibertahdidlarni boshqarish amaliyotiga tizimli tarzda yondashmayapti, bugungi o'ta o'zgaruvchan tahdid muhiti esa buni talab qilmoqda. Bu ularni tasdiqlanmagan tahdid darajalari oldida himoyasiz qilib qo'y-moqda, shuningdek ularni qabul qilishlari kerak bo'lgan tahdidlardan qochishga undashi mumkin. Bu deyarli har doim korxonalarning tahdidlar uchun mo'ljallan-gan byudjetlarini va boshqa resurslarini noto'g'ri taqsimlashiga, ko'pincha kerak bo'lganidan ko'proq yoki kamroq sarflashiga yoki noto'g'ri joylarda va ko'pincha

⁹² AI (artificial intelligence) – sun'iy intellekt, inson intellektiga taqlid qilishga qodir bo'lgan mashina-lar yaratishga qaratilgan fan va texnologiya sohasi.

biznes yo'nalishini belgilamasdan sarflashiga olib keladi. Bu esa rasmiy CRMP ning zarur ekanligini bildiradi.

Aksariyat korxonalarda hech bo'lmaganda tahdidlarni boshqarish amaliyotlari yoki jarayonlari mavjud bo'lib, ko'pchiligi ba'zi ilg'or texnologiyalarni ham joriy qilgan. Biroq kamdan kam korxonalar boshqaruvga ushbu kitobda talab qilingan va huquqiy va tartibga soluvchi organlar tobora ko'proq talab qilayotgan rasmiylashtirilgan, tizimli, butun korxona miqyosidagi tarzda yondashadilar. Tahdidlarni boshqarish sa'y-harakatlari tarqoq holda bo'lib, xavfsizlik tashkiloti, tahdidlarni boshqarish guruhi, tahdid uchun mas'ul shaxslar va boshqa muhim manfaatdor tomonlar faqat ahyon-ahyonda muloqot qilishadi va undan-da kamroq hamkorlikda ishlashadi. Ko'pincha xavfsizlik, tahdidli hodisalar sodir bo'lganidan keyingina, talablarga rioya qilish tekshiruvi yoki tezkor choralar ko'rish to'plami sifatida qabul qilinishi mumkin. Bu shuni anglatadiki, korxonalar, ehtimol, proaktiv tahdidlarni boshqarishga asoslangan qarorlar qabul qilmayaptilar va ular tahdidning maqbul darajalari va ushbu darajalarga erishish bilan bog'liq xarajatlarni hisobga oladigan tahdidlarni boshqarishga asoslangan strategiyani amalga oshirmayaptilar.

Xavfsizlik tashkilotining tahdidlarni boshqarishga asoslangan strategiya va uni amalga oshirishdagi vazifasi – bu tahdidlar bo'yicha mas'ul shaxslar va boshqa manfaatdor tomonlar bilan yaqindan hamkorlik qilib, ularga yordam berishdan iborat. Bunga ularning tahdidga moyillik va chidamliligini aniqlash uchun tahdid haqidagi ma'lumotga asoslangan tizimdan foydalanish orqali erishish mumkin. Shundan keyin, tashkilot ushbu moyillik va chidamlilikka mavjud byudjetlar, xodimlar va vositalar yordamida erishish mumkinligini aniqlay oladi. Agarda ikkinchi maqsadga erishish mumkin bo'lmasa, xavfsizlik xizmati tahdidlar bo'yicha mas'ul shaxsga murojaat qilishi va tahdidga moyillik va chidamlilikni o'zgartirish yoki yangi byudjet ajratish kerakligini tushuntirishi kerak.

Keling, faraziy misolga e'tibor qaratsak. Masalan, elektron tijorat platformasi singari biznes uchun muhim bo'lgan tizimga mas'ul bo'lgan yuqori lavozimli rahbar, axborot xavfsizligi bo'yicha rahbarga "besh to'qqizdan" (99,999%) past bo'lmagan xavfsizlik darajasi maqbul ekanligini hamda tizimning ishlamay qolishiga sabab bo'lishi mumkin bo'lgan tovlamachi-dasturlar va boshqa kiberhujumlardan tizimni to'liq himoya qilish kerakligini aytishi mumkin. Shundan so'ng, axborot xavfsizligi bo'yicha rahbar mavjud bo'lgan xavfsizlik jarayonlari va texnologiyalarini ushbu tahdid chidamliligiga erishish imkoniyatiga ega ekanligini aniqlash uchun baholashi kerak. Ba'zi hollarda ular bunday imkoniyatga ega bo'lmaydi yoki qo'shimcha byudjet talab qilinadi yoki aktiv egasi yuqoriroq tahdid chidamliligini qabul qilishiga to'g'ri keladi. Bunday hollarda, axborot xavfsizligi bo'yicha rahbar aktiv egasiga qayta murojaat qilib, tahdid va foyda muvozanati haqida doimiy va takroriy muhokama o'tkazishi lozim. (Oldingi faraziy misolda, besh-to'qqiz darajadagi xavfsizlik shunchaki erishib bo'lmazligini aniq ko'rsatish

kerak bo'lishi mumkin.) Aktiv egasi, aniqrog'i, tahdid bo'yicha mas'ul shaxs, biz bundan oldingi bobda keltirgan formulaga asoslanib, qiyin qarorlarni qabul qilishi kerak bo'ladi. *Tahdid = Ehtimollik (zaiflikdan foydalanadigan tahdid) x Ta'sir (korxona faoliyati jarayoni, aktivi yoki maqsadiga)*. Barcha ma'lum tahdid omillarini hisobga olgan holda, aktiv egasi kamroq xarajat talab qiladigan himoyaning pastroq darajasi maqbul yoki tizim juda muhim, uni xavf ostiga qo'yish mumkin emas hamda xavfsizlik uchun yangi sarmoyalar zarur degan qaror qabul qilinishi mumkin.

Tahdid haqidagi munozaralar faqat bir kishining bo'ynida bo'lmasligi, shaxsiy munosabatlar yoki hodisalar bilan bog'liq bo'lgan tasodifiy munosabatlarga asoslanmasligi kerakligini anglash muhimdir. Odamlar va vazifalar doimiy ravishda o'zgarib turadi va tahdid bilan bog'liq hodisalar tasodifiy va to'satdan sodir bo'ladi, shuning uchun ikkala haqiqat ham voqea sodir bo'lishidan oldin har bir kishining vazifasi va mas'uliyatini belgilaydigan tizimli yondashuvni talab qiladi. Ushbu yondashuv – biz oldingi ikki bobda muhokama qilgan tahdidlarga asoslangan tizim va moslashuvchan boshqaruv amaliyotiga asoslanishi zarur. Bu juda muhim, chunki hech bir inson, shu jumladan, axborot xavfsizligi rahbari yoki boshqa xavfsizlik idoralari rahbarlari ham xavfsizlik qarorlari uchun javobgar bo'la olmaydi. Bu, shuningdek, tegishli shaxslar byudjet va resurslar to'g'risida vaziyat bo'yicha ma'lumotlarga asoslangan holda qarorlar qabul qilishlarini anglatadi. Axborot texnologiyalari uchun sarflanadigan yangi xarajatlarni oqlash qiyin bo'lishi mumkin: talabni qondirish uchun doim yetarli mablag' mavjud emas va bir sohada sarflanadigan har bir dollar boshqa sohada sarflanmagan dollardir. Bu ayniqsa kiberxavfsizlik sohasiga xosdir, chunki bu sohada tobora yangi tahdidlar va zaifliklar paydo bo'lyapti hamda bu bilan bog'liq korxonaga tegishli tahdidlar yetarlicha tushunilmayapti. Aktiv egasi, axborot xavfsizligi bo'yicha rahbar va ko'p hollarda boshqa manfaatdor tomonlar har qanday yangi resurslar uchun foydalanish tartibini ishlab chiqishlari kerak bo'ladi. Hatto ular yuqori darajadagi tahdid maqbulligi to'g'risida qarama-qarshi xulosaga kelsalar ham, bu qaror ham butun korxona muhitiga asoslangan bo'lishi kerak. Afzalliklar va kamchiliklar hisobga olinishi lozim.

AKTIV EGASI VA MANFAATDOR TOMON O'RTASIDAGI FARQLAR

Aktiv egasi va manfaatdor tomon har biri o'ziga xos mas'uliyat va manfaatlarga ega bo'lgan ikki xil vazifani ifodalaydi. Aktiv egasi – bu ma'lum bir aktivning farovonligi va ishlashi uchun mutlaq mas'uliyatga ega bo'lgan va aktivning to'g'ri saqlanishi, himoya qilinishi va ishlatilishini ta'minlaydigan shaxs yoki tashkilot. Ushbu shaxs yoki guruh ushbu aktiv bilan bog'liq bo'lgan har qanday tahdid uchun to'g'ridan to'g'ri javobgar bo'ladi. Manfaatdor tomon, aksincha, ma'lum bir kibertahdid yoki aktiv bilan bog'liq qaror yoki natijaga ta'sir qilishi, undan manfaatdor bo'lishi yoki unga ta'sir qilish huquqiga ega bo'lgan har qanday shaxs, guruh yoki tashkilotdir.

Manfaatdor tomonlar aktiv ustidan to'g'ridan to'g'ri nazorat qilishlari shart emas, lekin ular uning xavfsizligidan manfaatdor. Masalan, kiberjarayonda kompaniya mijozlarining ma'lumotlar bazasini ko'rib chiqaylik. Ma'lumotlar bazasining xavfsizligini ta'minlaydigan AT direktori aktiv egasi bo'ladi. Bu jarayonda, kompaniyaning mijozlari, xodimlari, aksiyadorlari va hatto tartibga soluvchi organlar manfaatdor tomonlar bo'ladi, chunki ma'lumotlar buzilishi ularga to'g'ridan to'g'ri yoki bilvosita ta'sir qilishi mumkin. Tahdidga asoslangan strategiya va uni amalga oshirishda xavfsizlikning roli – tahdid bo'yicha mas'ul shaxslarga tahdid haqidagi ma'lumotga asoslangan qarorlarni qabul qilishlarida yo'l-yo'riq ko'rsatishdir.

Bu texnologik qarorlar emas, balki biznes qarorlari ekanligini tan olish muhimdir. Xavfsizlikning ushbu jarayondagi o'rni – bu tahdidga mas'ul shaxslar va potensial boshqa ko'plab manfaatdor tomonlarni, shu jumladan, korxona boshqaruv organini, ma'lumotlarga asoslangan tahdid haqida qarorlar qabul qilishga yo'naltirishdir. Barcha aloqador manfaatdor tomonlarning ma'lumotlarini hamda tahdid haqidagi samarali ma'lumotlarni qo'llaydigan hamkorlikdagi yondashuv – korxona sharoitlariga mos keladigan maqbul tahdid darajasini belgilashga imkon beradi. Masalan, CISO tahdid bo'yicha mas'ul shaxsga, ular o'rnatmoqchi bo'lgan qat'iy xavfsizlik texnologiyalari ularning tizimlarini sekinlashtirishi mumkinligini tushuntirishi kerak, bu esa uning ish faoliyatiga ta'sir etishi va innovatsiyalar uchun potensial imkoniyatlarni qo'ldan boy berishiga olib kelishi mumkin.

Ushbu omillar tahdidlarni boshqarishga asoslangan strategiyani ishlab chiqish va uni amalga oshirish jarayonining juda muhimligini anglatadi. Bu har qanday haqiqiy CRMPning asosiy maqsadi bo'lishi kerak. Bu har doim shunday bo'lib kelgan, ayniqsa dunyo jadallik bilan o'zgarayotgan hozirgi vaziyatda. Ushbu o'zgarishlar bilan bog'liq tahdidlar bizlarga shunchalik tez va shiddat bilan yaqinlashib kelmoqdaki, ulardan ortda qolmaslik deyarli imkonsiz bo'lmoqda. Haqiqat shundaki, hatto tahdidlarni boshqarish bo'yicha eng tajribali mutaxassis ham yangi texnologik rivojlanishdan karaxt holatga kelishi mumkin. Ushbu kitobni yozayotganimizda, biz yuqori ta'sirli, yuqori tahdidli va potensial yuqori foyda keltiradigan raqamli o'zgarishlarning ajoyib namunasiga duch keldik.

ChatGPT biznes dunyosini larzaga solmoqda

Korxona biznes muhitidagi doimiy o'zgarishlar e'tiborga olinishi kerak bo'lgan holatlar qatoriga biznes modellaridagi katta o'zgarishlar, kutilmagan yoki noan'anaviy raqobatchilardan kelgan yangi raqobat muammolari, inqilobiy yangi texnologiyalar yoki ularning uchalasi bir vaqtning o'zida kirishi mumkin. 2022-yilning noyabr oyida OpenAI kompaniyasi ChatGPT 3.5 nomli AI vositasini ishga tushirib, uni sinov tariqasida keng jamoatchilikka taqdim etganda shunday hol yuz berdi.

ChatGPT – bu AI vositasi bo'lib, so'rovlarga juda qulay usullarda javob berish uchun katta til modellari, ochiq va xususiy axborot xizmatlari hamda nazorat

qilinadigan va mustahkamlovchi o'rganish usullaridan foydalanadi. Bu amalda shuni anglatadiki, foydalanuvchilar ChatGPTga oddiy, tushunarli ingliz tilida savollar yoki ko'rsatmalar berishlari va xuddi shu tarzda javob olishlari mumkin. ChatGPT latifa aytishi, xayku, ya'ni uch baytli yapon she'rini yoza olishi, o'nlab tillarda tarjima qilishi, kompyuter kodini yaratishi va boshqa ko'plab vazifalarni bajarishi mumkin.

Jamoatchilikning munosabati hayratlanarli edi. ChatGPT mobil telefonlar kashf qilingan davrdan beri har qanday yangi texnologiyadan ko'ra tezroq va zavqliroq qabul qilindi. OpenAI kompaniyasi birinchi ikki oy ichida 100 milliondan ortiq ChatGPT foydalanuvchisi mavjudligini ma'lum qildi va 2023-yil boshiga kelib har kuni 100 million foydalanuvchi undan foydalandi. (Taqqoslash uchun, Instagram 100 million foydalanuvchiga ega bo'lish uchun ikki yarim yil sarflagan.) Albatta, ko'plab odamlar undan shunchaki o'yinchoq sifatida foydalanган, lekin ko'pchilik uni jiddiy vosita sifatida ishlatish imkoniyatini ko'rishdi va biznes ilovalari deyarli darhol paydo bo'la boshladi.

ChatGPT butun dunyoga, shu jumladan, biznesga inqilobiy va oldindan taxmin qilib bo'lmaydigan darajada ta'sir ko'rsatishi boshidan ayon edi. Biznes foydalanuvchilari ChatGPTni darhol korxona hisobotlari va boshqa korporativ aloqa materiallarini yaratish jarayonini soddalashtirish vositasi sifatida ko'rishdi. Dasturchilar uni kodlashda vaqtini tejash usuli sifatida ishlatish boshlashdi (ma'lum bo'lishicha, bu kodlarning ba'zilar noto'g'ri bo'lgan). Tez orada bu kabi asosiy funksiyalar sayoz o'rganilganligi ma'lum bo'ldi. Yakuniy foydalanuvchilar ChatGPT bilan ko'proq tanishib, unga ko'nikib borgan sari, bu vosita uchun yangi foydalanish imkoniyatlari paydo bo'la boshladi va vaqt o'tishi bilan yana ko'plari paydo bo'lishi aniq bo'ldi. Ko'rinib turganidek, kelajakda ChatGPT kabi AI vositalari, kundalik vazifalarni – mijozlarga xizmat ko'rsatish va ma'lumotlarni kiritishni avtomatlashtirish uchun ishlatiladi. Bu xodimlarni qo'shimcha qiymatga ega bo'lgan loyihalarga e'tibor qaratishdan ozod qiladi va katta ma'lumotlar to'plamini batafsil tahlil qilish va natijalar haqida asosli bashorat qilish orqali inson qaror qabul qilish jarayonlarini takomillashtirish imkonini beradi.

AI bilan bog'liq tahdid: Ikki qudratli texnologiya kompaniyalari ikki xil yo'lni tanlaydi

Agar ChatGPT kabi AI vositalarining potensial afzalliklari haqiqiy va oldindan aytib bo'lmaydigan bo'lsa, ular bilan bog'liq xavflar ham shu kabidir. Ularning ba'zilarini ushbu bobning keyingi qismida batafsil ko'rib chiqamiz, ammo hozircha OpenAI raqobatchilarining ayrimlari tomonidan tahdidni hisobga olgan holda qabul qilingan qarorlariga e'tibor qaratmoqchimiz. ChatGPT ommaga e'lon qilingan birinchi yirik AI tashabbusi bo'lib, ammo yagona emas edi. Keling, ularning ikkitasini – Microsoft va Google kompaniyalarini hamda bu ikki raqamli gi-

gantning qabul qilgan qarorlarini ko'rib chiqaylik. Shunisi aniqki, bu ikkala kompaniya hamda boshqa ko'plab kompaniyalar ChatGPTni zudlik bilan foydalanish mumkin bo'lgan imkoniyat yoki jiddiy raqobat tahdidi sifatida ko'rishdi va unga shunday yondashish uchun choralar ko'rishni boshladi. Ammo ular buni butunlay boshqacha yo'llar bilan, tahdidlarni hisobga olgan holda strategik qarorlar qabul qilish orqali amalga oshirishdi.

Microsoft kompaniyasi allaqachon OpenAIga sarmoya kiritgan edi va ChatGPT ishga tushirilgandan so'ng, uni moliyalashtirish uchun yana milliardlab dollar qo'shdi. So'ng 2023-yil fevral oyida (ChatGPT joriy etilganidan ikki oy o'tmay) u sinov asosida o'zining Bing qidiruv tizimiga AI imkoniyatlarini qo'shdi. Tizimni ishga tushirish jarayoni silliq o'tmadi. Bing qidiruv tizimi ChatGPT bilan birga asosiy matematik xatolarga, shu jumladan kompaniyalarning moliyaviy hisobotlarini taqdim etishda xatolarga yo'l qo'ydi. U ba'zi foydalanuvchilarga yil 2023-yil emas, 2022-yil ekanligini ta'kidlagan hamda geografik hududni aytishda xatolikka yo'l qo'ygan. Bundan-da yomoni, ba'zi foydalanuvchilar AI bilan jihozlangan Bing tizimidan foydalanganda haqoratlarga, jumladan, irqiy va etnik haqoratlarga duchor bo'lganliklarini xabar qilishdi. (Microsoft kompaniyasi bu muammoni tuzatganini aytdi, ammo keyinchalik yangi muammoga duch kelinganligi haqida xabar tarqaldi.)

Biz ushbu bobda muhokama qilayotgan masalalarning (ya'ni tahdid va foyda muvozanati) qiziq jihati shundaki, Google o'zining AI qidiruv tizimi taklifini darhol jamoatchilikka taqdim etmadi. Bu, shubhasiz, ChatGPT tahdid sifatida ko'rilmagani uchun emas edi. Xabarlariga ko'ra, Google kompaniyasining ta'sischi kompaniyasi Alphabet buni shu qadar jiddiy qabul qilganki, Google asoschilari Larri Peyj va Sergey Brin uning *DeepMind AI* loyihasini boshqarishni o'z zimmlariga olishdi. Garchi Google ishlab chiqarishda sun'iy intellektga asoslangan *Bard* bilan *LaMDA* deb nomlangan qidiruv tizimiga ega va ko'plab sanoat kuzatuvchilari Google AIsohasida texnik yetakchilikka ega ekanligiga ishonishgan bo'lsa-da, Google kompaniyasi uni darhol ommaga taqdim qilmaslik yo'lini tanladi (Google o'z loyihasini ommaga namoyish etdi va Microsoft kompaniyasining loyihasi kabi, bu loyiha ham muvaffaqiyatsiz kechdi: Googlening sun'iy intellekti ham asosiy moliyaviy hisob-kitoblarda xatoga yo'l qo'ydi va ehtimol, "faktlarni" o'ylab topdi). Buning o'rniga, Google LaMDAni faqat "ishonchli sinovchilar"ga taqdim etishni tanladi va Bardni omma uchun taqdim etishni keyinga surdi.

Xo'sh, bu ikki global texnologiya provayderlarini imkoniyatlar va raqobat tahdidi oldida butunlay boshqacha qarorlar qabul qilishga nima majbur qilgan bo'lishi mumkin? Ikkala kompaniya ham juda badavlat bo'lib, ular cheksiz texnik resurslarga ega va foydalanuvchilarni o'z qidiruv tizimlariga jalb qilishdan manfaatdordirlar. Ammo ular bir-biridan farqli kompaniyalar bo'lib, qidiruv tizimi sohasida turli xil yo'nalishga ega. Shubhasiz, Google dunyodagi yetakchi qidiruv

tizimi bo'lib, u qidiruv tizimi bozorining deyarli 85% ulushiga ega. Microsoft kompaniyasi esa qidiruv tizimi bozorida ikkinchi o'rinni egallaydi, u Google dan ancha orqada bo'lib, bunda Bing ulushi 9% dan kam. Bu degani, qidiruv tizimi Microsoft kompaniyasi faoliyatining muhim tarkibiy qismi emas. Bizning fikrimizcha, ushbu ikki muhim fakt Google va Microsoft kompaniyalarining Chat-GPT ning joriy etilishiga javoban bir-biridan keskin farq qiladigan qarorlari uchun muhim ahamiyatga ega edi. Bu qarorlar, ehtimol, korxona imkoniyatlari va xatarlarini hisobga olgan ma'lumotlarga asoslangan bo'lib, tahdid va mukofotni muvozanatlashtirishning pirovard maqsadiga yo'naltirilgan edi.

NISTning AI bilan bog'liq tahdidlarni boshqarish tizimi

Dunyo bo'ylab hukumatlar AI keltirib chiqaradigan yangi va bashorat qilib bo'lmaydigan tahdidlarga rasmiy yondashuv zarurligini tan olishadi. AQSH hukumatining bu boradagi tashvishi NISTning 2023-yil yanvarida o'zining "AI bilan bog'liq tahdidlarni boshqarish tizimi" RMF 1.0 nashrida va tegishli materiallarda aks ettirilgan. Ushbu tizimda belgilangan funksiyalar (boshqarish, nazorat qilish, xaritalash va o'lgash) turli atamalardan foydalansa-da, ular ushbu kitobda bayon etilgan CRMPning to'rt asosiy tushunchasiga juda mos keladi.

Bunday xulosaga kelishimizning sababi shunday. Ko'p yillar davomida AI va mashina o'rganuvi (machine learning⁹³) texnologiyalarini qo'llagan Googlening qidiruv imkoniyatlari eng yaxshi deb qabul qilingan va kompaniyaning biznes modeli ko'p jihatdan ushbu obro'ni yo'qotmasligiga bog'liq. Agar Google jiddiy kamchilikka ega AI loyihasini joriy qilganida, buning natijasida obro'ga yetkazilgan zarar kompaniya bozor ulushini va u bilan birga muhim reklama daromadlarini yo'qotishiga olib kelishi mumkin edi. Microsoft esa, aksincha, o'z daromadining ko'p qismini qidiruvga mutlaqo aloqasi bo'lmagan sohalaridan oladi va u sun'iy intellektni joriy etish orqali Bingga yo'naltirilgan har qanday tijorat faqat foydali bo'lishi mumkin va ehtimol kompaniyaga jiddiy zarar yetkazmaydi deb qaror qilgan bo'lishi mumkin.

Ehtimol, ikkala kompaniyada ham aniq belgilangan tahdidlar strategiyasi va uni amalga oshirish rejası mavjud bo'lgan, ular o'zlarining Alga oid strategik qarorlarini korxona tahdidini hisobga olgan holda qabul qilgan.

"Uoll-strit" gazetasi: Tez harakat qiling, aks holda sizing o'rningizni boshqalar egallaydi

Biznes uchun juda muhim va alohida e'tiborga loyiq bo'lgan bitta tahdid mavjud. Bu yangilik bo'lmasa-da, bu tahdid raqamlashtirish va ayniqsa AI tufayli keskin tus olmoqda: boshqa narsa bilan almashtirish xavfi. Sodda qilib aytganda,

⁹³ Machine learning – mashina o'rganuvi, bu sun'iy intellekt sohasi bo'lib, kompyuterlarga algoritmlar va katta hajmdagi ma'lumotlardan foydalangan holda inson ko'magisiz ham o'zi o'rganish hamda o'rganan ma'lumotlari asosida bashorat qilish va qaror chiqarish imkoniyatini beradi.

bu korxonaning biznes modeli yoki korxonaning o'zi yangi, tajovuzkor, mutlaqo kutilmagan raqobatchi bilan almashtirilishi yoki uning mahsulotlari yoki xizmatlari eskirishi mumkinligini anglatadi. Uzoq muddatli tadqiqot shuni ko'rsatadiki, "Standard & Poor's" (S&P) 500 indeksida (uzoq vaqtdan beri asosiy bozor ko'rsatkichlaridan biri bo'lib kelgan kompaniya) ro'yxatga olingan kompaniyalarning umr ko'rish davomiyligi bu o'nyillikda 15–20 yilga qisqaradi. Buning sababi, kompaniyalar birlashishi, sotib olinishi yoki butunlay biznesdan chiqib ketishi mumkin. Ba'zi hollarda bu korxonaning haddan tashqari katta yoki noto'g'ri risklarni o'z zimmasiga olganligi tufayli yuz beradi. Ammo shuni tan olish muhimki, ayrim korxonalar raqobatdoshligini saqlab qolish uchun zarur bo'lgan risklarni o'z zimmasiga olmaganligi sababli tugatiladi.

Raqamli asrda korxona tavakkal qilish kerak bo'lgan joyda tavakkal qilmagani yoki lozim bo'lmagan joyda tavakkal qilgani uchun o'z faoliyatini tugatishi mumkin.

Eski korxonalarning tugatilishi va yangilarining yaratilishi natijasida kiber va boshqa turdagi tahdidlar tezlashib kengayadi, ularning aksariyatini hech bir ishonch bilan oldindan aytib bo'lmaydi. Aynan shu noaniqlik korxonalarga aniq belgilangan strategiyalarga asoslangan va aniq belgilangan tamoyillarga muvofiq amalga oshiriladigan rasmiy CRMPga ehtiyoj tug'diradi.

Agar xavfsizlik jamoasi rahbarlarga yaqinlashib kelayotgan tahdidlar haqida xabar bera olsa, o'z ijro imkoniyatlari orqali bu tahdidlarni qanchalik tez aniqlashi va to'xtatishi mumkinligi hamda bu to'xtashlarning kechikish vaqtini bilgan holda muloqot qila olsa, kompaniya tahdid va foyda o'rtasidagi muvozanatni to'g'ri bajarib, raqobatchilaridan tezroq harakat qilishi mumkin. Dasturiy yondashuv bunday puxtalik va tahdidlarni baholash tuzilishi va natijalariga ishonchni ta'minlashga imkon beradi.

Dunyoni o'zgartiruvchi raqamli texnologiyalar paydo bo'lishda davom etmoqda

ChatGPT va bozorda paydo bo'layotgan o'nlab boshqa AI tashabbuslari hozirda barchaning e'tiborini tortmoqda, ammo AI yangi va kutilmagan tahdidlarni keltirib chiqaradigan yagona o'zgartiruvchi va buzuvchi texnologiya emas. McKinsey, xalqaro konsalting kompaniyasi kelgusi 10 yil ichida oldingi asrga qaraganda ko'proq texnologik taraqqiyot bo'lishini bashorat qilib, yaqin o'nyillikda bo'ladigan eng muhim 10 ta texnologik tendensiyani aniqladi:

Jarayonlarni virtuallashtirish va avtomatlashtirish

Robotlar, avtomatlashtirish, 3D chop etish, sanoat internet buyumlari (IIoT) va boshqa texnologiyalar ish tabiatini tubdan o'zgartiradi.

Ulanish kelajagi

5G va IoT orqali amalga oshiriladigan tezkor raqamli aloqalar va keng tarqalgan tarmoqning mavjudligi iqtisodiy faoliyatning raqamlashtirilishi va markazlashmagan tizimga o'tish imkoniyatini oshiradi.

Taqsimlangan infratuzilma

Bulutli hisoblash, ayniqsa gibrid va ko'p bulutli hisoblash, korxona ish faoliyatining tezroq, chaqqonroq va arzonroq bo'lishiga yordam beradi.

Keyingi avlod hisoblashlari

Bu tendensiya kvant hisoblash va avtonom transport vositalari kabi keng ko'lamli texnologiyalarga asoslanib, korxonalarining raqamli imkoniyatlarini keskin darajada oshiradi.

Amaliy AI

MakKinsey kompaniyasining fikriga ko'ra, AI kelajakda juda ko'plab amaliy dasturlarda qo'llaniladi. Shuni unutmash kerakki, u hali o'zining shakllanish bosqichida. Masalan, konsalting kompaniyasi 2024-yilga kelib, odamlarning kompyuterlar bilan muloqotining 50 foizdan ortig'i AI tomonidan yaratilgan nutq orqali amalga oshiriladi deb taxmin qilmoqda.

Dasturlashning kelajagi

Neyron tarmoqlar va mashina o'rganuvi kabi usullar kod yozish jarayonini yanada ko'proq avtomatlashtiradi, bu esa dasturiy ta'minotni yaratishni tezroq, arzonroq va yanada kengaytirilishiga olib keladi.

Ishonchli arxitektura

Ishonchli arxitektura (masalan, blokcheyn kabi taqsimlangan daftarlardan foydalanish) maxfiy ma'lumotlar xavfsizligini yaxshilash uchun ishlatiladi.

"Bio inqilob"

Hayotiy fanlar, jumladan, DNK ketma-ketligi va gen terapiyasi sohasidagi yutuqlar qishloq xo'jaligi va sog'liqni saqlash kabi sohalarga sezilarli ta'sir ko'rsatadi.

Keyingi avlod xomashyosi

Xomashyo sohasidagi yangi kashfiyotlar natijasida oldingilardan baquvvatroq, yengilroq, elektr energiyasini yaxshi o'tkazadigan yangi xomashyolar paydo bo'lmoqda. Natijada ko'plab sohalarda, jumladan, energiya, yarimo'tkazgichlar, transport va ishlab chiqarish sohasida tub o'zgarishlar yuz beradi.

Ekologik toza texnologiya

Qayta tiklanuvchi energiya, tejamkor binolar va elektr transport vositalari kabi ekologik toza texnologiyalar narxining keskin pasayishi, bu texnologiyalarining keng qo'llanilishiga va an'anaviy texnologiya modellarining yanada ko'proq buzilishiga olib kelmoqda.

Tahdidlarni baholashga asoslangan strategiya va uning ijrosi

AI va boshqa raqamli texnologiyalar sababli yuzaga kelayotgan hujumlar va tahdidlarga qarshi kurashishda xavfsizlik o'ziga xos muhim rol o'ynaydi, rasmiy CRMP esa xavfsizlik tashkilotiga ushbu vazifani bajarishi uchun zarur. Tahdidlar bo'yicha mas'ul shaxslarni kibertahdidlarga doir qarorlar qabul qilish jarayoniga yo'naltirish orqali va ularga yangi texnologiyalardan kelib chiqadigan yangi kibertahdidlarni tushunishga yordam bergan holda, dastur belgilangan tahdid chegarasiga asoslangan strategiyani ishlab chiqish va amalga oshirishni rag'batlantiradi. Yana bir muhim jihat shuki, bu o'zaro kelishilgan va asoslangan byudjetni yaratishga imkon beradi, u xodimlar soni va byudjet resurslari, vositalar, tashqi tashkilotlar bilan aloqalar va boshqa masalalar uchun maqsad, yo'nalish va ustuvorliklarni belgilaydi.

Xavfsizlik tahdidlari va zaifliklari – tahdidlarni baholashga asoslangan ijroni amalga oshirganda korxonalar va ularning xavfsizlik bo'linmalari duch keladigan yagona muammo emas. Biznes (va texnik) muhitdagi o'zgarishlar boshqa ko'plab shakllarni qabul qilishi mumkin va ular tahdid omillarining o'sishini anglatmaydi. Aslida, aksincha bo'lishi mumkin. Masalan, yangi xavfsizlik vositasining mavjudligi hal qilinmagan tahdid darajasini pasaytirishi, bartaraf etilmagan zaiflik esa biznes aktivlari yoki operatsion jarayonlarga xavf tug'dirishi va tahdid ta'sirini oshirishi mumkin. Tahdid, umumiy korxona muhiti singari, doimo o'zgarib turadi va bu ayniqsa kibertahdidga tegishli. Bu esa CRMP ko'rinishidagi tahdidlarni baholashga asoslangan strategiya va uni amalga oshirish jarayonini korxonaning omon qolishi uchun juda zarurligini bildiradi.

CRMP tamoyillarining tarkibiy qismlari, tamoyillari va havolalari haqida qisqacha ma'lumot olish uchun *5.1-jadvalga* qarang. *Ilovada* CRMP tamoyillari haqida batafsil ma'lumot berilgan. Keyingi bo'limda biz keng ko'lamli CRMP ning bir qismi sifatida tahdidlarni baholashga asoslangan samarali strategiya va uni amalga oshirish modelini shakllantirish uchun zarur tamoyillarni muhokama qilamiz.

Keng qamrovli CRMP tamoyillari haqida batafsil ma'lumot olish uchun *Ilova*, amalga oshirishning muayyan masalalari bo'yicha ko'proq ma'lumot olish uchun esa *7-bogga* qarang.

**Tahdidlarni baholashga asoslangan
strategiya va uning ijrosi**

CRMP tarkibiy qismlari	Tamoyillar	Ma'lumot manbalari
Moslashuvchan boshqaruv	75-betda "Moslashuvchan boshqaruvning yetti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • NIST 8286 • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • ISO 31000:2018 • AICPAning CRMP
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	94-betda "Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.02.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	120-betda "Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	151-betda "Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • AICPAning CRMP

**Tahdidga baholashga asoslangan strategiya va
uni amalga oshirishning olti tamoyili**

Korxona tahdid muhitining tez sur'atlarda o'zgarishi tahdidlarni boshqarish va ayniqsa kibertahdidlarni boshqarish bo'yicha butunlay yangicha yondashuvni talab qiladi. Qoidalarga rioya qilish yoki korporativ talablarga rioya qilish asosida tashkil etilgan maxsus, tezkor harakatlar va tashabbuslar bugungi va ertaning iqtisodiy, ijtimoiy, siyosiy va texnologik muhitiga mos kelmaydi.

Xavfsizlik tashkiloti korxonalarning tahdidni baholashga asoslangan strategiya va uni amalga oshirishning dolzarb ehtiyojini hal qilishda muhim, hatto hal qiluvchi rol o'ynaydi, ammo u haqiqiy biznes qiymatini yanada ko'proq oshirishi uchun rivojlanishi kerak. Bu boshqaruv organini korxonaning tahdidga moyillik va chidamlilik haqida ma'lumot beruvchi tahdid ma'lumotlari bilan ta'minlashni, so'ngra tahdidlarni bartaraf etishning strategik rejasini va tegishli byudjetni yaratishni anglatadi, bu esa ushbu moyillik va chidamlilikka erishish uchun siyosatni ishlab chiqish imkonini beradi.

Albatta, tahdidni baholashga asoslangan strategiya va uning ijrosini loyihalash hamda amalga oshirishning ko'plab usullari mavjud, ammo ba'zi asosiy tamoyillarga doimo amal qilinishi kerak. Keling, shularni ko'rib chiqaylik.

1-TAMOYIL: MAQBUL TAHDID CHEGARALARINI ANIQLASH

Maqbul kibertahdid chegaralari tahdid tizimi va metodologiyasiga asoslanib, tahdid bo'yicha mas'ul shaxslar tomonidan aniq tushunilishi, belgilanishi va tasdiqlanishi zarur.

Oldingi bobda biz tahdidga moyillik va chidamlilik nuqtayi nazaridan maqbul tahdid darajasini aniqlash metodologiyasini yaratishning muhim ahamiyatini muhokama qildik. Boshqaruv organi bilan hamkorlikda ishlab chiqilgan kelajakdagi maqbul tahdidlarni aniqlash – korxonaning o'zgaruvchan va yuzaga keladigan xavf-xatarlarni boshqarish bo'yicha sa'y-harakatlariga ustuvorlik berish imkonini beradi. Biroq, tahdidlarni baholashga asoslangan samarali strategiya va uning ijrosi, ya'ni tahdidlarni boshqarish korxonaning strategik maqsadlariga erishish uchun haqiqatan ham samarali ishlayotganini ta'minlash – muayyan tahdid bo'yicha mas'ullarning ushbu jarayonda aniq rol o'ynashini talab qiladi. Joriy holat haqida tushunchani hosil qilish uchun, avvalambor tahdid bo'yicha mas'ullar bilan ishlashdan boshlash lozim. Barcha manfaatdor tomonlar o'zlarining hozirgi holatlarini tahdid va uni bartaraf etish uchun ko'rilyotgan choralar nuqtayi nazaridan tushunib yetgandan keyingina, ular kelajakdagi haqiqiy holatni tasvirlashni boshlashlari mumkin.

Tahdid bo'yicha mas'ullar – bu ma'lum bir korxona aktivi uchun mas'ul bo'lgan shaxslar, biznes yo'nalishidagi rahbarlar, yuqori lavozimli rahbarlar yoki hatto direktorlar kengashi bo'lishi mumkin. Ularning vazifasi qanday bo'lishidan qat'i nazar, ular ma'lum bir tahdidga oid qarorda nima e'tiborga olinayotganini aniq tushunishlari shart, shunda tahdid va foyda o'rtasidagi tegishli muvozanatni aniqlash mumkin bo'ladi. Misol uchun, tahdid bo'yicha mas'ullar kiberhujum natijasida yuz berishi mumkin bo'lgan ish to'xtatishining potentsial qiymati va bunday hujumning oldini olish uchun zarur bo'lgan chora-tadbirlar xarajatlari to'g'risida qaror qabul qilishlari mumkin. Bu borada xavfsizlik xizmatining vazifasi yo'l-yo'riq ko'rsatish va tahdid bo'yicha mas'ullar tegishli chidamlilikni belgilash

da asosli qarorlar qabul qilishlari uchun zarur ma'lumotlarga ega bo'lishlarini ta'minlashdir.

Ushbu standartlarning barchasi shuni aniq ko'rsatadiki, tahdidni butunlay bartaraf etish imkonsizdir, shu sababli, tahdid va foyda o'rtasida to'g'ri muvozanatni o'rnatish muhim bo'lib, faqatgina tahdid bo'yicha mas'ullargina buni aniqlay olishadi. Ular buni xavfsizlik tashkiloti rahbarligi ostida takrorlanadigan va aniq natijalarga ega tahdidga moyillik va chidamlilik metodologiyasi asosida amalga oshirishlari mumkin. Ushbu natijalar strategik ijroni ta'minlash uchun yetarlicha aniq bo'lgan atamalarga o'girilishi lozim.

Tahdidga moyillik va chidamlilik tahdid bo'yicha mas'ullar tomonidan aniq tushunilgan va o'rnatilgandan so'ng, ular tegishli boshqaruv darajasida (ko'pincha ijro etuvchi rahbariyat tomonidan) tasdiqlanishi lozim. Bu joriy va kelajakdagi chidamlilik darajasini belgilaydigan hamda zarur byudjet va boshqa resurslarni asoslovchi imkoniyat modellarini yaratishga o'tish imkonini beradi.

Byudjet har doimgidek eng muhim masala hisoblanadi. Xarajat uchun mablag'lar miqdori cheklangan bo'lib, ko'p hollarda kibertahdid masalalari uchun zarur mablag'lar boshqa sohalaridan olinishiga to'g'ri keladi, masalan, marketing, tadqiqot va rivojlanish yoki xavfsizlik sohalaridan. Lekin shuni tan olish joizki, kibertahdidning biz xohlagan kelajak holatini yaratish uchun (yangi xavfsizlik choralari yoki yangi texnologiyalar uchun) ko'proq pul sarflash shart emas. Bu aslida, korxona yuqori darajadagi tahdidni maqbul deb qaror qilganini hamda kam byudjet mablag'lari boshqa joyga sarflanishi mumkinligini anglatishi mumkin.

Tahdidlarni hisobga olgan holda byudjetlashtirish strategik ahamiyatga ega bo'lib, uni korxonaning tahdid va foyda muvozanatini topishiga yordam berish g'oyasidan ajratib bo'lmaydi. Korxonalar ko'pincha birinchi navbatda tahdid byudjetini tuzadilar, keyin undan xodimlar soni va zarur asbob-uskunalarni aniqlash uchun foydalanadilar. Bu ishlarni teskari tartibda bajarishning an'anaviy holati hisoblanadi. Ba'zan byudjet AT umumiy byudjetining foiziga asoslanadi yoki u o'tgan yilga nisbatan belgilangan foizni yoxud yana bir tahdidni bartaraf etish uchun qo'shimcha vositaning narxiga asoslanadi. Bunday qarorlarning barchasi korxonaning aniq belgilangan chidamlilik darajasini hisobga olmasdan qabul qilinadi.

Ushbu tamoyil bir nechta kiberga oid maxsus standartlar va protokollar bilan boshqariladi va qo'llab-quvvatlanadi, jumladan:

NACDning 2023-yilgi direktorlar qo'llanmasi, 1-tamoyil

Kiberxavfsizlikni "strategik tahdid" sifatida ko'rish uchun, uni boshqarishda biznes tomonidan tasdiqlangan aniq asos va tahdid chegaralari bo'lishi kerak ("Tahdidlar haqidagi ma'lumotlarga asoslangan tizim"ning 1-tamoyilida belgilanganidek). Boshqacha qilib aytadigan bo'lsak, tahdidning qaysi darajasi maqbul ekanligi to'g'risida strategik qaror qabul qilish tahdid bo'yicha mas'ullarning qo'lida. Ushbu yondashuv kiberxavfsizlikka oid tahdidlarni nafaqat texnik muam-

mo, balki tashkilot faoliyatiga va maqsadlariga sezilarli ta'sir ko'rsatishi mumkin bo'lgan strategik muammo sifatida ko'rib chiqilishini ta'minlaydi.

NISTning 2023-yilgi kiberxavfsizlik asoslari GV. RM-02 loyihasi

Ushbu kichik turkum tashkilotning tahdidga moyilligi va chidamliligini aniqlash hamda ular haqida xabar berishni anglatadi. Bu korxona muhitining o'ziga xos sharoitlaridan kelib chiqqan holda, tashkilot uchun maqbul bo'lgan tahdid chegaralarini belgilashni o'z ichiga oladi.

2-TAMOYIL: STRATEGIYA VA BYUDJETNI MAQBUL TAHDID CHERGASI BILAN MUVOFIQLASHTIRISH

Kibertahdidni bartaraf etish rejasi va byudjeti – tasdiqlangan tahdid chegarasi bilan muvofiqlashtirilishi kerak.

Tahdidga moyillik va chidamlilik aniq o'rnatilgan va tasdiqlanganidan so'ng, ko'zlangan kelajak holatiga erishish uchun strategiya ishlab chiqilishi lozim. Tahdid va foyda o'rtasidagi muvozanatni saqlash zarurati cheklangan tahdid resurslarini boshqarish va ulardan maksimal darajada foydalanishni o'ta muhim masalaga aylantiradi. Bunda xavfsizlik tashkiloti muhim vazifani bajaradi. U tahdidlarni boshqarish strategiyalarini baholash, loyihalash, amalga oshirish va nazorat qilish bilan shug'ullanadi. Bu jarayonlarga nafaqat tahdid ta'sirini kamaytirish, ularni uzatish va qabul qilish, balki tahdid oldi qabul qilish jarayonlari, balki tahdidan keyingi tahlilni ham o'z ichiga oladi.

Har bir tahdidga oid qaror deyarli har doim moliyaviy ta'sirga ega, bu esa tahdidga oid asosiy qarorlarni qabul qilishda har doim moliya bo'limi rahbari (CFO⁹⁴) yoki boshqa yuqori darajadagi moliyaviy qaror qabul qiluvchi shaxslar ishtirok etishi kerakligini anglatadi.

Yana bir bor ta'kidlash joizki, byudjetlar hal qiluvchi omil bo'ladi va bu xavfsizlik tashkiloti rahbariyati korxona biznes maqsadlarini tahdidlar strategiyasi, xavfsizlik amaliyotlari va mavjud resurslarning umumiy portfeli va pirovardida korxonaning biznes ehtiyojlari bilan moslashtirish uchun rahbarlar yoki boshqaruv organi bilan yaqindan hamkorlik qilishi kerakligini anglatadi. Zamonaviy korxonalarning murakkabligini hisobga olgan holda, biznes strategiyasiga moslashish qiyin bo'lishi mumkin. Misol uchun, bir nechta yirik kompaniyalar birlashish yoki sotib olish jarayonidan keyin tegishli tekshiruvni amalga oshira olmagan uchun juda zararli kiberhujumlarga duch kelishdi, bu esa muqarrar ravishda korxonaning tahdid muhitini o'zgartiradi.

⁹⁴ CFO (Chief financial officer) – moliya bo'limi rahbari.

Xavfsizlik biznesning uzluksizligi va favqulodda vaziyatlarni bartaraf etish, xavfsizlik operatsiyalari markazi (SOC⁹⁵) va umumiy AT tashkiloti imkoniyatlari va uchinchi tomon vakolatlari kabi masalalarni ko'rib chiqishi uchun tahdid bilan bog'liq boshqa operatsion vazifalar bilan moslashtirilishi kerak. Tahdidlarning ustuvorligini belgilash va ularni bartaraf etish choralari butun jarayon davomida hisobga olinishi va baholanishi lozim. Ushbu qarorni qabul qilishda asosiy omil vaqt bo'ladi: korxona uzoq muddatli strategiyani tanlashi mumkin (masalan, x yil davomida tahdid darajasini x million dollarga kamaytirish to'g'risidagi qarori), ammo u zudlik bilan hal qilishni talab qiladigan jiddiy tahdidga duch kelishi mumkin. Bularning barchasi faqat tasdiqlangan tahdid darajalariga to'liq mos keladigan holda qabul qilinishi mumkin bo'lgan qarorlardir va ularning barchasi moliyaviy oqibatlariga olib keladi. Korxona hech bo'lmaganda yillik tekshiruv o'tkazib, operatsion va kapital xarajatlarda qanday o'zgarishlar kiritilishi kerakligini aniqlashi kerak. Biroq, kibertahdidning o'zgaruvchan tabiati, muqarrar ravishda tezkor choralar ko'rishni va tuzatishlar kiritishni talab qiladi.

Bir qator standartlar (ba'zilar, ammo hammasi ham kiberxavfsizlikka tegishli emas) ushbu tamoyilga tegishli, ular jumlasiga quyidagilar kiradi:

NISTning 2023-yilgi kiberxavfsizlik asoslari 2.0 GV. RM-04 loyihasi

NIST tegishli tahdidlarga javob berish variantlarini o'z ichiga olgan strategik yo'nalishni belgilash va uni yetkazishga alohida e'tibor qaratadi. Ushbu variantlarga sug'urta, tahdidlar ta'sirini kamaytirish uchun sarmoya kiritish, tahdidlarning oldini olish va ularni qabul qilish kabi tahdidlarni boshqa tomonga o'tkazish mexanizmlari kirishi mumkin, bularning barchasi kiberxavfsizlik uchun ajratilgan byudjetga mos kelishi kerak.

Kibertahdidlariga qarshi chora ko'rish turlari uchun 5.2-jadvalga va tahdidga qarshi chora ko'rishning namunaviy sxemasi uchun 5.1-chizmaga qarang.

NACDning 2023-yilgi direktorlar qo'llanmasi, 1-tamoyil

Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning 1-tamoyili singari, NACDning 1-tamoyilida ham maqbul tahdid chegaralarini strategik tushunish va shunga mos ravishda kiberxavfsizlik tartib-qoidalarini moslashtirish zarurligi ta'kidlanadi. Tashkilotning butun kiberxavfsizlik strategiyasi maqbul tahdid chegaralari bo'yicha qabul qilingan qarorlar asosida shakllantiriladi. Bu kiberxavfsizlikning strategik tabiatini ko'rsatadi, chunki u tashkilotning kiberxavfsizlikka oid strategik qarorlari va sarmoyalari ular qabul qilishga tayyor bo'lgan xavf darajasiga mos kelishi zarurligini tan oladi.

ISO 31000 6.5.1, 6.5.2

ISOning ushbu standarti tahdidni bartaraf etishning maqsadini – tahdidlarga qarshi chora ko'rish variantlarini tanlash va uni amalga oshirish sifatida belgilaydi,

⁹⁵ COC (Security Operations Center) – xavfsizlik operatsiyalari markazi.

bu jarayon variantlarning potensial foydalarini ularni amalga oshirish xarajatlari, sa'y-harakatlari yoki kamchiliklari bilan muvozanatlashtirishni o'z ichiga oladi.

AICPAning 2017-yilgi CRMP tavsif mezonlari, DC17

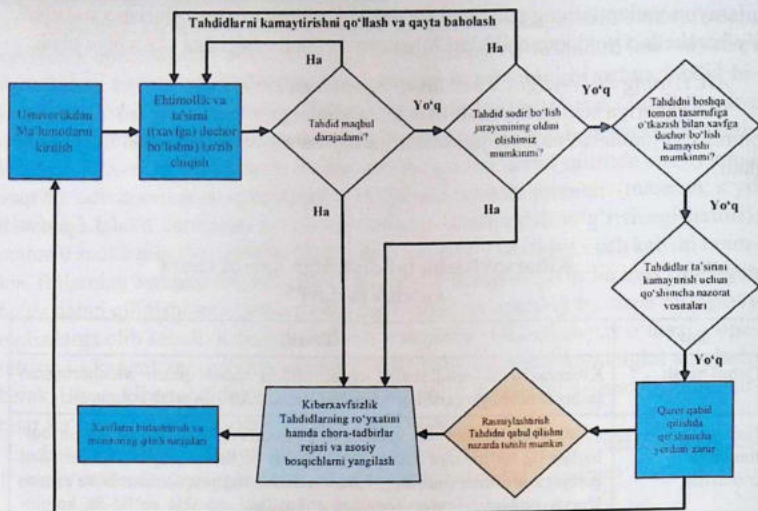
Buxgalteriya standartlari baholangan tahdidlarga nisbatan chora ko'rish jarayonini, shu jumladan nazorat jarayonlarini loyihalash va amalga oshirishni talab qiladi.

5.2-jadval

Kiberxavfsizlik tahdidlariga qarshi chora ko'rish turlari⁹⁶

Tur	Tavsif
Qabul qilish	Kiberxavfsizlik tahdidlariga chidamlilikni qabul qilish. Monitoringdan tashqari tahdidga qarshi qo'shimcha choralar ko'rish talab etilmaydi.
Boshqa tomonga o'tkazish	Chidamlilik darajasidan oshadigan kiberxavfsizlik tahdidlari uchun oqibatlarining bir qismini boshqa tomon bilan bo'lishish orqali ularni maqbul darajaga tushirish (masalan, kiberxavfsizlik sug'urtasi). Garchi ba'zi moliyaviy oqibatlar boshqa tomonga o'tkazilishi mumkin bo'lsa-da, ko'pincha shunday oqibatlar borki, ularni boshqa tomonga o'tkazib bo'lmaydi, mijozlarning ishonchini yo'qotish shular jumlasidandir (ba'zan <i>Bo'lishish</i> deb yuritiladi).
Ta'sirini kamaytirish	Tahdidning zaif tomonlari va ta'sirini maqbul darajagacha kamaytiradigan choralarni qo'llash (masalan, 3.5.1-bo'limda muhokama qilingan xavfsizlikning nazorat vositalari). Choralar o'z ichiga zararining oldini olishga yordam beradigan (ya'ni tahdid hodisasining sodir bo'lishi yoki muvaffaqiyatli bo'lish ehtimolini kamaytirish) yoki zarar va javobgarlikni kamaytirish orqali bunday yo'qotishlarni cheklashga yordam beradigan harakatlarni o'z ichiga olishi mumkin.
Oldini olish	Tahdidni keltirib chiqaradigan faoliyat yoki sharoitlarni bartaraf etish bo'yicha choralar ko'rish. Agar kiberxavfsizlik tahdidini maqbul darajagacha kamaytirish uchun iqtisodiy jihatdan samarali usul mavjud bo'lmasa, tahdidning oldini olish eng yaxshi tanlov bo'lishi mumkin. Bunday qaror bilan bog'liq bo'lgan yo'qotilgan imkoniyatning qiymati ham hisobga olinishi kerak.

⁹⁶ Manba: Kevin Stayn, Stiven Kvinn, Greg Vitt, R. K. Gardner, "Kiberxavfsizlik va korxona tahdidlarini boshqarishni integratsiyalash", NISTIR 8286, 2020-yil oktyabr.



5.1-chizma. Tahdidga qarshi chora ko'rish sxemasi⁹⁷

3-TAMOYIL: MAQBUL TAHDID CHEGARALARI DOIRASIDA IJRO

Kibertahdidlarni bartaraf etish rejasi tasdiqlangan tahdid chegaralariga muvofiq amalga oshirilishi lozim.

Muayyan tahdidlarni bartaraf etishning strategik rejasini amalga oshirish (qo'llaniladigan jarayonlar, mexanizmlar, texnikalar va vositalarni kunlik boshqarish) korxona tomonidan belgilangan chidamlilik darajasiga erishishga qaratilgan rejani tuzish va tasdiqlash jarayoni kabi rasmiy va tizimli bo'lishi kerak. Bu tahdidlarni tartibga solish jarayonining dolzarb bo'lib qolishiga va o'rnatilgan tahdid va nazorat tizimiga mos kelishiga, tahdidlarni baholash va auditning faol bo'lib qolishiga hamda joriy tahdid va kamchiliklarga mos kelishiga imkon beradi. Bu belgilangan vaqt va byudjet doirasida kerakli chegaralarga erishish demakdir.

⁹⁷ Manba: Kevin Stayn, Stiven Kvinn, Greg Vitt, R. K. Gardner. Kiberxavfsizlik va korxona tahdidlarini boshqarishni integratsiyalash.

Kibertahdid va sug'urta

Tahdidlarga oid qarorlar qabul qilishda ko'p asrlik tajribaga ega sohalaridan biri sug'urta sohasidir. Yuqori ixtisoslashgan bu soha kibertahdidni sinchkovlik bilan o'rganmoqda va ko'rayotgan narsalardan xursand emas. Misol uchun, tovlamachi dasturlari va boshqa kiberhujumlar natijasida yuzaga kelgan tizimdagi uzilishlar xarajatlarini qoplaydigan kibernug'urta polislarini sezilarli qoplovchi imtiyozlari bilan, juda yuqori mukofotlarni o'z ichiga oladi, buning sababi shundaki, sug'urtachilar tashkilotning tahdidga duchor bo'lish darajasini aniqlash uchun zarur bo'lgan ma'lumotlarga ega emaslar (bundan farqli o'laroq, hayotni sug'urtalash bo'yicha sug'urta mukofoti millionlab ma'lumotlar asosida hisoblanishi mumkin). Natijada, ko'pgina korxonalar kibersug'urta juda qimmat degan xulosaga kelishadi va tahdidlarni boshqarish bo'yicha maqsadlarga erishish uchun o'zlarining cheklangan resurslarini boshqa joylarga sarflashni afzal ko'rishadi.

Ijro bilan bog'liq jarayon komponentlari xavfsizlik hodisalarining oldini olish, aniqlash va ularga chora ko'rish, shuningdek, favqulodda hodisalar sodir bo'lganda ulardan keyin tiklanish faoliyati va imkoniyatlarni boshqarishni (masalan, ofatlardan keyingi tiklanish) o'z ichiga oladi. Ammo ular yuqori ahamiyatga ega aktivlarni aniqlash va korxona faoliyatidagi muhim o'zgarishlarni belgilashga ham taalluqli, shuningdek, qonunlar, me'yoriy hujjatlar va boshqa majburiyatlarning tahdidlarni tartibga solish faoliyatiga qo'llash mumkinligini ham o'z ichiga oladi. Har doimgidek, bu jarayon operatsion tahdidlarni boshqarishning yaxlit tizimi yoki umumiy xavfsizlik xavfini boshqarish tuzilmasi doirasida amalga oshirilishi lozim. Bu tezkorlikni talab qiladi, chunki, ko'p marotaba ta'kidlanganidek, biznesning ehtiyojlari va tahdidlari juda tez va keskin darajada o'zgarib turadi. Byudjet o'zgarmas narsa bo'lib tuyulishi va yillik byudjetni boshqarish, shubhasiz, muhim maqsad hisoblanishi mumkin. Lekin, aslida byudjet ma'lum bir vaqtning aksi bo'lishi lozim, tahdidlarni boshqarishga asoslangan ijro modeli bilan esa u moslashuvchan bo'lishi kerak.

Tahdidlarni boshqarishni strategik amalga oshirish bo'yicha tegishli standartlar va protokollar quyidagilarni o'z ichiga oladi:

NISTning 2023-yilgi kiberxavfsizlik asoslari 2.0 GV. RR-03 loyihasi

Ushbu subkategoriyada kiberxavfsizlik tahdidlari bo'yicha strategiy va majburiyatlarga hamda ko'riladigan choralarga mos keladigan yetarli ajratilishi ta'kidlanadi.

ISO 31000 6.5.3

ISO standartining ushbu qismi tahdidni tartibga solish rejalarini shakllantirish va amalga oshirishning mantiqiy asoslarini belgilaydi. Maqsad – manfaatdor tomonlar o'rtasida yagona tushunchani ta'minlash uchun tanlangan tartibga solish strategiyalarini aniq ifodalashdir. Bu jarayonni nazorat qilishni osonlashtiradi va tahdidlarni tartibga solish jarayonini amalga oshirish ketma-ketligini aniq belgilaydi hamda ijroda aniqlik va uyg'unlikni ta'minlaydi.

4-TAMOYIL: DOIMIIY RAVISHDA NAZORAT QILISH

Kibertahdidlarni bartaraf etish rejasining ijrosi belgilangan samaradorlik ko'rsatkichlari va operatsion mezonlar asosida doimiy ravishda nazorat qilib borilishi lozim

Aniqlangan tahdid va samaradorlik ko'rsatkichlari hamda operatsion mezonlar yordamida tahdidlarni kamaytirish samaradorligini doimiy ravishda ko'rib chiqish, biznes maqsadlarini aniqlangan tahdidlar bilan muvozanatlash, tahdidga asoslangan muvaffaqiyatli strategiya va ijro uchun juda muhim ahamiyatga ega. Ushbu monitoring jarayoni boshqaruv organi tomonidan nazorat qilinadi, tasdiqlangan va qabul qilingan asosiy samaradorlik ko'rsatkichlari (KPI⁹⁸) va asosiy tahdid ko'rsatkichlari (KRI⁹⁹) kabi muhim ko'rsatkichlardan foydalanilgan holda belgilangan vaqt oralig'ida amalga oshiriladi. Ushbu jarayon odamlar, jarayonlar va texnologiyaning qabul qilinadigan tahdid parametrlari doirasida samarali ishlashini ta'minlaydi. U o'zgaruvchan tahdid portfeli asosida resurslarni mos va moslashuvchan taqsimlash orqali tahdid muhitidagi o'zgarishlarni oldindan ko'ra bilishga va ularga moslashishga imkon beradi. Doimiy nazorat umumiy muhitdagi o'zgarishlarni, shuningdek yangi biznes operatsiyalari va maqsadlari, yangi tahdidlar, yangi texnologiyalar va tahdid ta'sirini kamaytirishning yangi strategiyalarining paydo bo'lishini aniqlash va ularga javob berishga imkon beradi. Shuningdek, u xavfsizlik dasturining doimiy o'zgaruvchan tahdid darajalariga moslashishga imkon beradi, bu esa tahdidga chidamlilik darajasi uchun zarur bo'lgan o'zgarishlarni keltirib chiqarishi mumkin. Keyinchalik bunday o'zgarishlar korxona boshqaruv organiga va barcha manfaatdor tomonlarga tegishli ravishda yetkazilishi kerak.

Ushbu tamoyilga tegishli bo'lgan sohaga doir standartlar quyidagilarni o'z ichiga oladi:

NACDning 2023-yilgi direktorlar qo'llanmasi, 5-tamoyil

NACDning ushbu tamoyili kiberxavfsizlik samaradorligini hisobga olish va nazorat qilish uchun doimiy, tizimli yondashuv zarurligini ta'kidlaydi, bu tashkilotlarga asosli qarorlar qabul qilish, kerak bo'lganda strategiyalarni moslashtirish va tahdidlarni tartibga solish rejalari samarali bajarilishini ta'minlash imkonini beradi. Bunday muvofiqlik kiberxavfsizlik tahdidlarini boshqarish va ishonchli hamda barqaror mudofaa pozitsiyasini saqlab qolishda o'lchash va hisobot berishning ahamiyatini ta'kidlaydi.

⁹⁸ KPI (A key performance indicator) – asosiy samaradorlik ko'rsatkichlari.

⁹⁹ KRI (A key risk indicator) – asosiy tahdid ko'rsatkichlari.

NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi, 2.0 GV.OV-01 dan 03 gacha

Ushbu subkategoriyalar kiberxavfsizlik tahdidlarini boshqarish strategiyasi va uning natijalarining samaradorligi va yetarliligini baholash va ko'rib chiqish jarayonini ichiga oladi. Ushbu jarayon strategiyani amalga oshirishni nazorat qilish va moslashtirish jarayonining ajralmas qismi hisoblanadi.

AICPAning 2017-yilgi CRMP tavsif mezonlari, DC15, DC16

Buxgalteriya hisobiga yo'naltirilgan ushbu standartlar asosiy boshqaruv vositalari va kiberxavfsizlik bilan bog'liq boshqa komponentlarning ishlash samaradorligini doimiy va davriy baholash jarayonlarini tavsiflaydi. Ushbu standartlar, shuningdek, xavfsizlikka tahdidlar, zaifliklar va nazorat kamchiliklarini baholaydi va ularni tuzatish choralari ko'rish uchun mas'ul tomonlarga yetkazadi.

5-TAMOYIL: TAHDIDNING CHEGARAVIY DARAJALARIGA NISBATAN AUDIT TEKSHIRUVI

Audit xizmati tahdidning tasdiqlangan chegaraviy darajalariga asoslangan kibertahdidni bartaraf etish rejasining to'g'ri bajarilishini ko'rib chiqishi va baholashi kerak.

Uchinchi bobda aniqlangan uchinchi himoya chizig'i bo'lgan audit xizmati korxonaning kibertahdid strategiyasini uning umumiy biznes strategiyasiga muvofiqligini ta'minlashda, ayniqsa, tahdidlarni bartaraf etish rejasining belgilangan tahdidga moyillik va chidamlilik darajalariga mos kelishini ta'minlash uchun juda muhimdir. Tahdidlarni boshqarish rejasini va uning bajarilishini doimiy va davriy tekshirish CRMPning to'g'ri ishlashini va uning belgilangan tahdid doirasida bajarilishini ta'minlaydi.

Audit faqatgina korxonalarning tahdidlarni bartaraf etish rejasini belgilagan eng yaxshi amaliyot va boshqaruv standartlari bilan taqqoslab o'lchash bilan kifoyalanmaydi. Audit xizmati, shuningdek, korxonaning umumiy tahdidlarni boshqarish dasturi manfaatdor tomonlarga tahdidlar haqidagi ma'lumotlarni hisobga olgan holda strategik qarorlar qabul qilish uchun zarur bo'lgan ma'lumotlarni yetarlicha aniq darajada taqdim etyaptimi yoki yo'qligini aniqlashi lozim. Ushbu bo'linma, shuningdek, tahdid va foyda o'rtasidagi to'g'ri muvozanatning tegishli darajalarda o'rnatilishi va qabul qilinishini ta'minlaydi. Ijroni nazarda tutadigan bo'lsak, audit ham xavfsizlik tashkiloti, ham tahdid uchun mas'ullar tahdidning belgilangan chidamlilik darajalari doirasida qolishlarini, chidamlilikni amalga oshirish o'z vaqtida va moslashuvchan bo'lishini hamda tahdid uchun ajratilgan byudjet tahdidning aniqlangan omillariga asoslanganligini tasdiqlashi kerak.

Sohaga doir standartlarning ikkita asosiy to'plami audit xizmatiga alohida taalluqlidir:

AICPAning 2017-yilgi CRMP tavsif mezonlari

Audit bilan bog'liq faoliyatga qiziqish ko'rsatayotgan AICPA tashkiloti, CRMPni ko'rib chiqish, baholash va tavsiflash uchun foydalanish mumkin bo'lgan tizimni belgilab beradi.

IIAning 2020-yilgi Uch chiziqli himoya modeli, 4-tamoyil

Ushbu tamoyil ichki auditning tizimli jarayonlar orqali doimiy takomillash-tirishdagi rolini ta'kidlaydi, bunda tahdidlarni tartibga solish rejalarining to'g'ri bajarilishini nazorat qilish hamda tahdidlarni izchil va samarali boshqarishni rag'batlantirishga urg'u beradi.

6-TAMOYIL: TAHDIDLARNI BARTARAF ETISH REJASIGA UCHIN-CHI TOMONLARNI KIRITISH

Kibertahdidlarni bartaraf etish rejasi uchinchi tomonlarni, jumladan hamkorlar, ta'minotchilar va ta'minot zanjiri ishtirokchilarini hisobga olishi kerak.

Bugungi tadbirkorlik muhitida korxona uchinchi tomon subyektlari, shu jumladan hamkorlar, ta'minotchilar, logistika bo'yicha xizmat ko'rsatuvchilar va ta'minot zanjirining boshqa ishtirokchilari, ba'zan hatto raqobatchilar bilan murakkab ish munosabatlariga ega bo'ladi. Bu korxona doirasidan tashqariga chiqadigan tahdidni bartaraf etish strategiyasini talab qiladi. Korxonaning ushbu uchinchi tomonlar bilan munosabatlari uni keng ko'lamli xavflarga duchor qiladi: ta'minot zanjiridagi nosozliklardan tortib, intellektual mulkning oshkor bo'lishi, hamkorning axloqsiz xatti-harakatlari tufayli obro'siga putur yetkazishi va hokazo. Aslida, ko'plab korxonalar uchun eng katta xavf manbayi aynan uchinchi tomonlar hisoblanadi, chunki korxonalarning uchinchi tomonlarning faoliyatini kuzatish imkoniyati ko'p emas. Ushbu tahdidlar butun ekotizimni qamrab oladigan tahdidni bartaraf etishning keng qamrovli strategiyasi orqali boshqarilishi kerak.

Uchinchi tomon kiberxavfsizlik tahdidining yorqin namunasi 2020-yil sodir bo'ldi. Rossiya hukumati tomonidan qo'llab-quvvatlanayotgani taxmin qilingan keng ko'lamli kiberhujum butun dunyo bo'ylab minglab davlat va xususiy sektor subyektlariga kirib bordi. Xakerlar AQSHda joylashgan AT boshqaruvi dasturiy ta'minotining muhim provayderi bo'lgan SolarWinds tizimiga buzib kirishdi va uning Orion platformasiga zararli kodni joylashtirishdi. Bu kod kompaniyaning o'n minglab mijozlariga muntazam dasturiy yangilanishlar orqali tarqaldi. Kod mijozlarning tizimlarida g'ayriqonuniy yo'l yaratdi, bu xakerlarga Boeing, Microsoft, VMWare kompaniyalari, Shimoliy Atlantika shartnomasi tashkiloti, AQSH kasalliklarni nazorat qilish markazlari va Yevropa parlamenti kabi ko'plab tashkilotlardan maxfiy ma'lumotlarni olish imkonini berdi. Hujum natijasida yetkazilgan zararning to'liq hajmi hali aniq emas (hukumat va korpo-

rativ maxfiylik tufayli), Solar-Winds kompaniyasi taxminan 18,000 ga yaqin mijozni xavfli dasturiy ta'minotni yuklab olganini ma'lum qildi.

Ushbu so'nggi statistik ma'lumotlarning o'zi kibertahdidni boshqarish bilan shug'ullanadigan har qanday shaxsni sergak bo'lishga undashi kerak. Bitta korxonaga qilingan hujum minglab boshqa korxonalarga potensial zarar yetkazishi aniq bo'lsa, uchinchi tomon bilan bog'liq tahdid korxona va uning boshqaruv organlari tomonidan jiddiy masala sifatida tan olinishi va uning CRMP tomonidan ko'rib chiqilishi kerakligini ko'rsatadi.

Ko'pgina korxonalarning eng katta tahdid manbayi – bu ularning uchinchi tomon bilan aloqasidir.

Bir qator standartlar to'plami uchinchi tomon/ta'minot zanjiri tahdidlarini boshqarishning o'ziga xos muammosini hal qilishga qaratilgan:

NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi, 2.0 GV. SC , ID.IM-02

NISTning "Kiberxavfsizlik ta'minot zanjiri tahdidlarini boshqarish" turkumi, shuningdek, "Takomillashtirish" 02 subkategoriyasi tahdidlarni tartibga solish strategiyalarining bir qismi sifatida uchinchi tomonlarni aniqlash, boshqarish va doimiy ravishda kuzatib borishning muhimligini ta'kidlaydi.

SEC yo'riqnomasi S-K 106(b) bandi – Tahdidlarni boshqarish va strategiya

Ushbu tamoyil SEC yo'riqnomasi S-K 106(b) bandi bilan qo'llab-quvvatlanadi, ushbu band ro'yxatdan o'tgan korxonaning kiberxavfsizlik tahdidlarini boshqarish va strategiyasini oshkor qilish zarurligini ta'kidlaydi. Xususan, ro'yxatdan o'tgan korxonaning kiberxavfsizlik tahdidlaridan kelib chiqadigan muhim xatarlarni, ayniqsa, uchinchi tomon xizmat ko'rsatuvchi provayderlar bilan bog'liq bo'lgan tahdidlarni nazorat qilish va aniqlash qobiliyatiga e'tibor qaratish zarurligini ta'kidlaydi, chunki ular biznes uchun muhim bo'lishi mumkin. Keyinchalik, ilg'or amaliyotga muvofiq, tashkilotning tahdidlarni boshqarish rejasi uchinchi tomonda yuzaga keladigan xavfsizlik tahdidlarini boshqarishni hisobga olishi lozim.

Yakuniy xulosa

Har bir xavfsizlik jamoasi o'z strategiyasi va ijro modeliga ega. Asosiy farq shundaki, tahdidlarni baholashga asoslangan strategiya va uni amalga oshirish modeli tahdid haqidagi ma'lumotlarga asoslangan tizimdan foydalangan holda biznesni boshqaradi. Bunda ularning maqsadi byudjet, xodimlar soni va ko'nikmalar to'plamlari bilan qo'llab-quvvatlanadigan tahdidga chidamlilik darajasini belgilashdir. Resurslar va ijro etish ustuvorliklarini tahdidga moyillik va chidamlilikning maqbul darajalari doirasida muvofiqlashtirish – bu uzluksiz muvozanat saqlash jarayonidir. Bu korxonaning strategik qarashlariga singdirilgan dinamik

jarayon bo'lib, CRMPning asosiy tarkibiy qismlari o'zaro hamjihatlikda ishlashi orqali amalga oshiriladi.

Tahdidlarni boshqarishga asoslangan tizim va uni amalga oshirishning muhim tarkibiy qismlaridan biri tahdid muhitida o'zgarishlar yuz berganda, ya'ni tahdidlar chidamlilik chegarasidan oshib ketganda, muayyan manfaatdor tomonlar nima qilishlari kerakligini aniqlashdir. Jumladan: qanday qarorlar qabul qilinishi va qanday harakatlar amalga oshirilishi hamda bular kim tomonidan bajarilishi kerakligi; bu haqida korxona ichida va tashqarisida kimlarni xabardor qilish zarurligi. Ushbu muhim funksiya tahdidlar eskalatsiyasi hamda ma'lumotlarning oshkor qilinishi bo'lib, ushbu masala keyingi bobning asosiy mavzusidir.

VI BOB.

TAHDIDLAR ESKALATSIYASI VA MA'LUMOTLARNING OSHKOR ETILISHI

Oldingi boblarda CRMPning asosiy tarkibiy qismlari ko'rib chiqildi. Bu dastur korxona va uning manfaatdor tomonlarini raqamlashtirish olib keladigan ma'lum va noma'lum xatarlarning keng doirasiga qarshi himoya qilish uchun zarur imkoniyatlarni ta'minlaydi. Moslashuvchan boshqaruvning zarurligi aniqlandi, bunday boshqaruvda tegishli odamlar tahdidga oid qarorlar qabul qiladi hamda bu qarorlarga javobgar bo'ladi. Tahdidlar to'g'risida aniq, amaliy ahamiyatga ega bo'lgan ma'lumotlarning tegishli tomonlarga, shu jumladan, tahdid bo'yicha mas'ul shaxslar va boshqaruv organiga yetkazilishini ta'minlash uchun tahdid haqidagi ma'lumotlarga asoslangan tizimga ega bo'lish muhimligi ta'kidlandi. Tahdidlar strategiyasi va uni amalga oshirish asoslari belgilandi, bu – tahdidlar bo'yicha qarorlar qabul qilish va ularga muvofiq harakat qilish jarayoni. Endi esa CRMPning oxirgi asosiy komponentini – tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi hamda uning dastur muvaffaqiyati uchun juda muhim ekanligi sabablarini ko'rib chiqamiz.

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi – tegishli shaxslar va tashkilotlarni tahdid masalalari to'g'risida o'z vaqtida va to'g'ri usulda xabardor qilinishini ta'minlash – muammolarning falokatga aylanishini oldini olishga yordam berishi hamda jamoatchilik va nazorat organlarining ishonchini saqlab qolishi yoki tiklashi mumkin.

Kibertahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish zarurati, korxonaning tahdid muhiti muqarrar ravishda tez va oldindan aytib bo'lmaydigan tarzda o'zgarishi bilan bog'liq. Agar ushbu o'zgarishlar, rasmiy va faol ravishda hal qilinmasa, ular korxona va uning yuqori bo'g'indagi qaror qabul qiluvchilariga jiddiy, ba'zan tuzatib bo'lmaydigan zarar yetkazishi mumkin. Bu korxona va uning obro'siga putur yetkazishi yoki mijozlar, investorlar, hamkorlar ishonchining yo'qolishiga olib kelishi mumkin (ma'lum bir korxona yoki sanoatga qarab, bu omillar ko'p yoki kamroq darajada ta'sir qilishi mumkin). Ammo CRMP samarali tahdid eskalatsiyasi va ma'lumotlarni oshkor qilish amaliyotlarini o'z ichiga olishi kerakligining eng muhim sababi – bu sudlar va nazorat qiluvchi organlarning kuchli tazyiqidir.

Cheksiz sud qarorlari shuni ko'rsatadiki, sudlar korxonalarning kibertahdid amaliyotlaridan qoniqmaydi. Shuningdek, sudlarning fikricha, korxonalar, ayniqsa, ochiq savdo kompaniyalar xavfsizlik hodisalari va boshqa kibertahdid masalalarini oshkor qilishda yetarlicha shaffof va tez harakat qilishmayapti. Tartibga soluvchi organlar, xususan SEC, ushbu qarorlarga tayanib, korxonalar to'liq rioya qilishlari kerak bo'lgan tobora qat'iy talablarni joriy qilmoqda. Sudlar ham, tartibga soluvchi organlar ham tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish masalasiga nisbatan jiddiy munosabatda ekanliklarini yuz millionlab, hatto milliardlab dollarga yetadigan mukofotlar, jarimalar va boshqa kelishuvlar orqali namoyon etmoqdalar.

TAHDIDLAR ESKALATSIYASI VA MA'LUMOTLARNING OSHKOR ETISH TAVSIFI

Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish bir-biriga chambarchas bog'liq tushunchalar bo'lsa-da, ular mutlaqo farqli tushunchalardir. Shuning uchun, keling, avvalo ularning ma'nosini aniqlab olaylik.

Tahdidlar eskalatsiyasi – bu tahdid yoki tahdid bilan bog'liq hodisani tegishli va javobgar ichki manfaatdor tomonlar (masalan, korxona tahdidlarini boshqaruvchi organ yoki direktorlar kengashi)ga yetkazish jarayonidir. Shuni e'tiborga olish lozimki, bu favqulodda hodisaga qarshi chora ko'rish bilan bir xil emas. Favqulodda hodisa deyarli har doim qandaydir chora ko'rishni talab qiladi, ammo ancha keng ko'lamdagi tahdidlar faqatgina qandaydir darajada eskalatsiyani talab qiladi. Eskalatsiya darajasi to'g'risidagi qaror – hodisa korxonaning tahdid tasnifi va tahdidga chidamlilik darajalari bilan belgilangan muayyan chegaradan oshib ketishiga asoslanadi.

Tahdidlarga oid ma'lumotlarni oshkor etish – bu ma'lum shaxslar va tashkilotlarga tahdid aniqlanganligi yoki hodisa yuz berganligi to'g'risida ma'lumot berish. Ushbu jarayon ham oldindan belgilangan tahdid darajasiga asoslangan bo'ladi. Tahdid to'g'risida ogohlantirish yuzasidan tushunilishi kerak bo'lgan ikkita asosiy fakt mavjud. Birinchidan, yuqorida ta'kidlanganidek, ko'p hollarda bu qonunlar yoki me'yoriy muvofiqlik talablarga rioya qilish bilan bog'liq bo'lib, tahdid bilan bog'liq hodisani oshkor qilmaslik juda jiddiy oqibatlariga olib kelishi mumkin. Ikkinchidan, tahdid eskalatsiyasidan farqli o'laroq, ko'p hollarda tahdidlarga oid ma'lumotlarni oshkor etish degani korxona ichidagi va tashqarisidagi tomonlarni xabardor qilishni anglatadi. Bunga direktorlar kengashi, korxonaning boshqaruv organi, aksiyadorlar, mijozlar va eng muhimi, nazorat organlar kirishi mumkin. Ba'zi hollarda, hatto sudlar ham bunga jalb qilinadi. Tahdidlarga oid ma'lumotlarni oshkor etish zarurligining to'rtta asosiy sababi bor:

- Ommaviy kompaniyalarning moddiy tahdidlarni oshkor qilish majburiyati (bu tushuncha bobning keyingi qismida batafsil muhokama qilinadi)
- Normativ-huquqiy hujjatlariga rioya qilish majburiyatlari
- Qonuniy talablar (masalan, Yevropa Ittifoqining Umumiy ma'lumotlarni muhofaza qilish reglamenti [GDPR¹⁰⁰] dagi ma'lumotlarning maxfiyligi bo'yicha majburiyatlari)
- Jamoatchilik ishonchini saqlash zarurati

¹⁰⁰ GDPR (General Data Protection Regulation) – Ma'lumotlarni himoya qilish umumiy reglamenti.

SEC va tahdid haqidagi ma'lumotlarning oshkoraligi

Butun dunyoda kibertahdidlarni nazorat qilish va tahdidlarga oid ma'lumotlarni oshkor etish bilan shug'ullanadigan juda ko'plab nazorat organlari mavjud. Ushbu bobda, asosan SEC va uning o'ziga xos talablariga e'tibor qaratiladi. Buning sababi shundaki, SEC AQSHdagi barcha ochiq aksiyadorlik jamiyatlari us-tidan nazorat qilish vakolatiga ega va bu uni korxonalar, shu jumladan AQSHdan tashqarida faoliyat ko'rsatadigan ba'zi kompaniyalar uchun eng muhim tartibga soluvchi organga aylantiradi. Dunyoda ko'plab boshqa tartibga soluvchi organ-lar mavjud bo'lib, ularning talablarini korxonalar tushunishi hamda ularga rio-ya qilishlari lozim. Ularning muvofiqlik talablari bir-biriga to'g'ri kelishi, ba'zi hollarda ustun kelishi va hatto bir-biriga zid bo'lishi ham mumkin. Misol uchun, Nyu York fond birjasi (NYSE¹⁰¹) va Nasdaq kabi AQSH birjalarida ro'yxatdan o'tgan xorijiy kompaniyalar ham SEC talablariga, ham o'z mamlakatlarining tar-tibga soluvchi organlari talablariga ham javob berishlari kerak bo'ladi, bu talablar bir-biridan sezilarli farq qilishi mumkin. Kibertahdidlarga oid ma'lumotlarni osh-kor etish SEC uchun tobora jiddiy qiziqish va harakat yo'nalishiga aylanmoq-da. Sudlarning tajribasiga tayangan holda, SEC korxonalarning tahdidlarga oid ma'lumotlarni yetarlicha shaffof va o'z vaqtida oshkor qilmayotganligiga, bu joriy va bo'lajak investorlarning o'zlarining asosli investitsiya qarorlarini qabul qilish-lariga ishonish imkoniyatini cheklayotganiga ishonadi. Investorlarning ishonchini ta'minlash SECning eng muhim vazifasi bo'lgani uchun, uning oshkoralik bo'yi-cha tashvishi yangi va tobora qat'iylashib borayotgan me'yoriy muvofiqlik talab-larini keltirib chiqarmoqda.

Yuqorida aytib o'tilganidek, 2023-yil iyul oyida SEC yangi qoidalar to'pla-mini joriy etdi, bu esa ochiq aksiyadorlik jamiyatlaridan kiberhodisalar to'g'risida xabar berishlarini hamda vaqti-vaqti bilan o'zlarining kiberxavflarni boshqarish amaliyoti, strategiyalari va boshqaruvlari to'g'risida hisobot berishlarini talab qi-ladi (ularning negizida joylashgan kiberqoidalar va asoslar ushbu kitobning maq-sadi va niyati bilan chambarchas bog'liq).

SEC va boshqa ko'plab tartibga soluvchi organlar tomonidan amalga oshiril-gan ushbu harakatdan kelib chiqadigan muqarrar xulosa shuki, barcha korxonalar o'zlarining kibertahdidga oid ma'lumotlarini oshkor etish va eskalatsiya amaliyot-larini keskin ravishda takomillashtirishlari zarur. Korxonalar o'zlarining huquqiy va me'yoriy majburiyatlarini bajarishlari hamda xavflarni aniq va o'z vaqtida oshkor qilishlarining yagona yo'li – bu CRMPning barcha tarkibiy qismlarining uzluksiz hamkorlikda ishlashidir.

¹⁰¹ NYSE (New York Stock Exchange) – Nyu York fond birjasi.

Butunjahon tartibga soluvchi organlari tahdidga oid ma'lumotlarni oshkor qilishni talab qiladi

SEC AQSHdagi eng muhim moliyaviy tartibga soluvchi organ hisoblanadi, lekin u dunyodagi yoki hatto AQSHdagi yagona organ emas. Turli mintaqalarda va yurisdiksiyalarda faoliyat ko'rsatayotgan korxonalar tahdidga oid ma'lumotlarni oshkor etish bo'yicha ko'plab tartibga soluvchi organlarning talablariga javob berishi kerak, shu jumladan:

- Avstraliya Qimmatli qog'ozlar va investitsiyalar komissiyasi (ASIC¹⁰²): Avstraliyaning mustaqil hukumat organi bo'lib, mamlakat korporatsiyalarini tartibga solish uchun mas'uldir.
- Autorite des Marches Financiers (Moliyaviy bozorlar boshqarmasi – AMF¹⁰³): Fransiya'dagi moliyaviy bozorlarning asosiy tartibga soluvchi organi
- Bundesanstalt für Finanzdienstleistungsaufsicht (Federal moliyaviy nazorat organi – BaFin¹⁰⁴): Germaniyaning moliyaviy xizmatlar sanoatini tartibga solish uchun mas'ul bo'lgan nazorat organi
- Kanada qimmatli qog'ozlar ma'murlari (CSA¹⁰⁵) mamlakat kapital bozorlarini tartibga solishni uyq'unlashtirish uchun Kanada provinsiyalari va hududlari uchun qimmatli qog'ozlar tartibga soluvchi organlarini birlashtirgan tashkilot
- Xitoy Qimmatli qog'ozlarni tartibga solish komissiyasi (CSRC¹⁰⁶): Xitoy Xalq Respublikasida qimmatli qog'ozlarni tartibga soluvchi asosiy organ
- Yevropa qimmatli qog'ozlari va bozorlar boshqarmasi (ESMA¹⁰⁷): Yevropa Ittifoqi moliyaviy tizimlari barqarorligini himoya qilish uchun ishlaydigan mustaqil organ
- Moliyaviy xulq-atvor nazorati boshqarmasi (FCA¹⁰⁸): Buyuk Britaniya'dagi moliyaviy xizmatlar kompaniyalari va moliyaviy bozorlarni tartibga soluvchi organ
- Moliya sanoatini tartibga soluvchi vakolatli idora (FINRA¹⁰⁹): AQSHda brokerlar va broker-dilerlar uchun qoidalarni yozuvchi va amalga oshiradigan organ
- Qimmatli qog'ozlar komissiyalari xalqaro tashkiloti (IOSCO¹¹⁰): jahon qimmatli qog'ozlar bozorini tartibga soluvchi tashkilotlarni birlashtirgan xalqaro organ

¹⁰² ASIC (Australian Securities and Investments Commission) – Avstraliya Qimmatli qog'ozlar va investitsiyalar komissiyasi.

¹⁰³ AMF (Financial Markets Authority) – Moliyaviy bozorlar boshqarmasi.

¹⁰⁴ BaFin (Federal Financial Supervisory Authority) – Federal moliyaviy nazorat organi.

¹⁰⁵ CSA (Canadian Securities Administrators) – Kanada qimmatli qog'ozlar ma'murlari.

¹⁰⁶ CSRC (China Securities Regulatory Commission) – Xitoy qimmatli qog'ozlarni tartibga solish komissiyasi.

¹⁰⁷ ESMA (European Securities and Markets) – Yevropa qimmatli qog'ozlar va bozorlar boshqarmasi.

¹⁰⁸ FCA (Financial Conduct Authority) – Moliyaviy xulq-atvor nazorati boshqarmasi.

¹⁰⁹ FINRA (Financial Industry Regulatory Authority) – Moliya sanoatini tartibga soluvchi vakolatli idora.

¹¹⁰ IOSCO (International Organization of Securities Commissions) – Qimmatli qog'ozlar komissiyalari xalqaro tashkiloti.

• Yaponiya moliyaviy xizmatlar agentligi (JFSA¹¹¹): Yaponiya moliyaviy xizmatlar sanoatini nazorat qilish uchun mas'ul davlat agentligi

• Hindiston Qimmatli qog'ozlar va birja kengashi (SEBI¹¹²): Hindiston qimmatli qog'ozlar bozori uchun mas'ul tartibga soluvchi organ

• Shveysariya moliya bozorini nazorat qilish organi (FINMA¹¹³): Shveysariyaning bank sanoati va boshqa moliya institutlari uchun mas'ul tartibga soluvchi organ.

Ushbu tartibga soluvchi organlar va boshqalar o'zlarining noyob milliy yoki mintaqaviy muammolarini hal qilish uchun turlicha faoliyat ko'rsatadilar. Shunga qaramay, ularning barchasi ushbu kitobda yoritilgan va CRMP tomonidan bajariishi kerak bo'lgan izchil majburiyatlarni o'rnatganlar. Oddiy qilib aytganda, bu majburiyatlar quyidagilarni ta'minlashdan iborat: to'g'ri boshqaruv modeli orqali tegishli odamlar nazorat uchun mas'ul bo'lishlari, ular muntazam ravishda tahdid haqidagi ma'lumotlarga asoslangan samarali strategiya va uning ijrosi yo'lga qo'yilganligi, risklar eskalatsiyasi va zarur bo'lganda, o'z vaqtida va aniq tarzda tahdidlar haqidagi ma'lumotlarning oshkor etilishi.

IKKI MUHIM TUSHUNCHA: TAHDID OMILLARI VA MODDIY TAHDID

Tahdidlar eskalatsiyasi va tahdidlarga oid ma'lumotlarni oshkor qilish bo'yicha muhokamalarda ikki tushuncha markaziy ahamiyatga ega bo'lib, ular chuqur o'rganilishi lozim. Yaqinda SEC ushbu ikki tushuncha, ya'ni tahdid omillari va moddiy tahdid bo'yicha o'z qoidalarini va yo'riqnomalarini yangiladi. Bu masalaning SEC uchun muhimligi sababli, bu yangilanishlarni tushunish uchun ajoyib boshlang'ich nuqtaga aylantiradi.

Tahdid omillari: 2020-yilda SEC tahdid omillarini modernizatsiyalash va ma'lumotlarni oshkor qilish bo'yicha o'z qoidalarini va yo'riqnomalarini yangiladi.

Bunda asosiy maqsad tahdidlar haqidagi ma'lumotlarni yanada dolzarb va aniqroq qilib, tahdid omillarini oshkor etish sifatini oshirish edi. SEC yangilanishlari tahdid omillari qisqa, tushunarli va shaffof bo'lishi kerakligini aniq-ravshan ko'rsatdi. Ular, shuningdek, tegishli sarlavhalar ostida tashkil etilishi va investorlar kompaniyalarni baholashda foydali deb hisoblaydigan eng muhim tahdidlarga qaratilgan bo'lishi kerak. SEC tahdid omillarini uch toifaga ajratdi:

- Kompaniyaga xos tahdidlar
- Sanoat tahdidlari
- Muayyan qimmatli qog'ozlar (ya'ni muayyan investitsiyalar) bilan bog'liq tahdidlar

Muhim tahdid: Moliyaviy bozorlar asosan shaffoflikka tayanadi. Oddiy qilib aytganda, bu kompaniyaga sarmoya kiritmoqchi bo'lgan har qanday shaxs ushbu qarorga ta'sir qilishi mumkin bo'lgan har qanday ma'lumotni bilish huquqiga ega ekanligini anglatadi.

¹¹¹ JFSA (Japan Financial Services Agency) – Yaponiya moliyaviy xizmatlar agentligi.

¹¹² SEBI (Securities and Exchange Board of India) – Hindiston Qimmatli qog'ozlar va birja kengashi.

¹¹³ FINMA (Swiss Financial Market Supervisory Authority) – Shveysariya moliya bozorini nazorat qilish organi.

SECning 1972-yilgi oliy sudning nufuzli qaroriga asoslangan ma'lumotlariga ko'ra, muhimlik "qimmatli qog'ozlarni sotib olish yoki sotib olmasligini aniqlashda oqil sarmoyador muhim ahamiyat berishi mumkin bo'lgan masalalarga" taalluqlidir. Biz "muhim ahamiyatga ega" (yoki "muhim") tahdid ma'lumotlarini aynan shunday tushunamiz va u shubhasiz kibertahdidga ham tegishli. Biroq barcha tahdid haqidagi ma'lumotlar ham muhim ahamiyatga ega emas. Tezda bartaraf etilgan kichik ma'lumotlar buzilishi yoki firibgarlikning birlamchi holati muhim ahamiyatga ega emas. Ammo, millionlab iste'molchilarga ta'sir ko'rsatadigan keng ko'lamli buzg'unchilik holatlari, shuningdek, uzoq muddatli firibgarlik amaliyotlari muhim ahamiyatga ega. Bunday muhim ahamiyatga ega bo'lgan tahdidlar va hodisalar tegishli tartibga soluvchi organlarga xabar qilinishi shart. AQSHdagi ochiq aksiyadorlik kompaniyasi bo'lsa, birinchi navbatda, SECga xabar berish kerakligini anglatadi.

Tahdidlar eskalatsiyasi

Tahdidlar eskalatsiyasi, yuqorida ta'kidlab o'tilganidek, tahdidga asoslangan tizimdan foydalanib, ehtimolligi, ta'siri yoki har ikkalasi bo'yicha ortgan xavflarni aniqlash, baholash va ustuvorligini belgilash hamda ularni tegishli choralar ko'rishlari uchun belgilangan shaxslar yoki tashkilotlar e'tiboriga yetkazish jarayonidir.

Ushbu kontekstda qo'llanilgan *tahdid* so'zi faqatgina ma'lumotlar buzilishi yoki zararli dastur hujumlari kabi sodir bo'lgan va chora ko'rishni talab qiladigan hodisalarni nazarda tutmaydi. Shuningdek, tahdidlar eskalatsiyasi favqulodda hodisaga chora ko'rish jarayoni bilan bir xil emasligini tan olish ham juda muhimdir. Tahdid hodisasi ko'plab omillar, masalan, korxonaning ish faoliyati muhitidagi o'zgarishlar tufayli yuzaga kelishi mumkin. Ushbu omillar tahdid chegaralarini qayta baholashni talab qilishi mumkin, ammo allaqachon sodir bo'lgan haqiqiy yo'qotish hodisasiga muayyan chora ko'rishni talab qilmaydi.

Tahdidlar eskalatsiyasi noxush hodisa (insident)larga chora ko'rish jarayoni bilan bir xil emas. Noxush hodisa deyarli har doim qandaydir chora ko'rilishini talab qiladi, ammo u strategik tahdid eskalatsiyaga sabab bo'ladigan tahdid darajasini o'zgartirishi yoki o'zgartirmasligi mumkin.

Korxonalarning yuqori bo'g'in qaror qabul qiluvchilari tahdid hodisalari eskalatsiya yoki ma'lumotlarni oshkor etishni talab qiladigan chegaralarga yetishi yoki undan oshishini aniqlashda, ya'ni ular muhim ahamiyatga ega bo'ladimi yoki yo'qligini aniqlashda boy tajribaga ega. Biroq, kibertahdidlarni boshqarishdagi juda ko'plab muvaffaqiyatsizliklar shuni ko'rsatadiki, o'zlarining boy tajribalariga qaramay, qaror qabul qiluvchilar raqamlashtirish tahdidi oqibatlarini haqida yetarli-chi tushunchaga ega emas yoki ularni e'tiborsiz qoldirishmoqda. Shu bilan birga,

qonun chiqaruvchilar, tartibga soluvchilar va sudlar buni nomaqbul deb hisoblab, tashkilotlar kiberxavfsizlik va kiber javobgarlik bo'yicha yuqori darajadagi tajribaga ega bo'lishlari zarurligini ta'kidlamoqda.

Rasmiy kibertahdidlar eskalatsiyasi jarayonlari korxonalarning ish faoliyatida muhim ijobiy o'zgarishlarni taqdim etadi. Buning bir misoli, tahdidni oldindan aniqlashdir, bu tashkilotlarga potensial muammolarni ertaroq aniqlash hamda ularning zararli oqibatlarini oldini olish yoki kamaytirish uchun o'z vaqtida samarali choralar ko'rish imkonini beradi.

Muammolarni erta aniqlash tahdidga oid qaror qabul qilish jarayonini sezilarli darajada yaxshilaydi, shuning uchun tahdid bo'yicha mas'ul shaxslar, boshqaruv organlari va boshqa muhim manfaatdor tomonlar yuzaga kelayotgan tahdidlar, tahdid muhitidagi boshqa o'zgarishlarga oid asosli qarorlar qabul qilishlari mumkin, bu qarorlar korxonaning belgilangan tahdid chegarasiga mos keladi. Tahdidlar eskalatsiyasi ochiq muloqot va hamkorlik madaniyatini shakllantirishga yordam beradi, bunda xodimlar xavf-xatarlar haqidagi tashvishlarini erkin va hatto majburiy tarzda baham ko'radilar. (Shuningdek, bu xavfsizlik va boshqa tahdid bo'yicha mutaxassislariga tahdid eskalatsiyasini birinchi o'ringa qo'yishga imkon beradi, yuqori darajali qaror qabul qiluvchilarning e'tibori keraksiz masalalarga qaratilmaydi). Bu ayniqsa muhim hisoblanadi, chunki qaror qabul qilish jarayonini aniqlash va javobgarlikni belgilash xodimlardan ichki "siyosiy" bosimni olib tashlaydi. Bu ularga, hatto nufuzli shaxs yoki ichki tashkilotni yomon ahvolga solsa ham, rahbariyat tomonidan tasdiqlangan va yuqori bosqichga o'tkazishni talab qiladigan siyosatni ko'rsatishga imkon beradi.

Bu omillarning barchasi biz muhokama qilib kelayotgan CRMPning asosiy afzalliklariga hissa qo'shadi. Ular korxonaning obro'sini oshiradi, uning tahdidlarni boshqarish bo'yicha qat'iyligini namoyish etadi va mijozlardan tortib investorlar hamda sheriklarga ham bo'lgan turli manfaatdor tomonlarning ishonchini oshiradi. Albatta, kibertahdidlarni eskalatsiya qilishning samarali usullari boshqa moliyaviy manfaatlarga ham ega: tahdidlarni zudlik bilan bartaraf etish uchun tahdidlarni eskalatsiya qilish jarayoni, korxonalarga o'z vaqtida samarali hal qilinmagan tahdidlardan kelib chiqadigan katta xarajatlarni tejash imkonini beradi.

Eng muhimi, tahdidlar eskalatsiyasi, tahdid funksiyasi sifatida korxonaning xavfsizlikni boshqarish bo'yicha o'z huquqiy va me'yoriy talablarga rioya qilish majburiyatlarini bajarish uchun muhim sa'y-harakatlarida markaziy o'rinni egallaydi. Sudlar va tartibga soluvchi organlar tahdidga oid qaror qabul qiluvchilarni, hatto direktorlar kengashini, tahdid haqida xabardor qilinmaganliklari hamda tahdid bilan bog'liq muammolarni hal qilishga qodir emasligi tufayli jazolashga to'liq tayyor. Boshqacha qilib aytganda, biror hodisa sodir bo'lganda "menga ma'lumot berilmagandi" degan so'zlar himoya uchun maqbul bahona bo'lolmaydi.

Kibertahdidlar eskalatsiyasi – bu tegishli odamlarning zarur paytda kerakli ma'lumotlarga ega bo'lishini ta'minlashning rasmiy amaliyotidir. Ammo bu oson

ish emas. Tahdidlar va ayniqsa kibertahdidlar murakkab, tez o'zgaruvchan hamda aniqlash va ustuvorlik qilish qiyin bo'lgan masaladir.

Har bir korxona tahdidlar eskalatsiyasi bo'yicha sa'y-harakatlarida foydalanishi kerak bo'lgan muhim mexanizmlardan biri to'rtinchi bobda batafsil bayon qilingan tahdidlar haqidagi ma'lumotlarga asoslangan tizim yordamida amalga oshiriladigan baholash jarayonidir.

Kibertahdid tasnifi

Kiber hodisaning potensial ta'sirini tahdid bo'yicha mas'ul shaxslar va boshqa manfaatdor tomonlar aniq tushunishi mumkin bo'lgan biznesga doir atamalar bilan ifodalash zarurligi to'rtinchi bobda ta'kidlab o'tildi. Korxonaning umumiy tahdidlarini boshqarish yondashuviga muvofiq bo'lgan, aniq tushuniladigan biznes terminologiyasidan foydalanish texnik bo'lmagan auditoriyaga tahdidni tushunish va u bo'yicha asosli qarorlar qabul qilish imkoniyatini yaratadi.

Tahdidni baholash va hal etilmagan tahdidlarni tasniflash (o'ta muhim, yuqori, o'rta, past) CRMPning tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish komponentining zaruriy qismlaridir. Manfaatdor tomonlar tahdidni baholash jarayonida aniq tushunishlari va aniqlashlari kerak bo'lgan yana ikkita masala mavjud: aniqlangan tahdid muhimmi yoki u korxonaning belgilangan tahdidga moyillik yoki chidamlilik darajalari imkoniyatidan tashqaridami:

Muhim tahdid

Muhim tahdid – bu investitsiya qarorlari va investorlarning ishonchiga ta'sir qilishi mumkin tahdid turi bo'lib, u kibermuhit nuqtayi nazaridan, korxona tomonidan allaqachon o'rnatilgan muhimlikni aniqlash jarayoniga kiritilishi mumkin.

Moyillik yoki chidamlilik darajasidan oshgan tahdidlar

Bu tashkilotning moyillik yoki chidamlilik darajasidan oshgan tahdid turi bo'lib, u korxona yoki uning xodimlari yoki boshqa manfaatdor tomonlarga jiddiy zarar yetkazishi mumkin bo'lgan (masalan, o'lim) tahdidlardir (bu CRMPning tahdidlarni baholashga asoslangan strategiya va uning ijrosi nomli komponenti bilan belgilanadi). Ba'zi korxonalar uchun tahdidga moyillik va chidamlilik darajasi tahdidlarni tasniflashning umumiy darajasida aniqlanishi mumkin. Boshqa korxonalar esa chidamlilikni ta'sir toifasi darajasida belgilashi mumkin (masalan, korxona amaliy tahdid toifasiga yuqori ta'sirni maqbul deb belgilashi, ammo ekologik tahdid toifasiga esa faqat past ta'sirni maqbul deb belgilashi mumkin).

Tegishli kontekst o'rnatilganidan so'ng, ma'lumotlar tahdid darajasiga qarab, dasturiy tarzda boshqaruv organi yoki manfaatdor tomonlarning ma'lum bir iyerarxiyasi orqali yetkazilishi mumkin (6.1-chizmaga qarang).

Tahdid darajasiga va tegishli boshqaruv darajasiga qarab, majburiyatlar quyidagicha taqsimlanishi mumkin:

Tavsiya etish

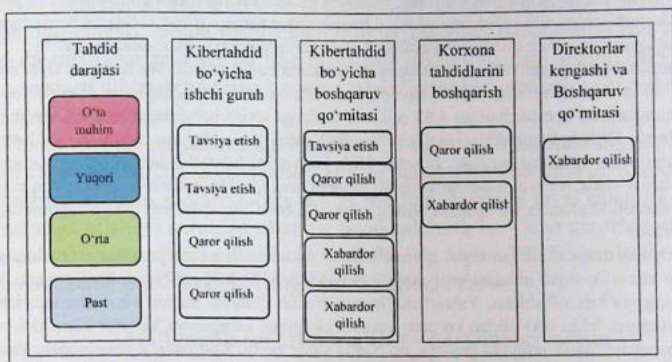
Maxsus guruh yoki qo'mita boshqaruvning keyingi darajasiga kibertahdid bo'yicha tavsiyalar berish uchun javobgardir.

Qaror qilish

Maxsus guruh yoki qo'mita tahlil va taqdim etilgan tavsiyalarga asoslanib kibertahdid bo'yicha qarorlar qabul qilish uchun javobgardir.

Xabardor qilish

Maxsus guruh yoki qo'mita kibertahdidga javob berish bo'yicha qabul qilingan har qanday qarorlar to'g'risida xabardor qilinadi.



6.1-chizma. Tahdidlar eskalatsiyasining namunaviy iyerarxiyasi

YAHOO¹¹⁴ KOMPANIYASIDA MA'LUMOTLARINING KENG MIQYOSDA SIZIB CHIQISHI

2013-yillardan boshlab, internet xizmatlari provayderi Yahoo! bir qator hujumlarni boshdan kechirdi (bu hujumlar Rossiya tomonidan amalga oshirilgan degan taxminlar bo'lgan), bu hujum bugungi kunga qadar tarixdagi eng yirik ma'lumotlar sizib chiqishi holati bo'lib qolmoqda. Yana bir ma'lumotlar sizib chiqishi holati 2014-yil oxirida yuz berib, bu 500 milliondan ortiq Yahoo! foydalanuvchi akkauntlariga ta'sir etdi, lekin bu haqida 2016-yilning ikkinchi yarmigacha oshkor etilmadi. Yahoo! oxir-oqibatda allaqachon milliardlab foydalanuvchilarning akkauntlariga ta'sir qilgan deb hisoblangan bu hujum, aslida uning barcha uch milliard foydalanuvchi akkauntlarini buzganligini tan oldi. Bu kiberhujum kompaniya foydalanuvchilari uchun dahshatli oqibatlariga olib keldi. Yuz millionlab Yahoo foydalanuvchilari haqidagi maxfiy ma'lumotlar yashirin internet (Dark web¹¹⁵)da sotuvga qo'yildi.

¹¹⁴ Yahoo – Amerikaning veb xizmatlari ta'minotchisi.

¹¹⁵ Dark Web – maxsus brauzerlar orqali kiriladigan, oddiy qidiruv tizimlari tomonidan indekslanmaydigan Internetning yashirin qismi.

Yahoo! kompaniyasi oxir-oqibat hujumchilar kirish ma'lumotlarini soxtalashtirish imkoniyatiga ega bo'lganligi, bu esa ularga istalgan akkauntga parolsiz kirish imkonini berganligi haqida xabar qildi.

Yahoo! kompaniyasiga qarshi chora ko'rish to'g'risidagi buyrug'ida SEC shunday deya ta'kidladi: "2014-yildagi ma'lumotlar sizib chiqishi haqida xabardor bo'lishiga qaramay, Yahoo! kompaniyasi ikki yil davomida bu haqida o'zining ommaviy hisobotlarida ma'lumot bermadi. Aksincha, kompaniyaning 2014–2016-yillardagi yillik va choraklik hisobotlarda tahdid omillarini oshkor qilishda jiddiy tarzda chalg'ituvchi ma'lumotlarni taqdim etilgan. Hisobotlarda kompaniya faqat kelajakda yuz berishi mumkin bo'lgan ma'lumotlarning sizib chiqishi xavfiga duch kelishi va bu axborot tizimlarida saqlanayotgan foydalanuvchilarning shaxsiy ma'lumotlari yo'qolishiga, shuningdek, kelajakda sud jarayonlari, tuzatish ishlari, xavfsizlik choralarini kuchaytirish xarajatlarining oshishi, daromadning yo'qolishi, obro'siga putur yetishi va javobgarlikka tortilishiga olib kelishi mumkinligi haqida xabar bergan. Biroq, aslida ma'lumotlarning keng miqyosda sizib chiqishi ancha oldinroq sodir bo'lganligini oshkor qilinmagan"¹¹⁶.

Kompaniya ushbu muvaffaqiyatsizliklar uchun katta badal to'ladi. Ma'lumotlar sizib chiqishi e'lon qilinishidan oldin, Yahoo! kompaniyasi o'z operatsiyalarining katta qismini Verizon Communications kompaniyasiga 4,83 milliard dollarga sotish bo'yicha muzokaralar olib bormoqda edi. Verizon kompaniyasi ma'lumotlar sizib chiqishi haqida jamoatchilik bilishidan atigi ikki kun oldin xabardor bo'lgan. U sotib olish jarayonini to'xtatish uchun qonuniy choralar ko'rishni o'yladi, lekin oxir-oqibat kelishib olingan narxdan 350 million dollar kamroq narxda bitim tuzildi. Shubhasiz, kompaniya bosh direktori va bosh huquqshunosi o'z lavozimini saqlab qololmadi.

Moliyaviy zarar shu bilan tugab qolmadi. Yahoo! kompaniyasi ma'lumotlar sizib chiqishini oshkor etmaslik orqali investorlarni chalg'itgani uchun SECga 35 million dollar jarima to'ladi. SECning ma'lum qilishicha, Yahoo! ma'lumotlar sizib chiqishi haqida bir necha kun ichida xabar topgan, lekin ikki yildan ko'proq vaqt o'tgachgina, kompaniya Verizon bilan oldi-sotdi shartnomasini tuzish jarayoni paytida, bu haqda xabar berdi. Kompaniya, shuningdek, Yahoo! foydalanuvchilari nomidan jamoaviy da'voni 117 million dollardan ortiq mablag' evaziga hal qildi.

Bu muhim ahamiyatga ega bo'lgan tahdid ma'lumotlari deganda nimani nazarda tutishimizning ajoyib misolidir. Ko'plab tomonlar, jumladan, yakka foydalanuvchilar, hozirgi va bo'lajak aksiyadorlar hamda "Verizon" singari kompaniyalar Yahoo! kompaniyasi xavfsizlik sohasida ulkan muvaffaqiyatsizlikka duchor bo'lganini bilish huquqiga ega edi. Kompaniya ahamiyatga ega bo'lgan ma'lumotlarni o'z vaqtida oshkor qilmaganligi sababli, ushbu tomonlarning hech biri kompaniya xizmatlaridan foydalanish, uning aksiyalariga sarmoya kiritish yoki Verizon misolida – uning aktivlarining katta qismini sotib olish to'g'risida asosli qaror qabul qilish imkoniyatiga ega emas edi. Bu o'z-o'zidan paydo bo'lgan va oldini olish mumkin bo'lgan mavjud inqirozga qo'shilgan yangi inqiroz edi.

Tahdidlar eskalatsiyasi va ma'lumotlar oshkoraligi – faqatgina xavfsizlikka oid hodisalar emas

Shuni bilish muhimki, kibertahdidlarning eskalatsiya qilinishi va oshkor etilishi deganda, biz faqatgina zararli dasturlar, ma'lumotlarning sizib chiqishi,

¹¹⁶ Altaba Inc., f/d/b/a Yahoo! Inc., 2018-yil 24-aprel, <https://oreil.ly/cVzfG>

shaxsiy ma'lumotlarning o'g'irlanishi yoki tovlamachi dasturlar hujumlari kabi kiberhodisalarni nazarda tutmasligimiz lozim. Keng va tobora ko'payib borayotgan omillar ko'lamini korxonaning tahdid holatiga ijobiy va salbiy ta'sir ko'rsatishi mumkin.

Bulutli hisoblash yoki avtomatlashtirish kabi yangi texnologiyani joriy etish oqibatida yangi hujum turi yoki yangi xavfsizlik zaifliklari kelib chiqishi mumkin. Korxonaning faoliyat yuritish modeli yoki hatto u biznes yuritadigan hududlardagi o'zgarishlar yangi me'yoriy muvofiqlik talablarini keltirib chiqarishi mumkin. Hatto yangi mahsulot yoki xizmatni joriy etish to'g'risidagi qaror ham obro'ga putur yetkazish xavfini keltirib chiqarishi mumkin, bu esa yana bir bor ko'rib chiqishni talab qiladi. Samarali CRMP tomonidan ko'rib chiqiladigan boshqa barcha omillar singari, tahdid muhiti ham doimiy ravishda nazorat qilinishi hamda ERM dasturi (agar mavjud bo'lsa) bilan muvofiqlashtirilishi lozim. NISTning 8286 standarti kibertahdid bilan korxona tahdidlarini birlashtirish uchun mukammal asosni taqdim etadi.

Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish zaruratining asosiy tamoyili shundaki, barcha xavf-xatarlarni to'liq bartaraf etib bo'lmaydi. Korxonalar raqobatbardoshligini saqlab qolish uchun ma'lum darajada tavakkalchilikni o'z zimmalariga olishlari kerak va ularning tavakkalchilik bo'yicha qarorlari tegishli tomonlar tomonidan qabul qilinishi va tasdiqlanishi lozim. Tahdid omillari o'zgaranda, bu haqda tegishli rahbariyatga xabar berilishi zarur.

Ma'lumotlarni oshkor qilish – korxonalar uchun majburiy talab

Kibertahdidga oid ma'lumotlarni oshkor qilish, asosan, ma'lumotlarni korxona tashqarisidagi shaxslar va tashkilotlarga yetkazish jarayoni eskalatsiyadan ham muhimroq bo'lib, tahdidga oid ma'lumotlarni oshkor qilmaslik oqibatlari jiddiy va u hatto korxonaning mavjudligiga tahdid soladigan haqiqiy zararga olib kelishi mumkin.

Tahdid to'g'risidagi ma'lumotlar oshkor qilinishi kerak bo'lgan manfaatdor tomonlarni uch asosiy toifaga bo'lish mumkin:

Aksiyadorlar va boshqa sarmoyadorlar (joriy va kelajakdagi)

Ko'rib o'tganimizdek, butun dunyo bo'ylab moliyaviy tartibga soluvchi organlarning keng doirasi ochiq aksiyadorlik kompaniyalarning oshkor qilish talablari ustidan vakolatga ega. Ularning vakolatlari bir-biridan farq qiladi, biroq ularning barchasi bir maqsadga ega: investorlarning shaffof va aniq ma'lumot olishini ta'minlash orqali bozorlarga jamoatchilik ishonchini oshirish. Tartibga soluvchi organlarning aksariyati, ma'lumotlarni oshkor qilish talablariga rioya qilmaydigan kompaniyalarga nisbatan jiddiy choralar ko'rishga tayyor ekanliklarini tobora aniq ko'rsatmoqda.

Tartibga soluvchi organlar

Turli soha korxonalariga moliyaviy ma'lumotlarni oshkor qilishdan tashqari, yana boshqa ko'plab me'yoriy muvofiqlik talablari (ko'plab sabablarga ko'ra) tatbiq etiladi. Maxfiy va boshqa turdagi nozik ma'lumotlarning xavfsizligi ular hal qiladigan eng muhim masalalardan biridir. Ko'pgina mintaqalardagi maxfiylik qoidalari, xususan, Yevropa Ittifoqining GDPRi maxfiy ma'lumotlar qayerda va qanday saqlanishi mumkinligini aniq ko'rsatadi hamda qoidalarini buzganlik va qoidabuzarliklarni oshkor qilmaganlik uchun jiddiy jazolar belgilangan. 2021-yilda, Amazon kompaniyasi GDPRning ma'lumotlarni yig'ish qoidalarini buzgani uchun 746 million yevro (taxminan 877 million AQSH dollari) miqdorida jarimaga tortildi.

Yevropa Ittifoqi a'zosi Fransiya davlati ham Amazon kompaniyasiga tegishli huquqbuzarlik uchun 35 million yevro (taxminan 38 million dollar) miqdorida jarimaga soldi, bu korxonalar bir nechta va ba'zan bir-biriga zid bo'lgan me'yoriy talablar bilan ishlashga tayyor bo'lishi kerakligini ko'rsatdi. Shuningdek, turli soha tartibga soluvchi organlari alohida korxonalarning o'ziga xos holatlari va sharoitlariga moslashtirilgan tahdid va hodisalar haqida hisobot berishning aniq mezonlari va chegaralarni ishlab chiqdi.

Jamoatchilik

Korxona uchun uning ko'plab manfaatdor tomonlari, jumladan mijozlari, investorlari, hamkorlari va xodimlarining ishonchidan muhimroq aktiv kamdan kam topiladi. Ishonch qimmatli resurs sifatida hatto korxona faoliyatida bevosita ishtiroki bo'lmagan shaxslar uchun ham muhim ahamiyatga ega bo'lishi mumkin, chunki u davlat va tartibga soluvchi tashkilotlar hamda jamoat (masalan, iste'molchilar huquqlarini himoya qiluvchi) tashkilotlarning harakatlariga ta'sir ko'rsatadi.

Cheksiz xavfsizlik muammolari bilan to'la bo'lgan kiberxavf muhiti, shubhasiz, keng jamoatchilikni korxonalarga, ayniqsa ularning shaxsiy ma'lumotlari va raqamlashtirilgan mahsulotlarini himoya qilish masalasida ishonchsizlikka moyil qilib qo'ydi. Korxonalarning tahdid boshqaruviga oid amaliyotlarini to'liq va shaffof tarzda oshkor qilishi jamoatchilik ishonchini saqlab qolish yoki qayta tiklash uchun juda ahamiyatlidir.

Ekvifaks (Equifax¹¹⁷) mojarosi

Dunyoning eng muhim kredit hisobotlari agentliklaridan biri bo'lgan Equifax bilan bog'liq yaqinda sodir bo'lgan voqea tahdidlarni oshkor qilish bo'yicha tegishli amaliyotlar mavjud bo'lmaganda yoki agar ular mavjud bo'lsa, ularga rioya qilinmasa, nima sodir bo'lishi mumkinligi haqida ajoyib misolni taqdim etadi. 2017-yil may va iyul oylarida AQSHning Atlanta shahrida joylashgan Equifax

¹¹⁷ EQUIFAX – AQSHning Atlanta shahrida joylashgan ko'pmillatli iste'mol kredit hisobotlari agentligi.

agentligi bugungi kungacha tarixdagi eng yomon ma'lumotlar sizib chiqishi hodisasini boshdan kechirdi. AQSH, Buyuk Britaniya va Kanadadagi 160 milliondan ortiq odamning shaxsiy ma'lumotlari ruxsatsiz oshkor etildi, AQSH hukumati-ning da'vo qilishicha, ushbu keng miqyosdagi maxfiy va boshqa ma'lumotlarning o'g'irlanish hodisasi Xitoy Xalq Respublikasida davlat tomonidan homiylik qilingan jinoyatchilar tomonidan amalga oshirilgan. Xakerlar Equifaxning server xavfsizligi yangilanishlarini amalga oshirmaganidan foydalanib, kompaniyaning ma'lumotlar bazalarini ikki oydan ortiq vaqt davomida yashirin tarzda skanerlashga muvaffaq bo'lishdi.

Equifax agentligining xavfsizlik amaliyotidagi beparvoligi kamida uch mamlakatdagi kompaniya mijozlari, aksiyadorlari va tartibga soluvchilari uchun katta muammo tug'dirdi. Ammo Equifax amalga oshira olmagan yana bir narsa kompaniyaga ayniqsa katta zarar keltirdi va bu narsa ushbu bob uchun alohida ahamiyatga ega.

Kompaniya ma'lumotlarning o'g'irlanishi holatini 2017-yil iyul oyida aniqladi, faqatgina bu haqda sentyabrda xabar berdi va hatto o'sha paytda ham buzg'unchilikning to'liq ko'lami haqida aniq ma'lumot berilmadi. (Kompaniyaning yuqori bo'g'indagi rahbarlarini tez harakat qilmaganliklari uchun ayblab bo'lmaydi, chunki bu ularning shaxsiy manfaatlariga mos edi. Ulardan uchta, shu jumladan moliyaviy direktor, buzg'unchilik aniqlanganidan ko'p o'tmay, ammo hodisa oshkor etilishidan va aksiyalar narxi tushib ketishidan ancha oldin Equifax aksiyalarini deyarli 1,8 million dollarga sotgan.) 2018-yilning mart oyi oxirida Equifax ma'lumotlari o'g'irlangan shaxslar soni bo'yicha o'z hisob-kitoblarini qayta ko'rib chiqqan, shuningdek, qanday ma'lumotlar o'g'irlanganligi to'g'risidagi hisobotini o'zgartirgan. Shuni aytish joizki, sud va tartibga soluvchi organlar, ayniqsa SEC talab qilganidek, ma'lumotlar sizib chiqishi hodisasi to'g'risidagi ma'lumotlarning o'z vaqtida va to'g'ri tarzda eskalatsiya hamda oshkor qilinmaganligi sababli bu hodisa juda katta zarar olib keldi.

Bu hujumdan ko'rilgan zararlar, ushbu kitob o'quvchilariga tanish bo'lgan namuna bo'yicha sodir bo'ldi. Equifax ma'lumotlarining o'g'irlanishi haqidagi ma'lumotlar oshkor qilinganidan bir necha kun o'tgach, uning aksiyalari qiymati hayratlanarli darajada 4 milliard dollarga tushib ketdi. Equifax kompaniyasi obro'si, ayniqsa, moliyaviy xizmatlarda jiddiy zarar ko'rdi, chunki bu sohada ishonch — bu kompaniyaning eng muhim aktivlaridan biri sanaladi. Albatta, sud jarayonlari bo'lib o'tdi, 2021-yilda taxminan 425 million dollar evaziga hal qilingan ommaviy sud da'vosi shular jumlasidandir. FTC, boshqa nazorat organlari va ko'plab shtat hukumatlari tomonidan ko'rilgan choralar natijasida Equifax jabrlanuvchilarga yetkazilgan zararni qoplash jamg'armasiga 300 million dollar, AQSH shtatlari va hududlariga 175 million dollar va federal jarimalar sifatida 100 million dollar to'lashga majbur bo'ldi.

Shubhasiz, bunday miqyosdagi ma'lumotlarning sizib chiqishi Equifax yoki boshqa har qanday korxonaga katta zarar yetkazishi mumkin edi, ammo aynan kompaniyaning ma'lumotlar sizib chiqishi to'g'risidagi ma'lumotlarni oshkor qilish bo'yicha o'z majburiyatini bajarmaganligi falokatni fojiga aylantirdi. Qo'shma Shtatlarda faoliyat yuritayotgan ochiq aksiyadorlik kompaniyasi sifatida Equifax "muhiim ahamiyatli" deb belgilangan har qanday tahdidlarni o'z vaqtida oshkor qilish majburiyatiga ega edi. Oqilona me'yorlarga amal qilmaslik orqali kompaniya o'zini tasavvur qilish mumkin bo'lgan eng jiddiy huquqiy va normativ javobgarlikka duchor etdi. Sodda qilib aytganda, muhiim ahamiyatga ega bo'lgan tahdid – bu kompaniyaga sarmoya kiritish yoki kiritmaslik to'g'risidagi qarorga ta'sir qilishi mumkin bo'lgan tahdiddir. SEC tahdidning muhiim ahamiyatga ega ekanligini aniqlash uchun aniq va tushunarli standartni o'rnatdi: "oqil investor qaror qabul qilishda ma'lumotni muhiim deb hisoblashi ehtimoli mavjudmi yoki oqil investor ushbu ma'lumotni mavjud bo'lgan ma'lumotlar «umumiy to'plamining» muhiim o'zgarishi sifatida qabul qiladimi»¹¹⁸.

Aynan muhiim ahamiyatga ega masalalarni oshkor qilmaslik Equifax uchun juda halokatli bo'ldi. Equifax kompaniyasining tahdid bilan bog'liq hodisani oshkor qilmaslikning ko'plab holatlari oqibatida yuzaga kelgan moliyaviy, obro'-e'tibor va boshqa zararlarni hisoblashning iloji yo'q. Faqatgina pul ko'rinishdagi xarajatlarning o'zi milliardlab dollarga yetdi, agar kompaniya SEC va boshqa me'yoriy ko'rsatmalarga rioya qilganida, bu xarajatlar ancha kamroq bo'lar edi.

Bir nechta tahdidlar birlashib, jiddiy tahdidga aylanganda

2016-yilning oxiridan boshlab, AQSHning eng yirik va eng muhiim moliyaviy tashkilotlaridan biri bo'lgan Wells Fargo kompaniyasining roziligisiz millionlab soxta bank hisobvaraqlarini ochish bilan bog'liq katta janjalga aralashib qoldi. AQSHning Wells Fargo banki vakillari mijozlarning mavjud bank hisoblariga yangi hisoblarni qo'shdilar, faqat jamg'arma hisoblariga ega bo'lgan mijozlar uchun esa ularning roziligisiz yoki hatto ularning xabardorligisiz kredit karta hisoblarini ochdilar, natijada ushbu mijozlardan qo'shimcha to'lovlar va yig'implar undirildi.

AQSHning Iste'molchilarni moliyaviy himoya qilish byurosi (CFPB)¹¹⁹ kabi tartibga soluvchi organlar Wells Fargo kompaniyasiga jami 185 million dollar miqdorida jarima soldi, chunki tashkilot keng ko'lamli soxtalashtirish bilan shug'ullanganligi aniqlangandi. Hali ham davom etayotgan ko'plab sud jarayon-

¹¹⁸ Sidni Pozner, "S-K Nizomini modernizatsiya qilish bo'yicha SEC taklifi", Garvard yuridik maktabining korxona boshqaruvi bo'yicha forumi, 2019-yil 20-avgust, <https://oreil.ly/zDzTt>.)

¹¹⁹ CFPB (Consumer Financial Protection Bureau) – Iste'molchilarni moliyaviy himoya qilish byurosi.

lari qariyb 3 milliard dollar miqdorida zarar undirishni talab qilmoqda. Bank bosh direktori iste'foga chiqishga majbur bo'ldi, kompaniyaning obro'siga jiddiy ziyon yetkazildi va bu hamon davom etmoqda.

“Bir nechta tahdidlar yig'indisi jiddiy tahdidga aylanadi” deganda nima nazarda tutilayotganiga Wells Fargo kompaniyasi bilan bog'liq mojaro ajoyib misol bo'la oladi. Har bir soxta hisobni yaratish nisbatan kichik bir huquqbuzarlikni ifoda etadi (aniqrog'i, ularning har biri deyarli jinoyiy firibgarlik bo'lgan, ammo har bir mijoz uchun yetkazilgan zarar aksariyat hollarda juda kam edi). Agarda, masalan, ushbu amaliyot faqat bitta bank filiali yoki hatto bitta faoliyat ko'rsatish hududi bilan cheklangan bo'lganida, u muhim ahamiyatga ega bo'lgan tahdidni anglatmas edi, ya'ni SEC va boshqa nazorat organlariga oshkor qilish shart bo'lmagan bo'lardi. Biroq, ish bo'yicha o'tkazilgan tergov-tekshiruvlar shuni aniq ko'rsatdiki, firibgarlik keng ko'lamlı bo'lib, filial vakillariga “kesishma savdo” (cross-selling) deb nomlangan amaliyot bilan shug'ullanish uchun kuchli korporativ bosim natijasida kelib chiqqan. Tergovlar shuni ham ko'rsatdiki, Wells Fargo kompaniyasining yuqori bo'g'in rahbarlari keng ko'lamlı firibgarlik sodir bo'layotganligini bilishgan yoki bilgan bo'lishlari kerak edi. Bu barcha mayda firibgarlik operatsiyalarini “umumiy miqdorda ahamiyatli” qilib qo'ydi, shu sababli ular SEC hamda boshqa tartibga soluvchi organlarning oshkoralik qoidalariga bo'ysunishi kerak edi. Natijada, kichik muammolar katta muammoga aylandi va hozirgi kungacha Wells Fargo kompaniyasi hamda uning aksiyadorlariga jiddiy zarar yetkazishni davom ettirmoqda.

Kiberhujumlarga nisbatan bunday holatning qanday ishlashiga misol keltiramiz: bir qator kichik buzg'unchilik holatlari (barcha kichik firibgarliklarning raqamli muqobili) umumiy hisobda muhim ahamiyatga ega bo'lishi mumkin. Bu, albatta, korxona aksiyalarini sotib olish yoki sotishni o'ylayotgan investor uchun muhim bo'lishi mumkin hamda aynan shu narsa uni muhim hodisaga aylantiradi. SEC o'zining so'nggi kiberqoidalarida “kiberxavfsizlik hodisasi”ning ta'rifi “bir-biri bilan bog'liq bo'lgan ruqsatsiz holatlar qatori”ni ham o'z ichiga olishini alohida ta'kidlagan. Misol tariqasida, aynan bir jinoyatchining vaqt va shaklda bir-biri bilan bog'liq bo'lgan bir qator kichik kiberhujumlarni amalga oshirishi yoki bir nechta jinoyatchining bir xil zaiflikdan foydalanib, birgalikda kompaniyaning samarali faoliyatiga to'sqinlik qiladigan bir-biriga aloqador hujumlarni amalga oshirish jarayonini keltirishimiz mumkin.

SECning muhimlik haqidagi mezonlari

SEC ochiq aksiyadorlik jamiyatlari kiberxavfsizlikka oid tahdidlarni oshkor etish yoki etmaslikni aniqlashda e'tiborga olishi kerak bo'lgan masalalar ro'yxatini taqdim etdi. (Ta'kidlash joizki, ushbu ro'yxat hali to'liq shakllangan emas.) Muhimlik darajasini aniqlash umumiy tahlil asosida yoki SEC ta'biri bilan aytganda, quyidagi mezonlarning “umumiy to'plami” asosida amalga oshirilishi lozim:

• Ilgari yuz bergan kiberxavfsizlik hodisalari, shu jumladan, ularning jiddiy-ligi va takrorlanish darajasi

• Kiberxavfsizlik hodisalarining yuz berish ehtimoli va ularning potentsial ta'siri

• Kiberxavfsizlikka oid tahdidlarni kamaytirish uchun ko'rilgan profilaktik choralarning samaradorligi hamda ularga bog'liq xarajatlar, shu bilan birga, kompaniyaning muayyan kiberxavfsizlik tahdidlarini oldini olish yoki yumshatish imkoniyatlarining cheklovlari haqidagi muhokamalarni o'z ichiga oladi

• Kompaniya biznes va faoliyatining muhim kiberxavfsizlik tahdidlarini keltirib chiqaradigan jihatlari va bunday tahdidlarning ehtimoliy xarajatlari hamda oqibatlari, shu jumladan sohaga xos tahdidlar va uchinchi tomon ta'minotchilari hamda xizmat ko'rsatuvchi provayderlar bilan bog'liq xavf-xatarlar

• Kiberxavfsizlikni ta'minlash bilan bog'liq xarajatlar, shu jumladan kiberxavfsizlik hodisalari yoki xizmat ko'rsatuvchi provayderlarga to'lovlar bilan bog'liq har qanday sug'urta qoplamasi

• Obro'ga zarar yetkazish ehtimoli

• Kompaniyaning kiberxavfsizlik talablariga va ular bilan bog'liq xarajatlarga ta'sir ko'rsatishi mumkin bo'lgan amaldagi yoki taklif etilayotgan qonun va qoidalar

• Kiberxavfsizlik hodisalari bilan bog'liq bo'lgan sud jarayonlari, nazorat organlari tomonidan o'tkaziladigan tekshiruvlar va zararni bartaraf etish xarajatlari

Tahdid to'g'risidagi qarorlar umumiy ma'lumot va umumiy tushunchaga asoslangan holda qabul qilinishini ta'minlash maqsadida, korxonalarning tahdidlarni boshqarish amaliyoti bilan tahdidlarni boshqarish amaliyotlari to'liq muvofiqlashtirilishi kerak.

INQIROZ FOJIAGA AYLANMASLIGINI TA'MINLASH

2021-yilda Colonial Pipeline¹²⁰ kompaniyasiga qarshi amalga oshirilgan ransomware hujumi nafaqat kiberxavf muhiti qanchalik xatarli bo'lib qolganini ko'rsatadigan misol, balki u tez va to'g'ri choralar ko'rish hamda ma'lumotlarni oshkor etishning afzalliklarini ham yaqqol namoyish etadi. Bu afzalliklar hujumga duchor bo'lgan korxona, uning aksiyadorlari va jamoatchilik uchun tezkor, tegishli eskalasiya va oshkor qilishning afzalliklarini aniq ko'rsatadi. Ekvifaks va jiddiy kibertahdidlarga duch kelgan ko'plab boshqa korxonalardan farqli o'laroq, Colonial kompaniyasi o'z muammolarini tezda ko'tarib chiqdi hamda vaziyat, uning ehtimoliy oqibatlari va o'zi amalga oshirayotgan choralar haqida ochiq va samimiy ravishda ma'lumot berdi. Keling, 2021-yildagi voqealar xronologiyasiga e'tibor qarataylik:

¹²⁰ Colonial Pipeline – AQSHda qayta ishlangan neft mahsulotlari uchun eng yirik quvur liniyasi tizimi.

• 6-may: xakerlar Colonial kompaniyasi tizimlariga hujum qilib, ma'lumotlarni o'g'irlashadi, kompyuterlarni blokirovka qilishadi va to'lov talab qilishadi.

• 7-may: Colonial kompaniyasi to'lov sifatida 4,4 million dollar to'laydi.

• 8-9-may: Kompaniya hujumga uchraganini ochiq e'lon qiladi va ba'zi quvurlar va boshqa tizimlarni o'chirib qo'yadi, so'ngra tizimlarni qayta ishga tushirish rejalarini batafsil bayon qiladi.

• 10-11-may: Federal tekshirishlar byurosi (FTB) hujumda maxsus to'lov dasturi (DarkSide) ishlatilganligini tasdiqladi va u bilan to'qnashadigan korxonalar uchun axborot byulleteni chiqaradi.

• 12-may: Colonial kompaniyasi o'z faoliyatini davom ettiradi, sotib olish bilan bog'liq vahimani kamaytirish maqsadida yoqilg'i yetkazib berish muddatini e'lon qiladi.

Bir haftaning o'zida, Colonial kompaniyasi o'z faoliyatini to'xtatib qo'ygan halokatli kiberhujumdan to'liq tiklandi. Kompaniya obro'siga putur yetkazishi mumkin bo'lgan zararni kamaytirdi, chunki u o'zi bajarishi lozim bo'lgan barcha ishlarni aniq bajargan va nazorat qiluvchi organlar yoki qonun chiqaruvchi organlar tomonidan jiddiy tanqidga duch kelmagan. Darhaqiqat, hujum jamoat manfaati yo'lida muhim harakatlarga olib keldi, jumladan, quvurlar xavfsizligi to'g'risidagi qonunning qayta joriy etilishi, neft va gaz quvurlari uchun xavfsizlik mas'uliyatlarini aniqlashtirish to'g'risidagi qonun loyihasini va ichki xavfsizlik departamentining yangi quvur liniyasi kiberxavfsizlik talablarini tavsiflovchi dasturini qayta joriy etishga olib keldi. Colonial kompaniyasi ko'rgan choralarni g'ayrioddiy yutuq deb atash mumkin, korxonalarning kibertahdid hodisalariga javob reaksiyalari aynan shunday bo'lishi kerak. Sudlar va nazorat qiluvchi organlar ulardan aynan shunday javob reaksiyasini kutishadi. Ular masalalarni tegishli va javobgar shaxslarga yetkazishlari va tahdid haqidagi ma'lumotlarni tegishli manfaatdor tomonlar hamda vakolatli organlarga oshkor qilishlari kerak. Buni izchil va samarali tarzda amalga oshirishining yagona yo'li – bu korxonaning rasmiy CRMPga ega bo'lishidir.

CRMP bilan ERMni muvofiqlashtirish

ERM va kibertahdidlarni boshqarish amaliyoti korxonalarni hamda ularning xodimlarini himoya qilish va biznesning uzluksizligini ta'minlash uchun zarur bo'lib, ikkalasi ham huquqiy va normativ talablar va sohaga doir tamoyillarga tayanadi. Ularning ikkalasi ham ko'plab korxona manfaatdor tomonlarining, shu jumladan, direktorlar kengashi, yuqori rahbariyat va bo'limlarning hamda yuridik, muvofiqlik va auditning yaqin hamkorligini hamda axborot texnologiyalari ishtirokini talab qiladi. Lekin ular orasida muhim farqlar mavjud. ERM barcha turdagi tahdidlarni qamrab oladi. Bundan farqli o'laroq, kibertahdidlarni boshqarish asosan korxonalarning murakkab o'zaro bog'langan raqamli texnologiyalarga tobora ko'proq tayanishi natijasida yuzaga keladigan zararli xavflarga qaratilgan bo'lib, bu ko'proq texnik bilim va maxsus vositalar hamda texnologiyalarni talab etadi. Bu farqlarni aniq belgilash juda muhim, chunki ko'plab korxonalar asosan kibertahdidni korxona tahdid ostida "yashirib" qo'yishadi, bu esa aynan kibertahdidlarni aniqlash va ularni eskalatsiya qilish hamda tahdidlar bilan bog'liq ma'lumotlarni oshkor qilishni ancha qiyinlashtiradi.

Shunday bo'lsa-da, kibertahdid bu korxona tahdididir, sudlar va tartibga soluvchi organlar uni shunday deb hisoblash kerakligini aniq ko'rsatdilar. Shu sababli, kibertahdid to'g'risidagi qarorlar mavjud bo'lgan har qanday umumiy tahdidlarni boshqarish dasturiga mos kelishi kerak (bu rasmiy ERM dasturi bo'lishi yoki bo'lmasligi mumkin). Bu juda ko'plab "siyosiy" muammolarni keltirib chiqaradigan tashkiliy muvofiqlashtirish masalasi emas, balki dasturlar va dastur maqsadlarini muvofiqlashtirishga, ma'lumot to'plashni muvofiqlashtirish, hisobot berish, tahdid va foydaning tegishli muvozanatini kelishib olishga qaratilgan. Bu CRMPning qolgan uchta komponentini belgilaydigan tamoyillarda umumiy mavzu bo'lib kelgan (3–5-boblar).

Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili

Kitobda biz taqdim etgan dastur, tashkilotning tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlarini ishlab chiqish, ko'rib chiqish va amalga oshirishda asosiy omil bo'ladigan muhim tamoyillarni aniqlash uchun qo'llanilishi mumkin (6.1-jadvalga qarang).

6.1-jadval

CRMP-Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish

CRMP tarkibiy qismlari	Tamoyillar	Ma'lumot manbalari
Moslashuvchan boshqaruv	75-betda "Moslashuvchan boshqaruvning yetti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACD¹²¹ning direktorlar qo'llanmasi • ISO 27001:2022 • NIST 8286 • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • ISO 31000:2018 • AICPAning CRMP
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	94-betda "Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP

¹²¹ NACD (National Association of Corporate Directors) – Korxona rahbarlari milliy uyushmasi.

Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	120-betda "Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	151-betda "Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • AICPAning CRMP

Keng qamrovli tizimning o'zi haqida batafsil ma'lumot olish uchun Ilovaga qarang.

Kibertahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi, CRMPning boshqa tarkibiy qismlari singari, barcha holatlarga mos keladigan yagona yechim emas. Korxonalar biz muhokama qilib kelayotgan barcha omillardan ta'sirlangan holda turli xil kibertahdid muhitlariga duch kelishadi. Ular, shuningdek, tahdidni bartaraf etish uchun turli xil imkoniyatlarga ega va eng muhimi, turli huquqiy standartlar va tartibga solish talablariga muvofiq faoliyat olib boradilar. Ya'ni barcha samarali kibertahdidlar eskalatsiyasi va ular bilan bog'liq ma'lumotlarni oshkor qilish amaliyotlari muayyan asosiy tamoyillarga asoslanadi.

1-TAMOYIL: ESKALATSIYA JARAYONLARINI O'RNATISH

Kibertahdidlarni eskalatsiyasi qilish jarayonlari ishlab chiqilishi va joriy etilishi lozim.

Ushbu kitob davomida biz aniq belgilangan rollar, funksiyalar, mas'uliyat va javobgarlik bilan rasmiylashtirilgan jarayonlarning muhimligini ta'kidladik va bu jarayon tahdidlar eskalatsiyasi amaliyotida juda muhimdir. Ushbu amaliyotlar, kibertahdidlarni boshqarishning ko'plab boshqa jihatlarini kabi, ko'pincha norasmiy, vaqtinchalik yoki shaxsiy munosabatlarga asoslangan holda amalga oshiriladi. Hatto tahdidlar eskalatsiyasi jarayonlari mavjud bo'lgan taqdirda ham, ular ko'pincha yetarli darajada aniqlanmagan bo'lib, tahdidlarni tasniflash mexanizmlari tegishli manfaatdor tomonlarni tahdidlar haqida xabardor qilish hamda ularni tegishli boshqaruv darajalariga yetkazish majburiyatlarini aniq belgilamaydi. Yana bir zaif tomoni, tahdidning haqiqiy darajasini aniqlash uchun zarur bo'lgan biznes konteksti bo'lmagan nazoratning nosozliklari yoki zaifliklarining eskalatsiyasi hisoblanadi. Tahdidni aniqlash tenglamasini esda tutish muhimdir: *Ehtimollik (Zaiflikdan foydalanadigan tahdid) x Ta'sir (korxona jarayoni, aktivlari yoki*

maqsadiga). Lekin nazorat muvaffaqiyatsizligi yoki zaiflik bu tenglamaning faqat yarmini aks ettiradi.

Korxonaga xos mezonlarga asoslangan va boshqaruv organi tomonidan tasdiqlangan tahdid tasniflari CRMPning asosini tashkil etadi. Ular tahdidning jiddiyligi va shoshilinchlik darajasini belgilash uchun ishlatiladi, shunda tahdidlarni kamaytirish yoki boshqarish uchun tegishli ustuvorlik qarorlari qabul qilinishi va tegishli choralar ko'rilishi mumkin. Har bir tasnif uchun aniq mezonlarni belgilash tashkilotlarga eskalatsiya va oshkor qilish jarayonini ustuvorlashtirishga, eskalatsiya va ma'lumotlarni oshkor qilishda shaxslar yoki tashkilotlarning javobgarligini belgilashga va tahdidga oid qarorlar qabul qilish, ma'lumot berish va eskalatsiya qilish boshqaruvning tegishli darajalarida amalga oshirilishini ta'minlashga imkon beradi.

Belgilangan tahdid tasniflari va tegishli boshqaruv darajalariga muvofiqlashtiriladigan tahdidlar eskalatsiyasi jarayonlariga bo'lgan ehtiyoj keng ko'lamli standartlar va protokollarga tayanadi, jumladan:

SEC yo'riqnomasi S-K 106(c) bandi – Boshqaruv

Rasmiy eskalatsiya jarayonlari – kiberxavfsizlik tahdidlaridan kelib chiqadigan xavflarni nazorat qiluvchi kengash va bu tahdidlarni baholab boshqaradigan rahbariyat uchun juda zarur. Bu jarayonlar kengashga yo'l-yo'riq ko'rsatish, kiberxavfsizlik tahdidlaridan kelib chiqadigan muhim xavflarni baholash hamda ularni boshqarish, tahdid haqidagi ma'lumotlarning tegishli shaffofligini ta'minlash uchun kerak. Kompaniyalar muhim kibertahdidlar va xavflarni boshqaruv organi orqali ma'lum qilishlari kerak, bu esa eskalatsiya uchun belgilangan yo'l-larning muhimligini ko'rsatadi.

SECning 2018-yilgi bayonoti va Ochiq aksiyadorlik jamiyatlarining kiberxavfsizlik bo'yicha ma'lumotlarni oshkor qilish bo'yicha yo'riqnomasi

SEC o'zining 2018-yilgi yo'riqnomasida kibertahdidlarni samarali boshqarish hamda korxonalarning potensial kibertahdidlarni tezda aniqlash, baholash va ularga chora ko'rish imkoniyatini ta'minlash uchun tahdidlarni eskalatsiya qilishning rasmiy tartiblarini yaratish muhimligini ta'kidladi. Shunday qilish orqali, kompaniya o'z faoliyatiga, mijozlariga va umumiy bozor barqarorligiga tahdid va potensial ta'sirni kamaytirishi mumkin. SEC bayonoti va yo'riqnomasining uchta komponenti, ayniqsa, ma'lumotlarni oshkor qilish masalasiga tegishli:

- “Ochiq aksiyadorlik jamiyatlarining kibertahdidlar va xavfsizlik hodisalari to'g'risidagi ma'lumotlarni o'z vaqtida oshkor qilish qobiliyati uchun, nazorat va oshkor etish tartib-taomillari juda muhimdir, ular bunday masalalar kompaniya va uning biznesi, moliyaviy ahvoli va ish faoliyati natijalariga ta'sirini aniqlashning tegishli usulini, shuningdek bunday tahdid va hodisalarning potensial ahamiyatini aniqlash uchun protokolni ta'minlaydi” (1-bet, 1-band).

- “Kompaniyalar kibertahdidlar va hodisalar to‘g‘risidagi tegishli ma’lumotlar qayta ishlanishini va tegishli xodimlarga, shu jumladan yuqori boshqaruv bo‘g‘inlariga yetkazilishini ta’minlash uchun yetarli darajada oshkor qilish nazorati va tartib-qoidalariga ega ekanligini baholashlari kerak. Bu jarayon yuqori rahbariyatga ma’lumotlarni oshkor qilish bo‘yicha qarorlar qabul qilish imkonini beradi” (18-bet, 3-band).

- “Nazorat va tartib-qoidalar kompaniyalarga kiberxavfsizlik tahdidlari va hodisalarini aniqlash, ularning kompaniya faoliyatiga ta’sirini baholash va tahlil qilish, bunday tahdidlar va hodisalarning ahamiyatini aniqlash, texnik mutaxassislar va ma’lumotni oshkor qilish bo‘yicha maslahatchilar o‘rtasida ochiq aloqalarni ta’minlash hamda bunday tahdidlar va hodisalar to‘g‘risida o‘z vaqtida ma’lumotlarni oshkor qilish imkonini berishi kerak” (20-bet, 1-band).

AICPAning 2017-yilgi CRMP tavsif mezonlari DC13, DC16.

Buxgalteriya sohasiga oid ushbu ikki standart kibertahdidlar to‘g‘risidagi tegishli ma’lumotlarni, shu jumladan maqsadlar va majburiyatlarni hamda eng muhimi, xavfsizlik hodisalarini aniqlash va ularga chora ko‘rish chegaralarini ichki aloqa orqali yetkazish uchun belgilangan jarayonlarni talab qiladi. AICPA, shuningdek, aniqlangan xavfsizlik tahdidlari, zaifliklar va kamchiliklarni o‘z vaqtida baholash va tegishli tomonlarga, shu jumladan, zarur bo‘lganda direktorlar kengashiga ham xabar berish jarayonini talab qiladi.

NACDning 2023-yilgi Kibertahdidlarni nazorat qilish bo‘yicha direktorlar qo‘llanmasi, 2-tamoyil.

NACD qo‘llanmasining 2-tamoyilida tahdidlarni eskalatsiya qilish uchun rasmiy jarayonlar zarurligi ta’kidlanadi. Kiberxavfsizlik nuqtayi nazaridan, bu kibertahdid qachon huquqiy chora ko‘rish yoki ma’lumotlarni oshkor qilishni talab qiladigan darajaga yetishini aniqlashni anglatadi. Samarasiz tahdid eskalatsiyasi, agar to‘g‘ri amalga oshirilmasa, qonuniy javobgarlikka olib kelishi mumkin.

2-TAMOYIL: BARCHA KORXONALAR UCHUN MA'LUMOTLARNI OSHKOR QILISH JARAYONLARINI YO'LGA QO'YISH

Korxonaning kiberma'lumotlarini oshkor etish jarayonlari uning o'ziga xos tahdid omillarini, tashkiliy sharoitlarini va talablarini inobatga olgan holda ishlab chiqilishi lozim.

Turli korxonalarining tahdid muhitlari o‘rtasidagi keng tafovutlar shuni anglatadiki, ularning ma’lumotlarni oshkor qilish jarayonlari va tartib-qoidalar har bir korxonaga xos bo‘lgan tahdid omillari, muhit va talablarga moslashtirilishi kerak. Tahdidlarni boshqarishning rasmiy jarayonlari korxonaga xos bo‘lgan barcha tahdidlarni to‘liq aniqlash va tahlil qilish uchun mavjud bo‘lishi kerak (nafaqat allaqachon sodir bo‘lgan tahdid yoki hodisani, balki umumiy tahdid muhitidagi o‘zgarishlarni ham) va ular qanday boshqarilishini, shu jumladan tahdidlarni qabul qilish, kamaytirish va o‘tkazish orqali hujjatlashtirish kerak.

Tahdidlarga oid ma'lumotlarni oshkor qilish tahdid va hodisalar-ga chora ko'rishdan ko'ra ko'proq narsani anglatadi.

Korxonaning mas'ul tomonlari: tahdidlar bo'yicha mas'ul xodimlar, boshqaruv organlari, yuqori darajadagi rahbarlar va direktorlar kengashi o'zlarining tahdid muhitini va unga qarshi choralar ko'rishdagi mas'uliyatlarini aniq tushunishlari kerak. Ushbu bobda ilgari muhokama qilingan bir nechta tushunchalar ushbu masala bo'yicha ayniqsa dolzarbdir. Ulardan biri, shubhasiz, muhimlik masalasidir: tahdidga oid ma'lumotlarni oshkor qilish tartib-qoidalarini nimaning muhim tahdid va nimaning muhim tahdid emasligini aniqlashga hamda bunday tahdidlarga javoban qanday choralar ko'rilishi kerakligini tan olishga asoslanishi lozim. Qoidalarga rioya qilish yana bir muhim masala bo'lib, rioya qilish talablari korxona sohasi, faoliyat ko'rsatadigan mintaqalar, uning hajmi va hatto tashkiliy tuzilishiga qarab farq qiladi. Bularning barchasi va yana ko'plab boshqa narsalar, qanday tahdid va tahdidga oid masalalar oshkor qilinishi kerakligini, kimga va eng muhimi, qanchalik tez oshkor qilinishi kerakligini belgilaydi.

Ma'lumotlarni oshkor qilish – bu kibertahdidni umumiy korxona tahdididan aniq farqlash kerak bo'lgan yana bir sohadir. SEC va boshqa nazorat qiluvchi organlar, keng tarqalgan tahdid turlarini umumlashtirish amaliyoti maqbul emasligini aniq ko'rsatdi. Buning natijasida, kibertahdid korxona tahdidi ortida qolib ketadi hamda uning o'ziga xos maxsus talablari yetarli darajada tan olinmasligi va e'tiborga olinmasligi mumkin. SEC, xususan, ochiq aksiyadorlik jamiyatlari-ni kibertahdidlarni oshkor qilish amaliyoti o'ziga xos, aniq yoki o'z vaqtida emasligini ta'kidlab o'tdi. Aytilishicha, ba'zida SEC kompaniyaning kibertahdid hodisasi haqida ommaviy axborot vositalaridan, kompaniya bu haqida oshkor qilmasidan oldin (agar muammo umuman oshkor etilsa) bilib oladi. Shularni hamda kibertahdidlarning o'ziga xos darajada tez rivojlanayotganini tan olgan holda, SEC va boshqa tartibga soluvchilar kibertahdidni umumiy korxona tahdididan alohida aniqlash va u haqida hisobot berishni tobora ko'proq talab qilmoqda.

Korxonaga xos ma'lumotlarni oshkor qilish tartib-qoidalariga bo'lgan ehtiyoj standartlar va protokollar bilan belgilanadi, shu jumladan:

NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 2-tamoyil.

Ochiq aksiyadorlik jamiyatlari kiberxavfsizlik bilan bog'liq jiddiy tahdidlar-ni, tahdid omillarini va hodisalarini oshkor qilishlari kerak. Bunday muhim ma'lumotlarni oshkor qilish ko'pincha huquqiy ta'sirga ega va ko'pincha qonun hujjat-lari bilan belgilanadi, shuning uchun NACD bu masalaga alohida e'tibor qaratadi.

AICPAning 2017-yilgi CRMP tavsif mezonlari, DC6 va DC14

Ajablanarli emaski, buxgalteriya hisobi bilan bog'liq standartlar, ayniqsa, kiberxavfni oshkor qilish tartib-qoidalarini haqida gap borganda qat'iy talablarga ega.

DC6 oldingi 12 oy ichida aniqlangan, korxonaning kiberxavfsizlik maqsadlariga erishishiga sezilarli darajada putur yetkazgan xavfsizlik insidentlarini, shuningdek, hodisalarning tabiati, vaqti, darajasi yoki ta'siri va ularning joylashuvi haqidagi ma'lumotlarni oshkor qilishni taklif qiladi. DC14 tashkilotning CRMP faoliyatiga ta'sir qiladigan masalalar bo'yicha tashqi tomonlar bilan muloqot qilish jarayonini belgilaydi.

NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi, 2.0 GVOC-03

NISTning ushbu kichik turkumida kiberxavfsizlik bo'yicha huquqiy, tartibga soluvchi va shartnomaviy talablar, shu jumladan shaxsiy hayot daxlsizligi va fuqarolik erkinliklari bilan bog'liq majburiyatlarni tushunish va boshqarishga e'tibor qaratiladi. Ushbu talablar ko'pincha oshkor qilish bo'yicha maxsus qoidalarni o'z ichiga oladi, shuning uchun ushbu talablarni tushunish va boshqarish ma'lumotlarni to'g'ri oshkor qilish tartib-qoidalari uchun muhim ahamiyatga ega.

3-TAMOYIL: OCHIQ AKSIYADORLIK JAMIYATLARI UCHUN MA'LUMOTLARNI OSHKOR QILISH JARAYONLARINI O'RNATISH

Ochiq aksiyadorlik jamiyatlari jiddiy tahdidlarni, tahdid omillarini, kibertahdidlarni boshqarish jarayonlarini, boshqaruv tizimi va jiddiy hodisalar haqidagi ma'lumotlarini oshkor qilishlari shart.

Mahalliy va xalqaro ochiq aksiyadorlik jamiyatlari, hozirgi va kelajakdagi sarmoyadorlarning ishonchini saqlab qolish uchun tahdidlarni oshkor qilish bo'yicha qat'iy mas'uliyatga ega. Sarmoyadorlar, huquqiy jarayonlar va me'yoriy talablar bilan aniq belgilangan huquqqa ega bo'lib, ular asosli investitsiya qarorlarini qabul qilish, kompaniyaning faoliyatini baholash hamda kompaniya rahbariyatini, shu jumladan, direktorlar kengashini javobgarlikka tortish huquqiga egadirlar. Ushbu huquqlar, shubhasiz, ochiq aksiyadorlik jamiyatlarining kibertahdidlarni boshqarish amaliyotiga, jumladan ularning umumiy strategiyasi, boshqaruv amaliyotlari va hodisalarga javob berish choralariga ham taalluqlidir. Kibertahdidlarni boshqarishning barcha jihatlarini ma'lumotlarni aniq va o'z vaqtida oshkor etish jarayonining to'liq shaffofligini talab qiladi.

Ma'lumotlarni oshkor qilish amaliyotlariga bo'lgan ehtiyoj ko'plab omillar tufayli kelib chiqadi, jumladan bu kompaniyaning brend obro'sini himoya qilish, uning nufuziga putur yetkazmaslik va aksiyadorlarning ishonchini saqlab qolish zaruriyati bilan bog'liq. Biroq ochiq aksiyadorlik jamiyatlari uchun ma'lumotni oshkor qilishning eng muhim harakatlantiruvchi omili, shubhasiz, AQSHning SEC tomonidan tartibga solish talablarining keng va tez rivojlanayotgan majmuyi hisoblanadi. Oldingi boblarda muhokama qilib o'tilgan bir qator sud qarorlari shuni ko'rsatadiki, agar ochiq aksiyadorlik jamiyatlari kibertahdidlarni, jumladan xavfsizlik hodisalarini oshkor qilmasa, SEC ularni javobgarlikka tortish vakolati-

ga ega. Shuningdek, ochiq aksiyadorlik jamiyatlari o'z majburiyatlarini bajarma-sa, SEC tegishli choralar ko'rinishini ochiqchasiga ma'lum qildi.

Ochiq aksiyadorlik jamiyatlari uchun ushbu majburiyatlarni bajarishning yagona yo'li – bu kiberxavfsizlik tahdidlarini boshqarish, jumladan strategiya, boshqaruv va javobgarlik, ayniqsa, kiberxavfsizlik hodisalari va boshqa muhim kiberxavf muammolarini o'z vaqtida va to'g'ri oshkor qilish uchun aniq belgilan-gan tartib-qoidalarga ega bo'lishdir.

Ma'lumotlarni oshkor qilish majburiyatlarini belgilaydigan va ularni hal qi-lish tartib-qoidalarini taklif qiladigan asosiy organlar va standartlar quyidagilardir:

SECning 2023-yilgi yakuniy qoidasi, kiberxavfsizlikka oid tahdidlarni bosh-qarish, strategiya, boshqaruv, hodisalarni oshkor qilish qoidasi

Qoidaga kiritilgan har bir bandeda (tahdidlarni boshqarish, strategiya, boshqa-ruv, hodisalarni oshkor qilish) aksiyadorlar va jamoatchilik uchun muhim kiber-tahdid va hodisalarni oshkor qilishda shaffoflikning muhimligi yana bir bor ta'kid-lanadi. Ular, ayniqsa, ochiq aksiyadorlik jamiyatlari o'zlarining kibertahdidlar va muhim voqealar to'g'risida shaffof ma'lumotlar berish mas'uliyatini o'z zimma-lariga olishlari kerak degan tamoyilga mos keladi.

NISTning 2023-yilgi kiberxavfsizlik asoslari loyihasi, 2.0 GVOC-03

Bu tamoyil, xususan, o'zlarining kiberxavfsizlikka oid tahdidlarini boshqa-rish amaliyotlarini oshkor etish bo'yicha muayyan huquqiy va me'yoriy majbu-riyatlarga ega bo'lgan ommaviy kompaniyalarga taalluqlidir. GVOC-03 muhim ahamiyatga ega, chunki u kiberxavfsizlik bo'yicha huquqiy, me'yoriy va shartno-maviy talablarni tushunish va boshqarishga qaratilgan bo'lib, ommaviy kompani-yalar uchun bu o'z ichiga ma'lum oshkor etish talablarini oladi.

SECning 2018-yilgi ochiq aksiyadorlik jamiyatlarining kiberxavfsizlikka oid ma'lumotlarni oshkor qilish bo'yicha bayonoti va yo'riqnomasi

SECning ko'plab qoidalari ko'ra, muhim tahdid – bu korxona tahdidi bo'lib, ular ochiq aksiyadorlik jamiyatlarining kibertahdid bo'yicha mas'uliyatini ular-ni korxona tahdidlari bilan bir xil standartlarga muvofiqlashtiradi:

- “SECning fikriga ko'ra, ochiq aksiyadorlik jamiyatlari investorlarni ki-berxavfsizlik tahdidi va hodisalari to'g'risida o'z vaqtida xabardor qilish uchun barcha zarur choralarni ko'rishlari juda muhimdir, shu jumladan, kiberxavfsizlik riski mavjud bo'lgan, ammo hali kiberhujumning qurboni bo'lmagan kompaniya-lar ham” (4-bet, 1-band).

- “Kompaniyalar muhim hodisalalar, jumladan kiberxavfsizlik bilan bog'liq hodisalarni aniq va o'z vaqtida oshkor etishga imkon beradigan tegishli va sama-rali oshkoralik nazorati va tartib-qoidalarini o'rnatishlari va saqlab turishlari shart. Bunday ishonchli nazorat vositalari va ma'lumotni oshkor qilish tartib-taomilla-ri kompaniyalarga qimmatli qog'ozlar to'g'risidagi federal qonunlarga muvofiq

ma'lumotni oshkor qilish bo'yicha o'z majburiyatlarini bajarishda yordam beradi" (6 va 7-betlar, 2-band).

- "Kompaniyalar 1933-yilgi «Qimmatli qog'ozlar to'g'risidagi qonun» va 1934-yilgi «Qimmatli qog'ozlar va birja to'g'risidagi qonun» bo'yicha ro'yxatdan o'tish bayonnomalarida, shuningdek, Birja to'g'risidagi qonunga muvofiq davriy va joriy hisobotlarda talab qilinadigan ma'lumotlarni taqdim etishda kiberxavfsizlik tahdidlari va hodisalarining ahamiyatini hisobga olishlari kerak" (7-bet, 3-band).

- "Kiberxavfsizlikka oid tahdidlar va hodisalarining jiddiyligi bunday hodisalar keltirib chiqarishi mumkin bo'lgan zarar ko'lamiga ham bog'liq. Bu kompaniya obro'siga, moliyaviy ishlashiga va mijozlar va sotuvchilar o'rtasidagi munosabatlarga zarar yetkazilishini, shuningdek, sud jarayonlari, tergovlar yoki tartibga soluvchi organlar tomonidan, shu jumladan shtat va federal hukumat davlat organlari, AQSHdan tashqaridagi hokimiyat organlari tomonidan tartibga soluvchi tekshiruvlar va choralar ko'rilishi ehtimolini o'z ichiga oladi (11-bet, 1-band).

SECning yangi kiberqoidalariga ko'ra, jamoat kompaniyalari kiberhodisalarni oshkor qilishlari, o'zlarining kibertahdidlarni boshqarish strategiyalari hamda tahdidlarni boshqarish amaliyotlari haqida batafsil ma'lumot berishlari kerak bo'ladi (2-bobda SECning kiber qoidalariga qarang). Aniq belgilangan va amalga oshirilgan CRMP SECning maqsadlariga mos keladi va agar zarur ma'lumotlar tegishli ravishda taqdim etilsa, u ushbu majburiy oshkor etish talablariga javob beradi. Keyingi bo'limlarda SEC qoidalari qamrab oladigan masalalar batafsil yoritilgan.

Jiddiy hodisalar haqida hisobot berish

Qoidaga ko'ra, ochiq aksiyadorlik kompaniyalari jiddiy kiberxavfsizlik hodisalari sodir bo'lganini aniqlaganidan so'ng, to'rt ish kuni ichida ular haqida oshkor qilishlari kerak. Ushbu talab sarmoyadorlar va bozor ishtirokchilariga o'z vaqtida, tegishli va standartlashtirilgan ma'lumotlarni taqdim etishga qaratilgan bo'lib, ularga jiddiy kiberxavfsizlik hodisalari ro'yxatga oluvchining moliyaviy va operatsion holatiga qanday ta'sir qilishi mumkinligini baholash imkonini beradi.

Jiddiyligni baholash kiberxavfsizlik hodisasi bilan bog'liq barcha tegishli faktlar va holatlarni, shu jumladan, miqdoriy va sifat omillarni hisobga olgan holda, ma'lumotlarning umumiy turini puxta va xolisona baholashni o'z ichiga olishi kerak.

Ro'yxatdan o'tuvchilar hodisaning muhimligini oqilona investor nuqtayi nazaridan, asosli va xolis yondashuvga tayanib, ma'lumotlarning umumiy majmua-sini hisobga olgan holda sinchkovlik bilan baholashlari lozim.

Shuningdek, kiberxavfsizlik hodisalari jamuljam holda jiddiy tahdid hodisasini tashkil etganda, u haqidagi ma'lumotlarni oshkor qilish talab etiladi. Ro'yxatdan o'tuvchilar kiberxavfsizlik bilan bog'liq hodisalarni ham alohida, ham jamoa-

viy ravishda muhimlik nuqtayi nazaridan tahlil qilishlari kerak. Agar bunday hodisalar umumiy hisobda muhim bo'lsa, ro'yxatdan o'tuvchilar tegishli ma'lumotlarni oshkor qilishlari kerak. Ushbu talab ro'yxatdan o'tuvchiga birgalikda muhim ta'sir ko'rsatadigan doimiy yoki o'zaro bog'liq kiberhujumlarning shaffoqligi va oshkor etilishini ta'minlaydi.

Tahdidlarni boshqarish va strategiya

Ushbu qoida ochiq aksiyadorli jamiyatining kiberxavfsizlik bilan bog'liq tahdidlarni boshqarish va strategiyasini oshkor etishga qaratilgan. Ushbu talab investorlarga ro'yxatdan o'tganlar kiberxavfsizlik tahdidlarini qanday aniqlashi, baholashi va boshqarishi, shuningdek, ushbu tahdidlarning ularning biznes strategiyasi, moliyaviy istiqbollari va moliyaviy rejalashtirishiga ta'siri to'g'risida yanada izchil va foydali ma'lumotlarni taqdim etishni maqsad qiladi. Bunday oshkor etish talabi investorlarga ro'yxatdan o'tuvchilarning kiberxavfsizlik tahdidlarini boshqarish bo'yicha strategiyalari va harakatlari to'g'risida shaffof ma'lumot beradi hamda bu ularga yaxshiroq investitsiya qarorlarini qabul qilishga imkon beradi.

Boshqaruv

Mazkur qoida ro'yxatdan o'tgan tashkilotning kiberxavfsizlikni boshqarish amaliyotini oshkor qilishga qaratilgan bo'lib, bunda kengashning kiberxavfsizlik tahdidlarini nazorat qilishi va rahbariyatning ushbu tahdidlarni baholash hamda boshqarishdagi o'rni alohida e'tiborga olinadi. Bu risklarni baholash va boshqarishdagi roliga e'tibor qaratadi. Mazkur oshkoralik talablari investorlarga ochiq aksiyadorlik jamiyatining kiberxavfsizlik tahdidlarini boshqarishga bo'lgan yondashuvini yaxshiroq tushunishga yordam beradi, bu esa ularning kompaniyaga sarmoya kiritish to'g'risidagi qarorlariga ta'sir ko'rsatishi mumkin.

4-TAMOYIL: ESKALATSIYA VA MA'LUMOTLARNI OSHKOR QILISH JARAYONLARINI SINOV DAN O'TKAZISH

Kibertahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilish jarayonlari o'zlashtirilgan saboqlarni inobatga olish maqsadida doimiy ravishda tekshirilishi, sinovdan o'tkazilishi va yangilanishi kerak.

Kibertahdidlarni boshqarish – bu doimiy ravishda o'zgarib borayotgan sharoitlar va ayniqsa tahdid muhitidagi o'zgarishlardan xabardor bo'lish va ularga javob berish kerak bo'lgan doimiy amaliyotdir. (Bu, albatta, barcha tahdidlarni boshqarishga taalluqlidir, lekin bu raqamli o'zgarishlar tezligi tufayli kibertahdidlarni boshqarish uchun juda muhim bo'lib qoldi.) Buning mohiyati shundaki, CRMPning asosiy tarkibiy qismi bo'lgan eskalatsiya va ma'lumotlarni oshkor qilish jarayonlari doimiy ravishda tekshirilishi, sinovdan o'tkazilishi va yangilanishi kerak, shundagina butun korxona muvaffaqiyat hamda muvaffaqiyatsizliklardan saboq olishi mumkin.

Xavfsizlik va tahdid bo'yicha mutaxassislar, mas'ullar, boshqaruv organlari va boshqa manfaatdor tomonlar o'zlarining eskalatsiya va ma'lumotlarni oshkor qilish jarayonlarini shubha ostiga qo'yishga tayyor bo'lishlari kerak. Dasturning kibertahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish talablari to'g'risidagi taxminlarini muntazam ravishda sinab ko'rish uchun doimiy, o'zaro ta'sirli jara-yon bo'lishi lozim. Bunda nafaqat yuzaga kelayotgan tahdidlar va zaifliklar, balki sanoat muhitidagi o'zgarishlar va operatsion modellar ham inobatga olinishi zarur. 3-bobda muhokama qilingan "ikkinchi chiziq"ning mas'ullari, ya'ni tahdidlarni boshqarish bo'yicha tajribaga ega bo'lgan mutaxassislar, tahdidlar o'z vaqtida, aniq tarzda va belgilangan darajaga eskalatsiya qilinayotganligini aniqlash uchun mashg'ulotlar olib borishlari lozim. Bunday mashg'ulotlarning asosiy maqsa-di tahdidning muhimligi va jiddiyligini aniqlashdir, u korxonaning belgilangan tahdidga chidamlilik darajasidan yuqorida bo'ladimi yoki yo'qmi, javobgarlikni oshirishi mumkin bo'lgan vaziyatni yaratadimi yoki yo'qligini aniqlashdir. Shu-ningdek, u oldingi bobda muhokama qilingan strategiya va uni amalga oshirishni ta'minlashi kerak, bu esa tahdid bo'yicha mas'ullar va boshqa manfaatdor tomon-larga tahdidga chidamlilikning belgilangan darajasini o'zgartirish kerakmi yoki yo'qligini va agar shunday bo'lsa, o'zgartirishlarni ma'qullash kerakligini aniqlashda yordam beradi.

Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish jarayonlarini doimiy ravishda sinovdan o'tkazish va yangilash zarurligi quyidagi ko'rsatmalarda ko'r-satilgan:

SECning 2023-yilgi yakuniy qoidasi, kiberxavfsizlikka oid tahdidlarni bosh-qarish, strategiya, boshqaruv, hodisalarni oshkor qilish qoidasi

Ushbu talablar oshkor qilishning dinamik va rivojlanayotgan yondashuvi ta-moyili bilan uyg'un keladi. Yangi bilim va tajribalardan foydalanish uchun amali-yotlarni yangilashni ta'minlash va tahdidlarni boshqarish, rahbarlik, strategiya va hodisalar to'g'risida ma'lumotlarni oshkor qilishning kompleks ko'rinishini taq-dim etish orqali kompaniyalar manfaatdor tomonlarning ishonchini yanada yax-shiroq saqlab qolishlari mumkin.

NISTning 2023-yilgi kiberxavfsizlik asoslari, 2.0 ID.IM-01-04

Mazkur subkategoriyalar ushbu tamoyilga mos keladi, chunki u tashkilot ta-blablari va tahdidlarini qamrab olishini ta'minlash uchun tahdidlarni boshqarish jarayonlarini qayta ko'rib chiqish, o'zgartirish va takomillashtirishni nazarda tutadi. Eskalatsiya va ma'lumotlarni oshkor qilish amaliyotlari umumiy tahdidlar-ni boshqarish strategiyasining bir qismi bo'lganligi sababli, tahdidlarni samarali boshqarish uchun o'rganilgan saboqlarga asoslanib, ular muntazam ravishda qayta ko'rib chiqilishi va o'zgartirilishi zarur.

5-TAMOYIL: ESKALATSIYA VA MA'LUMOTLARNI OSHKOR QILISH JARAYONLARINI TEKSHIRISH

Korxonaning samaradorligi, izchilligi hamda tegishli qoidalar va siyosatlar-ga muvofiqligini ta'minlash maqsadida, audit xizmati korxonaning kibertahdid-lar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlarini ko'rib chiqishi va baholashi kerak.

Audit xizmati korxona tahdidlarini eskalatsiya qilish va ma'lumotlarni osh-kor qilish jarayonlari hamda tartib-qoidalarining samaradorligi va muvofiqligini ta'minlashda muhim rol o'ynaydi. Ushbu jarayonlar va tartib-taomillarni loyiha-lash va amalga oshirishni baholash, kamchiliklar va zaif tomonlarni aniqlash va takomillashtirishni tavsiya etish orqali auditorlar korxonalarga kibertahdidlarni yanada samarali boshqarishga va manfaatdor tomonlarning, shu jumladan inves-torlar, mijozlar va tartibga soluvchilarning ishonchini saqlashga yordam beradi. Auditorlarning tahdidlarni eskalatsiya qilish va oshkor qilish jarayonlari hamda tartib-taomillari bilan bog'liq asosiy majburiyatlariga quyidagilar kiradi:

Loyihani baholash

Auditorlar korxonaning tahdidlarni eskalatsiya qilish va ma'lumotlarni osh-kor qilish jarayonlari va tartib-qoidalarining loyihasini ularning aniq, keng qam-rovli va tahdidlarni boshqarish bo'yicha umumiy maqsadlari va tartibga solish ta-lablariga muvofiqligini ta'minlash uchun baholaydilar. Bu tarkibiy tuzilmani, va-zifalar va mas'uliyatlarni, aloqa kanallarini va hujjatlashtirish amaliyotini ko'rib chiqishni o'z ichiga oladi.

Ijro ta'minlanishini sinovdan o'tkazish

Auditorlar tahdidlarni aniqlash va eskalatsiya qilish jarayonlari hamda tartib-qoidalarini butun korxona bo'ylab izchil va samarali joriy etilganiga ishonch hosil qilish uchun tekshiruvlar o'tkazadilar. Bu muayyan hodisalarni ko'rib chiqish, xo-dimlar bilan suhbatlar o'tkazish va belgilangan tartiblarga muvofiqligini baholash uchun hujjatlarni tekshirishni o'z ichiga olishi mumkin.

Bo'shliqlar va zaif tomonlarni aniqlash

Auditorlar o'z baholashlari va sinov tekshiruvlari yordamida korxonalarining tahdidlarni eskalatsiya qilish va ma'lumotlarni oshkor qilish jarayonlari va tartib-larida mavjud bo'lgan har qanday bo'shliqlarni yoki kamchiliklarni aniqlaydilar. Bularga amalga oshirishdagi nomuvofiqliklar, xodimlar orasida bilim yoki xabar-dorlikning yetishmasligi, shuningdek, yetarli bo'lmagan aloqa va hujjatlashtirish amaliyotlari kirishi mumkin.

Ijroiy o'zgarishlarni tavsiya qilish

O'z xulosalariga asoslanib, auditorlar korxonaning tahdidlarni eskalatsiya qilish va oshkor qilish jarayonlari hamda tartib-qoidalarini yaxshilash bo'yicha tavsiyalar beradi. Ushbu tavsiyalar ta'lim va xabardorlik, aloqa kanallari, hujjatlar,

jarayonlar va protseduralarning umumiy tuzilishi va loyihasi kabi sohalarga taalluqli bo'lishi mumkin.

Auditga xos bo'lgan ushbu talablar II Aning "Uch chiziqli himoya modeli" tomonidan boshqariladi va qo'llab-quvvatlanadi. Bu model uchinchi chiziqlarning vazifasini va uning xolislik hamda ishonchlilik uchun mustaqilligining muhim ahamiyatini ta'kidlaydi.

Yakuniy xulosa

Ushbu bobni yakunlar ekanmiz, biz yana bir bor e'tiborni tahdidlar eskalatsiyasi hamda ma'lumotlarni oshkor qilish bilan bog'liq tegishli javobgarlikka qaratmoqchimiz. Bular shunchaki "yoqimli" fikrlar emas. Ular juda muhim bo'lib, eskalatsiya va ma'lumotlarni oshkor qilish jarayoni samarali bo'lishi uchun (ular barcha to'rtta asosiy komponentlar birgalikda muvofiqlashtirgan holda) keng ko'lamli CRMPning bir qismi sifatida rasmiylashtirilishi kerak. Hukumatlar, tartibga soluvchi organlar, sudlar, shuningdek, soha tashkilotlari va keng jamoatchilik buni tartibga solish choralari orqali, belgilangan qoidalarni buzganlik uchun jiddiy jarimalarni belgilash, rahbarlar va direktorlar kengashi a'zolari uchun shaxsiy javobgarlikni kuchaytirish orqali aniq ko'rsatmoqdalar. Faqatgina ular emas: jamoatchilik o'zlari ishonmaydigan kompaniyalardan uzoqlashishga tayyor ekanliklarini aniq ko'rsatmoqdalar.

Tahdidlarni eskalatsiya qilish va ma'lumotlarni oshkor qilish amaliyotining mavjudligini ta'minlash oson ish emas va bu CRMPning boshqa qismlari bilan to'liq integratsiyani talab qiladi. Ishonchli manbalarga asoslanib, CRMP nima ekanligiga oydinlik kiritildi, keyingi bobda uni joriy etish bo'yicha ba'zi strategiyalar va fikrlarni ko'rib chiqamiz.

VII BOB. CRMPNI JORIY ETISH

Ushbu kitobda to'rt asosiy komponentga asoslangan rasmiy CRMPning muhim ahamiyatini ta'kidlab o'tdik: moslashuvchan boshqaruv, tahdidlar haqidagi ma'lumotlarga asoslangan tizim, tahdidlarni baholashga asoslangan strategiya va uning ijrosi hamda tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi. Ushbu komponentlarning barchasi bir-biri bilan uzluksiz ishlashi lozim, eng muhimi ular korxonaning boshqa ko'plab mutaxassislari hamda ichki va tashqi manfaatdor tomonlari bilan o'zaro hamkorlik qilishlari kerak. Bu uzluksiz jarayon bo'lib, unga erishish oson emas. Ushbu bobda bu dasturni joriy etishda sizga yordam berishi mumkin bo'lgan masalalar va muhim muammolarga e'tibor qaratiladi. 7.1-jadvalda to'rt tarkibiy qismning har biriga tegishli tamoyillar va ma'lumotnomalar to'plami keltirilgan.

Samarali CRMP yuqori rahbariyat darajasidagi majburiyatlarni, yangi vazifalar va javobgarliklarni, byudjet va boshqa resurslarni o'zgartirishni va ko'p hollarda korxona madaniyatida tub o'zgarishlarni talab qiladi. Bu bir martalik mashg'ulot yoki shunchaki bir marta yozilib, tasdiqlanib, so'roqlarsiz, o'zgarishsiz yoki yangilanishsiz amal qilinadigan siyosat ham emas. Bu favqulodda yoki reaktiv tarzda amalga oshiriladigan jarayon ham emas. Bu jarayon xavfsizlik tashkiloti, tahdid bo'yicha mas'ul shaxslar, boshqaruv organlari va boshqa ko'plab manfaatdor tomonlar o'rtasidagi doimiy va izchil aloqalarni talab qiladi. Bu hamkorlik tahdidlarni boshqarish jarayonini korxona uchun shunchaki xarajat markazi yoki to'siq emas, balki imkoniyat yaratuvchi omil sifatida aniq belgilaydigan ishonchli va uzoq muddatli munosabatlarni o'rnatish imkonini beradi.

Tahdid muhiti doimiy ravishda o'zgarib turganligi sababli, dastur moslashuvchan bo'lishi va atrof-muhitdagi o'zgarishlarga tezkor javob bera olishi kerak.

7.1-jadval

CRMP tamoyillari

CRMP tarkibiy qismlari	Tamoyillar	Ma'lumot manbalari
Moslashuvchan boshqaruv	75-betda “Moslashuvchan boshqaruvning yetti tamoyili”ga qarag.	- SECning yakuniy kiberqoidasi - NIST CSF 2.0 - NACDning 2023-yilgi direktorlar qo'llanmasi - ISO 27001:2022 - NIST 8286 - IIAning uch chiziqli himoya modeli

		• SEC qo'llanmasi 2018 • ISO 31000:2018 • AICPAning CRMP
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	94-betda "Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • ISO 27001:2022 • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	120-betda "Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • ISO 31000:2018 • AICPAning CRMP
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	151-betda "Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili"ga qarang.	• SECning yakuniy kiberqoidasi • NIST CSF 2.0 • 2023-yilgi NACDning direktorlar qo'llanmasi • IIAning uch chiziqli himoya modeli • SEC qo'llanmasi 2018 • AICPAning CRMP

Kibertahdidlarni boshqarish jarayonlari

Kibertahdidlarni boshqarishni har bir korxona uchun o'ziga xos sayohat deb tasavvur qilish foydali bo'lishi mumkin. Bu sayohatning boshlang'ich nuqtasi korxonaning hajmi, faoliyat sohasi, tartibga solish muhiti, kibertahdidlarni boshqarishdagi joriy yetuklik darajasi va boshqa ko'plab omillarga qarab farqlanishi mumkin. Bu sayohat hech qachon tugamaydi va tugashi ham kerak emas. Bu dasturni joriy etish va uni korxonaga qanday yetkazish muhim ahamiyatga ega. Shuning uchun, CRMPning to'rt tarkibiy qismining har biri uchun biz yangi tashabbusning dastlabki 30 kunida, so'ngra keyingi 60 kun ichida nima qilish kerakligi bo'yicha tavsiyalar beramiz. Shuni yodda tutish kerakki, bular umumiy ko'rsatmalar bo'lib, muddatlar korxonaga xos talablar, imkoniyatlar va dasturning yetuklik darajasiga qarab moslashtirilishi mumkin.

Xavfsizlik xizmati faoliyatining natijasi hamda uning asosiy mahsuloti – bu tahdid haqidagi ma'lumotlardir.

Xavfsizlik bo'limi ko'pincha CRMPni amalga oshirishga rahbarlik qiladi, ammo bu har doim ham shunday bo'lavermaydi va bu mukammal darajada

bo'lishi shart emas. Xavfsizlik bo'limining kibertahdidlarni boshqarishdagi asosiy roli korxonani (tahdid bo'yicha mas'ul shaxslar, boshqaruv organlari va boshqa ko'plab manfaatdor tomonlarni) tahdid jarayonlariga oid asosli qarorlar qabul qilish uchun faol yo'naltirish hisoblanadi. Xavfsizlik tashkiloti va umuman korxona uchun pirovard maqsad – bu tahdid va foyda o'rtasida tegishli muvozanatni o'rnatishdir: bu jarayon korxonani va uning manfaatdor tomonlarini himoya qilish bilan bir qatorda, unga raqobatbardoshlikni saqlab qolish imkonini beradi va ideal holatda uning raqobatbardoshligiga hissa qo'shadi.

Korxonalar va ko'plab manfaatdor tomonlar kibertahdidlarni boshqarish yo'lini boshlashda turli xil qiyinchiliklarga duch keladi. Shunga qaramay, ular hal qilishlari kerak bo'lgan umumiy muammolarga duch kelishadi. Bu dasturga yuqori darajadagi rahbarlarning qo'llab-quvvatlashi va doimiy sodiqligini, tashkiliy madaniyatdagi o'zgarishlarni, barcha manfaatdor tomonlar o'rtasidagi uzluksiz muloqot va hamkorlikni, shuningdek, byudjet, xodimlar, vositalar va boshqa resurslarni o'z ichiga oladi. Haqiqat shuki, bugungi kunda juda oz korxonalar buni samarali amalga oshirmoqda. Ko'p korxonalar hozirda kibertahdidlarni boshqarish amaliyotlaridan ortda qolmagan bo'lishi mumkin. Biroq tez o'zgaruvchan tahdid muhiti va jadal sur'atda ortib borayotgan tartibga solish hamda huquqiy javobgarlik tufayli, agar ular tez harakat qilmasa, tez orada orqada qolib ketishi mumkin. Korxonalar katta yoki kichik bo'ladimi, davlat va xususiy sektorga qarashligidan qat'i nazar, o'zlarining mavjud yondashuv va amaliyotlariga tub o'zgarishlar kiritishlari zarur.

Kibertahdidlarni boshqarish yo'lidagi yaxshi boshlang'ich nuqta – bu dastur rahbari (ko'pincha CISO, tahdidlarni boshqarish bo'yicha bosh direktor (CRO)¹²²) yoki bosh maslahatchi)ning quyidagi ko'rinishdan oddiy, aslida esa murakkab savollar ustida ishlashidan iborat:

- “Direktorlar kengashi va yuqori lavozimli rahbarlar CRMPni amalga oshirish va nazorat qilish uchun mas'ul ekanliklaridan xabardormi?”

- “Ushbu yuqori darajadagi qaror qabul qiluvchilar CRMP ularni javobgarlikdan himoya qilishi mumkinligini biladilarmi?”

- “Xavfsizlik tashkiloti tahdidlarni boshqarishda yetuk rol o'ynaydimi va yuqori darajadagi rahbariyat ulardan buni kutadimi?”

- “CRMPni yaratish uchun zarur asoslar (masalan, boshqaruv organi) mavjudmi?”

- “Qaysi manfaatdor tomonlar bilan ish munosabatlarini rivojlantirishim kerak va bu jarayonni boshlashning eng yaxshi usuli nima?”

Dastur rahbari xoh xavfsizlik bo'limida, xoh korxonaning boshqa bo'limida bo'lsin, bu savollarga yolg'iz javob bera olmaydi. Bilim va tushunchaning bu asosini yaratish uchun keng doiradagi manfaatdor tomonlarning fikr-mulohazala-

¹²² CRO (chief risk officer) – tahdidlarni boshqarish bo'yicha bosh direktor.

ri talab etiladi. Ular bilan maslahatlashish hamda ularning fikrlarini jiddiy qabul qilish dasturni amalga oshirish va boshqarish uchun zarur bo'lgan uzoq muddatli hamkorlik munosabatlarini rivojlantirishga yordam beradi.

Kibertahdidlarni boshqarish jarayonini boshlash

Ushbu kitob korxonaning kiberxavfsizlikni boshqarish amaliyoti uchun kutilayotgan kelajakdagi holat haqidagi tasavvurni taqdim etadi. Bu holat eng yuqori rahbariyat tomonidan ishlab chiqilgan, amalga oshirilgan, tasdiqlangan va boshqariladigan rasmiy dastur orqali belgilanadi. Bunda yuqori rahbariyat tahdid bo'yicha mas'ul shaxslar va xavfsizlik tashkiloti bilan hamkorlikda ishlaydilar. Kelajakdagi bu holat korxonaning tahdid muhitiga va boshqa ko'plab omillarga bog'liq holda sezilarli darajada farqlanadi. Ammo barcha korxonalar tahdidlarni boshqarishning o'zaro uyg'un, integratsiyalashgan amaliyotlariga erishishni istaydi, bu esa korxonani muvozanatli tahdid portfeli bilan ta'minlaydi. Yuqorida ta'kidlanganidek, bu holatga erishish yo'llari juda xilma-xil bo'ladi. Ammo CRMPni joriy etayotganda, har bir korxona quyidagi to'rt asosiy qadamni bajarishi kerak:

1. CRMPni "yetakchi" etib belgilash.
2. Korxonaning kibertahdidlarni boshqarish amaliyotining joriy holatini har tomonlama baholash.
3. Kelishilgan maqsadli holatni belgilash hamda jarayonlar va vaqt oraliqlarini rejalashtirish.
4. Dasturni ishlab chiqish uzoq muddatli jarayon bo'lishini tan olib, yo'l xaritasini yaratish.

Yuqori rahbariyatning qo'llab-quvvatlashsiz hech qanday yirik korxonaning tashabbusi muvaffaqiyatli bo'lmaydi. CRMPni joriy etish keng qamrovli, asosiy va uzoq muddatli qo'llab-quvvatlashni talab qiladi. Kam korxonalargina boshidanoq kibertahdidning barcha sohalarini aniqlash va bartaraf etish uchun yetarli resurslarga ega bo'ladi, shuning uchun dasturni amalga oshirish muqarrar ravishda uzoq muddatli jarayon bo'lib qoladi. Bu omillarning barchasi tahdidlarni boshqarishga katta sarmoya kiritadigan mansabdor shaxs yoki yuqori lavozimli rahbar (ehtimol, CRO yoki bosh yurist)ning ishtirokini talab qiladi. Bu shaxslar xolis va mustaqil bo'lishi kerak. Qanday bo'lmasin, kuchli rahbarlik, maqsadning aniqligi va "yetakchi"ning qo'llab-quvvatlashi mutlaqo zarur hisoblanadi.

Kibertahdid sohasidagi yetakchi mutaxassislar hamda manfaatdor tomonlar CRMPning muhimligini, ya'ni uning korxonaning muhim biznes maqsadlariga erishishdagi hissasini tushunishlari kerak. Bu shaxslar nafaqat kibertahdid, balki butun korxona miqyosidagi barcha tahdidlar doirasi haqida keng tasavvurga ega bo'lishi kerak. Kim tanlanmasin, ular shubhasiz, belgilangan va tasdiqlangan tahdidga moyillik va chidamlilik darajalari bilan mos keladigan tahdid haqidagi ma'lumotlarga asoslangan qarorlar qabul qilishning korxona uchun ahamiyatini tan olishadi, chunki ular kibersohaga aloqasi bo'lmagan barcha faoliyatlarda bu

amaliyotga o'rganib qolishgan. Xavfsizlik tashkilotining tavsiyalari va ma'lumotlari yordamida, ular bu qadriyatlarni o'z hamkasblariga yetkaza olishadi.

CRMP ishlab chiqayotgan har qanday xavfsizlik yoki tahdid bo'yicha mutaxassis CRMPning to'rt tarkibiy qismi va ularni qo'llab-quvvatlovchi tamoyillar bo'yicha mavjud tahdidlar amaliyoti va imkoniyatlarini ochiq va halol baholashdan boshlashi kerak. Bu hozirda mavjud bo'lgan tushunchalarni tanqidiy ko'rib chiqishni talab etadi. Bu keng doiradagi tegishli manfaatdor tomonlardan, jumladan, CISO, CRO, ERM dasturi rahbari, auditorlik tashkiloti vakillari hamda kengashning tanlangan a'zolaridan asosli ma'lumotlarni talab qiladi.

Kichik korxonalar uchun bu jarayonni osongina ishtirok etuvchi a'zolarining tegishli soniga moslashtirib qisqartirish mumkin. Baholash jarayoni tegishli manfaatdor tomonlar bilan suhbatlarni va mavjud hujjatlarni, siyosat va jarayonlarni, boshqaruv tuzilmalari, tahdidlarni baholash, tahdidlar bo'yicha hisobotlar, tahdidlar registrlari, tahdidlar taksonomiyalari va boshqa yordamchi texnologiyalarni ko'rib chiqishni o'z ichiga olishi kerak.

Tahdid vositalarining ro'yxati yoki munosabatlarga asoslangan jarayonlar to'plami foydali boshlang'ich nuqta bo'lishi mumkin. Baholash, shuningdek, korxonaning tahdid muhitini, jumladan unga ta'sir ko'rsatadigan me'yoriy-huquqiy asoslar va standartlarni ham o'z ichiga olishi lozim. Agar qarshilik yoki mustaqillikning yetishmasligi sezilsa, ko'pincha uchinchi tomon nuqtayi nazarini jalb etish foydali bo'ladi. Bu vaziyatni tashqi tomondan kuzatishga yordam berib, sanoatning ilg'or tajribalarini rahbarlar hamda boshqaruv kengashi a'zolari bilan bo'lishish imkonini beradi. Bu jarayonning natijasi esa dastlabki bazaviy ma'lumotlar bo'lib, u bo'shliqlarni aniqlash hamda korxonaning eng muhim ehtiyojlarini dastlabki bosqichda ustuvor tartibda belgilash imkonini beradi.

Joriy holat aniqlangandan so'ng, keyingi qadam rahbarlar bilan birgalikda kелиshilgan maqsadli holatni aniqlash va dasturni yaratish yoki rivojlantirish uchun batafsil yo'l xaritasini tuzishdir. Ushbu maqsadli holat va yo'l xaritasi baholash natijalariga asoslanadi. Bu, ehtimol, qisqa va uzoq muddatli maqsadlarni o'rnatish, tashabbuslarga ustuvorlik berish va resurslarni tegishli tarzda taqsimlash hamda eng muhimi, dasturning korxonaning umumiy biznes maqsadlari va tahdidga moyilligini tushunishi va ularga moslashganligini ta'minlashga olib keladi.

Hamma narsani bir vaqtning o'zida bajarishga intilish tabiiy, biroq kamdan kam korxonalar avval boshidanoq kibertahdidning barcha sohalarini aniqlash va bartaraf etish uchun zarur resurslarga yoki tajribaga ega bo'ladi. Buning o'rni, dastur rahbari va boshqa manfaatdor tomonlar yo'l xaritasiga ustuvorlik berishlari, zarur resurslar uchun ruxsat olishlari va yetuklikka erishish bosqichlarini real va amaliy tarzda amalga oshirishlari lozim. Ushbu bosqich davomida boshqaruv organi bilan muloqotda to'liq shaffof bo'lish juda muhim, chunki bu xavfsizlik tashkilotining rejani amalga oshirishini, tegishli resurslarning qo'llanilishini va to'liq hisobdorlikni ta'minlaydi.

CRMPni joriy etish

Ushbu kitobda bayon etilgan CRMPning to'rt asosiy tarkibiy qismi o'zining maxsus amalga oshirish talablari va muammolarini taqdim etadi. Quyida ularning har birini yaqindan ko'rib chiqib, amalga oshirishdagi umumiy qiyinchiliklar va ularni bartaraf etish usullariga e'tibor qaratamiz.

Moslashuvchan boshqaruv

Moslashuvchan boshqaruv kibertahdidlarni boshqarishda korxona muvaffaqiyati uchun juda muhimdir. Aniq va ravshan belgilangan boshqaruv amaliyotlari, aniq vazifa va mas'uliyatlar hamda tahdidga oid qarorlar uchun o'rnatilgan javobgarlik bo'lmasa, korxonalar va ularning qaror qabul qiluvchilari (direktorlar kengashidan tortib boshqalargacha) halokatli oqibatlariga duch kelishi mumkin. Ko'rib o'tganimizdek, boshqaruv talablari korxona va shaxsiy javobgarlikni yanada aniqroq belgilaydigan sud qarorlarining uzoq va davom etayotgan qatoriga, shuningdek, tegishli me'yoriy-huquqiy bazalarning keng doirasi hamda sanoat standartlari va protokollariga asoslanadi. Bu omillar moslashuvchan va tezkor boshqaruv usullarini tobora muhimroq qilmoqda, shu bilan birga ularni amalga oshirishni murakkab va qiyin vazifaga aylantirmoqda.

3-bobda batafsil bayon qilingan Moslashuvchan boshqaruvning yetti tamoyili amalga oshirish jarayonining barcha bosqichlarida qo'llaniladi:

"1-tamoyil: Siyosat va jarayonlarni joriy etish"

CRMPni yaratish uchun butun korxona miqyosida siyosat va jarayonlar joriy etilishi kerak.

"2-tamoyil: "Uch chiziqli himoya modeli" doirasida boshqaruv, vazifalar va majburiyatlarni o'rnatish"

"Uch chiziqli himoya modeli" doirasida CRMP aniq belgilangan vazifalar, majburiyatlar va natijalar bilan o'rnatilishi kerak.

"3-tamoyil: Boshqaruv amaliyotlarini mavjud tahdidlarni boshqarish tizimi bilan muvofiqlashtirish"

Kibertahdidlarni boshqarish amaliyotlari korxonaning har qanday mavjud tahdidlarni boshqarish tizimiga moslashtirilishi lozim.

"4-tamoyil: Direktorlar kengashi va rahbariyat qamrov doirasini belgilaydi"

Korxonada kibertahdidlarga qarshi kurash amaliyotlarining qamrov doirasi direktorlar kengashi va yuqori rahbariyat tomonidan belgilanishi va tasdiqlanishi lozim.

"5-tamoyil: Direktorlar kengashi va yuqori bo'g'in rahbarlari nazoratni amalga oshiradilar"

Direktorlar kengashi va yuqori darajadagi rahbarlar korxonaning kibertahdidlar bilan kurashida tegishli nazoratni ta'minlashi zarur.

"6-tamoyil: Boshqaruv jarayonlari auditi"

Audit jarayonlari korxonaning kibertahdidlarni boshqarish amaliyotini tegishli tarzda tahlil qilib, ularni baholashi lozim.

"7-tamoyil: Resurslarni belgilangan vazifa va majburiyatlarga muvofiq-lashtirish"

Tegishli resurslar va malakalar to'plami belgilangan vazifalar va majburiyatlarga muvofiq bo'lishi kerak va doimiy mashg'ulotlar o'tkazilishi zarur.

Birinci 30 kun ichida quyidagilarni ko'rib chiqing:

- Moslashuvchan boshqaruv va keng qamrovli CRMPni joriy etishga rahbarlik qilish uchun turli biznes bo'linmalari vakillaridan iborat kibertahdidlar boshqaruv qo'mitasini tuzish va uning yig'ilishini o'tkazish. Qo'mita uchun vazifa bayonoti hamda qisqa va uzoq muddatli maqsadlar belgilash.

- 3-bobda batafsil tavsiflangan "Uch chiziqli himoya modeli" bo'yicha boshqaruv vazifalari va majburiyatlarini aniq belgilash.

- O'rnatilgan kiberboshqaruv amaliyotlari korxona yoki tashkilotning mavjud tahdidlar boshqaruvi tizimlariga mos kelishini ta'minlash.

- Korxona miqyosidagi CRMP uchun keng qamrovli siyosat va tartib-qoidalar to'plamini ishlab chiqish.

- Tegishli manfaatdor tomonlarga boshqaruvning rejalashtirilgan chora-tadbirlari va ularning sabablari haqida xabar berish.

- Boshqaruvning turli sohalariga mas'ul bo'lgan shaxslar va vazifalarni belgilash hamda bu shaxslarning o'z vazifalarini to'liq tushunishiga ishonch hosil qilish.

Keyingi 60 kun ichida quyidagilarni ko'rib chiqing:

- Kibertahdidlar amaliyotini nazorat qilish vazifasi yuklatilgan boshqaruv organi, jumladan boshqaruv kengashi va yuqori darajadagi rahbarlar aniq belgilanishi kerak.

- Siyosat va tartiblarni tasdiqlash, takomillashtirish va amalga oshirish.

- Boshqaruv amaliyoti ustidan nazoratni ta'minlash vazifasi yuklatilgan kengash yoki yuqori martabali rahbarlar aniq belgilanishi kerak.

- Belgilangan vazifa va majburiyatlarni bajarish uchun zarur bo'lgan resurslar va ko'nikmalarni aniqlash maqsadida bo'shliqlar tahlilini o'tkazish kerak.

- Belgilangan siyosat va tartib-qoidalarga muvofiq boshqaruv amaliyotini tekshirish uchun muntazam ichki audit jarayonini joriy etish.

- Xodimlarning belgilangan vazifa va mas'uliyatlariga mos keladigan uzluk-siz o'quv dasturini yaratish, bu orqali jamoani yangi ma'lumotlar bilan ta'minlash va ularning ko'nikmalarini oshirish.

- Xabardorlik dasturini keng miqyosda korxonaga yetkazish, yangi amaliyotlar va ularning sabablarini baham ko'rish hamda har bir xodimning yangi tuzilmadagi vazifasini tushunishini ta'minlash.

Moslashuvchan boshqaruv bilan bog'liq umumiy muammolar

Ushbu bo'limda CRMPning tarkibiy qismi bo'lgan *moslashuvchan boshqaruvni* amalga oshirishda, korxonalar duch keladigan umumiy muammolarni hal qilishga harakat qilamiz.

Boshlang'ich nuqtani belgilash. Yuqorida muhokama qilingan *dastlabki baholash* boshqaruv dasturining ilk ustuvor yo'nalishlarini aniqlab beradi. Agar korxonada allaqachon tahdidlarni boshqarish organi mavjud bo'lsa-yu, lekin kibertahdidlarni boshqarish masalalari bilan shug'ullanmasa, u boshqaruv tashabbusi uchun poydevor bo'lib xizmat qilishi mumkin. Har qanday holatda ham, tashabbus korxonaning o'ziga xos tahdid muhitidagi eng muhim masalani hal etishdan boshlanishi lozim. Bu – korxonaning sanoat tarmog'i, bozor sharoitlari, tartibga solish talablariga muvofiqligi va mavjud majburiyatlarni o'z ichiga olishi mumkin.

Yuqori darajadagi rahbariyatning qo'llab-quvvatlashiga erishish. Har qanday yirik tashabbus yuqori darajadagi qaror qabul qiluvchilarning boshlang'ich va doimiy qo'llab-quvvatlashini talab etadi, chunki u korxonaning ko'plab sohalariga ta'sir ko'rsatadi. Shunday bo'lsa-da, Jahon iqtisodiy forumining 2022-yilgi "Global xavfsizlik istiqbollari" nomli so'rovnoma qatnashgan kiberrahbarlarning uchdan bir qismi "rahbariyat tomonidan qo'llab-quvvatlanishga erishish" kibernetika qurilishini boshqarishning eng qiyin jihati ekanligini ta'kidlagan. Kibertahdidlarni boshqarish bo'yicha rahbarlar bu muammoni bartaraf etish uchun, direktorlar kengashi yoki yuqori darajadagi rahbarlarga moslashuvchan boshqaruv tizimini joriy etish zarurligi haqidagi g'oyalarni korxona biznesining ustuvor yo'nalishlari va sohaga xos talablarga moslashtirilgan tarzda taqdim etishlari mumkin.

Bu shunday sohaki, unda kibertahdidlarni boshqarish bo'yicha yetakchi mutaxassisni aniqlash va uning qo'llab-quvvatlashini qozonish ayniqsa muhim bo'ladidi. Bu mutaxassis biznes boshqaruv tarixini tushunadigan tarzda tushuntira olishi kerak. Avval ta'kidlaganimizdek, boshqaruv amaliyoti va uni joriy etishga xavfsizlik tashkiloti rahbarlik qilmasligi lozim. Auditorlik tashkiloti ham qimmatli va ishonchli ma'lumotlar taqdim etishi mumkin. Tashqi maslahatchilar ham mustaqil va xolisona nuqtayi nazarni taqdim etishda foydali bo'lishi mumkin.

Kibertahdidlarni tezkor va moslashuvchan boshqarish masalasini kim ko'tarmasin, bir asosiy g'oyani aniq yetkazish muhim: boshqaruv uchun javobgarlik xavfsizlik rahbariyati darajasidan ancha yuqorida turadi. Boshqaruv zaruriyatini hal qilmaydigan yuqori lavozimdagi rahbarlar bu qaror bilan bog'liq tahdid va mas'uliyatni bilvosita o'z zimmasiga olgan bo'ladi.

Agar korxona rahbarlari boshqaruv zaruriyatini hal qilmasalar, ular beixtiyor bu qaror bilan bog'liq tahdid va mas'uliyatni o'z zimmalariga olgan bo'ladilar.

Zarur byudjet va boshqa resurs cheklovlarini aniqlash. Yangi tashabbuslar uchun moliyalashtirish doimo muammo hisoblanadi. CRMP ko'p resurs talab qilmasligi mumkin, lekin agar tahdidlar haqida xabar berishning ilg'or imkoniyatlarini (masalan, kibertahdidlarni miqdoriy baholash) qo'llash to'g'risida qaror qabul qilinsa, bu yangi vositalarni talab qilishi mumkin. Yuqori lavozimdagi qaror qabul qiluvchi shaxslarni xodimlar va vositalar uchun mablag' ajratishga ishonitirishning kaliti yana bir bor shuni ko'rsatadiki, kibertahdidni bartaraf eta olmaslik – bu tahdidni qabul qilishni anglatadi. Biroq, agar boshqaruv dasturi qimmatligi, juda murakkab yoki qiyinligi sababli, uni qo'llab-quvvatlash uchun mablag' mavjud bo'lmasa, tashabbusni soddalashtirish va tegishli CRMPning mavjud emasligi bilan bog'liq yuqori darajadagi tahdidni qabul qilish zarur bo'ladi.

Muayyan korxona muhitiga moslashish. Boshqaruv tashabbusi to'rt muhim elementni aniqlash va o'rnatish orqali korxonaning o'ziga xos talablarini hisobga olishi kerak. Bular:

Qamrov

Kiberboshqaruv tashabbusi qamrab oladigan sohalar boshqaruv organi tomonidan aniq belgilanishi kerak. Masalan, u faqat AT yoki operativ tizimlar, IoT va hatto tashqi hamkorlar kabi uchinchi tomonlarni ham qamrab oladimi?

Mustaqillik

Tahdid masalalari bo'yicha ziddiyat yuzaga kelganda, ba'zi ichki manfaatdor tomonlar boshqaruv organiga bosim o'tkazish uchun yetarlicha nufuzga ega bo'lganligi sababli, samarali boshqaruvni ta'minlashda mustaqillik hal qiluvchi ahamiyat kasb etadi.

Vakolat

Boshqaruv organi o'z qarorlarini amalga oshirish vakolatiga ega bo'lishi va bu vakolat barcha manfaatdor tomonlarga yetkazilishi kerak.

Shaffoflik

Korxonaning boshqaruv amaliyoti, uning muvaffaqiyatlari va muvaffaqiyatsizliklari, shuningdek, tahdid muhitidagi aniqlangan o'zgarishlar natijasida yuzaga kelgan har qanday boshqaruv o'zgarishlari muntazam ravishda boshqaruv kengashiga yoki boshqa yuqori rahbariyatga yetkazib turilishi shart. Bu muntazam kuzatuv va tahlilni talab qiladi.

Boshqaruv, tahdid va muvofiqlik (GRC¹²³) dasturi

Korxonaning **GRC** dasturi CRMPni amalga oshirishda muhim rol o'ynashi mumkin, ammo ko'plab boshqaruv, tahdid va muvofiqlik dasturlarida, muvofiqlik funksiyalari boshqaruv va tahdid elementlarini deyarli to'liq soyada qoldiradi. Bu quyidagi bir nechta omillarning natijasi bo'lishi mumkin:

Tor doira

Ko'pgina GRC dasturlari asosan huquqiy va tartibga soluvchi majburiyatlarni bajarishga qaratilgan bo'lib, xavfsizlikni biznes maqsadlari bilan strategik muvofiqlashtirishga kam e'tibor beradi yoki umuman e'tibor qaratmaydi.

Biznes bilan cheklangan aloqa

GRC funksiyalari ko'pincha boshqa biznes bo'linmalaridan ajralib, alohida faoliyat olib boradi.

Moslashtirilmagan tahdid tuzilmalari

To'liq moslashtirilmagan va muvofiqlashtirilmagan turli xil tuzilmalar to'plami aniqlikning yetishmasligiga va tahdidlarni boshqarish bo'yicha harakatlarga jiddiy e'tibor berilmasligiga olib keladi. Agar ma'lumotlar turli biznes funksiyalariga ustuvorlik berib yoki turli xil tahdid matritsalaridan foydalanib taqdim etilsa, maqsadli auditoriya chalkashib qolishi mumkin. Shuningdek, kibertahdidlarni boshqarish tuzilmasi keng ko'lami biznes jarayonlari bilan kamroq bog'liq bo'lib ko'rinishi va shu sababli kamroq amaliy qiymatga ega bo'lishi mumkin.

Nazoratga ortiqcha urg'u berish

GRC dasturlari ko'pincha nazoratni joriy etish va uni saqlab turishga e'tibor qaratadi, bu esa aksariyat hollarda biznes muhitini tushunish va nazoratni biznes faoliyatini qo'llab-quvvatlashga moslashtirishni e'tibordan chetda qoldiradi. Bu ortiqcha xarajatlarga, resurslarning behuda sarflanishiga va samarasiz nazoratga olib kelishi mumkin.

Tahdidlar haqidagi ma'lumotlarga asoslangan tizim

Tahdid haqidagi ma'lumotlar nafaqat xavfsizlikka oid tahdidlar va zaifliklar haqidagi ma'lumotlarni, balki korxonaning kibertahdid muhiti to'g'risidagi batafsil va amaliy ma'lumotlarni ham o'z ichiga oladi. U har qanday muvaffaqiyatli CRMPning asosini tashkil etadi. To'rtinchi bobda batafsil bayon qilingan real hayotdagi voqealar shuni ko'rsatadiki, butun dunyo bo'ylab sudlar va nazorat organlari endi tahdidlarni boshqarishda tasodifiy yondashuvni qabul qilishmaydi. Tahdidlar haqidagi ma'lumotlarga asoslangan tizimni joriy etish bo'yicha ko'rsatmalar mavjud. Sudlar va nazorat qiluvchi organlar kiberxavfsizlik uchun javobgarlik endi direktorlar kengashi, korxonaning mansabdor shaxslari va boshqa ko'plab mas'ul shaxslarga ham taalluqli ekanligini aniq ta'kidlashmoqda. CRMP ning muhim tarkibiy qismi bo'lgan tahdidlar haqidagi ma'lumotlar, korxonaning jamoatchilik oldidagi obro'si va brend imidjiga yetkazilishi mumkin bo'lgan zararning oldini olish yoki uni kamaytirish uchun ham juda muhim hisoblanadi. Eng asosiysi, bu doimiy o'zgarib turuvchi biznes muhitida raqobatbardoshlikni saqlab qolish uchun ham zarurdir.

¹²³ GRC (Governance, Risk and Compliance Program) – Boshqaruv, tahdid va muvofiqlik dasturi

Tahdidlar haqidagi ma'lumotlarga asoslangan tizim joriy etilayotganda, to'rtinchi bobda keltirilgan beshta asosiy tamoyil har doim e'tiborda tutilishi lozim:

1-tamoyil: Tahdidlarni baholash tizimi va metodologiyasini aniqlash

Tashkilotda kibertahdidni aniqlash, baholash va o'lchash uchun tahdid asoslari va metodologiyasini aniqlash va uni amalga oshirish lozim.

2-tamoyil: Tahdid chegaralarini aniqlash metodologiyasini ishlab chiqish

Tahdidning maqbul darajalari uchun tasdiqlangan va takrorlanadigan metodologiya yaratilishi lozim.

3-tamoyil: Tahdid haqidagi ma'lumotlarga asoslangan ehtiyojlar tushunchasini shakllantirish

Boshqaruv organi aniqlanib, o'zining kibertahdidlarga oid ma'lumotlarga asoslangan ehtiyojlarini har tomonlama tushunishni shakllantirish jarayoniga jalb qilinishi lozim.

4-tamoyil: Tahdidlarni baholash muddati bo'yicha kelishib olish

Tahdidni baholash jarayoni kelishilgan vaqt oralig'ida amalga oshirilishi va uning natijalari muntazam ravishda baholanib turishi lozim.

5-tamoyil: Hisobot jarayonlarini yo'lga qo'yish

Hisobot berish jarayonlari boshqaruv organiga kibertahdidlarning mavjud amaliyotlarga va strategik qarorlarga ta'siri to'g'risida ma'lumot berishi kerak.

Dastlabki 30 kun ichida quyidagilarni ko'rib chiqing:

- Korxonaning o'ziga xos biznes ehtiyojlari, qonuniy talablari va sanoat muhitini inobatga oladigan kibertahdidlarni aniqlash, baholash va o'lchash uchun mos tizimni tanlang. Boshqaruv organidan ruxsat oling.
- Biznes tuzilmasiga asoslanib baholanadigan aktivlar doirasini belgilang, baholash chastotasini aniqlang va asosiy manfaatdor tomonlarni jalb qilish uchun eng maqbul yondashuvni ishlab chiqing.
- Korxonaning tahdid muhitini aniqlang yoki muvofiqlashtiring. Tahdid mezonlari va tasniflari tegishli manfaatdor tomonlar tomonidan belgilanishi va tasdiqlanishi kerak.
- Tahdid darajalari va chegaralarini belgilash uchun asos yarating. Korxonaning tahdidga moyilligi va bardoshlilikini aniqlash uchun kelishilgan metodologiyani tanlang.

Keyingi 60 kun ichida quyidagilarni ko'rib chiqing:

- Korxonaning tahdidga moyillik va chidamlilik darajalarini aniqlash metodologiyasini yakunlash va uni boshqaruv tizimidagi tegishli tomonlar orqali tasdiqlash.
- Manfaatdor tomonlarning doimiy ishtirokini ta'minlash va korxonaning tahdidlar bo'yicha hisobot berish ehtiyojlarini chuqurroq tushunish maqsadida yig'ilishlar yoki seminarlar tashkil etish.

- Tahdidlarni baholashni rejalashtirish. Korxonaning tahdid profiliga qarab, tahdidlarni baholashning kelishilgan tartibi va hajmini (choraklik, yarim yillik yoki yillik) belgilash.

- Joriy tahdid holatini tushunish uchun yangi metodologiya yordamida tahdidni dastlabki baholashni o'tkazish. Bunga bitta biznes bo'linmasi uchun tahdidlarni baholash bo'yicha tajriba-sinov ishlarini olib borish kiradi. Zarur hollarda tashqi maslahatchi yoki boshqa uchinchi tomonni jalb qilish.

- Boshqaruv organiga tahdid haqidagi ma'lumotlarni taqdim etish uchun hisobot jarayonini ishlab chiqish. Bu jarayon korxona muhitidagi o'zgarishlarni aks ettirishi kerak, taqdim etilgan ma'lumotlar tahdidlarni boshqarish amaliyotlariga ta'sir ko'rsatishi mumkin.

- Boshqaruv organiga tahdidlarning joriy holati va biznes muhitidagi o'zgarishlarning korxona tahdid profiliga qanday ta'sir qilishi mumkinligi haqida hisobot berish.

- Metodologiya va aniqlangan tahdidlardan kelib chiqib, korxona duch kelishi mumkin bo'lgan eng muhim tahdidlar to'plamini baholash va kuzatib borish uchun to'g'ri chegaralangan uchtdan beshtagacha asosiy KRIning ishlab chiqish.

Tahdidlar haqidagi ma'lumotlarga asoslangan tizim bilan bog'liq umumiy muammolar

Quyida tahdidlar haqidagi ma'lumotlarga asoslangan tizimni amalga oshirishda korxonalar duch kelishi mumkin bo'lgan ba'zi odatiy muammolar keltirilgan:

Juda ko'p ma'lumot yoki noto'g'ri turdagi ma'lumotlar bilan ishlash.

Bu samarali tahdidlar haqidagi ma'lumotlarga asoslangan tizimni amalga oshirishda eng katta to'siq bo'lishi mumkin. Korxonalar operatsion ko'rsatkichlarga doir ma'lumotlar bilan to'lib-toshgan, bu ma'lumotlarning ba'zilar kiber-tahdidlarni boshqarish uchun muhim bo'lsa, ba'zilar esa mohiyatan ahamiyatsiz. (Xavfsizlikka oid ma'lumotlar ko'p va keng qamrovli, ammo ularning barchasi ham tahdidga oid ma'lumot bo'lavermaydi.) Tahdid bo'yicha mas'ul shaxslar, boshqaruv organlari va boshqa manfaatdor tomonlar tahdid bilan bog'liq qarorlar qabul qilishda foydasiz ma'lumotlar bilan to'lib ketmasligi juda muhimdir. Agar ma'lumotlar haddan ziyod bo'lsa, ahamiyatli ma'lumotlarni e'tiborsiz qoldirish ehtimoli yuqori bo'ladi.

Bu sa'y-harakatlarning kaliti shundaki, foydalaniladigan va xabar qilinadigan ko'rsatkichlar mazmunli, tegishli darajada batafsil hamda kelishilgan tahdid tamoyillari va chegaralari bilan uyg'un bo'lishini ta'minlashdir. Dastlabki qadamlardan biri – bu mavjud tahdidlarni baholash jarayonidan foydalanib, KRI hamda KPIning ishlab chiqishidir. Barcha sohalarda bo'lgani kabi, dastlabki bosqichda kam ma'lumot yetarli bo'ladi. Ushbu faoliyatning dastlabki bosqichidanoq manfaatdor

tomonlarni ortiqcha axborot bilan yuklash, ularni maqsad va niyatidan chalg'itishi mumkin.

Ma'lumotlarni ma'lum bir manfaatdor tomonlar tushunadigan va qabul qiladigan tarzda yetkazish.

Ma'lumot yetkazishda maqsadli auditoriyani har doim yodda tutish muhimdir. Manfaatdor tomonlar nafaqat tahdidga oid turli xil ma'lumotlarni xohlashadi, balki bu ma'lumotlarning ularga turli xil usullarda yetkazilishini ham talab qilishadi. Masalan, direktorlar kengashi, biznesga ta'sir ko'rsatuvchi yuqori darajadagi tahdidlar haqida ma'lumot olishni xohlaydi. Ehtimol, CISO, CIO yoki texnologiyalar bo'yicha bosh direktor (CTO¹²⁴) samaradorlik va operatsion ko'rsatkichlar bo'yicha batafsil texnik hisobotlarni, shuningdek, tahdid va taktik mezonlar haqida yanada aniqroq ma'lumotlarni talab qilishi mumkin. Dastur rivojlanib borgan sayin, CFO va biznes rahbarlari tahdidlar haqidagi ma'lumotlarni miqdoriy shaklda ko'rishni istashi mumkin. Maqsadli auditoriyaga mos tildan foydalanish, tahdidga oid ma'lumotlarining aniq tushunilishini va tahdidlarni hisobga olgan holda qaror qabul qilishni ta'minlashning kalitidir.

Kerakli ma'lumotni kerakli odamlarga o'z vaqtida yetkazish.

Bu vazifa oldingi masala bilan chambarchas bog'liq. Tahdid haqidagi ma'lumotlar manfaatdor tomonlar (boshqaruv kengashi, yuqori lavozimli rahbarlar, aktivlar va tahdid bo'yicha mas'ul shaxslar)ga yetib borsa va ular buni tahdid haqidagi ma'lumotlarga asoslangan qarorlar qabul qilishlari uchun yetarlicha erta qabul qilsalargina, ular amaliy ahamiyatga ega bo'ladi. Ilk samarali qadamlardan biri – bu aniqlangan biznes muammolariga mos keladigan tahdid ko'rsatkichlarini ishlab chiqish va biznes bilan hamkorlikda tegishli tahdid chegaralari va maqsadlarini belgilashdir. Shuningdek, vaqt o'tishi bilan ma'lumotlar tendensiyasini ko'rsatish ham qiymatli bo'lishi mumkin.

Qo'shimcha mulohazalar

Ushbu kitobning maqsadi boshqa kitoblarda ko'p muhokama qilinadigan tahdidlarni boshqarish amaliyotlarini qanday bajarishni "o'rgatish" emas. Aksincha, ushbu kitob doimiy ravishda rivojlanib borayotgan raqamli asrda tashkilotlarga kibertahdidlarni boshqarishga yordam beradigan CRMPni belgilashga qaratilgan. Shuni aytish joizki, tahdid haqidagi ma'lumotlarga asoslangan tizimning ba'zi tamoyillari ortidagi "qanday qilib" degan savol biz uchun qo'shimcha e'tibor talab qiladigan soha hisoblanadi.

To'rtinchi bobda, 2-tamoyilni ishlab chiqishda hisobga olinishi mumkin bo'lgan uchta keng tarqalgan metodologiyaga to'xtalib o'tgan edik: "Tahdidning maqbul darajalari uchun tasdiqlangan va takrorlanadigan metodologiya yaratilishi lozim. Tavsiya etilgan uchta metodologiya quyidagilardan iborat:

¹²⁴ CTO (chief technology officer) – texnologiyalar bo'yicha bosh direktor.

- *Yetuklikni modellashtirish*
- *Ko'rsatkichlar bo'yicha hisobot (KPI va KRI)*
- *Tahdidni baholash (sifat va miqdoriy baholash)*

Har uchala yondashuv ham boshqaruv organi tomonidan maqbul tahdid darajalarini muvofiqlashtirish va tahdidlarni boshqarish bo'yicha qarorlar qabul qilishni rag'batlantirish uchun foydalanishi mumkin bo'lgan foydali ma'lumotlarni yaratishi mumkin. (Bu masala beshinchi bobda ham muhokama qilingan.) Keling, quyida ularning har birini batafsil ko'rib chiqamiz:

Yetuklikni modellashtirish.

Yetuklikni modellashtirish – bu korxonaning odamlar, jarayonlar va texnologiyalar nuqtayi nazaridan yetuklik darajasini va uning kelajakdagi istalgan holatini aniqlash jarayonidir. Bu jarayon har qanday bo'shliqlarni aniqlash va yetuklik darajasini haqiqiy tahdid sharoitlariga o'tkazishni aniqlash uchun zarurdir. Ko'pgina korxonalarda kiberxavfsizlik bo'yicha yetuklik darajalari sanoat standartlariga muvofiq (NISTning kiberxavfsizlik asoslari kabi), ichki yoki mustaqil uchinchi tomon tomonidan baholanadi. Odatda, har yili o'tkaziladigan ushbu baholash ikki umumiy maqsadga ega: korxona o'tgan yillarga nisbatan qanday rivojlanganligini aniqlash va uning o'z sohasidagi raqobatchilarga nisbatan qanday holatda ekanligini ko'rsatish.

Yetuklikni baholash yondashuvi real qiymatga ega. Yetuklik darajalari haqidagi hisobotlar muhim maqsadlarga xizmat qiladi. Ular dasturlar va muayyan xavfsizlik amaliyotlari rivojlanayotganini ko'rsatish uchun qo'llanilishi mumkin. Shuningdek, bu yondashuv umumiy sohadagi yoki bir xil miqyosdagi o'xshash tashkilotdagi yetuklikni o'lchash uchun qiyosiy hisobot sifatida ishlatilishi mumkin. Ammo bu yondashuvda ham bir qator kamchiliklar mavjud. Eng muhimi shundaki, yetuklikni modellashtirishning o'zi biznes amalga oshirishi mumkin bo'lgan tahdid haqida foydali ma'lumot bermaydi. Masalan, u biznes sohalari bo'yicha muayyan tahdidlarning ustuvorliklarini yoki bu tahdidlarni yumshatish byudjetlar va boshqa resurslarga qanday ta'sir ko'rsatishini ifodalab bermaydi.

KPI va KRI

KPI va KRI – ikkalasi ham korxonaning vaqt o'tishi bilan xavfsizlik holatini baholash imkoniyatini ta'minlashda muhim ahamiyatga ega. Biroq ularning farqini tushunish zarur: KPI muayyan dastur yoki jarayonning samaradorligini o'lchasa, KRI esa tahdidlarning korxonaning o'z maqsadlariga erishish qobiliyatiga ko'rsatadigan ta'sirini o'lchaydi. Ba'zan, o'lehevning o'zi ham KRI, ham KPI sifatida xizmat qilishi mumkin, bu uning qo'llanilayotgan kontekstiga va uni kim tushunishi kerakligiga bog'liq.

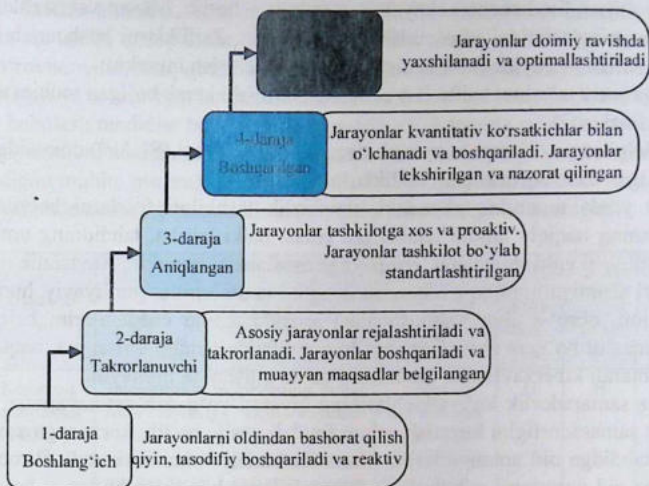
Bu jarayonda qiyosiy tahlil, ya'ni sohadagi boshqa korxonalar bilan o'zini taqqoslash foydali bo'ladi. Biroq qiyosiy tahlilning o'zi tahdid haqida foydali ma'lumot bermaydi. Eng muhimi, u ma'lum bir kompaniyaga xos bo'lgan tahdid muhitidagi potensial o'zgarishlarni, ayniqsa raqamlashtirish natijasida yuzaga keladigan tez rivojlanuvchi tahdid turlarini inobatga olmaydi. Masalan, tahdid bo'yicha mas'ul shaxslar uchun joriy yoki maqsadli tahdidning yetuklik darajasini shunchaki u sanoatdagi o'rtacha ko'rsatkichdan yaxshiroq bo'lgani uchun maqbul deb hisoblash jiddiy xato bo'ladi. Tahdidni anglash jarayonida qiyosiy tahlildan faqat dastlabki qadam sifatida foydalanish ancha samaraliroq yondashuvdir. Ammo, keyinchalik bu jarayon ma'lum bir yetuklik darajasi bilan bog'liq bo'lgan batafsil tahdid bayonotlari bilan, shuningdek, tahdid muhitining vaqt o'tishi bilan qanday o'zgarishi va bu o'zgarishlarning nafaqat tahdidlarni boshqarish amaliyotlariga, balki byudjetlarga ham qanday ta'sir ko'rsatishi to'g'risidagi tahlil bilan birlashishi lozim. Tahdid bo'yicha mas'ul shaxs tahdidlarni kamaytirish bo'yicha yetuklikning juda yuqori darajasiga erishishni xohlashi mumkin, lekin bu qanchalik qimmatga tushishi mumkinligi haqida xabardor qilinganda, fikrni o'zgartirishi mumkin (bu yana tahdid va foyda muhokamasi).

Har bir yetuklik darajasiga aloqador tahdidga oid bayonotlar vaqt o'tishi bilan, ko'pincha yangi tahdidlar yoki mavjud yangi vositalar tufayli, o'zgarib boradi. Bundan qat'i nazar, yetuklik holati tegishli tahdidga oid bayonotlar bilan birga boshqaruv organi tomonidan ko'rib chiqilib tasdiqlangandan so'ng, aynan shu nuqtada muayyan "chidamlilik" darajasini belgilash mumkin bo'ladi.

Imkoniyatning yetuklik modeli integratsiyasi

CMMI¹²⁵ Karnegi Mellon dasturiy ta'minot muhandislik instituti tomonidan ishlab chiqilgan model bo'lib, eng keng qo'llaniladigan yetuklik modellashtirish metodologiyalaridan biridir. U bevosita tahdidga qaratilmagan, lekin undan tahdid yetukligini aniqlash uchun foydalanish mumkin. 7.1-rasmda ko'rsatilganidek, CMMI korxonaning ishlash samaradorligi va jarayonlarini besh bosqichli yetuklik darajasida baholaydi:

¹²⁵ CMMI (The Capability Maturity Model Integration) – Imkoniyatning yetuklik modeli integratsiyasi, bu tashkilotning jarayonlarini yaxshilash va ularning samaradorligini oshirishga mo'ljallangan model.



7.1-chizma. CMMI yetuklik darajalari

Metrik hisobot. Samaradorlikni o'lchash/metrika metodologiyasi mavjud jarayonlar va nazoratlarning samaradorligi hamda unumdorligini aniqlash uchun atrof-muhitdan olingan obyektiv ma'lumotlardan foydalanishni o'z ichiga oladi. Bu metodologiya joriy holat va kutilayotgan kelajak holati o'rtasidagi bo'shliqlarni aniqlaydi va olingan ma'lumotlardan maqbul tahdid darajalarini belgilash, muvofiqlashtirish va jamoatchilik e'tiboriga yetkazish uchun foydalanadi. U odatda umumiy KPIlarga asoslanadi, lekin KPI maqsadlari ko'pincha betartib ravishda va eng muhimi, tahdid bo'yicha mas'ul shaxs yoki boshqaruv organining tasdig'isiz belgilanadi. Natijada "pastdan yuqoriga qarab boshqaruv" yondashuvi paydo bo'ladi, bunda xavfsizlik xizmati o'zi ozmi-ko'pmi tasodifiy maqsadni belgilab, keyin o'zini unga nisbatan baholaydi. Bu korxona tomonidan kelishilgan haqiqiy tahdid chegarasini belgilashga imkon bermaydi, tahdid chegarasini belgilash – biznesni yuritishda qanday tahdid darajasi maqbul va o'rinli ekanligini aniqlashda muhim element hisoblanadi.

Tahdid chegarasini belgilash (korxona qabul qilishga tayyor bo'lgan tahdid miqdorini belgilash) jarayoni, samaradorlik ko'rsatkichlari qiymatini aniqlash imkonini beradi.

Bu asosan fundamental subyektiv yondashuv bo'lib, asosan xavfsizlik tashkiloti va uning tahdidni idrok etishi bilan bog'liq. Zaifliklarni boshqarish bilan bog'liq KPllarga quyidagi bir nechta misollarni keltirish mumkin:

- Dasturiy ta'minot zaifliklari uchun tekshirilishi kerak bo'lgan muhim aktivlarning foizi

- Belgilangan xizmat ko'rsatish darajasi shartnomasi (SLA¹²⁶) doirasida bar-
taraf etilgan dasturiy ta'minot zaifliklarining foizi

Bu yerda muammo shundaki, xavfsizlik tashkiloti foizlarni belgilashda korxonaning haqiqiy tahdid talablariga emas, balki tajriba, tahdidning umumiy qabul qilinishi yoki shunchaki intuitsiyaga asoslanishi mumkin. Xavfsizlik nuqtayi nazari ahamiyatli, biroq u faqatgina keng ko'lamlı omillar (moliyaviy, huquqiy, operatsion, obro'-e'tibor va boshqalar) asosida tahdid chegaralarini belgilash uchun mas'ul bo'lgan shaxslarga ma'lumot sifatida taqdim etilsagina, haqiqatan ham samarali kiberxavfsizlik qarorlarini qabul qilishni ta'minlaydi.

Biz samaradorlik ko'rsatkichlarining qiymati yo'q deb aytmayapmiz. Ular jarayon samaradorligini kuzatish uchun foydali vosita bo'lib, korxonaga xavfsizlik va tahdidga oid amaliyotlarini takomillashtirish imkonini beradi. Biroq ular tahdidga oid qarorlarni qabul qilish tizimini yaratishda zarur bo'lsa, u holda bu ko'rsatkichlar to'g'ri manbalardan olingan va tegishli shaxslar hamda lavozim egalari tomonidan tasdiqlangan bo'lishi lozim. Shunday ekan, keling, aynan shu talablarga javob beradigan ko'rsatkichlarni ko'rib chiqamiz.

Yuqori qiymatli samaradorlik ko'rsatkichlari korxona, ya'ni tahdid bo'yicha mas'ul shaxslar tomonidan kiritilgan ma'lumotlar asosida belgilanganda, ular tahdid chegaralarini o'rnatish uchun qo'llanilishi mumkin hamda bu ularni strategik qarorlar qabul qilishda haqiqatan ham ahamiyatli va foydali qiladi. Chegaraviy qiymatni KPI yoki KRI ko'rsatkichi sifatida tushunish mumkin, bu ko'rsatkich samaradorlik yoki tahdidning belgilangan maqsaddan yoki qabul qilingan tahdid darajasidan oshib ketishi mumkin bo'lgan nuqtani ko'rsatadi.

Tahdidlarni baholash (sifat va miqdoriy baholash). Tahdidlarni baholash muayyan tahdidning yuzaga kelish ehtimoli va potensial ta'sirini muntazam ravishda baholaydi hamda ushbu tahdidni boshqarish va kamaytirish uchun zarur chora-tadbirlarni tavsiya etadi. Tahdidlarni baholash ikkita asosiy shaklga ega:

Sifat tahlili

Ko'pchilik korxonalar tahdidlarni baholash uchun an'anaviy ravishda sifat yondashuvidan foydalanib kelgan, u ma'lum cheklavlarga ega bo'lsa-da, u haqiqiy qiymatga ham ega. O'z tabiatiga ko'ra, sifat baholashlari subyektiv hisoblanadi, chunki ular shaxsiy yoki subyektiv ma'lumotlarga asoslanadi hamda xatoliklar-

¹²⁶ SLA (service-level agreements) – xizmat ko'rsatish darajasi shartnomasi, bu xaridor bilan taqdim etiladigan xizmatlarni belgilaydigan aniq (ichki yoki tashqi) kelishuv.

ga olib kelishi mumkin. Ammo sifatli yondashuv ko'rinishidan tasodifiy bo'lib tuyulsa-da, aslida unday emas, ayniqsa bu yondashuv bir nechta shaxsiy suhbatlar, so'rovnomalar, tadqiqotlar hamda tashqi ekspertlarning ma'lumotlari bilan to'ldirilgan va o'zaro bog'langan bo'lsa ular tasodifiy bo'lmaydi. Shunday qilib, sifatli baholash tahdidlar bo'yicha qaror qabul qilish hamda tahdidga asoslangan strategiya va uni amalga oshirishga yordam beradi (bu keyingi bobda muhokama qilinadigan muhim mavzu). 7.2-rasmda sifatli tahlilning tahdidlar bo'yicha qaror qabul qilishda qanday samarali hissa qo'shishi mumkinligi ko'rsatilgan.

ID	Ustuvorlik	Tahdid tasnifi	Tahdid kategoriyasi	Hozirgi baholash		
				Ehtimollik	Ta'sir	Ta'sir darajasi
5	Keyinroq aniqlanadi (TBD ¹²⁷)	Jinoyatchilar mijozlarning mobil bank ilovasiga kirib, foydalanuvchi tekshiruvi yoki shifrlash muammosi tufayli, mijozlarning mablag'larini ruxsatsiz joyga o'tkazib yuborishi mumkin.	Tizim va ma'lumotlar yaxlitligi (SI ¹²⁸)/Tizim va aloqa himoyasi (SC ¹²⁹)	H	H	H

7.2-chizma. NISTIR 8286 sifat tahlili natijalariga misol

Miqdoriy tahlil

Korxonalar biznes qiymatini dollar va sentlarda ifodalovchi aniq ko'rsatkichlarga bo'lgan ehtiyojni tobora chuqurroq anglab borishi bilan, bu yondashuv tobora ommalashib boryapti. Bu muhim maqsad bo'lsa-da, unga erishish oson ish emas. Miqdoriy baholash murakkab va mashaqqatli jarayon hisoblanadi, chunki u aniqlik bilan o'lchash g'oyat qiyin bo'lgan tahdidlarga (masalan, obro'ga putur yetkazish) aniq qiymat belgilashga harakat qiladi. Bu jarayon vaqt talab qiladi va korxona faoliyatiga xalal beradi, chunki u ko'plab manfaatdor tomonlardan batafsil ma'lumot kiritishni talab etadi. Masalan, ma'lumotlar buzilishi natijasida kelib chiqadigan obro'ga ta'sirning haqiqiy xavfini miqdoriy baholashga urinish, eng kamida, yuridik bo'lim, davlat organlari bilan aloqalar bo'lim va muvofiqlik bo'limlaridan korxonada ilgari sodir bo'lgan shunga o'xshash hujumlar bilan bog'liq ma'lumotlarni talab qiladi.

¹²⁷ TBD (to be determined) – keyin aniqlanadi, bu ibora qaror qilinmagan yoki noma'lum bo'lgan vaziyatlarda ishlatiladi.

¹²⁸ SI (System and Information Integrity) – Tizim va axborot yaxlitligi.

¹²⁹ SC (System and Communications Protection) – Tizim va aloqa himoyasi.

Miqdoriy baholashning murakkabligi bois, kibertahdidni miqdoriy baholash (CRQ¹³⁰) dasturiy ilovalarining yangi sinfi tez sur'atda paydo bo'la boshladi. Bu dasturlar baholash jarayonini avtomatlashtiradi. Ushbu vositalar korxonaga xos biznes va texnologiya muhitiga tegishli tahdid ssenariylarini tahlil qilishda haqiqiy ma'lumotlarga asoslangan yondashuvni qo'llaydi (masalan, muhim elektron tijorat veb-saytining xizmatini to'xtatishga olib keladigan ransomware dasturiy ta'minot hujumi). Bu biznesga kibertahdidni moliyaviy jihatdan ifodalash hamda tahdidni kamaytirish nuqtayi nazaridan eng yuqori darajadagi investitsiya samaradorligini ta'minlaydigan qo'shimcha himoya choralari aniqlash imkonini beradi. Ushbu ma'lumotlarni tahdid bo'yicha mas'ul shaxslarga ulashish mumkin, shunda ular maqbul tahdid darajalari, byudjetlar va boshqa omillar haqida qaror qabul qilishlari mumkin.

Monte-Karlo usulida modellashtirish (Monte Carlo Simulation)¹³¹

Monte-Karlo usulida modellashtirish – bu murakkab o'zgaruvchilarni hisobga olishning yana bir foydali usuli bo'lib, u tahdid natijalarini modellashtirish va natijalar taqsimotini yaratish orqali xatarni yanada aniqroq baholashga imkon beradi. Bu ehtimoliy tahdidlarni yaxshiroq tahlil qilish va talqin etish imkonini beradi, tahdidni hisobga olgan holda qaror qabul qilish uchun obyektiv ma'lumotlar taqdim etadi, shuningdek, muayyan tahdid ssenariylarining maqsadga muvofiqligini baholash imkoniyatini yaratadi.

Shubhasiz, tahdidlarni baholashda miqdoriy yondashuvning ahamiyati katta, ammo uning kamchiliklari ham mavjud. Bu yondashuv ko'proq vaqt va resurslarni talab qilishi mumkin. Korxonaning qaror qabul qiluvchi shaxslari uchun mavjud ma'lumotlarga asoslanib eng mos vositani tanlash ham qiyin bo'lishi mumkin. Bundan tashqari, CRMP doirasida nimani aniq miqdoriy baholash va bu ma'lumotlardan qanday foydalanish to'g'risida aniq ko'rsatmalar mavjud bo'lmasa, miqdoriy baholash jarayoni amalda foydasiz bo'lishi mumkin. Misol uchun 7.3-rasmga qarang.

¹³⁰ CRQ (cyber risk quantification) – kibertahdidni miqdoriy baholash, bu muayyan kibertahdidning potensial moliyaviy ta'sirini baholash jarayonidir.

¹³¹ Monte Carlo Simulation – Monte-Karlo usuli noma'lum qiymatni taxmin qilish uchun tasodifiy tanlab olishdan foydalanadigan statistik usuldir.

ID	Ustuvorlik	Tahdid tasnifi	Tahdid kategoriyasi	Hozirgi baholash		
				Ehtimollik	Ta'sir	Ta'sir darajasi
1	Keyinroq aniqlanadi (TBD)	Autsayder (begona shaxs) doimiy ilg'or tahdid (APT ¹³²) tahlili yordamida tashkilotning tarmog'iga kirib, bir necha oy davomida aniqlanmay qoladi, imtiyozli hujum yordamida tashkilotning muhim intellektual mulkinining katta qismini o'g'irlaydi	Kirish nazorati (AC ¹³³)	0.6	\$2,000,000	\$1,200,000

7.3-rasm. NISTIR 8286 miqdoriy tahlil natijalariga misol

Har ikkala yondashuv ham qimmatli bo'lib, ularni birgalikda qo'llash orqali chegaraviy darajalarga oid qarorlar (ya'ni maqbul tahdid darajalarini aniqlash va ularni muvofiqlashtirish) qabul qilish mumkin. Chegaralarni belgilash eng muhim jarayon hisoblanadi, chunki u maqsad, jarayon va natijani muntazam sur'atda, tegishli darajadagi batafsil ma'lumotlar asosida hamda tegishli manfaatdor tomonlarning fikrlarini inobatga olgan holda ko'rib chiqadi.

Bu yondashuvlar foydali bo'lsa-da, ular ayniqsa tasodifiy yoki alohida qo'llanilganda, korxonaning tahdidga oid ma'lumotlariga bo'lgan ehtiyojlarini to'liq qondira olmasligini tan olish muhim. Faqatgina tahdid haqidagi ma'lumotlarga asoslangan rasmiy tizimgina CRMP uchun zarur ma'lumotlarni taqdim etishi, boshqaruv organi va tahdidlar bo'yicha mas'ul shaxslarga tahdidga moyillik va chidamlilikni muvofiqlashtirish hamda tahdidga asoslangan strategiya va ijroni amalga oshirish imkonini berishi mumkin.

¹³² APT (Advanced Persistent Threat) – doimiy ilg'or tahdid, haqiqiy hayotdagi hujum ssenariyalarini modellashtiradi va zararli shaxslar tashkilot tarmog'i va tizimlariga qanday kirib borishga urinishi va ular qanday ma'lumotlarga kirishi mumkinligini ko'rsatadi.

¹³³ AC (access control) – kirish nazorati.

Kibertahdidlarni boshqarishda Bayes metodi

Bayes metodi – bu ehtimoliy xulosalar chiqarish usuli bo'lib, unda oldingi bilimlar, tajriba va dalillar asosida ma'lum bir hodisa sodir bo'lish ehtimoli haqidagi tasavvurlarni baholash va yangilash amalga oshiriladi. Bu usul hozirda tibbiyot va marketing kabi turli sohalarida keng qo'llanilmoqda. Ushbu metodologiya korxonada tahdidga oid qarorlarni qabul qilishni qo'llab-quvvatlashda qimmatli vosita bo'lishi mumkin, chunki u murakkab jarayonlar haqida tasavvurga ega bo'lish imkonini beradi hamda noaniqlikni samarali hisobga oladi.

Quyida Bayes qarorlarini qabul qilishning oddiy misoli keltirilgan. Yangi bozorga sarmoya kiritish yoki kiritmaslik haqida qaror qabul qilishga urinayotgan biznes egasi maqsadli bozor haqida to'liq ma'lumotga ega bo'lmaydi. Bu iste'molchilarning afzalliklari, ularning daromadlari yoki qaror qabul qilish uchun zarur bo'lgan boshqa ma'lumotlarni o'z ichiga olishi mumkin. Biznes egasi Bayes metodidan foydalanib, o'xshash loyihalardan to'plangan ma'lumotlar asosida loyihaning foydalilik ehtimolini baholashi mumkin. Buni o'zining oldingi tajribasi va sohani tushunishi bilan birlashtirib, ongli qaror qabul qilishi mumkin.

Xuddi shu metod kiberxavfsizlikka oid tahdidlarni baholashda ham qo'llanilishi mumkin. Aytaylik, siz kiberxavfsizlik bo'yicha mutaxassissiz, tashkilotingiz xodimlariga qarshi yo'naltirilgan muvaffaqiyatli fishing¹³⁴ hujumining bo'lish ehtimolini bashorat qilmoqdasiz. Bunda bir qator omillarni inobatga olishingiz mumkin. Bularga o'tkazilgan xavfsizlik treninglarining sifati, fishing sinovlaridan o'ta olmagan xodimlar foizi hamda xodimlarning xavfsizlik bo'yicha xabardorligiga ta'sir ko'rsatishi mumkin bo'lgan kadrlar almashinuvi kabi omillar kiradi.

Bugungi kunda bozordagi ba'zi CRQ dasturiy vositalari Bayes usullaridan foydalanadi, masalan, tarmoqdagi barcha mumkin bo'lgan hujum yo'llarini hisoblab chiqish va turli vaziyatlarda tizimga ruxsatsiz kirishning ehtimolini baholash uchun. Bu dasturlar bir nechta ssenariylar bo'yicha xavfsizlik buzilishi ehtimolini taqdim etadi.

Tahdidlarni baholashga asoslangan strategiya va uning ijrosi

Tahdidlarni boshqarish, ya'ni tahdid va foydani muvozanatlash san'ati, hech qachon mukammal bo'lmaydi. Korxonani barcha tahdidlardan himoya qilish iloj-siz. Bunga urinishning o'zi muvaffaqiyatsizlikka olib keladi, shuningdek, korxonaning tahdid muhitidagi muqarrar o'zgarishlarga tezda javob berish qobiliyatini cheklashi va hatto to'g'ri faoliyat olib borishiga tahdid tug'dirishi mumkin. Tahdidlardan xoli muhitning mavjud emasligini anglash va buni tan olish hamda bu haqiqatni biznesning manfaatdor tomonlariga yetkazish – tahdidga asoslangan strategiya va uni amalga oshirishda eng yaxshi boshlang'ich nuqtadir.

Bu xavfsizlik tashkiloti, tahdid bo'yicha mas'ul shaxslar, boshqaruv organi, yuqori rahbariyat va ehtimol direktorlar kengashi ishtirokida doimiy va takroriy muzokaralarni talab etadi. Ushbu muzokaralar tahdid bo'yicha mas'ul shaxslarga tahdidga moyillik va chidamlilikni belgilashga imkon bersa, xavfsizlik tashkilotiga esa mavjud byudjet, xodimlar va texnologiyalar bilan ushbu belgilangan

¹³⁴ Fishing attack – fishing hujumi, bu tashkilot yoki jismoniy shaxsning shaxsiy ma'lumotlari yoki moliyaviy ma'lumotlarini o'g'irlash uchun elektron pochta, xabarlar yoki veb-saytlar kabi soxta aloqa usullaridan foydalanish.

moyillik va chidamlilik darajalariga erishish mumkinligini aniqlash imkonini beradi. Agar buning iloji bo'lmasa (ko'p hollarda shunday bo'ladi) tahdid bo'yicha mas'ul shaxs qo'shimcha resurslarni ajratish zarurligini asoslashi yoki tahdidlarni boshqarishga oid maqsadlarini qayta ko'rib chiqishiga to'g'ri keladi.

5-bobda aytib o'tilganidek, tahdidga oid qarorlar xavfsizlik qarorlari emas, balki biznes qarorlaridir. Tahdid va mukofotni muvozanatlash jarayonida xavfsizlikning roli – bu tahdid bo'yicha mas'ul shaxslar va boshqalarga kerakli ma'lumotlarni taqdim etish, so'ngra belgilangan maqsadlarni amalga oshirish uchun qanday resurslar kerakligini aniqlashdan iborat. Ko'p hollarda, tahdidlarni boshqarishga oid qarorlarini qabul qiluvchi shaxslar va xavfsizlik xizmati o'rtasida muayyan aktiv yoki jarayon uchun maqbul tahdid chegarasini belgilash va unga erishish uchun zarur resurslarni joriy etish bo'yicha uzoq muddatli muloqot jarayoni kuzatiladi.

Beshinchi bobda batafsil bayon etilgan tahdidlarni baholashga asoslangan strategiya va ijroning oltita tamoyili amalga oshirish jarayoniga asos bo'lishi kerak:

1-tamoyil: Maqbul tahdid chegaralarini aniqlash

Maqbul kibertahdid chegaralari tahdid tizimi va metodologiyasiga asoslanib, tahdid bo'yicha mas'ul shaxslar tomonidan aniq tushunilishi, belgilanishi va tasdiqlanishi zarur.

2-tamoyil: Strategiya va byudjetni tasdiqlangan tahdid chegaralari bilan muvofiqlashtirish

Kibertahdidni bartaraf etish rejasi va byudjeti – tasdiqlangan tahdid chegarasi bilan muvofiqlashtirilishi kerak

3-tamoyil: Maqbul tahdid chegaralari doirasida ijro etish

Kibertahdidlarni bartaraf etish rejasi tasdiqlangan tahdid chegaralariga muvofiq amalga oshirilishi lozim.

4-tamoyil: Doimiy ravishda nazorat qilish

Kibertahdidlarni bartaraf etish rejasining ijrosi belgilangan samaradorlik ko'rsatkichlari va operatsion mezonlar asosida doimiy ravishda nazorat qilib borilishi lozim.

5-tamoyil: Tahdidning chegaraviy darajalariga nisbatan audit tekshiruv

Audit xizmati tahdidning tasdiqlangan chegaraviy darajalariga asoslangan kibertahdidni bartaraf etish rejasining to'g'ri bajarilishini ko'rib chiqishi va baholashi kerak.

6-tamoyil: Tahdidlarni bartaraf etish rejasiga uchinchi tomonlarni kiritish

Kibertahdidlarni bartaraf etish rejasi uchinchi tomonlarni, jumladan hamkorlar, ta'minotchilar va ta'minot zanjiri ishtirokchilarini hisobga olishi kerak.

Birinchi 30 kun ichida quyidagilarni ko'rib chiqish lozim:

- Boshqaruv organi orqali tahdid bo'yicha mas'ul shaxslar tomonidan tasdiqlangan korxona uchun maqbul tahdid darajasini (tahdidga moyillik va chidamlilik) aniqlash.

- Belgilangan tahdid darajalariga mos keladigan tahdidlarni boshqarish strategiyasini ishlab chiqish. Bu aniqlangan tahdidlarga nisbatan tegishli choralarni: tahdidlarni oldini olish, ularni kamaytirish, boshqalarga o'tkazish va qabul qilishni o'z ichiga olishi kerak.

- Maqbul tahdid darajasi va potensial tahdidlarning ta'siriga mutanosib ravishda tahdidlarni boshqarish strategiyasi uchun byudjet tayyorlash.

- Tahdidni boshqarish strategiyasining samaradorligini o'lchashga yordam beradigan KPI va boshqa operatsion mezonlarni ishlab chiqish va belgilash.

Keyingi 60 kun ichida quyidagilarni ko'rib chiqish lozim:

- Bo'limlararo hamkorlikning muhimligiga alohida e'tibor qaratib, korxona miqyosidagi tahdidlarni bartaraf etish strategiyasini amalga oshirish.

- Oldindan belgilangan KPI va operatsion ko'rsatkichlardan foydalangan holda tahdidlarni boshqarish strategiyasining samaradorligini ta'minlash uchun doimiy monitoring jarayonini yo'lga qo'yish.

- Tahdidlarni bartaraf etish strategiyasi jarayoni va samaradorligi to'g'risida tegishli manfaatdor tomonlarga muntazam hisobot berish.

- Tahdidlarni bartaraf etish rejasining to'g'ri bajarilishini nazorat qilish va maqbul tahdid darajalarining muvofiqligini ta'minlash uchun audit xizmati faoliyatini nazorat qilish jarayonini boshlash.

Tahdidga asoslangan strategiya va ijro bilan bog'liq umumiy qiyinchiliklar

Tahdidga asoslangan strategiya va ijro modelini joriy etishga intilayotgan ko'plab xavfsizlik bo'linmalari orasida quyidagi o'zaro bog'liq qiyinchiliklar keng uchraydi.

Byudjet va boshqa resurslarning yetishligi. Tahdid va foyda o'rtasidagi muvozanatni saqlash – bu tahdidlar, resurslar va imkoniyatlar o'rtasidagi muvozanatni ham anglatadi. Tahdidga asoslangan strategiya va ijro ichki xodimlar yoki tashqi pudratchilar uchun har doim yangi texnologiyalarga, ba'zida esa yangi ko'nikmalarga sarmoya kiritishni talab qiladi. Tez-tez so'raladigan umumiy savol: "Agar byudjet jarayoni allaqachon belgilangan bo'lsa (masalan, CIO byudjetining foizi yoki o'tgan yilgi byudjetning foizi sifatida), ishni nimadan boshlash kerak?" Kelajakda byudjetni belgilash bevosita korxona tomonidan belgilangan tahdidga moyillik va chidamlilik darajasiga bog'liq bo'lishi kerak (5-bobda keltirilgan usullardan foydalangan holda). Bu tahdidni miqdoriy baholash, yetuklik modellashtirish yoki boshqa yondashuvlar yordamida amalga oshirilishi mumkin

bo'lsa-da, tahdid muhiti o'zgarishi bilan maqbul tahdid darajalarining ham muqarrar ravishda o'zgarishi bois, bu o'zgarishlarning xarajatlar va tahdidlarga ta'sirini aniq tushunish lozim.

Muvofiqlikka asoslangan strategiya (Qonunchilik talablariga rioya qilishga asoslangan strategiya). Tarixan, tashkilotlarda xavfsizlik dasturlari asosan qonunchilik talablariga rioya qilishga qaratilgan. O'sha paytda bu tushunarli edi, chunki biznes muhitida korxonalarga kiberhodisalar orqali ta'sir ko'rsatishning asosiy usullaridan biri aynan qoidalariga rioya qilmaslik edi. Muvofiqlikka asoslangan strategiya asosan qoidalar, me'yoriy hujjatlar va talablarga rioya etishga qaratilgan bo'lib, kibertahdidlarning biznesga keng ko'lamdagi ta'sirini tushunishga e'tibor qaratmaydi. Bu ta'sirlar faqatgina qoidabuzarliklar bilan cheklanib qolmaydi, balki moliyaviy, operatsion, obro'-e'tibor, ekologik hamda sog'liq va xavfsizlik kabi boshqa turdagi tahdidlarni ham o'z ichiga oladi. Hozirda kiberxavfsizlik korxona va korxonadagi boshqaruv kengashidan boshlab barcha darajadagi qaror qabul qiluvchilar uchun jiddiy tahdid sifatida tan olinmoqda. Masalan, kiberhujum natijasida ishlab chiqarish kompaniyasining ish faoliyati to'xtab qolishi va natijada bu kompaniyaga katta moliyaviy zarar yetkazilishi mumkin. Shu sababli, kompaniyaning kibertahdidga oid strategiyalari faqatgina muvofiqlik talablari asosida belgilanmasligi juda muhimdir. Buning o'rniga, xavfsizlik strategiyasi korxonaning tahdidga moyilligi va chidamliligini har tomonlama tushunishga asoslangan bo'lishi kerak. Bu qonun-qoidalarga muvofiqlik masalalarini o'z ichiga olishi mumkin, ammo faqat shu bilan cheklanib qolmasligi kerak. Strategik tashabbuslar va byudjet takliflarini kengroq belgilangan moyillik va chidamlilik darajasiga moslashtirish, tahdidni baholashga asoslangan strategiyani o'rnatish orqali ushbu qiyinchilikni hal qilishga yordam beradi.

Ushbu ikki muammo, ya'ni cheklangan resurslar va tor doiradagi muvofiqlik yo'nalishi, CRMPni amalga oshirish orqali hal qilinishi mumkin. Mohiyatan, xavfsizlik xizmati korxonaning muammolarini tushunib, ularning tahdidga moyillik va chidamlilik darajalari bilan moslashishi, so'ngra esa bu tushunchani strategiyani ishlab chiqish va amalga oshirishda qo'llashi lozim. Bu xavfsizlik strategiyasini AT xarajatlarining foizi yoki tartibga solish majburiyatlari ro'yxatiga moslashtirishni o'z ichiga olgan an'anaviy "oson yechim"dan voz kechish demakdir. Buning o'rniga, xavfsizlik xizmati strategik hamkor sifatida belgilanadi, natijada bu korxonaga tahdidlarni samarali boshqargan holda o'z biznes maqsadlariga erishish imkonini beradi.

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi korxona va uning qaror qabul qiluvchilarini himoya qilishda muhim ahamiyatga ega. Bu shunchaki xavfsizlik insidentlarini aniqlash, ularga chora ko'rish yoki o'rnatilgan munosa-

batlarni mustahkamlash masalasi emas, balki tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etish mas'uliyati xavfsizlik tashkiloti zimmasiga yuklanmasligi ham juda muhimdir. Bu yuqori rahbariyat va korxonaning boshqaruv organi tomonidan tasdiqlangan rasmiy jarayon bo'lishi lozim, unda vazifa va mas'uliyatlar aniq belgilanishi, jumladan tahdidlar eskalatsiyasi bo'yicha qarorlar qabul qilish uchun kim mas'ul ekanligi ko'rsatilishi lozim.

Tahdidga oid ma'lumotlarni oshkor qilish jarayoni korxonadan tashqaridagi subyektlarga, jumladan SEC kabi tartibga soluvchi organlarga va ba'zi hollarda hatto sudlarga ham tatbiq etiladi. U, shuningdek, tahdidga oid tegishli choralar belgilanganda qanday harakatlar qilinishi kerakligini aniq ko'rsatib beradigan tartib-qoidalarini ham o'z ichiga oladi. Bu esa barcha tomonlarning o'z vazifalarini, tahdidlarni baholash hamda boshqarish jarayonini aniq tushunishini ta'minlaydi.

6-bobda bayon etilgan tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish tamoyillari amalga oshirish uchun asos bo'lishi kerak:

1-tamoyil: Eskalatsiya jarayonlarini o'rnatish

Kibertahdidlarni eskalatsiyasi qilish jarayonlari ishlab chiqilishi va joriy etilishi lozim.

2-tamoyil: Barcha korxonalar uchun ma'lumotlarni oshkor qilish jarayonlarini yo'lga qo'yish

Korxonaning kibernetika ma'lumotlarini oshkor etish jarayonlari uning o'ziga xos tahdid omillarini, tashkiliy sharoitlarini va talablarini inobatga olgan holda ishlab chiqilishi lozim.

3-tamoyil: Ochiq aksiyadorlik jamiyatlari uchun ma'lumotni oshkor qilish jarayonlarini o'rnatish

Ochiq aksiyadorlik jamiyatlari jiddiy tahdidlarni, tahdid omillarini, kibertahdidlarni boshqarish jarayonlarini, boshqaruv tizimi va jiddiy hodisalar haqidagi ma'lumotlarini oshkor qilishlari shart.

4-tamoyil: Eskalatsiya va ma'lumotlarni oshkor etish jarayonlarini sinovdan o'tkazish

Kibertahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilish jarayonlari o'zlashtirilgan saboqlarni inobatga olish maqsadida doimiy ravishda tekshirilishi, sinovdan o'tkazilishi va yangilanishi kerak.

5-tamoyil: Eskalatsiya va ma'lumotlarni oshkor etish jarayonlarini tekshirish

Korxonaning samaradorligi, izchilligi hamda tegishli qoidalar va siyosatlariga muvofiqligini ta'minlash maqsadida, audit xizmati korxonaning kibertahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlarini ko'rib chiqishi va baholashi kerak.

Birinchi 30 kun ichida quyidagilarni ko'rib chiqish lozim:

• Aniqlangan tahdidlarni eskalatsiya qilish uchun aniq tartiblarni belgilash. Bu qanday tahdidlarni, qachon, kimga eskalatsiya qilish kerakligini va hisobotda nimalar aks ettirilishi kerakligini o'z ichiga oladi.

• Barcha manfaatdor tomonlarning kibertahdidlarni boshqarish, boshqaruv va muhim hodisalar haqida hisobot berishga oid majburiyatlarni tan olishlarini ta'minlash uchun barcha korxonalar harakat qilishi lozim.

• Korxonaning o'ziga xos tahdid omillari, muhiti va talablarini inobatga oladigan tahdidga oid ma'lumotlarni oshkor etish bo'yicha tartib-qoidalarini ishlab chiqish yoki yangilash.

• Yangi tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlari hamda tartib-qoidalarini bo'yicha asosiy xodimlarni o'qitish.

• Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlari va hamda tartib-qoidalarining oldindan tekshiruvini o'tkazishni ta'minlaydigan mexanizmlarni joriy etish.

Keyingi 60 kun ichida quyidagilarni ko'rib chiqish lozim:

• To'liq ishlab chiqilganidan va ko'rib chiqilgandan so'ng (amalga oshirishdan oldin) tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish tartib-qoidalarini yakunlash va boshqaruv organidan ruxsat olish.

• Tahdidlarning eskalatsiyasi va ma'lumotlarni oshkor qilish amaliyotlarini amalga oshirilishi va bajarilishini muntazam kuzatish.

• Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlarining samaradorligini hamda tegishli siyosat, tartib-qoidalar va qonun-qoidalariga muvofiqligini ta'minlash maqsadida ularning birinchi auditini o'tkazish. Natijalar va fikr-mulohazalarni to'plash va olingan ma'lumotlardan foydalanib, jarayonlarni takomillashtirish.

Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish bilan bog'liq umumiy muammolar

Bu sohada amalga oshirishning asosiy muammolari quyidagilardan iborat:

Eskalatsiya jarayonini tor doirada tushunish (eskalatsiyaga, ko'pincha faqat noxush voqeaga javob berish sifatida qaraladi). Tahdidlar eskalatsiyasi – bu korxonaga zarar yetkazishi mumkin bo'lgan potentsial tahdid va zaifliklarni faol boshqarish hisoblanadi. Asosiy xavfsizlik tashkilotlari va dasturlarining an'anaviy diqqat markazida bo'lgan “*hodalarga chora ko'rish*” esa – bu aniqlangan tahdid yoki zaifliklarga samarali munosabat ko'rsatishga qaratilgan. Ikkalasi ham keng qamrovli xavfsizlik dasturining muhim qismlari hisoblanadi, biroq hodisalarga chora ko'rishning yakka o'zi yetarli bo'lmaydi, chunki u sohada o'rnatilgan qat'iy huquqiy va me'yoriy majburiyatlarni qondira olmasligi mumkin. Moslashuvchan boshqaruv amaliyotlari va tahdidlar haqidagi ma'lumotlarga asoslangan tizim

joriy etilishi bilan, korxonaning potensial tahdidlarni aniqlash, ularning ta'sirini baholash hamda oldindan belgilangan me'yorlar asosida ularni eskalatsiya qilish qobiliyatiga ega bo'ladi. Ta'lim va o'qitish ham juda foydali bo'lishi mumkin, chunki ular xodimlarga tahdidlarni anglash madaniyatini shakllantirishga yordam beradi. Bunda xodimlar nafaqat sodir bo'lgan haqiqiy hodisalarni, balki potensial tahdidlarni ham eskalatsiya qilish muhimligini tushunishadi.

Korxonaga xos majburiyatlarni aniqlash va ularga e'tibor qaratish imkoniyatining yo'qligi. Turli korxonalarning tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish bo'yicha talablari bir-biridan jiddiy farq qiladi. SEC va boshqa nazorat organlari talablariga ko'ra, ochiq aksiyadorlik kompaniyalari muhim ahamiyatga ega bo'lgan tahdidlarga alohida e'tibor qaratishlari shart. Ko'pmillatli kompaniyalar esa o'zlari faoliyat yuritadigan turli mintaqalardagi har xil qonun-qoidalariga (ba'zida bu qonun-qoidalar o'zaro zid bo'ladi) amal qilishiga majbur bo'ladi. Turli sohalarida faoliyat yuritayotgan korxonalar keng ko'lamli va o'zgaruvchan sanoat standartlari hamda protokollariga javob berishlari zarur. Bularning aksariyati 6-bobda batafsil yoritilgan. Shuningdek, hajm va faoliyat turi jihatidan farqlanuvchi korxonalar ham har xil majburiyatlar to'plamiga duch keladi.

Tahdidlarni boshqarishda standart yondashuvdan foydalanish, muqarrar ravishda korxonaga xos majburiyatlar va xavf omillarini e'tibordan chetda qoldiradi. 4-bobda muhokama qilingan tahdidlarni hisobga oluvchi tizim joriy etilganda, korxona o'zining o'ziga xos biznes muhiti va aniqlangan tahdid profilini inobatga olgan holda keng qamrovli tahdidlarni baholashni amalga oshirish imkoniyatiga ega bo'ladi. Bunday tizim korxonaning o'ziga xos tahdidlarini, shuningdek, uning huquqiy va me'yoriy majburiyatlarini hamda turli tahdidlar korxona faoliyatiga qanday ta'sir qilishi mumkinligini batafsil tushunishga imkon beradi. Korxona ushbu ma'lumotlardan foydalanib, o'zining eskalatsiya va ma'lumotlarni oshkor etish talablarini tegishli ravishda moslashtirishi mumkin.

Qaror qabul qilishda umumiy, alohida yoki haddan tashqari ko'p qonun-qoidalariga rioya qilish. Qanday aktivlar va tahdidlar muhim ahamiyatga ega ekanligini aniqlash oddiy jarayon emas, ammo bu ko'pincha korxona muhiti-ning o'ziga xos xususiyatlarini hisobga olmagan holda umumiy amaliyot sifatida amalga oshiriladi. Ko'p hollarda, choraklik tahdid hisobotlarini tayyorlash va taqdim etish jarayoni xavfsizlik tashkiloti bilan samarali hamkorlikni ta'minlay olmaydi. Avvalroq batafsil muhokama qilinganidek, bu amaliyotga bo'lgan nazorat tobora kuchaymoqda, huquqiy va me'yoriy kutilmalar o'zgarimoqda, javobgarlik esa ortib bormoqda. Ushbu yangi muhit korxonalarga endilikda talablarga javob bermaydigan amaliyotlarini o'zgartirishdan boshqa iloj qoldirmaydi. Ushbu muammo tahdidlarning muhimligini baholash uchun ishlatiladigan mezonlarni takomillashtirish orqali hal etiladi. Bunga tahdid haqidagi ma'lumotlarga asoslangan

tizimga moslashish va tahdidlar eskalatsiyasi uchun aniq chegaralarni belgilash orqali erishish mumkin.

Dasturni sotish

CRMPni joriy etish shubhasiz korxonaning eng yuqori darajasidan tortib barcha lavozimlar va bo'limlardan jiddiy majburiyat va qo'llab-quvvatlashni talab qiladi. Dasturning muvaffaqiyati uchun keng doiradagi manfaatdor tomonlarning: direktorlar kengashi, CEO, CxO, yuqori lavozimdagi rahbarlar, huquqiy va muvofiqlik tashkilotlari hamda albatta xavfsizlik bo'limining doimiy ishtiroki hal qiluvchi ahamiyatga ega bo'ladi. Biroq dasturni barcha manfaatdor tomonlarga yetkazish, uning ahamiyatini va ularning turli hamda ba'zan bir-biriga zid bo'lgan manfaatlarini tan olishlarini ta'minlash oson yoki oddiy ish bo'lmaydi.

Xavfsizlik tashkiloti, shubhasiz, CRMPni amalga oshirishda va uning doimiy muvaffaqiyatiga hissa qo'shishda muhim rol o'ynaydi. CISO va boshqa xavfsizlik mutaxassisarlari turli darajadagi manfaatdor tomonlarning keng doirasi bilan yaqindan hamkorlik qilishlari kerak bo'ladi. Bular qatoriga direktorlar kengashi, korxona amaldorlari va yuqori darajadagi rahbarlar, shuningdek, yuridik bo'lim va boshqa ko'plab operatsion bo'limlar hamda tashqi tomonlar, masalan, nazorat organlari va biznes hamkorlar kiradi. Buning natijasida esa, xavfsizlik xizmati mutaxassisining shaxsiy qoniqishi oshib, kasbiy imkoniyatlari sezilarli darajada oshadi. Xavfsizlik xizmatining dastur muvaffaqiyatiga qo'shgan hissasi korxonaning turli sohalariga ham katta foyda keltiradi. Keling, kibertahdid amaliyotining ba'zi afzalliklari va ahamiyatini ko'rib chiqaylik.

Korxona miqyosida tahdid haqidagi ma'lumotlarga asoslangan qarorlar qabul qilish.

Xavfsizlik o'z vazifasini umumiy tahdid boshqaruvi funksiyasining bir qismi sifatida bajarganida, u tahdid va aktivlar bo'yicha mas'ul shaxslar, shuningdek boshqa ko'plab manfaatdor tomonlar o'zlarining biznes va operatsion qarorlarini qabul qilishda foydalanishlari mumkin bo'lgan strategik ma'lumotlarni taqdim etadi. Bu nafaqat xavfsizlik tashkilotlari an'anaviy ravishda e'tibor qaratib kelgan kibertahdidlar va zaifliklarni, balki to'liq tahdid muhitini ham o'z ichiga oladi. Tahdid va foyda muvozanatini ta'minlovchi bunday yondashuv qaror qabul qilish bo'yicha tayinlangan mas'ul shaxslarga potensial tahdidlarni oldindan ko'rish va ularga tayyorgarlik ko'rish imkonini beradi, shu bilan birga istiqbolli biznes imkoniyatlarini qo'ldan chiqarmaslikka yordam beradi.

Korxona uchun qiymati

Korxona miqyosida tahdid haqidagi ma'lumotlarga asoslanib qaror qabul qilish strategik zaruriyat hisoblanib, u nafaqat korxonaning xavfsizlik darajasini oshiradi, balki biznesning o'sishi va operatsion samaradorligini ham yuksaltiradi.

Bu murakkab tahdid muhitini boshqarish, yangi paydo bo'layotgan imkoniyatlardan foydalanish va kompaniyalarga tavakkal qilish imkonini beruvchi muhim vositadir, bu korxonaning raqobatchilariga nisbatan raqobat ustunligini ta'minlaydi.

Normativ-huquqiy talablarga rioya qilish

Butun dunyo bo'ylab tartibga soluvchi organlar va sudlar korxonaning kiberxavfsizlik amaliyotiga qo'yiladigan talablarini jadallik bilan kengaytirib, ularni yanada keng qamrovli va qat'iyroq qilib bormoqda. Ular korxonalar va korxonaning tobora ko'payib borayotgan manfaatdor tomonlarini kibermuvaffaqiyatsizliklar uchun javobgar deb hisoblashlarini aniq ko'rsatmoqdalar.

Korxona uchun qiymati

CRMP korxonaning barcha me'yoriy-huquqiy talablar va qonuniy majburiyatlarga to'liq rioya qilishini ta'minlaydi, bu esa rioya qilmaslik oqibatlarini jazolar, obro'ga putur yetkazish va sud jarayonlari xavfini kamaytiradi. Mohiyatiga ko'ra, keng qamrovli CRMP me'yoriy-huquqiy muvofiqlikni saqlash, korxona yaxlitligini himoya qilish va manfaatdor tomonlarning ishonchini mustahkamlash uchun muhim vosita hisoblanadi.

Jamoatchilik va iste'molchilar ishonchi

Iste'molchilar o'zlari hamkorlikda ishlaydigan kompaniyalar va boshqa korxonalarga katta umidlar bog'lashadi va kibermuvaffaqiyatsizliklar (masalan, ma'lumotlarning sizib chiqishi) shuni ko'rsatadiki, iste'molchilar o'zlarining maxfiy ma'lumotlarini himoya qilishga jiddiyroq qaraydigan raqobatchilarga murojaat qilib, ular bilan faoliyat olib borishadi. Jamoatchilik ham har qachongidan-da ko'proq uyushgan va iste'molchilar, atrof-muhit va boshqa targ'ibot guruhlarining bosimi korxona obro'si va brend imidjiga jiddiy zarar yetkazishi mumkin.

Korxona uchun qiymati

Kiberxavfsizlikning kuchli jihati shundaki, u iste'molchilar va jamoatchilikka korxona ularning shaxsiy ma'lumotlari va boshqa maxfiy ma'lumotlarni himoya qilishga jiddiy yondashayotganini ko'rsatadi. Mustahkam kiberxavfsizlik strategiyasi – bu jamiyat va iste'molchilar ishonchini saqlash va oshirish, korxona obro'sini himoya qilish hamda uning uzoq muddatli muvaffaqiyati va barqarorligini ta'minlashga qaratilgan asosiy sarmoyadir.

Tashqi tomonlar bilan munosabatlar

Korxonalar tobora ko'proq tashqi hamkorlar, texnologiya ta'minotchilari, sanoat tashkilotlari va hatto raqobatchilarni o'z ichiga olgan murakkab ekotizimlarda faoliyat yuritmoqda. Bu qimmatli munosabatlarda ishonch hal qiluvchi ahamiyatga ega, chunki ular intellektual mulk va boshqa maxfiy ma'lumotlarni o'zaro almashishni o'z ichiga oladi. Bunday ishonchni saqlab qolish va mustahkamlash uchun samarali CRMP nihoyatda zarurdir.

Korxona uchun qiymati

Mustahkam CRMPni joriy etish orqali korxona o'zini ishonchli hamkor sifatida namoyon etishi mumkin. Bu nafaqat mavjud aloqalarni mustahkamlaydi, balki potensial hamkorlarni ham jalb qilib, korxonaning hamkorlik tarmog'ini yanada kengaytiradi. Samarali CRMP – bu tashqi tomonlar bilan munosabatlarni yaxshilaydigan, ishonch madaniyatini shakllantiruvchi va tobora o'zaro bog'liq bo'lib borayotgan biznes muhitida hamkorlikdagi muvaffaqiyatga erishishga yordam beradigan strategik vositadir.

Innovatsiya

Ma'lumotlar va xavfsizlik tashkiloti nazorati ostida amalga oshiriladigan kibertahdidlarni samarali boshqarish jarayoni yangi texnologiyalarni, yangi operatsion jarayonlar, yangi mahsulot va xizmatlarni, hatto mutlaqo yangi biznes modellarni rivojlantirishga yordam berishi mumkin. Bu juda muhim, chunki bulutli hisoblash, IoT va AI kabi o'zgaruvchan raqamli texnologiyalar tufayli korxonalarning tahdid muhiti hayratlanarli tezlikda o'zgarmoqda. Bu texnologiyalar bir vaqtning o'zida ham yangi va zararli yetkazuvchi tahdidlarni, ham biznes rivojlanishi uchun muhim imkoniyatlarni yaratmoqda.

Korxona uchun qiymati

Samarali kibertahdidlarni boshqarish korxonalarga yangi texnologiyalar bilan bog'liq tahdidlarni xavfsiz bartaraf etish uchun ishonchli poydevor yaratadi, shu bilan birga yangi texnologiyalar imkoniyatlaridan samarali foydalanadi. Bu nafaqat potensial tahdidlarni kamaytiradi, balki innovatsiyalar va o'sishni ham rag'batlantiradi. Samarali kibertahdidlarni boshqarish – bu innovatsiyalarni amalga oshirishning strategik vositasi bo'lib, yangi texnologiyalar va biznes model-larini xavfsiz o'rganish va joriy etishga imkon yaratadi hamda raqamli davrda biznesning o'sishini ta'minlaydi.

Operatsion barqarorlik

Operatsion barqarorlik (ishdagi nosozliklarga moslashish va ularga qarshi turish qobiliyati) qaysidir ma'noda har qanday CRMPning pirovard maqsadidir. (Aslida, bu shunchalik muhimki, keyingi bob aynan shu mavzuga bag'ishlangan.) Korxonaning belgilangan tahdid chegaralari va chidamliligiga nisbatan barqarorligini ta'minlashga ko'maklashish orqali, xavfsizlik tizimi hatto vaziyat yomonlashganda ham, faoliyatning uzluksizligini ta'minlay oladi, shu bilan birga ishdagi nosozliklar va xavf darajasini kamaytiradi.

Korxona uchun qiymati

Ishonchli CRM tizimi korxonaga nosozliklar yuz berganda ularga tezkor javob berish va ulardan keyin qayta tiklanish uchun zarur vositalar va strategiyalarni taqdim etadi. Ushbu barqarorlik korxonaning operatsion yaxlitligini himoya qiladi, shuningdek, uning jamoatchilikdagi obro'si, brend imiji va mijozlarning

ishonchini saqlab qolishda yordam beradi. Beqaror va noaniq biznes muhitida barqarorlik zaruriyatga aylangan. Bu korxonaning nosozliklar jarayonida omon qilishi va rivojlanishini belgilaydigan hal qiluvchi omildir.

Kiberxavfsizlik bo'limi haqiqiy tahdid funksiyasi sifatida ishlasa va CRMP tizimini joriy etsa, u o'zining an'anaviy xavfsizlikni ta'minlash vazifasidan ancha yuqoriga ko'tariladi. U korxonaga raqamli taraqqiyot jarayonini xavfsiz va foydali boshqarishga yordam beradigan hamda haqiqiy biznes qiymatini yaratadigan strategik hamkorga aylanadi. O'zgarishlarni boshqarish korxona uchun ham, xavfsizlik bo'limi uchun ham qiyin bo'lishi mumkin. Shu sababli, jarayonni amalga oshirishni boshqarayotgan shaxslar barcha manfaatdor tomonlar bilan muntazam va doimiy muloqot olib borishlari kerak. Bu muloqotlar ko'rsatkichlarni belgilash, jarayonni kuzatish (muvaqqiyatlar va muvaqqiyatsizliklar), yo'l qo'yilgan xatolar va olingan saboqlarni tahlil qilish hamda rivojlanib borayotgan kibertahdidlar va tahdid muhitidagi boshqa o'zgarishlarga moslashish uchun dasturni yangilash bo'yicha ko'rsatmalar berishga qaratilgan bo'lishi lozim. CRMPni amalga oshirish yo'l xaritasi tuzilgandan va tasdiqlangandan so'ng, uni kamida yiliga bir marta qayta ko'rib chiqish lozim, shunda zarur hollarda uni qayta sozlash mumkin bo'ladi. CRMPni amalga oshirish va boshqarish uchun tayinlangan shaxsga bu dastur muhim afzalliklar taqdim etadi.

Keling, 7.2-jadvalda ushbu afzalliklarni an'anaviy xavfsizlik rahbari (CISO yoki xavfsizlik xizmati menejeri) va CRMP doirasida ishlaydigan rahbarning vazifalarini taqqoslash va solishtirish orqali ko'rib chiqaylik.

7.2-jadval

Kibertahdidlarni boshqarish va maxsus amaliyotlar

	CRMP	Maxsus xavfsizlik amaliyotlari
Xavfsizlik bo'limi va korxona o'rtasida qanday bog'liqlik bor?	Xavfsizlik bo'limi korxonaning tahdidga moyilligi va chidamliligiga yo'naltirilgan CRMP asosida ishlaydi.	Korxona ishtiroki asosan tahdid va zaifliklarga taktik javob berish bilan cheklanadi.
Byudjet va boshqa resursga oid qarorlar qanday qabul qilinadi?	Xavfsizlikka kiritilgan sarmoyalar korxona tomonidan belgilangan tahdid darajasiga muvofiq ravishda optimallashtirilib boriladi.	Korxona va xavfsizlik bo'limi o'rtasida aloqa yo'qligi tufayli xavfsizlikka kiritiladigan sarmoya noaniq.
Qarorlarni kim va qanday qabul qilindi?	Tahdidga oid ma'lumotlar korxona qarorlarini qabul qilish jarayoniga singdiriladi, bunda CISO yoki boshqa xavfsizlik bo'yicha rahbar korxonani strategik tahdidga oid qarorlar orqali boshqaradi.	Tahdidlarni boshqarish bo'yicha qarorlar asosan taktik xususiyatga ega bo'lib, xavfsizlik tashkilotiga yuklanadi va ko'pincha korxonaning tegishli talablariga rioya qilmasdan, tahdidlar va zaifliklarga asoslanadi.

Tahdidlar eskalatsiyasi qanday ishlaydi?	Tahdidlar eskalatsiyasi jarayoni korxona tomonidan tasdiqlangan tahdidlar matritsasiga asoslanib, ma'lumotning boshqaruvning tegishli darajalariga o'z vaqtida yetkazilishini ta'minlaydi. "Tahdid" tushunchasi "insidentlarga chora ko'rish" tushunchasidan kengroq ma'no kasb etadi.	Tahdidlar eskalatsiyasi odatda biror insident tufayli yuzaga keladi va bu insident jarayoniga asoslangan javob choralarini ishga tushiradi, lekin tahdidning o'ziga emas. Tahdidlarning o'zi eskalatsiyani avtomatik tarzda yuzaga keltirmaydi.
CISONing vazifasi va uning ta'siri nima-dan iborat?	CISONing vazifasi faqatgina tahdidga oid qarorlarni qabul qilish emas, balki ularni boshqarish ham bo'lgani uchun, ish xavfsizligi yanada barqaror bo'ladi.	CISO mustaqil qabul qilingan tahdidga oid qarorlari tufayli yuzaga kelgan har qanday salbiy natijalar uchun javobgar bo'lishi mumkin, bu esa ish joyini yo'qotishga olib kelishi mumkin.
Xavfsizlik bo'limining korxona barqarorligiga ta'siri qanday?	Korxona CISO yoki boshqa xavfsizlik yetakchisining strategik rahbarligi ostida barqaror ishlaydi.	Korxona barqarorligi tahdidlarni sifatli boshqarish funksiyasi sifatida emas, balki halokatli hodisalardan qayta tiklanish obyekti orqali ko'rib chiqiladi.

Bu jarayon davomida, xavfsizlik xizmati, ushbu kitobda belgilab berilgan asosiy vazifalarni bajarishi kerak, ya'ni tahdid bo'yicha mas'ul shaxslar va boshqa manfaatdor tomonlarni ma'lumot, tajriba va texnologiyalar bilan ta'minlashi lozim, bu ularga belgilangan va tasdiqlangan kibertahdidga oid qaror qabul qilish jarayonini boshqarishda yordam beradi. Bu xavfsizlik tashkiloti va boshqa manfaatdor tomonlardan ushbu jarayondagi o'z vazifalarini aniq tushunishlarini va ayniqsa, kibertahdidlarni boshqarishning doimiy o'zgarib turuvchi mohiyatini anglab yetishlarini talab qiladi. Kibertahdidlar vaqt o'tishi bilan o'zgaradi, bu tahdidlarni boshqarish va kamaytirish uchun zarur bo'lgan texnologiyalar, vositalar va jarayonlar ham o'zgaradi, lekin xavfsizlik xizmatining yordamchi sifatidagi vazifasi hech qachon o'zgarmaydi. Xavfsizlik xizmati korxonaga uzoq muddatli foyda keltirish va yangi imkoniyatlarni o'zlashtirishga yordam berishda muhim hamkor bo'lib qoladi.

Yakuniy xulosa

CRMPni amalga oshirish oson ish emas. Vazifaning murakkabligi va korxona tahdid muhitidagi doimiy o'zgarishlar uzluksiz amalga oshirish jarayonini, muntazam kuzatuv va takomillashtirishni talab qiladi. Dasturni amalga oshirishga mas'ul shaxslar buni bir sayohat deb tasavvur qilishlari kerak, bu sayohat dastlabki asosiy qadamlardan boshlanib, ularga tayanib rivojlanadi, uning yo'nalishi va manzili vaqt o'tishi bilan muqarrar ravishda o'zgarib boradi. Dasturni amalga oshirishga mas'ul shaxslar bu jarayon keng doiradagi manfaatdor tomonlarning

doimiy hamkorligi va hamjihatligini ham talab qilishini anglashlari lozim. Xavfsizlik tashkiloti dasturni loyihalash va amalga oshirish uchun zarur bo'lgan ma'lumotlarni taqdim etadi, biroq haqiqiy qarorlar aktivlar va tahdid bo'yicha mas'ul shaxslar, boshqaruv organlari, auditorlik tashkiloti, yuqori lavozimli rahbarlar, korxona mansabdor shaxslari va direktorlar kengashi tomonidan qabul qilinadi. Natijada, korxona tez o'zgaruvchan tahdidlarni bartaraf etish va o'z faoliyatini samarali davom ettirish uchun ancha yaxshi mavqega ega bo'ladi.

Tez o'zgaruvchan muhitda korxonaning tegishli operatsion barqarorligiga erishishiga ko'maklashish uchun ta'minot zanjiri, jismoniy xavfsizlik va biznes uzluksizligi kabi boshqa operatsion xavf-xatar funksiyalari bilan hamkorlik qilish tobora muhim ahamiyat kasb etmoqda, bu esa keyingi bobning asosiy mavzusidir.

VIII BOB. AMALIY XAVF-XATAR VA BARQARORLIKKA NISBATAN QO'LLANILADIGAN CRMP

Ushbu kitobda korxonalarning tahdid muhitini tubdan qayta shakllantiruvchi ijtimoiy, siyosiy, iqtisodiy, madaniy va albatta texnologik o'zgarishlar ta'kidlab o'tildi. Agar korxonalar vujudga keladigan tahdidlarni rasmiy, dasturiy tarzda boshqara olmasa, ular duch keladigan jiddiy zarar va halokatli oqibatlariga misollar keltirildi. Shuningdek, tahdidlarni samarali boshqarish, ayniqsa kibertahdidlarni boshqarishning ko'plab usullari korxonalarga yangi va o'ta o'zgaruvchan muhitda omon qolish va rivojlanishga yordam berishi, tahdid va foydani muvozanatlash orqali yaxshiroq qarorlar qabul qilish mumkinligi batafsil bayon etildi.

Ushbu bobda CRMPning operatsion barqarorlikni ta'minlashdagi muhim ahamiyati va bu dasturning boshqa funksiyalar bilan uyg'unlashib, operatsion barqarorlikni ta'minlashda yanada keng qamrovli chora-tadbirlarga e'tibor qaratishi batafsil bayon etiladi. Kibertahdidlarni boshqarish, boshqa har qanday operatsion tahdidlarni boshqarish funksiyasi singari, yagona pirovard maqsadga ega: tahdid va foydani muvozanatlashtiruvchi operatsion barqarorlikka erishish.

Kibertahdidlar shubhasiz muhim, biroq ular korxonalar hisobga olishi lozim bo'lgan tahdid muhitining yagona jihati emas. Korxonalarning yuqori darajadagi qaror qabul qiluvchi shaxslari shunchaki zararli dasturlar, shaxsiy ma'lumotlarni o'g'irlash va ma'lumotlarning buzilishi haqida o'ylamaydilar. Ular ancha kengroq savollarga javob izlayaptilar. Asosiy muhim savol: "Biz doimo o'zgarib turadigan tahdid muhitiga qanchalik chidamli va moslashuvchanmiz?"

Korxonaning qaror qabul qiluvchi shaxslari bu savolni ta'minot zanjiri xavfi, uchinchi tomon xavfi, firibgarlikni boshqarish, biznes uzluksizligi, inqirozdan keyin qayta tiklanish va AT xavfi kabi savollarga ham javob izlashmoqda. Asosiy muammo shundaki, ularning barchasi bir xil natijaga intilsa-da, biroq o'z harakatlari tarqoq tarzda yondashmoqdalar. Bunday yondashuv avval ish bergan bo'lsa ham, endi hech qanday natijaga olib kelmaydi. Oxirgi voqealar shuni ko'rsatadiki, barcha funksiyalar bir-biri bilan uzviy bog'liq bo'lib, ularning barchasining vazifasi operatsion barqarorlikni ta'minlashdir.

O'tgan bir necha yil ichida biz nimalarni boshdan kechirganimiz va undan olgan saboqlarimiz haqida mulohaza yuritsak, hayratga tushamiz. Butun dunyo bo'ylab tarqalgan pandemiya o'zi bilan birga ta'minot zanjirida jiddiy muammolarni, ishlab chiqarishdagi tanqisliklarni va ish modellarida tub o'zgarishlarni olib keldi.

Yevropadagi urush energiya narxlarining beqarorligiga va oziq-ovqat narxlarining inflyatsiyasiga sabab bo'ldi. Dunyo bo'ylab rivojlanayotgan siyosiy tar-

tibzizliklar bilan bir qatorda, global iqlim o'zgarishi bilan bog'liq tabiiy ofatlar va kuchli ob-havo hodisalari ham sodir bo'ldi. Tabiiyki, kiberhujumlarning tezligi va jiddiyligi sezilarli darajada oshgani ham e'tibordan chetda qolmadi. Bularning barchasi ulkan ijtimoiy, iqtisodiy va siyosiy voqealar edi, korxona rahbarlari ularning barchasiga hamda ular bilan bog'liq tahdidlarni bir vaqtning o'zida hal qilishi kerak edi. Ba'zi korxonalar boshqalarga qaraganda ancha muvaffaqiyatli bo'ldi va ko'p hollarda ularning muvaffaqiyatining kaliti – bu barcha turdagi tahdidlarni boshqarish hamda bu tahdidlarning operatsion barqarorlikka ta'sirini yaxlit va keng qamrovli yondashuv orqali amalga oshirishdan iborat edi.

Yuqori darajadagi qaror qabul qiluvchilar operatsion barqarorlik masalalarini butun korxona miqyosida ko'rib chiqishlari zarur. Albatta, tafsilotlar muhim, biroq rahbar operatsion tahdidni yuqori bosqichlarga yetkazganda va kelajakda bu tahdidni boshqarish bo'yicha tegishli rejalarni ma'lum qilganda, rahbarlar ongidagi hal qiluvchi omil – bu korxonaning ular uchun maqbul bo'lgan barqarorlik darajasini aniqlashdir. Buni aniqlanish alohida-alohida emas, balki butun korxona miqyosida amalga oshiriladi. Raqamlashtirish va u bilan bog'liq o'zaro aloqadorlik – operatsion tahdidlarni boshqarish uchun mas'ul bo'lgan bo'linmalardan o'z sa'y-harakatlarini muvofiqlashtirishni talab etadi.

Bunda umumiy asoslar va muvofiqlashtirilgan hisobot amaliyoti orqali tahdidlarni boshqarishni muvofiqlashtirish nazarda tutilyapti. Bu ustuvor yo'nalishlarni muvofiqlashtirib, tabiiy ravishda hamkorlik qiladigan muvofiqlashtirilgan boshqaruvni anglatadi. Buning uchun bir xil tahdid matritsalarini, hisobot berish muddatlari va ketma-ketligi asosida ishlaydigan tahdid haqida ma'lumotga asoslangan tizimlar talab etiladi. Shuningdek, bu barcha tahdidlar bir xil emasligini hisobga olgan holda tahdid omillarini baholashni ham talab qiladi. Bu funksional bo'linmalarni faol boshqariladigan, tahdidlarni baholashga asoslangan va puxta o'ylangan strategiyalarni talab qiladi. Shuningdek, keng qamrovli rasmiy eskalatsiya va ma'lumotlarni oshkor etish jarayoni ham talab etiladi. Bularning barchasi ushbu kitobda bayon etilgan CRMPning asoslaridir. Operatsion tahdidlarni boshqarish funksiyalarining har biri o'z doirasini tashkil etuvchi aynan shu asosiy tahdid elementlariga asoslanib ishlashi kerak. To'g'ri yondashuv orqali, ushbu tahdid ekotizimlari muvofiqlashtirilib, yagona operatsion tahdid ekotizimi sifatida faoliyat yuritishi mumkin va lozim.

Tahdidlarni tizimli ravishda boshqarish va tahdidlar to'g'risida oson va tushunarli tilda ma'lumot berish, muvofiqlashtirilgan va bir xil tuzilmaga asoslangan yondashuv "Biz chidamlimizmi?" degan asosiy savolga aniqroq javobni taklif qiladi. Bu hisobot tayyorlayotgan tashkilot tomonidan taqdim etiladigan batafsil ma'lumotlarning jiddiyligini hech qanday tarzda kamaytirmaydi. Aslida, u tashkilotning maqsadlariga erishayotganini va yetuk rahbarlikni namoyish etayotganini ko'rsatadi, tashkilotning va uning vazifasining jiddiyligini ta'kidlaydi va tushuntiradi.

Operatsion barqarorlik haqida faqatgina yuqori lavozimdagi rahbarlar va boshqa yuqori darajadagi korxona qaror qabul qiluvchilari savollar berayotgani yo'q, butun dunyo bo'ylab nazorat organlari ham tahdidlarni boshqarishni operatsion barqarorlik nuqtayi nazaridan va operatsion tahdid funksiyalarini muvofiqlashtirish orqali ko'rib chiqa boshlashdi. Ular tobora ko'proq e'tiborni ilg'or amaliyotlarga, standartlarga, barqarorlik o'lchovlariga va belgilangan me'yoriy qoidalarga qaratmoqdalar. Buning asosiy sababi shundaki, ular haqiqiy muammo hodisalarning o'zida emasligini tushunib yetishgan. Masala shundaki, hodisa sabablaridan qat'i nazar, shu hodisaning barcha oqibatlarini bartaraf etish uchun korxona yetarlicha barqarormi? Ular o'z talablarini belgilab, tashkilotlarni shu nuqtayi nazardan baholashni boshlashdi. Maslahat va tekshiruvlar tahdidlarni boshqarishning dasturiy amaliyotiga qaratilgan.

Bu keng qamrovli qarash himoyaning ilg'or usullaridan muhim funksiyalarni aniqlash va boshqarish qobiliyatiga qarab o'zgaradi, shu orqali mazkur korxona uchun mos keladigan operatsion barqarorlikni ta'minlaydi. Angliya banki va Bank nazorati bo'yicha Bazel qo'mitasi (BSBS¹³⁵) kabi nufuzli tashkilotlar tomonidan tobora keng qo'llanilayotgan asosiy tushuncha – bu "og'ir, ammo ehtimolga yaqin ssenariy"dir.

Kiberxavfsizlik funksiyalari korxonaning boshqa barcha xavfsizlik funksiyalari bilan muvofiqlashtirilishi kerak. Aslida, agar boshqa vazifalar operatsion barqarorlikka qaratilgan bo'lmasa, kiberxavfsizlik ushbu hamkorlik sa'y-harakatlarda yetakchilik rolni o'z zimmasiga olishi lozim. Buning asosiy sababi, kibertahdid hozirgi kunda ko'pchilik korxonalar duch kelayotgan eng jiddiy tahdiddir. Boshqa tahdid funksiyalarining barchasi ham bunday turdagi muvofiqlashtirish uchun zarur bo'lgan yetuklik darajasiga erishmagan bo'lishi mumkin va bu normal holat. Yetuk operatsion barqarorlik dasturini bir zumda yaratib bo'lmaydi va ko'p hollarda bu uzoq vaqtni talab etadi. Ammo tahdidlarni boshqarishga butun korxonada miqyosidagi operatsion barqarorlik nuqtayi nazaridan yondashish va tizimli dastur tamoyillarini kibertahdidni boshqarish jarayonida qo'llash zarur yetuklik darajasiga erishishni ta'minlaydi.

Operatsion barqarorlik tasnifi

Operatsion barqarorlik – bu korxonaning har qanday turdagi nosozliklar va noaniqliklarning oldini olish, ularga bardosh berish va moslashish qobiliyati bo'lib, u korxona tomonidan tasdiqlangan muayyan daraja va aniqlikda amalga oshiriladi va bajariladi.

¹³⁵ BCBS (Basel Committee on Banking Supervision) – Bank nazorati bo'yicha Bazel qo'mitasi.

Operatsion barqarorlikni ta'minlash bo'yicha tahdidlarni boshqarish amaliyotlari ushbu turli xil elementlarni bir-biriga bog'laydigan birlashtiruvchi bo'g'indir. U turli xil vazifalar va mas'uliyatlarning rasmiy, aniq belgilangan tarzda ishlashini, o'zaro hamkorlik qilishini ta'minlaydi, shu bilan birga nafaqat kibertahdidlar, balki barcha turdagi tahdidlarni bartaraf etishga qaratilgan.

Korxonaning operatsion barqarorlik bilan bog'liq va uning o'sishiga yordam beradigan vazifalari

Xavfsizlik bo'yicha mutaxassislar va boshqa tahdid bo'yicha manfaatdor tomonlarning ko'plab vazifalari operatsion barqarorlikka xos bo'lmasa-da, ularning operatsion barqarorlikni ta'minlashdagi roli juda muhim. Ularning har biri mohiyatan shunchaki taktik vazifa emas, balki strategik tahdidlarni boshqarish amaliyotidir. Keling, ular nimadan iborat ekanligini va kibertahdidlarni boshqarish, ayniqsa operatsion barqarorlik bilan qanday bog'liqligini aniqlashtirish uchun ularning ba'zilarini yaqindan ko'rib chiqamiz:

AT xavflarini boshqarish

AT xavflarini boshqarish korxonaning AT aktivlaridan foydalanish, ularga egalik qilish, ulardan foydalanish va ularni joriy etish bilan bog'liq bo'lgan xavflarni aniqlash va kamaytirish jarayonini o'z ichiga oladi. Ushbu funktsiya operatsion barqarorlik uchun juda muhim bo'lib, ko'pincha kibertahdidlarni boshqarish bilan chambarchas bog'liq.

Jismoniy xavfsizlik

Jismoniy xavfsizlik xodimlar, apparat ta'minoti, dasturiy ta'minot, tarmoqlar va ma'lumotlarni korxonaga jiddiy zarar yetkazishi yoki yo'qotish keltirishi mumkin bo'lgan jismoniy hodisalardan himoya qilishga qaratilgan. Ushbu vazifa operatsion barqarorlik uchun muhimdir, chunki u kiber va operatsion jarayonlarni ta'minlaydigan jismoniy aktivlarning uzluksizligini ta'minlaydi, shuningdek raqamli aktivlarga noqonuniy kirishning oldini olib, kibertahdidni boshqarishga yordam beradi.

Firibgarlikni boshqarish / yo'qotishlarning oldini olish

Bu kiberfiribgarlik bilan birga, har qanday firibgarlikning oldini olish va unga qarshi kurashish, shuningdek resurslar, ma'lumotlar yoki mablag'lar yo'qolishini bartaraf etishga qaratilgan choralarni o'z ichiga oladi. Uning operatsion barqarorlikka qo'shgan hissasi tashkilot aktivlarini himoya qilishda namoyon bo'ladi. Kibertahdidni boshqarish nuqtayi nazaridan esa, u raqamli makondagi firibgarlik harakatlarining oldini olish, ularni aniqlash hamda ularga munosib javob berishni o'z ichiga oladi.

Ta'minot zanjiri/uchinchi tomon

Ushbu funksiya tashkilotning ta'minot zanjiri va uchinchi tomon ta'minotchilari bilan bog'liq bo'lgan tahdidlarni boshqarish bilan bog'liq. U operatsion barqarorlikni ta'minlashning ajralmas qismidir, chunki u tashqi tomonlar tomonidan taqdim etiladigan mahsulotlar, xizmatlar yoki ma'lumotlarning uzluksizligi va yaxlitligini ta'minlaydi. Shuningdek, kibertahdid nuqtayi nazaridan, bu funksiya yana ushbu tashqi subyektlar bilan bog'liq kibertahdidlarni boshqarishni ham o'z ichiga oladi.

Biznesning uzluksizligini boshqarish

Bu halokatli voqealardan keyin muhim biznes operatsiyalari va funksiyalarini tiklash uchun amaliy logistika rejasini yaratish va tasdiqlashni o'z ichiga olgan faol rejalashtirish jarayonidir. U tashkilotning katta inqiroz yoki tabiiy ofat paytida ham asosiy funksiyalarni bajarishda davom etishini ta'minlaydi hamda operatsion barqarorlikni sezilarli darajada oshiradi. Kibertahdidlarni boshqarish nuqtayi nazaridan, u muhim kibermuhit sharoitida ham raqamli operatsiyalarning uzluksizligini ta'minlaydi

Favqulodda vaziyatlardan keyin tiklanish

Favqulodda vaziyatlardan keyin tiklanish – bu korxonaning AT tizimlari (infratuzilma va ilovalar) hamda ma'lumotlarini favqulodda vaziyatdan so'ng normal faoliyatni davom ettirishi mumkin bo'lgan holatga qaytarish jarayonidir. Bu har qanday buzg'unchi hodisa (masalan, kiberhujum, ma'lumotlar buzilishi yoki tabiiy ofat) bo'lishi mumkin.

Inqirozlarni boshqarish

Bu korxonaga yoki uning manfaatdor tomonlariga zarar yetkazishi mumkin bo'lgan halokatli va kutilmagan hodisalarni boshqarish jarayonini o'z ichiga oladi. U operatsion barqarorlikni saqlashda muhim rol o'ynaydi, bu inqirozga muvofiq javob berishni ta'minlaydi, shu bilan zararni cheklaydi va tiklanish vaqtini qisqartiradi. Shuningdek, u ma'lumotlar sizib chiqishi va keng ko'lamlı kiberhujumlar kabi kiberinqirozlar paytida kibertahdidlarni boshqarish bilan ham chambarchas bog'liq.

Agar siz oldingi boblarda aytib o'tilgan inqirozlarga nazar tashlasangiz, operatsion tahdid funksiyalarining tayyorgarlik va javob berish choralarida o'zaro bog'liqligini ko'rishingiz mumkin. Bundan tashqari, agar har bir guruh rahbarlar va boshqa manfaatdor tomonlarning ofislariga borib, o'zlarining harakatlari haqida alohida-alohida ma'lumot berishsa, operatsion barqarorlikning haqiqiy ko'rinishini yaxlit holda tasavvur qilish mushkul bo'ladi.

Kibertahdidlarni boshqarish va operatsion barqarorlik

Nima uchun ushbu kitobda operatsion barqarorlik masalasiga bunchalik chuqur e'tibor qaratilayapti? Keling, buning asosiy sabablarini ko'rib chiqaylik:

- Kiberxavfsizlik va operatsion barqarorlik o'zaro bog'liq. Ma'lumotlarning sizib chiqishi yoki tovlamachi dastur (ransomware) hujumlari kabi kibertahdidlar korxona faoliyatiga jiddiy ta'sir ko'rsatishi mumkin. Yuzaga kelayotgan kibertahdidlar va umumiy kibermuhitdagi o'zgarishlar sharoitida kibertahdid operatsion barqarorlikni saqlab qolishga hissasini qo'shadi, shu nuqtayi nazaridan u yaxlit tarzda ko'rib chiqilishi zarur.

- Ushbu kitobda muhokama qilingan barcha sabablarga ko'ra, raqamlashtirish har bir korxonaning barcha biznes funksiyalarida yuqori tezlikda kuchaytirilgan kibertahdidlarni keltirishda davom etadi va bu xavflar tobora ortib boradi.

- Nazoratchilar kuzatib bormoqda. Butun dunyo bo'ylab tartibga soluvchi organlar operatsion barqarorlikka asosiy e'tiborni berib, korxonalardan kibertahdid va xatarlarga qarshi tayyorgarlikni rivojlantirish va namoyish etishni talab qiladigan ko'rsatmalarni belgilamoqda.

- Kibertahdidlar tobora murakkablashib, takomillashib hamda xavfliroq bo'lib bormoqda. Raqamli tahdidlar va zaifliklar, masalan, tovlamachi dastur hujumlari va ma'lumotlar buzilishlari ommaviy axborot vositalarining e'tiborini jalb qiladi va bu biznesga sezilarli ta'sir ko'rsatishi mumkin. Kibertahdidlar an'anaviy "xavfsizlik" masalalaridan ancha keng qamrovlidir. Faqatgina kiberfunksiyaga ta'sir qiladigan va boshqa operatsion sohalarga keng ta'sir ko'rsatmaydigan sof kiberhodosalar juda kam uchraydi.

- Kibertahdidni boshqarish korxonaning biznes qiymatini ta'minlashda muhim ahamiyatga ega. Keng ko'lamli operatsion va tahdidga chidamlilikni namoyish eta oladigan korxonalar mijozlar, sheriklar va manfaatdor tomonlarning ishonchini qozonish ehtimoli yuqoriroq bo'lib, bu, o'z navbatida, ularning brend obro'si va raqobatdagi ustunligini oshiradi.

Zararli dasturiy ta'minot hujumi sababli Maersk kompaniyasining butun dunyo bo'ylab tizimlari ishdan chiqdi

Korxona miqyosida keng qamrovli operatsion barqarorlikka erishishni kechiktirib bo'lmaydi, bunga eng yaxshi misol 2017-yilning iyun oyida sodir bo'lgan NotPetya nomli halokatli kiberhujumdur. Ayniqsa, bu hujumning Kopengagenda joylashgan ko'p millatli Maersk-Moller kompaniyasiga (asosan Maersk nomi bilan tanilgan) ko'rsatgan ta'siri operatsion barqarorlikka bo'lgan zaruratni yaqqol namoyon etadi. Bu Ukrainadagi tizimlarni ishdan chiqarishga mo'ljallangan Rossiyaning davlat homiyligidagi hujum bo'lib, hujum Maersk kompaniyasiga yoki boshqa biror yagona korxonaga qaratilmagan edi, lekin u hayratlanarli tezlikda tarqalib, butun dunyo bo'ylab xususiy va davlat sektori subyektlarini ishdan chiqardi.

Maersk kompaniyasida tizimda uzilishlar sodir bo'lib, nosozliklar yuzaga keldi, bu esa kompaniya aloqada bo'lgan yuzlab, hatto minglab boshqa korxonalariga ham salbiy ta'sir ko'rsatdi.

Maersk kompaniyasi bilan sodir bo'lgan bu voqea kompaniyaning barcha xavfsizlik va tahdidlarni boshqarish bo'limlari o'rtasidagi muloqot va hamkorlik orqali operatsion barqarorlikni ta'minlashning qanchalik muhimligini ko'rsatuv-

chi ibratli misol bo'lib xizmat qiladi. NotPetya dastlab kiberhujum sifatida boshlangan, biroq u tez orada ancha keng tarqalgan va yanada xavfliroq hodisaga aylandi. Shubhasiz, Maersk kompaniyasi bunday vaziyatga mutlaqo tayyor emas edi.

NotPetya butun dunyo bo'ylab tartibsizlikni keltirib chiqarmoqda

NotPetya hujumi, uni yaratgan shaxslar tasavvur qilganidan ham ancha muvaffaqiyatli va vayronkor bo'ldi. Ehtimol, xakerlar faqatgina Ukraina AT infratuzilmasiga zarar yetkazishni niyat qilishgan, ammo ular yaratgan zararli dastur shunchalik hayratlanarli tezlikda tarqalib ketdiki, u boshqa tizimlarni ham ishdan chiqarib yubordi. NotPetya korxona hisoblash tizimlarini butunlay ishdan chiqarishga mo'ljallangan bo'lib, Windows operatsion tizimidagi allaqachon aniqlangan zaiflikdan foydalanishiga qaramay, g'oyat samarali bo'ldi. Bu hujum juda keng tarqaldi. Quyidagi ro'yxatda hujum natijasida faoliyati to'xtab qolgan ayrim tashkilotlar ko'rsatilgan, bu hujumning g'ayritabiiy keng qamrovini tasvirlaydi:

- Ukrainadagi Chernobil atom elektr stansiyasi
- Germaniya pochta xizmati
- AQSHning dori-darmon mahsulotlarini ishlab chiqaruvchi yirik kompaniyasi
- Avstraliyadagi shokolad ishlab chiqarish korxonasi
- Fransiyaning qurilish materiallari yetkazib beruvchi kompaniyasi
- Dunyodagi eng yirik reklama agentligi

NotPetyaning moliyaviy oqibatlarini hisoblash deyarli imkonsiz bo'lib, hujumning ko'plab ta'sirlari hali ham sezilmoqda. (Hali hal qilinmagan muhim muammolardan biri kibersug'urta bo'lib, kamida bitta yirik sug'urta kompaniyasi NotPetya da'vosini to'lashdan bosh tortdi, chunki u hujumni "urush harakati" deb hisoblaydi.) Biroq, ba'zi kiberxavfsizlik mutaxassislari 2017-yildagi hujumlarning umumiy qiymati 10 milliard dollardan oshganini taxmin qilishdi.

Nima uchun Maersk kompaniyasi bu qadar kuchli zarar ko'rdi? Buning asosiy sabablaridan biri, kompaniyaning hajm jihatdan kattaligi va murakkab tuzilishga ega ekanligidir. Maersk hajmi bo'yicha dunyodagi ikkinchi yirik yuk tashish kompaniyasi bo'lib, u 700 dan ortiq tijorat kemasini boshqaradi va o'n millionlab tonna yuk tashiydi, bu dunyodagi barcha yuk tashish quvvatining deyarli beshdan bir qismini tashkil etadi. Bu shunchaki kemasozlik kompaniyasi emas. Shuningdek, u logistika, neft qazish, port operatsiyalari va ta'minot zanjiri bo'yicha xizmat ko'rsatish kabi sohalarda ham yetakchi o'rinni egallaydi. NotPetya hujumi kompaniyaning AT operatsiyalarini to'xtatib, uning barcha operatsiya ma'lumotlariga kirishini to'sib qo'yanida, Maersk dengizdagi yuzlab kemalarini boshqara olmay qoldi, port inshootlari esa konteynerlarni yuklash va tushirish uchun mo'ljallangan yuqori darajada avtomatlashtirilgan tizimlarni nazorat qila olmadi. Maersk kompaniyasining global qamrovi, uni biznes sheriklari, mijozlar va xaridorlar, texnologik va operatsion mahsulot hamda xizmatlar ta'minotchilari, davlat idoralari va boshqa uchinchi tomonlarning ulkan va murakkab o'zaro bog'liq ekotizimining markaziga joylashtiradi. (Maersk kompaniyasining boshqa korxonalar bilan keng raqamli aloqalari sababli, NotPetya hujumining kompa-

niya AT tizimlaridan tashqari boshqa tizimlarga ham ta'sir etishiga olib keldi.) Bu shuni anglatadiki, NotPetya hujumi Maersk kompaniyasi faoliyatini to'xtatib qo'yganida, bu shuningdek, global iqtisodiyotning katta qismini ham to'xtatib qo'ydi. Butun dunyo bo'ylab ishlab chiqaruvchi kompaniyalar deyarli darhol asosiy komponentlar tanqisligini boshdan kechirishdi. Avvalroq ta'kidlanganidek, bu bugungi kundagi raqamlashtirilgan iqtisodiyotning asosiy muammosi bo'lib, chakana sotuvchilarning mahsulot zaxiralari deyarli shu tezlikda bo'shab qoldi. NotPetya hujumining Maersk kompaniyasiga ta'siri batafsil o'rganishga loyiqdir, chunki u butun korxona miqyosidagi operatsion barqarorlik dasturining naqadar keng qamrovli va dolzarb ekanligini aniq ko'rsatib beradi. Ma'lum bo'lishicha, bu hujum Maerskning deyarli barcha faoliyat yo'nalishlarini bir haftaga yaqin vaqt davomida ishdan chiqargan. Zarar esa faqat yuk tashish va logistika bilan bog'liq aniq muammolar bilan cheklanib qolmadi. Kompaniyaning AT tizimi ishlamagan kunlari, Maersk o'zining 100,000 dan ortiq xodimlariga maosh to'lash kabi asosiy funksiyalarni bajara olmas edi. Ishga qabul qilish va xodimlar bilan ishlash bo'limining boshqa funksiyalari to'xtatib qo'yilgan bo'lar edi. Shuningdek, kompaniya moliyaviy bozorlarga yoki tartibga soluvchi organlarga aniq va dolzarb ma'lumotlarni taqdim eta olmas edi. Maersk hodisasi operatsion barqarorlikning naqadar muhimligini va bu borada kibertahdidlarni boshqarishning hal qiluvchi ahamiyatga ega ekanligini ko'rsatadi. Operatsion barqarorlik alohida CRMP yoki shunchaki biznes uzluksizligi haqidagi tushuncha emas.

Butun faoliyatning uzluksizligini ta'kidlaydigan kengroq tushunchani qabul qilish zarur. Bu tushuncha korxonalarning turli xil hodisalarga, shu jumladan, kiberhujumlarga moslashish va ulardan keyin tiklanish qobiliyatiga ega bo'lish zarurligini ta'kidlaydi. Bu zarurat korxonaning o'zi bilan cheklanib qolmaydi. NotPetya hujumiga haqiqatan ham samarali javob berish uchun Maerskning operatsion tahdidlarni boshqarish bo'limlari va u bilan hamkorlik qiladigan ko'plab uchinchi tomon korxonalari o'rtasida keng qamrovli aloqa va hamkorlik zarur edi. Xavfsizlik va operatsion tahdidlarni boshqarish bo'limlari bilan muloqot qiluvchi va hamkorlik qiladigan hamda butun korxona miqyosidagi sa'y-harakatlarni boshqaradigan CRMP, Maersk kompaniyasiga NotPetya kabi tahdidlarni aniqlashga, ularga qarshi himoya choralarini ishlab chiqishga va boshqa operatsion tahdidlarni boshqarish bo'limlari bilan hamkorlikda javob choralarga tayyorgarlik ko'rishda yanada muvofiqlashtirilgan imkoniyatlarni yaratishga yordam bergan bo'lardi.

NotPetya kabi kiberhujumlar hozirgi kunda asosiy e'tiborni tortsa-da, kiberxavfsizlik sohasi doirasidan tashqarida fikr yuritish nihoyatda muhimdir. Kiberxavfsizlik – tashkilotning barcha turdagi uzilishlarga bardosh berishi va ulardan keyin o'zini tiklash qobiliyatini ta'minlash uchun zarur bo'lgan umumiy maqsadning muhim tarkibiy qismidir. Kiberxavfsizlik operatsion barqaror-

likni ta'minlovchi asosiy vosita sifatida, kibertahdidlarga qarshi muhim biznes funksiyalarining uzluksizligini ta'minlaydi. Amaliy xavf-xatar va barqarorlikni boshqarishning funksional dasturini ishlab chiqish, har bir amaliy tahdid funksiyasi tahdidlarni boshqarishning asosiy komponentlari atrofida birlashishni talab etadi. CRMPning to'rt tarkibiy qismlari, ya'ni *moslashuvchan boshqaruv*, *tahdidlar haqidagi ma'lumotlarga asoslangan tizim*, *tahdidlarni baholashga asoslangan strategiya* va *uning ijrosi*, *tahdidlar eskalatsiyasi* va *ma'lumotlarning oshkor etilishi*, boshqa barcha operatsion tahdid funksiyalariga tatbiq etilishi hamda ular birgalikda operatsion tahdid funksiyalarini muvofiqlashtirishda, tahdidlarni bartaraf etishda va keng qamrovli barqarorlik holatini ta'minlashda samarali ishlashi mumkin.

CRMPning to'rt asosiy komponenti yordamida operatsion barqarorlikni ta'minlash bo'yicha ko'rsatma

Ushbu kitobda muhokama qilingan to'rtta tarkibiy qismni har xil biznes operatsiyalariga, shu jumladan, ta'minot zanjiri, AT xavflari, firibgarlikni boshqarish, jismoniy xavfsizlik, biznesning uzluksizligi, favqulodda vaziyatlardan keyin tiklanish va inqirozlarni boshqarish uchun universal ravishda qo'llash mumkin, bularning barchasi operatsion barqarorlikka erishish uchun juda muhimdir. Keling, ularning har birini ko'rib chiqaylik.

Moslashuvchan boshqaruv

Moslashuvchan boshqaruv CRMPning asosi bo'lib, u zarur nazoratni ta'minlab, muhim qarorlarni qabul qilishga yo'l ko'rsatadi. U, shuningdek, operatsion barqarorlikka erishish sa'y-harakatlarining asosini tashkil etadi. 3-bobda batafsil bayon etilganidek, moslashuvchan boshqaruv turli tahdid operatsiyalarini umumiy tamoyillar va nazorat ostida birlashtiradi, ammo o'z yondashuvini har bir tarkibiy guruhning o'ziga xos ehtiyojlariga moslashtirib boradi. Korxona tahdidlarini boshqarish qo'mitasi, operatsion barqarorlikni rivojlantirish qo'mitasi yoki integratsiyalashgan tahdid qo'mitasi kabi muvofiqlashtirilgan boshqaruv qo'mitasi turli operatsion tahdid funksiyalarini muvofiqlashtirish jarayonida muhim ahamiyat kasb etadi. Qo'mita asosiy manfaatdor tomonlarni birlashtiradi, ularni operatsion tahdid va barqarorlik (shu jumladan, tahdidga moyillik va chidamlilik) bo'yicha umumiy umidlar va maqsadlar atrofida muvofiqlashtiradi. Tahdidlar haqidagi ma'lumotlarga asoslangan tizimdan muntazam ravishda olingan hisobotlar orqali ushbu manfaatdor tomonlar korxonaning tahdid muhiti haqida xabardor bo'lib boradilar. Bu ularga xavf-xatarlarni oldindan bartaraf etish va keng qamrovli barqarorlik holatini oshirish imkonini beradi.

Tahdidlarni boshqarish bo'yicha turli funksiyalar muvofiqligini ta'minlash

Tashkilot ichidagi tahdidlarni boshqarish bo'yicha turli funksiyalarini muvofiqlashtirish oson ish emas. Bu tashkilot faoliyati haqida keng ko'lamli tasavvurga ega bo'lgan, shuningdek, turli manbalardan olingan ma'lumotlarni amaliy g'oyalarga umumlashtirish qobiliyatiga ega bo'lgan subyektni talab qiladi. Xo'sh, bunday guruhni tashkil etishda kim yetakchilik qiladi? U qanday tashkil etilishi va qanday nomlanishi kerak?

Bir nechta nomzodlar mavjud. Operatsion tahdidlar biznes strategiyasi nuqtayi nazaridan ba'zi korxonalarda jiddiy tashvish uyg'otadi, bu korxonalarda operatsion tahdidlar qo'mitasi yoki integratsiyalashgan qo'mita samarali bo'lishi mumkin. ERM qo'mitasi keng qamrovli yondashuvni qo'llab, nafaqat operatsion tahdidlarni, balki tashkilot duch keladigan barcha turdagi tahdidlarni, jumladan strategik, moliyaviy va obro'ga oid tahdidlarni ham o'z ichiga oladi. ERM qo'mitalari ko'pincha operatsion vazifalarni bajarmasa-da, ularga odatda tahdidlarni boshqarish tizimini yaratish va korxonaning tahdidga moyillik chegaralarini belgilash mas'uliyati yuklanadi. Bu chegara keyinchalik turli operatsion tahdidlarni boshqarish bo'limlariga tatbiq etiladi.

Qaysi model tanlanishidan qat'i nazar, qo'mitaning qaror qabul qilish vakolatiga ega bo'lishi va korxona rahbariyati tomonidan eng yuqori darajada qo'llab-quvvatlanishi muhimdir. Bundan tashqari, qo'mita o'z qarorlarini yo'naltirish uchun o'z vaqtida va tegishli ma'lumotlarni taqdim etadigan ishonchli va keng qamrovli tahdidlar haqidagi ma'lumotlarga asoslangan tizimga tayinishi kerak. Pirovardida, har qanday bu kabi qo'mitaning maqsadi tashkilotni yanada kuchli operatsion barqarorlikka va tahdidlarni samarali boshqarishga yo'naltirish bo'lishi kerak. Bu tashkiliy tuzilmani o'zgartirishni emas, balki tashkiliy hamkorlikni talab qiladi va aynan shu uning asosiy e'tibor markazida bo'lishi lozim.

Tahdid haqidagi ma'lumotlarga asoslangan tizim

Operatsion tahdidlar bilan bog'liq boshqa funksiyalarni muvofiqlashtiradigan tahdidlar haqidagi ma'lumotlarga asoslangan tizim barqarorlik haqidagi ma'lumotlarning asosiy manbasi bo'lib xizmat qiladi. Bu tizim operatsion tahdid haqidagi ma'lumotlarni o'z vaqtida, aniq, keng qamrovli va muvofiqlashtirilgan holda yetkazib berishi hamda rahbarlarning korxonaning umumiy operatsion tahdid profilini tushunishga va ularni boshqarishga yordam berishi, pirovardida esa operatsion barqarorlikni oshirishga xizmat qilishi kerak.

Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning asosiy maqsadi rahbarlarning asosiy muammosini, ya'ni korxona barqarorligining darajasini hal qilishdir. Rahbarlar yig'ilishlarda tahdidga oid muayyan savollar berishsa-da, ularning operatsion nuqtayi nazardan asosiy tashvishlari – bu korxonaning uzilishlarga qanchalik yaxshi bardosh bera olishi va moslasha olishini tushunishdir. Operatsion tahdidlar haqidagi ma'lumotlarga asoslangan tizim bu savolga tashkilotning barcha operatsion funksiyalaridan olingan ma'lumotlarni jamlash va taqdim etish orqali javob beradi.

Ushbu turdagi operatsion tahdid amaliyotining asosiy harakatlantiruvchi omillaridan biri – bu tahdidlar haqidagi ma'lumotlarga asoslangan tizim doirasi-dagi ma'lumotlarning muvofiqligidir. Tahdidlarni boshqarish funksiyalari bo'yi-

cha rahbarlarga nomuvofiq yoki noto'g'ri ma'lumotlarni taqdim etish hozirgi kunda ko'pgina korxonalarda keng tarqalgan muammodir, bu esa chalkashliklarni keltirib chiqarishi va tizimning samaradorligiga putur yetkazishi mumkin. Bunda izchillik va muvofiqlikni saqlash juda muhim hisoblanadi, chunki u barcha manfaatdor tomonlarga taqdim etilgan tahdid haqidagi ma'lumotlarini osonlik bilan tushunish va undan foydalanish imkoniyatini beradi. Shuningdek, bu korxonaning operatsion barqarorlikka oid asosli qarorlar qabul qilishiga yordam beradi. Shubhasiz, barcha xavf-xatarlar bir xil emas. Masalan, moliyaviy xizmatlarda kiber-tahdid ta'minot zanjiri tahdidiga nisbatan ancha yuqori ustuvorlikka ega bo'lishi, ishlab chiqarish sohasida esa buning aksi bo'lishi mumkin. Tahdidlarni tegishli tarzda ustuvorlash muhim hisoblanadi, ammo bu har doim operatsion tahdidga mos kelishiga e'tibor qaratgan holda amalga oshirilishi kerak.

Tahdidga asoslangan strategiya va uning ijrosi

Tahdidlarga asoslangan strategiya va uning ijrosi modelini amaliy tahdid funksiyalari bilan muvofiqlashtirish yagona asos yaratishda xizmat qiladi. Boshqaruv organi faoliyatini ta'minlaydigan tahdid haqida ma'lumotlarga asoslanuvchi tizim bilan birgalikda, strategik model korxonaning tahdidga moyilligi va bardoshlilikini belgilaydi, shuningdek operatsion tahdidni boshqarish bo'yicha chora-tadbirlarning ustuvorligini, amalga oshirilishini va bajarilishini belgilab beradi. Ushbu modelning tahdidga oid operatsiyalarning turli jihatlariga: AT va ta'minot zanjiri bilan bog'liq tahdidlar, firibgarlikni nazorat qilish, jismoniy xavfsizlik, biznes uzluksizligi, favqulodda vaziyatlardan tiklanish va inqirozlarni boshqarish kabi sohalarga universal tatbiq etilishi operatsion barqarorlikka erishishda uyg'unlashgan yondashuvni ta'minlaydi. Asosan, bu tashkiliy va tahdid ma'lumotlarini muvofiqlashtirish hamda muvofiqlashtirilgan ijro haqida bo'lib, xavf-xatarlarga ustuvorlik berish va ularni bartaraf etish hamda ularga javob qaytarish bo'yicha aniq, muvofiqlashtirilgan yondashuv orqali amalga oshiriladi. Operatsion tahdidlarni keng miqyosda ko'rib chiqish operatsion tahdidlar uchun mas'ul bo'lgan har bir alohida bo'limga kelajakdagi strategiyalar va byudjetni asoslashga yaxshiroq tayyorgarlik ko'rishga yordam beradi.

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi operatsion barqarorlikka erishishning yakuniy ustunidir. U moslashuvchan boshqaruv, tahdid haqidagi ma'lumotlarga asoslangan tizim, shuningdek, tahdidlarga asoslangan strategiya va uning ijrosi kabi komponentlar bilan bog'liq. Tahdidlar eskalatsiyasi – bu tizimli jarayon bo'lib, u boshqaruv organi tomonidan belgilangan amaliyotga muvofiq tahdidlar to'g'risidagi ma'lumotlarni tezkor ravishda taqdim etadi, shunda tezkor choralar ko'rilishi mumkin. Tahdidlar haqidagi ma'lumotlarni oshkor qilish tahdidga oid ma'lumotlarni ichki va tashqi manfaatdor tomonlarga yetkazishdir.

Ichki tomondan, tahdidga oid ma'lumotlarni samarali oshkor qilish operatsion tahdidlarni boshqarish bo'linmalari orasida shaffoflikni ta'minlaydi, bu esa tahdidni jamoaviy tushunish va uni boshqarishga hissa qo'shadi. Tashqi tomondan, u tartibga soluvchi organlar, aksiyadorlar va jamoatchilik oldida hisobdorlikni namoyish etib, korxona obro'si va ishonchini oshiradi. Bu funksiyaning muhimligini ko'rsatuvchi misollardan biri shundaki, bugungi kunda tahdidning butun korxonaga bo'lgan potensial ta'siri haqida ma'lumot bermasdan turib, tahdidni baholash va u haqida xabar berishning ilojisi yo'q. Operatsion tahdidlarga javobgar har bir bo'linma ushbu fikrlarni hisobga olishi lozim. Agar shunday qilinmasa, bo'shliqlar paydo bo'ladi, bu esa korxona va uning yuqori lavozimli qaror qabul qiluvchilarini tartibga solish, fuqarolik va hatto jinoiy javobgarlikka tortishi mumkin.

Yakuniy xulosa

Ushbu bobning oldingi bo'limlarida keng qamrovli CRMP uchun poydevor yaratildi. To'rt asosiy tarkibiy qism va bu qismlar mustahkam va chidamli strategiyani shakllantirishi uchun o'zaro bog'lanishi kerakligi ta'kidlab o'tildi. Ammo kibertahdidlarni boshqarish alohida vazifa emas. U keng qamrovli tuzilmaning bir qismi bo'lib, operatsion tahdidlar bilan bog'liq boshqa vazifalar bilan chambarchas bog'liq. To'rt komponentning har biri faqatgina kibertahdidlarni boshqarish bilan chegaralanib qolmaydi. Ular tahdid operatsiyalarining turli jihatlarini qamrab oluvchi keng qamrovli operatsion barqarorlik strategiyasini muvofiqlashtirish uchun mustahkam poydevor vazifasini o'taydi.

Oldinga qadam tashlar ekanmiz, operatsion barqarorlik – bu manzil emas, balki davomiy sayohat ekanligini yodda tutish muhim. Bu jarayon uzluksiz kuza-tishni, baholash va takomillashtirishni talab qiladi. Ushbu to'rtta asosiy tarkibiy qismni tushunish va ularni tashkilot amaliyotiga tatbiq etish orqali, kiberxavfsizlik va tahdidlarni boshqarish bo'yicha mutaxassislar barqarorlikka erishish uchun zarur bo'lgan muvofiqlashtirish yoki yaxlit yondashuvga samarali rahbarlik qilishga tayyor bo'ladilar.

Oxirgi bobda kelajak haqida so'z yuritiladi. Bunda asosiy e'tibor AI¹³⁶ bilan bog'liq tahdidlarni boshqarish va oldimizda turgan noma'lum tahdidlarni tahlil qilishga qaratiladi hamda CRMPning korxona yondashuvlari uchun poydevor bo'lib xizmat qilishi muhokama qilinadi.

¹³⁶ AI (Artificial intelligence) – sun'iy intellekt, bu tezkor hisoblash muhitida algoritmlar yaratish va qo'llash orqali insonning aql-idrok jarayonlariga taqlid qilishga asoslanadi.

IX BOB.

AI VA BOSHQALAR: RAQAMLASHTIRILGAN DUNYODA TAHDIDLARNI BOSHQARISHNING KELAJAGI

Ushbu kitobda allaqachon mavjud hamda yangi paydo bo'layotgan raqamli texnologiyalar tufayli yuzaga kelayotgan ijobiy va salbiy ta'sirlar batafsil bayon etildi. Har kuni raqamli texnologiyalar sohasida bizning kundalik hayotimizni, ish muhitimizni va hatto butun sanoatni to'liq qayta shakllantiradigan ajoyib yutuqlar haqida xabarlar eshitamiz. Bu rivojlanishlar yangi "raqamli chegarani" yaratmoqda, buning shunchalik tez harakatlanishi sababli, ba'zan oldinda bizni qanday tahdidlar kutayotganligini bilish qiyin bo'ladi. Ko'p hollarda, ushbu ilg'or texnologiyalarning real hayotdagi haqiqiy qiymati isbotlanmagan bo'lsa-da, shubha yo'qki, raqamli transformatsiyaning hozirgi to'liqini innovatsiyalar, samaradorlik va o'zaro bog'liqlikni takomillashtirish uchun misli ko'rilmagan imkoniyatlarni olib kelmoqda. Lekin shu bilan birga, ular murakkab, o'zaro bog'langan va oldindan aytib bo'lmaydigan yangi tahdidlarni olib kelmoqda, bu esa keng qamrovli, yetuk CRMPni joriy etishni talab qiladi.

Avvalgi bobdagi operatsion barqarorlik mavzusida muhokama qilinganidek, CRMPning tarkibiy qismlari va belgilangan tamoyillar tashkilotga yangi texnologiyalar bilan muvofiqlashtirishga yordam berishi va biznesni faollashtirish uchun tahdid haqidagi ma'lumotlarni yetkazib berishi mumkin. Bu kabi tahdidlarni boshqarish dasturi yangi texnologiyalarga yondashishda izchillik va ishonchni ta'minlaydi, xuddi operatsion barqarorlikka o'xshash tarzda ko'plab vazifalar bo'ylab rasmiy, muvofiqlashtirilgan harakatlarni amalga oshirish imkonini beradi.

Avvallari faqatgina yuqori malakali texnologlarga tanish bo'lgan atamalar – blokcheyn, kriptovalyuta, IoT, kvant hisoblash va boshqa ko'plab tushunchalar – hozirda biznes dunyosida ham, shaxsiy hayotda ham har kuni muhokama qilinadi. 2022-yil oxirida generativ AI ilovasi bo'lgan ChatGPTning jamoatchilikka taqdim etilishi dunyoni o'zgartiruvchi muhim voqea bo'ldi, bu hodisani internet paydo bo'lganidan buyon eng ahamiyatli hodisa deb baholash mumkin. ChatGPTning ahamiyati nihoyatda katta bo'lsa ham, undan so'ng darhol yangi AI ilovalari, loyihalari paydo bo'ldi. AI shu qadar tez rivojlanmoqdaki, bugungi eng umidbaxsh va istiqbolli tizimlar hamda ilovalarning ba'zilar ertaga osongina eskirishi mumkin.

Aldagi barcha o'zgarishlar yoki hatto eng muhim rivojlanishlar haqida to'liq, eng so'nggi ma'lumotlarga ega bo'lish imkonsiz. Shuni tan olish kerakki, bu kitob nashr etilganda, AI haqidagi ba'zi muhokamalar bugungi holatimizdan ancha oldinga siljigan bo'ladi. Sun'iy intellektning juda ko'p jihatlari mavjud, ular bir-biri

bilan va korxona faoliyatining deyarli barcha jihatlari bilan murakkab va o'zaro bog'langan. AI bilan bog'liq tahdidlarni boshqarish rasmiy va amaliy yondashuvni talab qiladi, ushbu bobda ayrim amaliyotlar muhokama qilinadi. Operatsion barqarorlikda bo'lgani kabi, AI bilan bog'liq tahdidlarni boshqarishda tashkilotning tahdidlarni boshqarish dasturi va yondashuvi ko'plab manfaatdor tomonlarning ishtirokini ta'minlab, sa'y-harakatlarni bog'lab turadi.

AI ta'rifi

Bugungi kunda Alga juda katta e'tibor qaratilmoqda, ayniqsa, AI ilovalari ni sotishga intilayotgan texnologiya ta'minotchilari tomonidan shunchalik ko'p shov-shuv ko'tarilmoqdaki, Alning mohiyatini va uning imkoniyatlarini, ayniqsa u keltirib chiqaradigan xavf-xatarlarni tushunish qiyin bo'lib qolmoqda. Avvalambor, AI va u bilan bog'liq boshqa atamalarni ta'riflashdan boshlasak, shuningdek, bugungi kunda AI va uning tarkibiy qismlaridan qanday foydalanilayotgani va kelajakda qanday ishlatilishi mumkinligini batafsil ko'rib chiqsak:

- NIST Alni quyidagicha ta'riflaydi: “(1) Kompyuter fanining bir sohasi bo'lib, u odatda inson intellekti bilan bog'liq bo'lgan mantiqiy fikrlash, o'rganish va o'z-o'zini takomillashtirish kabi funksiyalarni bajaradigan ma'lumotlarni qayta ishlash tizimlarini ishlab chiqishga bag'ishlangan; va (2) Qurilmaning mantiqiy fikrlash, o'rganish va o'z-o'zini takomillashtirish kabi inson intellekti bilan bog'liq funksiyalarni bajarish qobiliyati”¹³⁷. Ushbu “asosiy” AI ta'rifi ko'p yillar davomida keng qo'llanilib kelinmoqda.

- Generativ AI, masalan, ChatGPT, Googlening Bard va LaMDA kabi AIlari bugungi kunda shov-shuvlarga sabab bo'lmoqda. Bu “standart” Alning kichik bir qismi bo'lib, o'rgatilgan ma'lumotlarga asoslanib, yangi kontent yaratishga qodir modellar va algoritmlarni yaratish orqali o'z imkoniyatlarini kengaytiradi.

- Sun'iy umumiy intellekt (AGI¹³⁸) sun'iy intellektning faraziy shakli bo'lib, butun dunyo bo'ylab uni haqiqatga aylantirish uchun ilmiy-tadqiqot loyihalari olib borilmoqda. AGI (ba'zan “kuchli AI” deb ataladi) nazariy jihatdan insonlar bajara oladigan har qanday intellektual vazifani va undan ortig'ini bajarishi mumkin. Ba'zi kuzatuvchilar AGI noodatiy tahdidlarni keltirib chiqarishi mumkin deb hisoblaydilar (masalan, AGI ilovasi o'z yaratuvchilarining yoki hatto butun insoniyatning manfaatlariga zid bo'lgan harakatlarni mustaqil ravishda amalga oshirishi mumkin). AGI qachon paydo bo'lishi aniq emas, lekin uning salohiyati jiddiy qabul qilinishi kerak. Bugun bu shunchaki ilmiy fantastika bo'lib ko'rinishi mumkin, lekin shuni yodda tutish kerakki, ko'p jihatdan kechagi ilmiy fantastika ertangi kunning haqiqatiga aylanishi mumkin.

¹³⁷ “Sun'iy intellekt”, NIST, Iyul, 20, 2023, <https://oreil.ly/81irC>.

¹³⁸ AGI (Artificial general intelligence) – sun'iy umumiy intellekt.

Alni to'liq tushunish va uning imkoniyatlari hamda u keltirib chiqaradigan tahdidlarini aniq baholash uchun uning asosidagi texnologiyalar va komponentlarini tushunib olish zarur. Quyida eng muhimlarini ko'rib chiqamiz:

Mashinali o'qitish (ML)¹³⁹

ML atamasi AI bilan bog'liq boshqa atamalarga nisbatan ko'proq chalkashlikni keltirib chiqaradi. Aslida, bu ikki atama ko'pincha bir-birining o'rni ishlatiladi, bu esa xato hisoblanadi. ML – AIning asosiy va muhim tarkibiy qismi bo'lib, bu algoritmlar va statistik modellarni ishlab chiqarishga yo'naltirilgan. Ushbu modellar yordamida kompyuterlar ma'lumotlardan aniq dasturlanishsiz o'rganish imkoniyatiga ega bo'ladi. Masalan, Netflix o'z obunachilarining ko'rish odatlari va didiga qarab filmlar va TV ko'rsatuvlarini tavsiya qilishda MLdan foydalanadi.

Chuqur o'qitish¹⁴⁰

Bu MLning bir qismi bo'lib, ma'lumotlardan o'rganish uchun sun'iy neyron tarmoqlardan foydalanadi. Neyron tarmoqlar katta ma'lumotlar to'plamlarida o'rgatiladi va ular rasmini tasniflash, tillarni tarjima qilish va eng muhimi, bashorat qilish va qarorlar qabul qilish uchun ishlatilishi mumkin. Chuqur o'qitishga misol sifatida ReCAPTCHA ni keltirish mumkin; bu ko'plab veb-saytlar foydalanuvchining inson ekanligini aniqlash uchun yo'llar, binolar yoki boshqa landshaft elementlarini aniqlashni so'raydi. Deyarli har bir internet foydalanuvchisi ReCAPTCHA bilan to'qnash kelgan, ammo ko'pchilik ularning onlayn xaritalash xizmatlari va boshqa ma'lumotlar bazalarini yaxshilash uchun ishlatilishini bilmaydi.

Katta til modellari (LLMs)¹⁴¹

LLMs ham ChatGPT va Bard kabi generativ AI ilovalarining asosini tashkil etadi. LLMs matn, rasm va kodlarni o'z ichiga olgan ulkan ma'lumotlar bazasida o'qitilgan AI turi bo'lib, u ma'lumotlarning ma'nosini tushunish imkoniyatini beradi. Bu ulkan ma'lumotlar manbasi va LLMsning ularni tahlil qilish qobiliyati generativ AIga savollarga javob berish, mavzularni xulosalash va tillarni tarjima qilish imkonini beradi.

Takroriy neyron tarmoqlari (RNNs)¹⁴²

RNN – sun'iy neyron tarmog'ining bir turi bo'lib, u inson miyasining ishlash usuliga taqlid qiluvchi kompyuter dasturlashning bir usulidir. U ketma-ket ma'lumotlarni qayta ishlash uchun mo'ljallangan. Oddiy qilib aytganda, u qabul qilingan ma'lumotlardan o'rganishi va ulardan kelajakdagi kiritilishi mumkin bo'lgan ma'lumotlar haqida bashorat qilish uchun foydalanishi mumkin. RNNlar

¹³⁹ ML (machine learning) – mashinali o'qitish.

¹⁴⁰ Deep Learning – chuqur o'qitish.

¹⁴¹ LLMs (Large language models) – katta til modellari.

¹⁴² RNNs (Recurrent neural networks) – takroriy neyron tarmoqlari.

eng ilg'or rivojlanayotgan AI foydalanish holatlarining ba'zilarida markaziy rol o'ynaydi. Muhim misollardan biri: ular tabiiy tilni qayta ishlash (NLP¹⁴³) uchun qo'llanilishi mumkin, shunda kompyuter dasturi nafaqat shaxsning nutqini tanib, uni aniqlay oladi, ba'zi hollarda hatto uning hissiy holatini aniqlab, unga javob berishi mumkin.

Hatto AI mutaxassislari ham bu sohadagi yangiliklarning tuganmas oqimiga hamohang bo'lishga qiynalmoqdalar. Lekin, korxonaning tahdidlarni boshqarish dasturi AI va u taqdim etadigan imkoniyatlar hamda muammolari haqida keng qamrovli va doimiy ravishda yangilanib turadigan tushunchaga ega bo'lishi muhimdir. 2-bobda muhokama qilinganidek, ayniqsa kibertahdidlarni boshqarishda qonun chiqaruvchilar va nazorat organlari korxonalardan (xususan, yangi SEC qoidalari bo'yicha jamoat kompaniyalardan) kiberxavfsizlik bo'yicha hujjatlashtirilgan ekspertizani mavjud bo'lishini talab qilmoqda. Yaqin kelajakda kiberxavfsizlik bo'yicha mutaxassislardan hech bo'lmaganda Alni ma'lum darajada tushunish va ular bilan bog'liq tahdidlarni anglash talab qiladi. Bu korxonalar, tahdidlarni boshqarish bo'linmalari, boshqaruv organlari va tahdidlar ta'siriga uchragan manfaatdor tomonlarga tahdidlarni boshqarishning eng asosiy vazifasini, ya'ni Alning tahdidlarini uning foydalari bilan muvozanatlash bajara olishga imkon beradi.

AI: Butunlay yangi, xavfli dunyo

Hech kim Alning barcha xavflarini, ularning ma'lum bir korxona yoki sanoatga qanday ta'sir ko'rsatishini bilmasa-da, ayrim xavflar allaqachon aniq bo'lmog'da. Tahdidlarni boshqarish dasturlari, yaqin kelajakda e'tibor qaratishi lozim bo'lgan eng muhim tahdidlarning ayrimlarini ko'rib chiqaylik:

Ma'lumotlar va algoritmlarning xatoliklari

AI ilovalarning sifati faqat ularni shakllantiruvchi ma'lumotlar va ushbu ma'lumotlarni talqin qiladigan va qo'llaydigan algoritmlar darajasida bo'ladi, bu ikkala omil ham xatoliklarga moyil. AI tizimlarida qayta-qayta yosh, irq, jins va ijtimoiy kelib chiqish kabi omillar asosida xatoliklar mavjudligi aniqlangan. Masalan, 2015-yilda o'tkazilgan tadqiqot shuni ko'rsatadiki, Googlening yuzni aniqlash dasturi oq tanli odamlarga qaraganda qora tanli odamlarni noto'g'ri aniqlashga moyil ekanligi ko'rsatilgan. Bunga sabab, ehtimol, ushbu tizim asosan oq tanli odamlarning ma'lumotlar to'plamida o'qitilgani bo'lishi mumkin.

Xavfsizlik va maxfiylik muammolari

AI tizimlari, har qanday texnologiya kabi xakerlik hujumlariga uchrashi mumkin va ulkan ma'lumotlar bazasi yomon niyatli shaxslarga juda jozibador

¹⁴³ NLP (natural language processing) – tabiiy tilni qayta ishlash – bu Alning kichik to'plami bo'lib, u kompyuterlar va mashinalarga inson tilini tushunish, izohlash, manipulyatsiya qilish va muloqot qilish imkonini beradi.

maqsadni taqdim etadi. Bundan tashqari, AIning o'zi ham xavfsizlik hujumlarida ishlatilishi mumkin, masalan, ChatGPT kabi generativ AI dasturlari murakkab va maqsadli zararli dasturlarni yozishga qodir. (Bu tahdid haqida ushbu bobda batafsil muhokama qilinadi.) Bu kibertahdidlarni sezilarli darajada oshiradi, chunki xakerlar hujumlarni amalga oshirish uchun ko'p texnik ko'nikmalarga ega bo'lishlari shart bo'lmaydi. Ovozli yordamchilar kabi sun'iy intellekt tizimlari ham juda katta hajmdagi ma'lumotlarni to'playdi va ular maxfiy axborotni himoya qilish uchun zarur tuzilmalarga ega bo'lmasligi mumkin.

Intellektual mulk va boshqa maxfiy ma'lumotlarning yo'qolishi

Bu xavfsizlik va maxfiylik bilan chambarchas bog'liq muammodir. Katta ma'lumotlar to'plamlaridan foydalanish va ma'lumotlarning qanday darajadagi himoya talab qilishini aniqlashdagi qiyinchilik, maxfiy ma'lumotlarning yo'qolishi xavfini sezilarli darajada oshiradi. Bu intellektual mulk, ya'ni patentlar va boshqa tijorat sirlaridan tortib, sotuv raqamlari, bozor rejalari, mijozlar va xodimlar haqidagi shaxsiy ma'lumotlarga bo'lgan barcha narsalarni anglatishi mumkin.

Firibgarlik

Jinoyatchilar har doim yangi texnologiyalarning imkoniyatlarini birinchilardan bo'lib anglab yetadilar, AI ham bundan mustasno emas. Masalan, AIning ovozni aniqlas qobiliyati shunchalik kuchliki, ma'lum shaxslarning ovozlari benuqson taqlid qilinib, foydalanuvchilarni korxona tizimlariga kirishga ruxsat berishga ishontirish uchun "maqsadli fishing" (spear phishing) hujumlarida ishlatilmoqda. Bu masala atrofida shunchalik ko'p tashvish borki, ko'plab banklar va boshqa moliyaviy muassasalar ovozni tanib olishdan autentifikatsiya shakli sifatida foydalanishni to'xtatishdi.

Shaffoflikning yetishmasligi

Alda shaffoflikning yo'qligi qaror qabul qilish jarayonlarini noaniq qilib qo'yadi, bu esa javobgarlikdan xoli bo'lgan natijalarga va texnologiyaga bo'lgan ishonchning pasayishiga olib kelishi mumkin.

Korxona ustidan nazoratning yo'qolishi

Tadqiqotchilar va soha kuzatuvchilari AI tizimlari shunchalik murakkab, kuchli va mustaqil bo'lishi mumkinligidan jiddiy xavotirda, chunki AI hech qanday inson aralashuviziz va ehtimol hatto ularning bilimidan foydalanmasdan, ruxsatsiz qarorlar qabul qilishi va ularni amalga oshirishni boshlashi mumkin.

Ishchi kuchining o'zgarishi

2022-yil oxirida ChatGPTning joriy etilishi natijasida millionlab, hatto yuz millionlab ish o'rinlari yo'qolishi, AI keng ko'lamlı funksiyalarni amalga oshirishi bashorat qilindi. 2030-yilgacha AQSH iqtisodiyotida hozirgi kunda bajarilayotgan

ish soatlarining 30 foizigacha bo'lgan qismini tashkil etuvchi faoliyatlar avtomatlashtirilishi mumkin – bu tendensiya generativ sun'iy intellekt tufayli yanada tezlashmoqda. Bu tashvishlarning ba'zilari shubhasiz, asosli: AI bilan ishlaydigan virtual yordamchilar va chatbotlar allaqachon ishonch markazlari xodimlari vazifalarini o'z zimmlariga oldilar va katta miqdordagi onlayn kontentlardan matn va rasmlar hozirda avtomatik tarzda yaratilmoqda. Boshqa soha kuzatuvchilari esa, AI yangi millionlab ish o'rinlarini yaratishini bashorat qilmoqda. Kimning fikri to'g'ri bo'lishidan qat'i nazar, AI davrida mehnat bozorida g'oyat noaniqlik davri bo'lishi aniq. Korxonalar juda murakkab qarorlarni qabul qilishlari kerak bo'ladi. Ular o'z xodimlarini sinovdan o'tmagan texnologiya bilan almashtirishadimi, malakali xodimlar hamon tanqis bo'lgan mehnat bozorida o'zlarining qimmatli mutaxassislarini yo'qotishga tayyormi? Yoki ular AI ni qabul qilishdan bosh tortib, faolroq raqobatchilarga imkoniyatlarni berib qo'yish xavfini oladimi?

Bu va boshqa ko'plab o'ziga xos tahdidlar yuqori darajadagi korxona tahdidlariga olib keladi va ularga ta'sir ko'rsatadi. Aldan noto'g'ri foydalanish huquqi va tartibga solish bo'yicha javobgarlikka; obro' yo'qotilishiga, mijozlar, xodimlar va biznes hamkorlarning ishonchini yo'qotishga va boshqa ko'plab jiddiy, hattoki mavjudlikka xavf soladigan muammolarga sabab bo'lishi mumkin. Ammo shuni tan olish muhimki, AI bilan bog'liq tahdidlar faqatgina uni noto'g'ri qo'llash yoki mas'uliyatsizlik bilan joriy etish va nazorat qilishdan kelib chiqmaydi. AI butun dunyo ishlash uslubidagi tub o'zgarishlarni anglatadi, bu esa tahdidlarni boshqarish jarayonini yanada murakkablashtiradi.

Korxonalar Aldan foydalansalar ham, foydalanmasalar ham jiddiy xavflarga duch kelishadi.

AI hodisasini e'tiborsiz qoldirib bo'lmaydi. Korxonalar Aldan foydalansa ham, ulardan foydalanmasa ham jiddiy tahdidlarga duch kelishi mumkin. Bu esa har qachongidan ko'ra keng qamrovli va mustahkam CRMP yaratish zaruratini tug'diradi.

AI bilan bog'liq tahdidlarni samarali boshqarish, xuddi operatsion barqarorlikka erishish kabi, bir nechta biznes funksiyalari va amaliy tahdid funksiyalari o'rtasida muvofiqlashtirish va hamkorlikni talab qiladi. Keyingi bo'limda, AI bilan bog'liq tahdidlarni boshqarish tushunchalari, ular bilan bog'liq tamoyillar va amaliyotlar muhokama qilinadi. Bu tushunchalar tahdidlarni boshqarish harakatlari bog'liq bo'lib, dasturda bir-biriga uzviy bog'langan bo'lishi kerak. Ammo avval, kiberxavfsizlik va tahdidlarni boshqarish mutaxassislari bilishi kerak bo'lgan Alga oid atamalar va ular hal qilishi kerak bo'lgan eng muhim tahdidlarga nazar solamiz:

Tortishuvli mashinali o'qitish (AML¹⁴⁴):

NISTning taksonomiyasi va terminologiyasi

2023-yil mart oyida NIST o'zining AML uchun tuzilgan taksonomiya va terminologiyani yaratishga qaratilgan dastlabki jamoat loyihasini e'lon qildi. AML, ko'plab AI ilovalarini potensial tahdidlardan himoya qilish uchun ishlatiladigan ML texnologiyalarini xavfsizlashtirish texnikalarini o'z ichiga oladi. AML AI tizimining barcha tarkibiy qismlarini xavfsizlashtirishni o'z ichiga oladi, jumladan, ML ma'lumotlar, foydalaniladigan ML modellari, ushbu modellarni o'qitish, sinovdan o'tkazish va joriy etish jarayonlari, shuningdek, ulardan foydalanish uchun zarur bo'lgan infratuzilma kiradi. Mazkur hisobot, NISTning AI bilan bog'liq tahdidlarni boshqarish tamoyilidagi tizim xavfsizligi, barqarorlik va mustahkamlik kabi asosiy tushunchalariga bilan mos keladi.

NIST hisobotida alohida tashvish uyg'otadigan uchta turdagi potensial hujumlarga e'tibor qaratilgan. (U dizayndagi kamchiliklar, ma'lumotlar yoki algoritmining xatoliklari kabi tasodifiy omillarni hisobga olmaydi.) Dastlabki ommaviy loyihada tasvirlangan hujumlarning uch turi quyidagilar:

Qochish hujumlari

Qochish hujumlarining maqsadi AMLda qiziqish uyg'otdi, bunda hujumchining maqsadi, ML sinovlarining natijalarini joylashtirish vaqtida o'zgartira oladigan ziddiyatli misollarni yaratishdir. ML modelini aldash mumkin bo'lsa-da, insonlar uni hali ham asl sinfning bir qismi sifatida tan oladi. Mavjud himoyalarni buzadigan kuchliroq g'arazli hujumlar o'rtasida uzluksiz aylanma jarayon davom etmoqda. Bu kabi ziddiyatli misollarni bartaraf etish mushkul vazifa hisoblanadi. Bundan tashqari, kuchsiz raqobatdosh modellar asosida baholangan himoyalarning kuchliroq hujumlarga dosh bera olmasligi ham muntazam ravishda kuzatilmoqda. Bu hujumlarni bartaraf etish jiddiy muammolarni keltirib chiqarmoqda.

Zaharlanish (Poisoning) hujumlari va ularning oldini olish choralari

Zaharli hujumlar, ML algoritmini o'qitish bosqichida amalga oshiriladigan dushman hujumlari bo'lib, ML tizimlariga qarshi yana bir tahdid turidir. Bu hujumlar tizimning mavjudligi yoki yaxlitligini buzishi mumkin, natijada ML modelining barcha namunalardagi ishlashini yomonlashtirishi yoki maqsadli namunalarning kichik to'plamida aniqlanishi qiyin bo'lgan yashirin buzilishlarni keltirib chiqarishi mumkin. Har bir zaharlanish hujumlarining oldini olish usullari mavjud, ammo ularning samaradorligi tajovuzkor shaxsning ssenariylariga qarab farq qiladi.

Maxfiylikka nisbatan hujumlar

Maxfiylik hujumlari, yig'ilgan statistik ma'lumotlardan yoki o'qitish ma'lumotlarini eslab qolish orqali maxfiy ma'lumotlarni qayta tiklashni o'z ichiga oladi

¹⁴⁴ AML (adversarial machine learning) – tortishuvli mashinali o'qitish.

va bu hujum turi tobora keng tarqalmoqda. Maxfiylik hujumlarining ikkita keng tarqalgan turi mavjud: birinchisi, a'zolikni aniqlash hujumlari, bunda tajovuzkor shaxs ma'lum bir yozuv o'quv ma'lumotlar to'plamiga kiritilganligini aniqlashi mumkin, ikkinchisi esa modelni ajratib olish hujumlari, bular ML modeli haqida ma'lumot olishga qaratilgan. Ushbu hujumlarning oldini olish AML tadqiqotchilari va amaliyotchilari uchun katta qiyinchiliklarni tug'diradi.

Tahdidni alohida boshqarishning imkonsizligini esda tutish muhimdir. AI va uning asosidagi texnologiyalarning murakkabligi hamda qaror qabul qilishdagi mustaqilligi, shuningdek, ularga qarshi hujumlarning tobora murakkablashib borayotgani tahdid va zaifliklarni bashorat qilish, aniqlash va yumshatishni har qachongidan ham qiyinlashtirmoqda. Raqamli ekotizimimizning o'zaro chambarchas bog'liqligi shuni anglatadiki, bitta tizimning zaifliklari boshqa ko'plab tizimlarga kutilmagan va keng ko'lamli ta'sir ko'rsatishi mumkin.

AI bilan bog'liq tahdidlar va maxsus kibertahdidlarni boshqarish tashkilot bo'ylab boshqa tahdidlarni boshqarish funksiyalari bilan muvofiqlashtirilishi kerak.

Raqamli tizimlarning o'zaro bog'liqligi shuni anglatadiki, AIning bir sohaga olib kirgan zaifligi butun korxona tarmog'iga yoki undan tashqarisiga ham ta'sir ko'rsatishi mumkin. Turli sohalar mutaxassislarining tajribasini birlashtirgan holda, himoyaga yaxlit yondashuv qo'llash mutlaqo zarur. Shuningdek, zararli hujumlarining tobora murakkablashib borayotgan tabiati, himoyaga ham xuddi shunday murakkab va yaxlit yondashuvni talab qiladi, bu esa turli sohalar mutaxassislarining bilim va tajribalarini uyg'unlashtirish orqali amalga oshiriladi.

Sun'iy intellektidan foydalanish bilan bog'liq tahdidlarni boshqarish tizimlari

Korxonalarga AI bilan bog'liq bo'lgan tahdidlarni bartaraf etishda yordam berish uchun yaratilgan va ishlab chiqilayotgan tahdidlarni boshqarish tizimlari mavjud.

NISTning AI bilan bog'liq bo'lgan tahdidlarni boshqarish asoslari

2023-yil yanvar oyida ommaga taqdim etilgan NISTning AI bilan bog'liq bo'lgan tahdidlarni boshqarish asoslari, ushbu kitob yozilayotgan paytdagi holatga ko'ra, AI ni joriy etish bo'yicha eng zamonaviy va batafsil tahdidga asoslangan yo'riqnomani taqdim etadi. NISTning AI bilan bog'liq bo'lgan tahdidlarni boshqarish asoslari, AI ni joriy etishga oid tahdidga asoslangan qo'llanma bo'lib, korxonalar undan ixtiyoriy ravishda foydalanishlari mumkin. AQSH hukumati ning nazorat organlari, ayniqsa, muhim infratuzilma va ochiq aksiyadorlik jamiyatlariga nisbatan kelajakda mas'uliyatli ijro uchun ushbu prinsipni standart sifatida qo'llaydilar.

NISTning ushbu prinsipi to'rtta asosiy funksiyaga e'tibor qaratadi:

Boshqarish

Boshqaruv funksiyasi AI bilan bog'liq tahdidlarni umumiy boshqarishga qaratilgan bo'lib, 3-bobda CRMP doirasida muhokama qilingan ko'plab tamoyillarga muvofiq korxona miqyosida tahdidlarni boshqarish madaniyatini shakllantirishni nazarda tutadi. Bu hisobdorlik tizimlarini yaratish, AI dan mas'uliyatli foydalanishga intiluvchi ichki tashkilotlarni rivojlantirish hamda AI tizimlari va ulardan foydalanish korxonaning o'rnatilgan qadriyatlariga mos kelishini ta'minlashni o'z ichiga oladi.

Xaritalash

Ushbu kontekstda, xaritalash AI tizimlarini ishlab chiqish, ularni joriy etish va ulardan foydalanish bilan bog'liq xavflarni aniqlash va baholashni anglatadi. U barcha AI bilan bog'liq tizimlarni, ular foydalanadigan ma'lumotlar va algoritmlarni hamda ular ishtirokidagi muvaffaqiyatli hujumning potensial oqibatlarini aniqlashni o'z ichiga oladi.

O'lchash

AI tahdidlarini boshqarish nazoratining samaradorligini o'lchash o'z ichiga tizimning muvofiqligini kuzatish, kirib borish testlarini o'tkazish va hodisalar haqidagi hisobotlarni ko'rib chiqishni oladi.

Boshqarish

Bu funksiya AI bilan bog'liq xavf-xatarlarni boshqarish nazoratining samaradorligini ta'minlaydi va ularning to'g'ri amalga oshirilishini kafolatlaydi. Bu jara-yon AI bilan bog'liq xavf-xatarlarni boshqarish rejasi va siyosatini ko'rib chiqish hamda yangilash, shuningdek, foydalanuvchilarni o'qitish kabi faoliyatlar orqali amalga oshiriladi

Model xavfini boshqarish (MRM¹⁴⁵) va Federal zaxira kengashining ko'rsatmalari

MRM moliyaviy xizmatlarda ko'p qo'llaniladi, bu modellardan foydalanish bilan bog'liq tahdidlarni aniqlash, ularni baholash va kamaytirish jarayoni bo'lib, ayniqsa qaror qabul qilishda noaniq yoki yaxshi ishlab chiqilmagan modellardan foydalanish natijasida yuzaga keladigan tahdidlarni boshqarishga qaratilgan. Moliyaviy xizmatlar sohasi o'z tabiatiga ko'ra, albatta, tahdidlarni boshqarishga juda katta e'tibor qaratadi. Banklar har kuni qarz oluvchilarning to'lovga qobiliyatini baholaydi, sug'urta kompaniyalari shaxslarning umr ko'rish davomiyligini aniqlaydi va treyderlar qimmatli qog'ozlar va tovar bozorlaridagi tendensiyalarni oldindan aytib bera olishi kerak. Bu sohaga tahdidlarni boshqarish bo'yicha boy tajriba, ya'ni modellarni taqdim etadi, bu modellar boshqa sanoat va korxonalar-

¹⁴⁵ MRB (Model risk management) – model xavfini boshqarish, qaror qabul qilish uchun yetarli darajada aniq bo'lmagan modellardan foydalanish natijasida zarar ko'rish xavfini boshqarish.

ga, shuningdek AI olib kirayotgan turli tahdidlarga nisbatan qo'llanilishi mumkin. Keling, mas'uliyatli AI ni joriy etishga yo'naltirilgan eng muhim model xavflarini boshqarish asoslaridan birini ko'rib chiqaylik:

2011-yilda Federal xazina kengashi model xavflarini boshqarish bo'yicha SR 11-7 raqamli nazorat va tartibga solish maktubini chiqardi. Bu moliyaviy muassasalarga model xavfini boshqarishni baholashda yordam berish uchun ishonchli qo'llanma bo'lib xizmat qildi. O'rnatilgan tamoyillar va ko'rsatmalar AI modellari uchun qabul qilinishi mumkin bo'lgan asosni belgilab beradi, bu asosga mustahkam model tanlash, uni ishlab chiqish, amalga oshirish, samarali tasdiqlash, modelni sinash va albatta, siyosat hamda nazoratni o'z ichiga olgan boshqaruv kiradi. Ushbu yo'naltiruvchi tamoyillarini yanada chuqurroq tahlil qilib, ularni AI bilan bog'liq tahdidga qo'llash mumkin:

MRM uchun muvofiq boshqaruv tizimini joriy etish

MRMning samaradorligi uchun kuchli boshqaruv juda muhimdir. Bu siyosat, tartib-qoidalar, resurslarni taqsimlash va hujjatlashtirish jarayonlarini o'z ichiga oladi. MRM uchun mos boshqaruv tizimi tashkil etilishi va korxonadagi boshqa tahdidlarni boshqarish amaliyotlari bilan muvofiqlashtirilishi lozim, jumladan, barcha tegishli manfaatdor tomonlar uchun aniq vazifalar va majburiyatlar belgilanishi kerak. AI bilan bog'liq tahdidlarga kelsak, bu, shubhasiz, AI texnologiyalarida, jumladan generativ AI va ular asosidagi LLM sohasidagi yutuqlarda, shuningdek AI dan foydalanish bilan bog'liq hozirgi va kutilayotgan huquqiy hamda me'yoriy muhitda sezilarli tajribani talab qiladi.

MRMga tahdid haqidagi ma'lumotga asoslangan yondashuvni joriy etish

MRM modeliga xos bo'lgan xavflar aniq baholanishi va ushbu xavflarni kamaytirish uchun tegishli nazorat choralari amalga oshirilishi lozim.

Modellarni ishlab chiqish va moslashtirishda qo'llaniladigan ma'lumotlar ishonchli ekanligiga ishonch hosil qilish

AI boshqa har qanday texnologiyadan ko'ra, o'z natijalarining aniqqligini ta'minlashda kiritilgan ma'lumotlarning sifatiga ko'proq tayanadi. Korxona foydalanilayotgan ma'lumotlarning to'g'riligi va ishonchligini kafolatlash uchun mustahkam ma'lumotlarni boshqarish tizimiga ega bo'lishi lozim. Bu esa, AI olib kelayotgan ko'lam va tezlikda qo'llanilganda nihoyatda murakkab vazifa hisoblanadi.

Modellarni puxta ishlab chiqish va tasdiqlash

Korxona AI tashabbuslari tahdid modellari uchun ishonchli statistik usullarni talab etadi va bu modellar muntazam ravishda sinovdan o'tkazib turilishi lozim bo'ladi.

Modellardan ehtiyotkorlik bilan foydalanish

Bu shuni anglatadiki, tahdid modeli korxonaning belgilangan tahdidga moyillik va chidamlilik darajalariga mos ravishda qo'llanilishi kerak, bu esa AI nuqtayi nazaridan rivojlanishida yaqinda bo'lishi, doimiy va ko'pincha to'satdan o'zgarishi mumkin.

Modellarning ishlashini doimiy ravishda nazorat qilish

Qo'llanilayotgan AI tahdid modellaridagi muammolarni aniqlash va bartaraf etish uchun tegishli jarayonlar mavjud bo'lishi lozim. Bu, ayniqsa AI modellari uchun o'ta muhim masala hisoblanadi, chunki AIning o'zi, uning asosidagi texnologiyalar va ma'lumotlar manbalari uzluksiz ravishda o'zgarib bormoqda.

Model o'zgarishlarini boshqarish uchun mustahkam jarayonlarga ega bo'lish

AIning ishlash va qo'llanilish usullaridagi uzluksiz o'zgarishlar shuni anglatadiki, tegishli tahdid modellariga o'zgartirishlar kiritish zarur bo'ladi. Korxona ushbu o'zgarishlarni boshqarish uchun ishonchli jarayonni o'rnatishi kerak.

Model ishdan chiqqan taqdirda favqulodda vaziyatlar rejalarini ishlab chiqish

Korxonalar o'zlarining tahdid modellarining (har qanday sohada, ayniqsa sun'iy intellekt kabi o'zgaruvchan sohada) yetarli bo'lmasligi yoki butunlay ishlaymay qolishi mumkinligini tan olishlari kerak. Ular model ishdan chiqqan yoki kutilganidek ishlamaydigan holatlar bilan bog'liq bo'lgan keng ko'lamli tahdidlarni bartaraf etish uchun oldindan rejalar tuzib qo'yishlari lozim.

Model xavflari haqida samarali muloqot o'rnatish

Alga oid tahdidga aloqador bo'lgan har bir shaxs, tegishli va muntazam ravishda, korxonaning model xavflari to'g'risida xabardor etilishi lozim.

Model xavfini boshqarish uchun tegishli resurslar va tajribaga ega bo'lish

Bu shuni anglatadiki, Alga oid tahdid modellarini ishlab chiqish va tasdiqlash hamda ulardan samarali foydalanish uchun tegishli resurslar va tajriba (ichki, tashqi yoki ikkalasi ham) mavjud bo'lishi kerak.

MRM tizimini muntazam ravishda ko'rib chiqish

MRM tuzilmalarining samaradorligini ta'minlash uchun ularni muntazam ravishda baholab turish zarur. Sun'iy intellekt va uning xavflari shiddat bilan o'zgarayotgani sababli, bu masala alohida e'tibor talab etadi.

AIni joriy etishning asosiy tushunchalari va asoslari

Hech kim sizdan AI bo'yicha mutaxassis bo'lishingizni kutmayapti, lekin shunday tushunchalar borki, ular ayniqsa AI va AI xavfiga tegishlidir. Ushbu tushunchalarning ko'pchiligi, ushbu kitob davomida muhokama qilingan standartlar va tamoyillar, tartibga soluvchi idoralar va boshqaruv organlari tomonidan belgi-

lanadi. Keling, AI bilan bog'liq eng muhim tushunchalar va ularni o'z ichiga olgan asoslarni ko'rib chiqaylik.

Adolatlilik va noxolislik tahdidi

Biznes sohasida "adolatlilik" atamasining umumqabul qilingan ta'rifi bo'lmasa-da, bu tushunchaning keng tarqalgan talqinlari mavjud va ularning ba'zilari bevosita AIga taalluqlidir. Ta'riflar, odatda, uchta asosiy tamoyillar – tenglik, shaffoflik va javobgarlik tamoyillarining kombinatsiyasiga asoslangan va bu tamoyillar munozara uchun mustahkam boshlang'ich nuqta bo'lib xizmat qiladi. Tenglik, asosan, korxonalar barcha mijozlarga, xodimlarga va boshqa manfaatdor tomonlarga teng munosabatda bo'lishlari kerakligini anglatadi; shaffoflik ular barcha manfaatdor tomonlarga o'z amaliyot va siyosatlarini haqida aniq va to'g'ri ma'lumot taqdim etishlari kerakligini bildiradi; javobgarlik esa korxona keltirib chiqargan har qanday zarar uchun mas'uliyatni zimmasiga olishga tayyorlikni anglatadi.

AIning adolatga qanday ta'sir ko'rsatishini ko'rish oson, shu sababli bir qator tashkilotlar AIga alohida e'tibor qaratgan holda adolat standartlari va tamoyillarini ishlab chiqishga kirishganlar. Quyida eng muhim tashkilotlar va tashabbuslardan bir nechta keltiriladi:

- Amerika AI assotsiatsiyasining algoritmik adolat va javobgarlik bo'yicha ishchi guruhi 2016-yilda tashkil etilgan bo'lib, adolat mavzusida bir qator maqolalar yozgan

- AIga adolatlilik, mas'uliyat va shaffoflikni targ'ib qiluvchi AI bo'yicha hamkorlik tashkiloti

- NIST ishonchli va mas'uliyatli AI uchun resurs markazi tashkil etdi

Ushbu tashkilotlarning AI amaliyotlari haqidagi qarashlari ko'pincha adolatlilikni baholashning ikkita keng tan olingan mezoniga asoslanadi:

Shaxsiy adolat

Bu shunday g'oyaki, AI tizimlari o'xshash shaxslarga bir xil munosabatda bo'lishi kerak va eng muhimi, bu tizimlar asosli axloqiy sabab bo'lmasa irq, jins yoki jinsiy moyillik kabi omillarga asoslanib qaror qabul qilmasligi lozim.

Nomutanosib ta'sir

Ushbu tamoyilga ko'ra, AI tizimi ma'lum bir odamlar guruhiga salbiy ta'sir ko'rsatmasligi kerak.

Shuni yodda tutish lozimki, adolatlilik tamoyillari mustahkamlik, tushuntirishlilik va javobgarlik kabi boshqa omillarni ham hisobga olishi mumkin. Bularning barchasi quyida muhokama qilinadi:

Asoslilik

Asoslilik – bu qaror qabul qilishda puxta o'ylangan, mantiqli va ishonchli bo'lish sifatidir. Bu maqsadga muvofiqlik, hayotiylik, barqarorlik va axloqiy me-

zonlar kabi omillarni hisobga olishni o'z ichiga oladi. AI nuqtayi nazaridan, bu masala ikki muhim jihatni ko'rib chiqishni talab etadi:

Aniqlik (ma'lumotlar yaxlitligi va sifati)

Bu AI modellari o'qitish uchun ishlatiladigan ma'lumotlar sifatiga, ushbu modellarni yaratish uchun tanlangan algoritmlar va usullarga, shuningdek modelni amalga oshirish va undan foydalanish yo'llariga ehtiyotkorlik bilan va doimiy e'tibor berishni talab qiladi.

Izchillik

AI tizimlari bir xil kirish ma'lumotlaridan bir xil natijalarni ishlab chiqarib, izchil natijalarni taqdim etishi kerak.

AI tizimlarining ishonchligini oshirish uchun maxsus texnologiyalar, usullar va jarayonlar mavjud. Ularga ma'lumotlarni tozalash; algoritmik moslamalar va so'nggi qayta ishlash kiradi.

Ishonchlilik

Bu AI modelining kutilmagan yoki qarama-qarshi ma'lumotlar kiritilishiga duch kelganda ham o'z ishlashi va aniqligini saqlab qolish qobiliyatidir. Model keraksiz ma'lumotlarni nazorat qila olishi va uning ishlashiga sezilarli ta'sir ko'rsatmasdan atrof-muhitdagi o'zgarishlarga moslasha olishi kerak.

AI uchun bir qator umumiy chidamlilik tamoyillari ishlab chiqilgan. Bu tamoyillar AI tizimlarining hujumlar va nosozliklarga bardoshli bo'lishini ta'minlash, shuningdek, ular kutilmagan yoki ziddiyatli ma'lumotlarga duch kelganda ham to'g'ri ishlashda davom etishini kafolatlash uchun mo'ljallangan. Quyida eng keng tarqalgan tamoyillardan ba'zilari keltirilgan:

Kiritilgan ma'lumotlarni tekshirish

AI tizimlari barcha kiritilgan ma'lumotlarni ishlatishdan oldin tekshirishi va ularda xatoliklar yoki zararli kontentlar mavjudligini tekshirishi lozim.

Xatoliklarni qayta ishlash

Xatoliklar ehtiyotkorlik bilan bartaraf etilishi lozim. Amalda bu shuni anglatadiki, AI tizimi xatoga duch kelganda ishdan to'xtab qolmasligi yoki undan-da muhimroq, noto'g'ri yoxud butunlay boshqacha natijalar chiqarmasligi kerak.

Xatolar munosib ravishda hal qilinishi kerak. Amaliyotda, bu shuni anglatadiki, sun'iy intellektli tizim xatoga yo'l qo'ysa, ishlamay qolishi yoki, bundan ham muhimi, noto'g'ri yoki shunchaki boshqa natijalarni berishi mumkin emas.

Xatoliklarga chidamlilik

Bu shuni anglatadiki, tizim ma'lumotlar yoki funksionallikni yo'qotmasdan muvaffaqiyatsizlikdan keyin tiklanish qobiliyatiga ega bo'lishi kerak. Bu oddiy tizimdagi nosozlik yoki tizim modelining keng tarqalgan muvaffaqiyatsizligi bo'lishi mumkin (ChatGPT ommaviy ishga tushirilgandan bir necha oy o'tgach, uning natijalarining aniqligi pasayganligi kuzatilgani haqida xabar qilingan).

Xavfsizlik

AI tizimlari hujumlardan himoyalangan bo'lishi shart. Bu shuni anglatadiki, tizim ruxsatsiz kirish, uni o'zgartirish yoki yo'q qilishdan himoyalangan bo'lishi lozimligini anglatadi.

AI tizimlarining ishonchliligini oshirish uchun qo'llanilishi mumkin bo'lgan bir qator texnologiyalar va usullar mavjud, jumladan:

Ma'lumotlarni kengaytirish

O'quv ma'lumotlar to'plamining hajmini sun'iy ravishda, keraksiz va xato ma'lumotlar ataylab qo'shish orqali oshirish mumkin, bu tizimni haqiqiy xatoliklarga chidamli qiladi.

Jamoaviy o'rganish (Ensemble learning)¹⁴⁶

Ushbu usul bir nechta AI tizimlarning bashoratlarini birlashtirish orqali yanada ishonchliroq natija olishni nazarda tutadi, bu esa tizimni har qanday alohida tizimdagi xatolarga nisbatan bardoshliroq qiladi.

Ziddiyatli mashg'ulotlar

Alni ziddiyatli misollar (xatoga yo'l qo'yish uchun o'zgartirilgan kirish ma'lumotlari) asosida o'qitish AI tizimlarini jinoyatchilarning hujumlariga chidamliroq qiladi.

Tushuntirish

Oddiy qilib aytganda, tushuntirish – sun'iy intellekt tizimi nima uchun ma'lum bir qaror qabul qilgani yoki ma'lum bir harakatni amalga oshirganini tushunish qobiliyatidir. Bu muhim tushuncha, chunki tushuntirib berish tizimga ishonchni shakllantiradi, huquqiy va me'yoriy talablarga rioya etishga hissa qo'shadi.

Alni tushuntirishning bir qator asosiy tarkibiy qismlari mavjud:

Maqsad

AI tizimining tushuntirilishi har doim uning ko'zlangan maqsadiga mos kelishi kerak. Masalan, agar AI tizimining maqsadi mijozlarning xatti-harakatlari haqida bashorat qilish bo'lsa, u holda tushuntirishlar ushbu xatti-harakatlarda o'zgarishlarga olib kelishi mumkin bo'lgan eng muhim omillarga qaratilishi lozim.

Aniqlik

Tushuntirishlar AI tizimining ma'lum bir qarorga kelishining haqiqiy sabablarini aniq aks ettirishi kerak. Bu shuni anglatadiki, ular AI tizimi o'rganish va bashorat qilish uchun foydalangan haqiqiy ma'lumotlarga asoslanishi lozim.

¹⁴⁶ Ensemble learning – Jamoaviy o'rganish, bu yaxshiroq bashoratlarni ishlab chiqish uchun ikki yoki undan ortiq modellarni (masalan, regressiya modellari, neyron tarmoqlari) birlashtiradigan mashinaviy o'rganish usuli.

Shaffoflik

Shaffoflik, bu AI tizimi foydalanadigan ma'lumotlar va algoritmlarni ko'rish imkoniyati bo'lib, tushuntirishning mutlaqo muhim tarkibiy qismi hisoblanadi. Bu, ayniqsa, biznes hamkorlar va model ta'minotchilari kabi uchinchi tomonlar jalb qilinganda juda muhimdir.

Aloqadorlik

Tushuntirishlar qaror qabul qilish jarayonida eng muhim bo'lgan omillarga e'tibor qaratishi kerak.

Yetarlilik

Insonlar, AI tizimi nima uchun muayyan qaror qabul qilganini tushunish uchun yetarlicha ma'lumotga ega bo'lishlari kerak.

Muhit

Tushuntirish AI tizimi qaror qabul qilgan aniq vaziyatni hisobga olishi kerak va u tinglovchilarga hamda tushuntirish so'ralishining sabablariga moslashtirilgan bo'lishi lozim.

Audit tekshiruvi uchun shart-sharoitlarning mavjudligi

Muntazam ravishda o'tkaziladigan auditorlik tekshiruvlari, ya'ni algoritmlar va ma'lumotlarni kiritish va chiqarishning tizimli tekshiruvi, AI tizimlariga bo'lgan ishonchning asosini tashkil etadi, axloqiy me'yorlar, qonuniy talablar, tashkiliy siyosat va axloqiy standartlarga rioya etilishini ta'minlaydi.

Aldan tashqari: raqamli texnologiyalar hech qachon rivojlanishdan to'xtamaydi

Hozirgi kunda AIga shunchalik katta e'tibor qaratilmoqdaki, uni xavf-xatarlarni boshqarishda zarur bo'lgan so'nggi texnologik yutuq deb o'ylash oson va jozibali bo'lib qolmoqda. Shubhasiz, u kelgusi yillarda eng dolzarb tahdidlar masalasi bo'lib qoladi. Ammo haqiqat shuki, o'zgarishlar to'xtovsiz davom etmoqda va u hech qachon to'xtamaydi. Yangi texnologiyalarning g'ayrioddiy turlari va ushbu texnologiyalarning yangi qo'llanish usullari paydo bo'lishda davom etmoqda. Bularning barchasi tahdidlarni boshqarishga o'z ta'sirini ko'rsatadi.

Bugungi kunda e'tiborni jalb qilish uchun raqobatlashayotgan ko'plab yangi texnologiyalar mavjud bo'lib, ularning barchasini bilish deyarli mumkin emas, ularning barchasini batafsil tushunish yoki ular rivojlanib, takomillashganda qanday birgalikda ishlashini anglash yanada qiyin. Albatta, bu korxonalarga keng qamrovli CRMPning mavjud bo'lishi kerakligining asosiy sabablaridan biri bo'lib, u boshqa rivojlangan korxona tahdidlarini boshqarish dasturlari bilan uyg'unlikda ishlaydi. Bu nafaqat texnologik o'zgarishlarni, balki ushbu kitobda muhokama qilingan ijtimoiy, iqtisodiy, siyosiy, madaniy va boshqa o'zgarishlarning barcha turlarini anglatadi, ular korxonalarning tahdid muhitiga ta'sir

ko'rsatadi. Shubhasiz, texnologiya sohasidagi yangiliklar butun dunyo bo'ylab korxonalar uchun tahdidlarni boshqarishning eng dolzarb muammolaridan biri bo'lib qolaveradi.

"Keyingi muhim hodisa" nima bo'lishini aniq aytish mumkin bo'lmasa-da, bitta inqilobiy texnologiya, ya'ni kvant hisoblashlar, kompyuter, kiberxavfsizlik va tahdidlarni boshqarish tizimini hozirgi kunda AI kabi, balki undan ham ko'proq darajada tubdan o'zgartirish salohiyatiga ega. Kvant hisoblash – bu kompyuter texnologiyasining yangi rivojlanayotgan sohasi bo'lib, u kvant mexanikasi tamoyillaridan va kubitlar deb ataladigan ma'lumotlarning mayda, beqaror birliklaridan foydalanadi. Bu soha "oddiy" kompyuterlar bajara olmaydigan murakkab hisoblash vazifalarini bajarish va tezlikni keskin oshirish imkonini beradi.

Kvant hisoblash ochishi mumkin bo'lgan imkoniyatlarning ajoyib bir misoli quyidagicha: Google kompaniyasi 2019-yilda o'zining AI bo'limi tomonidan "Sycamore" nomli kvant protsessorini yaratganini e'lon qildi. Bu protsessor eng zamonaviy superkompyuter 10 ming yilda bajaradigan vazifani atigi 200 soniyada bajara olardi. 2021-yilda esa kompaniya Sycamorening yangilangan versiyasini e'lon qildi. Bu yangi versiya asl nusxasidan 350 million marta quvvatliroq edi.

Bu shuni anglatadiki, Googlening kvant hisoblash tashabbusi va boshqa ko'plab kompaniyalar (IBM, Honeywell va Microsoft kabi taniqli kompaniyalar; yaxshi moliyalashtirilgan startaplar va AQSH hamda uning demokratik ittifoqchilariga raqib bo'lgan davlatlar) hisoblash tezligini va quvvatini hozirgi holatidan milliardlab marta oshirish imkoniyatiga ega.

Kvant hisoblash, shubhasiz, turli sohalarda radikal va bashorat qilib bo'lmaydigan yutuqlarga olib keladi. Masalan, moliyaviy muassasalar undan bozor tendensiyalarini bashorat qilishning yangi modellarini ishlab chiqish va investisiya portfellarini optimallashtirish uchun foydalanishlari mumkin. Dori-darmon ishlab chiqaruvchi kompaniyalar yangi dori-darmonlar va davolash usullarini ishlab chiqish uchun molekulyar xatti-harakatlarni tez va aniq tarzda simulyatsiya qilishlari mumkin. Ishlab chiqaruvchilar xomashyo sohasidagi kvantga asoslangan yutuqlardan foydalanib, mahsulotlarni kuchliroq, yengilroq, energiya tejamkor va ekologik jihatdan barqarorroq qilib loyihalashtirishi mumkin. Bundan tashqari, aviakompaniyalardan tortib avtomobil ijarasi agentliklari va yuk tashish firmalarigacha bo'lgan transport va logistika xizmatlari, kvant texnologiyalaridan yo'nalishlarni optimallashtirish va transport vositalarini boshqarishni takomillashtirish uchun foydalanishlari, shu orqali o'zlarining energiya sarfini va uglerod chiqindilarini kamaytirishlari mumkin. Ehtimol, kvant hisoblashning ta'sirini kuzatishning eng qiziqarli sohasi bu – sun'iy intellektidir. Kvant kompyuterlari AI modellari va LLMLarni tezroq, samarali va aniqroq o'qitish uchun ishlatilishi mumkin, bu AIning yanada aniq va foydali qaror qabul qilishini ta'minlaydi.

Albatta, kvant hisoblash nafaqat imkoniyatlarni taqdim etadi. U muqarrar ravishda o'ziga xos qiyinchiliklarni ham keltirib chiqaradi, bu esa quyidagi sohalarda puxta o'ylangan va kelajakka yo'naltirilgan tahdidlarni boshqarishni talab qiladi:

Kriptografik xavflar

Kvant kompyuterlari nazariy jihatdan keng tarqalgan kriptografik algoritm-larni buzishi mumkin, masalan, shaxsiy maxfiy ma'lumotlar va onlayn tranzaksi-yalarni himoya qilish uchun ishlatiladigan algoritm-lar.

Operatsion murakkablik

Kvant hisoblash tizimlarining murakkabligi maxsus malakani talab etadi. Tegishli bilim va boshqaruv bo'lmasa, bu tizimlarning murakkabligi operatsion tahdidlarga olib kelishi mumkin.

Normativ talablarga muvofiqlik

Kvant texnologiyasi rivojlanishda davom etar ekan, u yangi me'yoriy-huquqiy bazalarni shakllantirishi mumkin. Ushbu o'zgaruvchan qonunlar va standartlarga rioya qilish tahdidlarni ehtiyotkorlik bilan boshqarishni, muvofiqlikni ta'minlash uchun dasturni doimiy ravishda o'zgartirish va moslashtirishni talab qiladi.

Strategik muvofiqlashtirish

Kvant hisoblashni biznes jarayonlariga joriy etish tashkilotning umumiy strate-gik yo'nalishi va tahdidlarni boshqarish usuli bilan uyg'un bo'lishi shart. Har qanday nomuvofiqlik moliyaviy xavfga, obro'ga putur yetkazuvchi yoki strategik xavf-xatarlarga olib kelishi mumkin.

Ushbu qiyinchiliklarni yengish uchun tashkilotlar kvant hisoblash keltirib chiqaradigan o'ziga xos tahdidlarga moslashtirilgan keng qamrovli tahdidlarni boshqarish dasturini qabul qilishlari zarur.

Yakuniy xulosa

Ushbu kitobning boshida butun dunyo bo'ylab pandemiya, aviahalokatlar va kiberhujumlar kabi zararli hodisalar bilan ifodalangan jiddiy korxona tah-didlari batafsil bayon qilindi. Bu xavf-xatarlar tahdidlarni boshqarishda rivoj-langan va yetuk yondashuvni talab qiladi. Kitobning yakunida esa, texnologik va boshqa rivojlanishlar, jumladan AI va kvant hisoblash kabi texnologiyalar bilan bog'liq yangi xavf-xatarlar haqida ma'lumotlar berildi. Bularning barchasi keng qamrovli, mustahkam va muvofiqlashtirilgan CRMPni qabul qilishni talab etadi. Bugungi kunda korxona qaror qabul qiluvchi shaxslari hayratlanarli dara-jada xilma-xil tahdidlarga duch kelmoqdalar, ularning ba'zilar insoniyat tarixi kabi qadimiy bo'lsa, ba'zilar esa shunchalik yangiki, hatto ularning nomlari hali ham mavjud emas.

CRMP uzoq vaqtdan beri o'rnatilgan tahdidni boshqarish tamoyillariga asoslanadi va ularni raqamli texnologiyalar tezligida o'zgarayotgan dunyoga tatbiq etadi.

CRMPning dolzarbligi raqamlashtirishning keng tarqalganligidan kelib chiqadi. Bugungi kunda biz qilayotgan har bir ish kibertahdid va yangi imkoniyatni keltirib chiqaradi. Bu shuni anglatadiki, har qanday tahdid va tahdidlarni boshqarish bo'yicha qarorlar kiberxavfsizlik tarkibiy qismiga ega.

Ushbu yakuniy bobda, o'zgarishlar tez sur'atlarda sodir bo'layotgani, ularni bashorat qilish mutlaqo imkonsizligi, shuningdek, bu o'zgarishlarning korxonalar, sanoat tarmoqlari yoki shaxslar va ular duch keladigan tahdidlarga bo'lgan ta'siri ham oldindan aytib bo'lmasligi ta'kidlab o'tildi. Albatta, yangi texnologiyalar doimiy ravishda paydo bo'lib turadi, ammo tahdid muhitidagi o'zgarishlar texnologiyadan ancha keng ko'lamni qamrab oladi.

Yashash va ishlash tarzimizdagi tub o'zgarishlar, jamiyatning korxonalar o'zini qanday tutishi borasidagi kutilmalari hamda huquqiy va me'yoriy muhitdagi o'zgarishlar tahdidlarni aniqlash, ularga yechim topish, ularni kamaytirish va ulardan foydalanishni har qachongidan ham murakkablashtirmoqda.

Oldinda cheksiz imkoniyatlar mavjud va bu tahdidlarni boshqarish, ayniqsa xavfsizlik sohasida faoliyat yuritish uchun juda qiziqarli davr hisoblanadi. Rasmiy CRMP kelajakka yo'naltirilgan, strategik va o'zaro bog'liq vazifani bajarishga imkon yaratadi hamda strategik hamkorlikni olib boradi. Ushbu dastur kelajakka mo'ljallangan yondashuvni ta'minlash uchun moslashuvchan va o'zgaruvchan bo'lib qoladi.

CRMP TIZIMI v.1.0

Raqamli transformatsiyalar natijasida hosil bo'lgan doimiy o'zgaruvchan muhitda kiberxavfsizlik nafaqat AT muammosi, balki biznes strategiyasi va qaror qabul qilishning ajralmas qismi ekanligini anglash juda muhimdir. Bu tushuncha bilan birga korxonalar o'z biznes faoliyatida kibertahdidlarni boshqarishning keng qamrovli dasturini joriy etish zarurati paydo bo'ladi. Ushbu Ilova CRMPni yaxlit tarzda amalga oshirish uchun, boshqaruvdan tortib operatsion eskalatsiya va ma'lumotlarni oshkor qilishgacha bo'lgan tizimni taqdim etadi.

Maqsad va sharh

So'nggi yillarda kibertahdidlar va va hodisalarning misli ko'rilmagan darajada ko'payishi kuzatilmoqda. Hokimiyat organlari va tartibga soluvchi tashkilotlar korxonalarning kiberxavfsizlik choralari kuchaytirish hamda manfaatdor tomonlarga kibertahdidlar haqida samarali axborot yetkazishning dolzarb zarurligini ta'kidlamodalar.

Boshqaruv va rahbariyat o'zlarining kibertahdid muhitini to'g'ri nazorat qila olishi kerak. Ko'pgina mavjud standartlar va tavsiyalar alohida ko'rib chiqilganda, biznes talablariga to'liq javob beradigan keng qamrovli dasturni ta'minlay olmasligi mumkin. Bu bo'shliq nufuzli yo'riqnomalar, qoidalar va standartlarni uyg'unlashtiradigan va talqin qiladigan yagona tizimga ehtiyoj mavjudligini ta'kidlaydi. Bunday tizimning mavjudligi korxonalarning kibertahdidlarni to'g'ri boshqarishi va nazorat qilishini ta'minlaydi.

CRMP tizimi yetakchi amaliyotlar va standartlardan olingan ma'lumotlarni umumlashtiradi, CRMP uchun tizimli va keng qamrovli yondashuvni ta'minlaydi. Dastur har bir korxonaning o'ziga xos ehtiyojlari va tartibga solish muhitiga moslashtirilishi mumkin. U CRMPni amaliyotga tatbiq etish uchun qo'llanma va-zifasini bajaradi, korxonalarga tahdidga oid asosli qarorlar qabul qilish va raqamli asrda rivojlanib, omon qolish uchun xavfsizlik strategiyalarini ishlab chiqishga imkon beradi.

CRMPning tuzilishi

CRMP to'rt asosiy qismdan tashkil topgan:

- “Moslashuvchan boshqaruv”
- “Tahdidlar haqidagi ma'lumotlarga asoslangan tizim”
- “Tahdidlarni baholashga asoslangan strategiya va uning ijrosi”
- “Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilinishi”

Ushbu komponentlarning har biri, amalga oshirish bo'yicha tavsiyalar beradigan ko'plab yordamchi tamoyillarga bo'linadi. Amaliy qo'llashni osonlashti-

rish va chuqurroq tushunish uchun ushbu tarkibiy qismlardagi tamoyillar tegishli ma'lumot beruvchi manbalar bilan bog'langan.

Ma'lumot beruvchi havolalar nufuzli manbalardan olingan, jumladan:

SECning 2023-yilgi yakuniy qoidasi: kiberxavfsizlikka oid tahdidlarni boshqarish, strategiya, boshqaruv, hodisalarni oshkor qilish qoidasi

SECning 2023-yilgi yakuniy qoidasi asosiy qoidalarni bayon qiluvchi keng qamrovli qo'llanma bo'lib, unda kiberxavfsizlik sohasidagi tahdidlar va hodisalarni boshqarish hamda ular haqida hisobot berishda ro'yxatdan o'tuvchilar rioya qilishlari kerak bo'lgan ma'lumotlarni oshkor qilishning asosiy talablari ko'rsatilgan. U tahdidlarni boshqarish, boshqaruv protokollari va ma'lumotlarni oshkor qilishga doir bir nechta tarkibiy qismlarni o'z ichiga oladi, direktorlar kengashi-ning majburiyatlari va kiberxavfsizlik sohasida jiddiy tahdid hodisasi yuz berganda talab qilinadigan maxsus hisobot taqdim etish talablari haqida batafsil ma'lumot beradi. Ushbu qoida kiberxavfsizlik sohasidagi tahdidlarni boshqarishning ham strategik, ham operatsion jihatlarini qamrab olgan holda, korxonalar ichida mustahkam kiberxavfsizlik tizimlarini rivojlantirishni osonlashtiradi, tahdidga oid ma'lumotlarni oshkor qilishda shaffoflik va izchillikni targ'ib qiladi va shu orqali investitsiyaga oid asosli qarorlar qabul qilishda xabardorlikni oshirishga yordam beradi.

NISTning 2023-yilgi dastlabki ommaviy loyihasi, CSF 2.0

NISTning yangilangan kiberxavfsizlik asoslari 2.0 loyihasi, korxonalarga kiberxavfsizlikka oid tahdidlarni boshqarish va ularni kamaytirish uchun sanoat standartlari va boshqaruv uchun eng yaxshi amaliyotlar to'plamini taqdim etishga qaratilgan. U o'zining avvalgi versiyasiga asoslanib, rivojlanib borayotgan kibertahdidlar va texnologiyalarni qamrab oluvchi takomillashtirilgan ko'rsatmalarni o'z ichiga oladi. Ushbu tizim, garchi moslashuvchan bo'lsa-da, korxonalarni kiberxavfsizlik strategiyasi bilan biznes maqsadlarini muvofiqlashtirishga undaydi, bu esa kiberxavfsizlikni faol boshqarish madaniyatini shakllantirishga yordam beradi.

NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi

Ushbu qo'llanma Kibertahdidlarni nazorat qilishning murakkab jarayonlarida kompaniya direktorlari uchun to'g'ri yo'l topishda yordam beruvchi keng qamrovli yo'riqnoma bo'lib xizmat qiladi. Unda kibermuhit haqida yaxshi ma'lumotga ega direktorlar kengashini tashkillashtirish bo'yicha ma'lumot va tavsiyalar mavjud bo'lib, qo'llanmada barqaror kibertahdidga oid strategiyalarini yaratishda direktorlar va rahbariyat o'rtasidagi hamkorlikning muhimligi ta'kidlanadi. Ushbu qo'llanma orqali direktorlar korxonaning kiberxavfsizlik tashabbuslarini samarali nazorat qilish va yo'naltirish uchun zarur vositalar va bilimlar bilan ta'minlanadi, shu tariqa aksiyadorlar qiymati va korxona obro'sini himoya qilishadi.

Ushbu xalqaro standartda axborot xavfsizligini boshqarish tizimini (ISMS¹⁴⁸) yaratish, joriy etish, saqlash va doimiy ravishda takomillashtirish talablari ko'rsatilgan. ISO 27001 doirasidagi standartlar tahdidlarni boshqarish jarayoni yordamida ma'lumotlarni himoya qilish asoslarini ta'minlaydi, tahdidlarni boshqarish jarayonlari, jismoniy xavfsizlik protokollari va biznes uzluksizligi rejalaridan foydalangan holda maxfiy ma'lumotlarni boshqarish va himoya qilishga tizimli yondashuvni taklif qiladi. Ushbu standartlar ma'lumot bilan xavfsiz va ishonchli ishlashni osonlashtiradi, korxonaning kibertahdidlarga qarshi himoya mexanizmlarini mustahkamlaydi.

NISTIR 8286

NISTIR 8286 hisoboti kiberxavfsizlik xavflarini korxona tahdidlarini boshqarishning keng qamrovli doirasiga kiritishga qaratilgan. Unda korxonaning kiberxavfsizlik faoliyatini ERM bilan muvofiqlashtirish afzalliklari bayon etilgan bo'lib, kiberxavfsizlik va ERM o'rtasidagi o'zaro bog'liqlik ta'kidlanadi. Bu munosabatda kiberxavfsizlikka oid tahdidlarni tushunish va boshqarish keng ko'lamli korxona tahdidlariga ta'sir ko'rsatishi va ayni paytda ulardan ta'sirlanishi ta'kidlangan. Bunda keng qamrovli korxona tahdidlari ham inobatga olinadi. Kiberxavfsizlik alohida tizim sifatida emas, balki korxonaning xavf-xatarlarni boshqarish amaliyotining ajralmas qismi sifatida qaraladi. Natijada, u korxonalarni tahdidlarni va ularning korxona uchun potensial ta'sirini har tomonlama tushunishga asoslangan ongli qarorlar qabul qilishga undaydi, bu esa mustahkam va chidamli kibertahdidlarni boshqarish strategiyalarini ishlab chiqishga yordam beradi.

IIAning 2020-yilgi Uch chiziqli himoya modeli

Ichki auditorlar institutining 2020-yilda yangilangan uch chiziqli himoya modeli korxonalar uchun tahdidlarni boshqarish va boshqaruv strategiyalarini shakllantirish bo'yicha keng qamrovli qo'llanma bo'lib xizmat qiladi. Ushbu model korxonalarni uchta chiziqli (yo'nalish) bo'yicha vazifalarni aniq belgilab berishga undaydi, ular: boshqaruv nazorati; tahdidlarni boshqarish, muvofiqlik, boshqa nazorat vazifalari; ichki audit. Bu model ushbu yo'nalishlarning hamkorlikda ishlashini ta'kidlaydi, natijada esa bu hamkorlik tashkilot maqsadlariga erishishga yordam beradi va tahdidlarni boshqarish hamda korporativ boshqaruvga nisbatan samarali yondashuvni ta'minlaydi. Model korxonalarga o'z maqsadlari va operatsion tuzilmalariga mos ravishda qo'llash imkoniyatini taqdim etish orqali moslashuvchanlikni rag'batlantiradi. Kiberxavfsizlik sohasida, ushbu model kibertahdidlarni aniqlash, ularni baholash va boshqarishda yaxshi tashkil etilgan yondashuvni ta'minlaydi, shuningdek, yaxlit va integratsiyalashgan tahdidlarni boshqarish madaniyatini shakllantiradi.

¹⁴⁷ IEC (International Electrotechnical Commission) – Xalqaro elektrotexnika komissiyasi.

¹⁴⁸ ISMS (information security management system) – axborot xavfsizligini boshqarish tizimi.

2018-yilgi SEC komissiyasining bayonoti va jamoatchilik kompaniyalari uchun kiberxavfsizlik ma'lumotlarini oshkor qilish bo'yicha ko'rsatmalari

SECning 2018-yilgi ushbu bayonoti ommaviy kompaniyalar kiberxavfsizlik sohasidagi tahdidlar va hodisalar haqida ma'lumotlarni qanday oshkor qilishi kerakligi bo'yicha yo'riqnomani taqdim etadi. Ushbu hujjatda korxonalar yaxshi o'rnatilgan kiberxavfsizlik siyosati va tartib-qoidalariga ega bo'lish zarurati ta'kidlanadi, shuningdek, kompaniyalarni kiberxavfsizlik tahdidlari bo'yicha oshkorlik nazoratlarini baholash va takomillashtirishda faol bo'lishga undaydi. Bundan tashqari, ushbu hujjat kiberxavfsizlik sohasidagi tahdidlarni boshqarishda direktorlar va rahbarlarning rollari haqida ma'lumot beradi va investorlarga kiberhodisalar va tahdidlar haqida o'z vaqtida shaffof ma'lumot yetkazishni ta'minlaydi.

ISO 31000:2018

Ushbu standart tahdidlarni boshqarish bo'yicha ko'rsatmalar beradi, kiberxavfsizlik kabi har qanday xavf turiga qo'llanilishi mumkin bo'lgan universal standartni taklif qiladi. U tashkilotlarga tizimli tarzda tahdidlarni aniqlash, ularni tahlil qilish va kamaytirishga yordam beradigan prinsiplar, tamoyillar va tahdidlarni boshqarish jarayonlari haqida tushuncha beradi. Ushbu standartga rioya qilib, korxonalar tahdidlardan xabardor madaniyatini shakllantirishi mumkin, bu esa tahdidlar va ularning potensial ta'sirlari haqida to'liq tushunishga asoslangan, o'z vaqtida asosli qarorlar qabul qilishni ta'minlaydi.

AICPAning 2017-yilgi CRMP tavsif mezonlari

AICPAning CRMP mezonlari tashkilotlarga o'zlarining kiberxavfsizlik sohasidagi tahdidlarni boshqarish dasturlarini tasvirlash uchun foydalanishlari mumkin bo'lgan tuzilmani taqdim etadi va bu mezonlar asosida sertifikatlangan jamoatchilik buxgalterlari dasturlarni tekshirish va ular haqida hisobot berishlari mumkin. Ushbu tuzilma rahbariyat va direktorlar kengashining kiberxavfsizlik choralari nazorat qilishdagi muhim rolini ta'kidlab, kibertahdidlarni samarali bartaraf etish uchun ularning oldini olish, aniqlash va ularga javob berish strategiyalarini o'z ichiga olgan keng qamrovli tahdidlarni boshqarish dasturining ahamiyatini alohida ta'kidlaydi. Shu bilan birga, u barqaror va mustahkam kiberxavfsizlik infratuzilmasini yaratishni osonlashtiradi, manfaatdor tomonlar o'rtasida ishonchni oshiradi.

Ushbu manbalar CRMP tizimining mustahkamligi va qo'llanilishini oshiradigan ma'lumotlar va amaliy tavsiyalarni taqdim etadi.

Eslatma: Tizim ma'lumotlarini oshkor qilish

CRMP yuqoridagi manbalarga to'liq mos kelsa-da, bugungi muhit uchun zarur bo'lgan yetuk CRMPning barcha jihatlarini to'liq qamrab oladigan yagona standart yoki yo'riqnoma mavjud emasligini tan olish muhimdir. Shunday qilib, ushbu tizimni yaratish va bu kitobni yozishning asosiy maqsadi turli manbalardan

olingan ma'lumotlarni umumlashtirib, yaxlit va uyg'unlashgan qarashni taqdim etishdir. Tashkilotingizning o'ziga xos xususiyatlari va nozik jihatlariga qarab boshqa standartlar ham foydali bo'lishi mumkin.

Umuman olganda, ushbu Ilovada ishonchli manbalarga asoslangan keng qamrovli CRMPning mohiyati izohlangan. Bu qo'llanma korxonalar va ularning qaror qabul qiluvchi shaxslariga CRMPni tushunishda, amalda qo'llash va joriy etishga yordam beradi. Qo'llanma korxonalarning raqamli muammolar oldida barqaror va moslashuvchan bo'lib qolishini ta'minlaydi, shu bilan birga ularni rivojlanayotgan huquqiy javobgarlik va tartibga solish xavflaridan himoya qiladi.

Tizimning nozik va murakkab jihatlarini o'rganar ekanmiz, uning pirovard maqsadi aniqlik kiritish, soha standartlariga muvofiq bo'lish va biznesga yanada samaraliroq qarorlar qabul qilish hamda raqamli davrda xavfsiz rivojlanishga yordam berish ekanligini esda tutishimiz lozim.

Komponent	Tamoyil	Ma'lumot beruvchi havola
Moslashuvchan boshqaruv	1-tamoyil: Siyosat va jarayonlarni joriy etish <i>CRMPni yaratish uchun butun korxona miqyosida siyosat va jarayonlar joriy etilishi kerak.</i>	• 2023-yilgi NIST CSF 2.0 GV: PO-01, GV: PO.02 • ISO/IEC 27001:2022 5.2 • ISO 31000:2018 6.1 • 2018-yilgi SEC komissiyasining bayonoti va jamoatchilik kompaniyalari uchun kiberxavfsizlik ma'lumotlarini oshkor qilish bo'yicha ko'rsatmalari, 18-bet, 2- va 3-paragraflar • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni DC4, DC7, DC19
Moslashuvchan boshqaruv	2-tamoyil: "Uch chiziqli himoya modeli" doirasida boshqaruv, vazifalar va majburiyatlarni o'rnatish <i>"Uch chiziqli himoya modeli" doirasida CRMP aniq belgilangan vazifalar, majburiyatlilar va natijalar bilan o'rnatilishi kerak.</i>	• 2023-yilgi SEC yo'riqnomasining S-K106(c) bandi – Boshqaruv va 20-F shakl • NISTning 2023-yilgi CSF2.0 GV: RR loyihasi • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 6-tamoyil • ISO/IEC 27001:2022 5.1, 5.3 • ISO 31000: 2018 5.2, 5.4.3 • IIAning 2020-yilgi Uch chiziqli himoya modeli, 2–4-tamoyillar
Moslashuvchan boshqaruv	3-tamoyil: Boshqaruv amaliyotlarini mavjud tahdidlarni boshqarish tizimi bilan muvofiq-lashtirish <i>Kibertahdidlarni boshqarish amaliyotlari korxonaning har qanday mavjud tahdidlarni boshqarish tizimiga moslashtirilishi lozim.</i>	• NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 1, 4-tamoyillar • NISTning 2023-yilgi CSF2.0 GV: RM-03 loyihasi • NISTIR 8286

Moslashuvchan boshqaruv	4-tamoyil: Direktorlar kengashi va rahbariyat qamrov doirasini belgilaydi <i>Korxonada kibertahdidlarga qarshi kurash amaliyotlarining qamrov doirasi direktorlar kengashi va yuqori rahbariyat tomonidan belgilanishi va tasdiqlanishi lozim.</i>	• NIST ning 2023-yilgi CSF2.0 GV. OC-01, GV. RR-01 loyihasi • ISO 31000:2018 5.2
Moslashuvchan boshqaruv	5-tamoyil: Direktorlar kengashi va yuqori bo'g'in rahbarlari nazoratni amalga oshiradilar <i>Direktorlar kengashi va yuqori darajadagi rahbarlar korxonaning kibertahdidlar bilan kurashida tegishli nazoratni ta'minlashi zarur.</i>	• 2023-yilgi SEC yo'riqnomasining S-K106(c) bandi – Boshqaruv va 20-F shakli • NISTning 2023-yilgi CSF 2.0 GV. RR-01 loyihasi • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 3-tamoyil • IIAning 2020-yilgi Uch chiziqli himoya modeli, 1-tamoyil • ISO 31000:2018 5.4.2 • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC8
Moslashuvchan boshqaruv	6-tamoyil: Boshqaruv jarayonlari auditi <i>Audit jarayonlari korxonaning kibertahdidlarni boshqarish amaliyotini tegishli tarzda tahlil qilib, ularni baholashi lozim.</i>	• IIAning 2020-yilgi Uch chiziqli himoya modeli, 4-tamoyil • 2018-yilgi SEC komissiyasining bayonoti va jamoatchilik kompaniyalari uchun kiberxavfsizlik ma'lumotlarini oshkor qilish bo'yicha ko'rsatmalari, 18-bet, 3-paragraf • ISO 31000:2018 5.4.2 • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC8
Moslashuvchan boshqaruv	7-tamoyil: Resurslarni belgilangan vazifa va majburiyatlarga muvofiqlashtirish <i>Tegishli resurslar va malakalar to'plami belgilangan vazifalar va majburiyatlarga muvofiq bo'lishi kerak va doimiy mashg'ulotlar o'tkazilishi zarur</i>	• NISTning 2023-yilgi CSF 2.0 GV. RR-03 loyihasi • ISO/IEC 27001:2022 7.1 • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 3-tamoyil • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC10
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	1-tamoyil: Tahdidlarni baholash tizimi va metodologiyasini aniqlash <i>Tashkilotda kibertahdidni aniqlash, baholash va o'lchash uchun tahdid asoslari va metodologiyasini aniqlash va uni amalga oshirish lozim.</i>	• SEC yo'riqnomasi S-K106(c) bandi – Tahdidlarni boshqarish va strategiya • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 1, 4, 5-tamoyillar • NIST ning 2023-yilgi CSF 2.0 GV. RM, ID. RA loyihasi • ISO/IEC 27001:2022 6.1.2, 6.1.3 • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC11 • ISO 31000:2018 6.1

Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	2-tamoyil: Tahdid chegaralarini aniqlash metodologiyasini ishlab chiqish <i>Tahdidning maqbul darajalari uchun tasdiqlangan va takrorlanadigan metodologiya yaratilishi lozim.</i>	• NIST ning 2023-yilgi CSF 2.0 GV. RM-02 loyihasi • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 1-va 5-tamoyillar
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	3-tamoyil: Tahdid haqidagi ma'lumotlarga asoslangan ehtiyojlar tushunchasini shakllantirish <i>Boshqaruv organi aniqlanib, o'zining kibertahdidlarga oid ma'lumotlarga asoslangan ehtiyojlarini har tomonlama tushunishni shakllantirish jarayoniga jalb qilinishi lozim.</i>	• NISTning 2023-yilgi CSF 2.0 GV. RM-02 loyihasi • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC13 • IIAning 2020-yilgi Uch chiziqli himoya mode-li, 1-tamoyil • ISO 31000:2018 6.2
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	4-tamoyil: Tahdidlarni baholash muddati bo'yicha kelishib olish <i>Tahdidni baholash jarayoni ke-lishilgan vaqt oralig'ida amal-ga oshirilishi va uning natijalari muntazam ravishda baholanib turishi lozim.</i>	• SEC yo'riqnomasi S-K106(c) bandi – Tahdid-larni boshqarish va strategiya • NACDning 2023-yilgi kibertahdidlarni na-zorat qilish bo'yicha direktorlar qo'llanmasi, 5-tamoyil • NISTning 2023-yilgi CSF 2.0 ID. RA, ID.IM loyihasi • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC11, DC12, DC15
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	5-tamoyil: Hisobot jarayonlarini yo'lga qo'yish <i>Hisobot berish jarayonlari boshqaruv organiga kibertah-didlarning mavjud amaliyotlar-ga va strategik qarorlarga ta'si-ri to'g'risida ma'lumot berishi kerak.</i>	• NISTning 2023-yilgi CSF 2.0 GV. OV loyihasi • NACDning 2023-yilgi kibertahdidlarni na-zorat qilish bo'yicha direktorlar qo'llanmasi, 5-tamoyil • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC13, DC16 • IIAning 2020-yilgi Uch chiziqli himoya mo-deli, 6-tamoyil
Tahdidlarni baho-lashga asoslangan strategiya va uning ijrosi	1-tamoyil: Maqbul tahdid che-galarini aniqlash <i>Maqbul kibertahdid chegaralari tahdid tizimi va metodologiya-siga asoslanib, tahdid bo'yicha mas'ul shaxslar tomonidan ani-q tushumilishi, belgilanishi va tas-diqlanishi zarur.</i>	• NACDning 2023-yilgi kibertahdidlarni na-zorat qilish bo'yicha direktorlar qo'llanmasi, 1-tamoyil • NISTning 2023-yilgi CSF 2.0 GV. RM-02 loyihasi
Tahdidlarni baho-lashga asoslangan strategiya va uning ijrosi	2-tamoyil: Strategiya va byud-jetni tasdiqlangan tahdid chega-ralari bilan muvofiqlashtirish <i>Kibertahdidni bartaraf etish re-ja-si va byudjeti – tasdiqlangan tahdid chegarasi bilan muvofiq-lashtirilishi kerak.</i>	• NISTning 2023-yilgi CSF 2.0 GV. RM-04 loyihasi • NACDning 2023-yilgi kibertahdidlarni na-zorat qilish bo'yicha direktorlar qo'llanmasi, 1-tamoyil • ISO 31000 6.5.1, 6.5.2 • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC17

Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	3-tamoyil: Maqbul tahdid chegaralari doirasida ijro etish <i>Kibertahdidlarni bartaraf etish rejasi tasdiqlangan tahdid chegaralariga muvofiq amalga oshirilishi lozim.</i>	• NISTning 2023-yilgi CSF 2.0 GV, RR-03 loyihasi • ISO 31000 6.5.3
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	4-tamoyil: Doimiy ravishda nazorat qilish <i>Kibertahdidlarni bartaraf etish rejasining ijrosi belgilangan samaradorlik ko'rsatkichlari va operatsion mezonlar asosida doimiy ravishda nazorat qilib borilishi lozim.</i>	• NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 5-tamoyil • NISTning 2023-yilgi CSF 2.0 GV,OV loyihasi • 2017-yilgi AICPAning CRMP ta'riflash mezo-ni, DC15, DC16
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	5-tamoyil: Tahdidning chegaraviy darajalariga nisbatan audit tekshiruvi <i>Audit xizmati tahdidning tasdiqlangan chegaraviy darajalariga asoslangan kibertahdidni bartaraf etish rejasining to'g'ri bajarilishini ko'rib chiqishi va baholashi kerak.</i>	• ILAning 2020-yilgi Uch chiziqli himoya modeli, 4-tamoyil • 2017-yilgi AICPAning CRMP ta'riflash me-zoni
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	6-tamoyil: Tahdidlarni bartaraf etish rejasiga uchinchi tomonlarni kiritish <i>Kibertahdidlarni bartaraf etish rejasi uchinchi tomonlarni, jumladan hamkorlar, ta'minotchilar va ta'minot zanjiri ishtirokchilarini hisobga olishi kerak.</i>	• NISTning 2023-yilgi CSF 2.0 GV, SC, ID.IM-02 loyihasi • SEC yo'riqnomasi S-K106(c) bandi – Tahdidlarni boshqarish va strategiya
Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish	1-tamoyil: Eskalatsiya jarayonlarini joriy etish <i>Kibertahdidlarni eskalatsiyasi qilish jarayonlari ishlab chiqilishi va joriy etilishi lozim.</i>	• SEC yo'riqnomasi S-K106(c) bandi – Boshqaruv • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 2-tamoyil • 2018-yilgi SEC komissiyasining bayonoti va jamoatchilik kompaniyalari uchun kiberxavfsizlik ma'lumotlarini oshkor qilish bo'yicha ko'rsatmalari, 18-bet, 3-paragraf hamda 20-bet, 1-paragraf • 2017-yilgi AICPAning CRMP ta'riflash me-zoni

Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish	2-tamoyil: Barcha korxonalar uchun ma'lumotlarni oshkor qilish jarayonlarini yo'lga qo'yish <i>Korxonaning kibernetika ma'lumotlarini oshkor etish jarayonlari uning o'ziga xos tahdid omillarini, tashkiliy sharoitlarini va talablarini inobatga olgan holda ishlab chiqilishi lozim.</i>	• NISTning 2023-yilgi CSF 2.0 GVOC-03 loyihasi • NACDning 2023-yilgi kibertahdidlarni nazorat qilish bo'yicha direktorlar qo'llanmasi, 2-tamoyil • 2017-yilgi AICPning CRMP ta'riflash mezonini, DC6, DC14
Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish	3-tamoyil: Ochiq aksiyadorlik jamiyatlari uchun ma'lumotni oshkor qilish jarayonlarini o'rnatish <i>Ochiq aksiyadorlik jamiyatlarini jiddiy tahdidlarni, tahdid omillarini, kibertahdidlarni boshqarish jarayonlarini, boshqaruv tizimi va jiddiy hodisalar haqidagi ma'lumotlarini oshkor qilishlari shart.</i>	• SECning 2023-yilgi yakuniy qoidasi: kiberxavfsizlikka oid tahdidlarni boshqarish, strategiya, boshqaruv, hodisalarni oshkor qilish • NISTning 2023-yilgi CSF 2.0 GVOC-03 loyihasi • 2018-yilgi SEC komissiyasining bayonoti va jamoatchilik kompaniyalari uchun kiberxavfsizlik ma'lumotlarini oshkor qilish bo'yicha ko'rsatmalari, 4-bet, 1-paragraf; 6-bet, 3-paragraf; 7-bet, 4-paragraf; 11-bet, 1-paragraf.
Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish	4-tamoyil: Eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlarini sinovdan o'tkazish <i>Kibertahdidlar eskalatsiyasi va ma'lumotlarning oshkor qilish jarayonlari o'zlashtirilgan saboqlarni inobatga olish maqsadida doimiy ravishda tekshirilishi, sinovdan o'tkazilishi va yangilanishi kerak.</i>	• SECning 2023-yilgi yakuniy qoidasi: kiberxavfsizlikka oid tahdidlarni boshqarish, strategiya, boshqaruv, hodisalarni oshkor qilish • NISTning 2023-yilgi CSF 2.0 ID.IM loyihasi
Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor etish	5-tamoyil: Eskalatsiya va ma'lumotlarni oshkor etish jarayonlarini tekshirish <i>Korxonaning samaradorligi, izchilligi hamda tegishli qoidalar va siyosatlariga muvofiqligini ta'minlash maqsadida, audit xizmati korxonaning kibertahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilish jarayonlarini ko'rib chiqishi va baholashi kerak.</i>	• IIAning 2020-yilgi Uch chiziqli himoya modeli, 4- va 5-tamoyillar

GLOSSARIY

AI (Artificial intelligence) – sun'iy intellekt, bu tezkor hisoblash muhitida algoritmlar yaratish va qo'llash orqali insonning aql-idrok jarayonlariga taqlid qilishga asoslanadi.

AICPA (The American Institute of Certified Public Accountants) – Amerika sertifikatlangan jamoat buxgalterlari instituti. Qo'shma Shtatlardagi Sertifikatlangan buxgalterlarning (CPAs) milliy professional tashkiloti bo'lib, 130 ta mamlakatda 428 000 dan ortiq a'zoga ega.

AMF (Financial Markets Authority) – Moliyaviy bozorlar boshqarmasi.

APT (Advanced Persistent Threat) – doimiy ilg'or tahdid, haqiqiy hayotdagi hujum ssenariylarini modellashtiradi va zararli shaxslar tashkilot tarmog'i va tizimlariga qanday kirib borishga urinishi va ular qanday ma'lumotlarga kirishi mumkinligini ko'rsatadi.

ASIC (Australian Securities and Investments Commission) – Avstraliya Qimmatli qog'ozlar va investitsiyalar komissiyasi. Avstraliyaning integratsiyalashgan korporativ, bozorlar, moliyaviy xizmatlar va iste'mol kreditlari regulyatoridir va Avstraliya hamjamiyatiga xizmat qiladi.

BaFin (Federal Financial Supervisory Authority) – Federal moliyaviy nazorat organi. Germaniyaning integratsiyalashgan moliyaviy tartibga solish organi hisoblanadi.

Bug Bounty – bu ba'zi veb-saytlar va dasturiy ta'minot ishlab chiquvchilari tomonidan taqdim etilgan dastur bo'lib, u orqali odamlar xatolarni, ayniqsa ekspluatatsiya va zaifliklarni topganliklari uchun mukofotlanadi.

CFO (Chief financial officer) – moliya bo'limi rahbari. Kompaniyaning moliyasini boshqarish bilan bog'liq bo'lgan yuqori martabali rahbar hisoblanadi. Bu moliyaviy va pul oqimlarini rejalashtirishning barcha jihatlarini boshqarishni, shuningdek, uning moliyaviy holatini tahlil qilishni o'z ichiga oladi.

CFPB (Consumer Financial Protection Bureau) – Iste'molchilarni moliyaviy himoya qilish byurosi. Amerika Qo'shma Shtatlari hukumatining moliyaviy sektorda iste'molchilar huquqlarini himoya qilish uchun mas'ul bo'lgan mustaqil agentligidir. CFPB yurisdiksiyasiga banklar, kredit uyushmalari, qimmatli qog'ozlar firmalari, ish haqi bo'yicha kreditorlar, ipoteka bo'yicha xizmat ko'rsatish operatsiyalari, garovdan xalos bo'lish xizmatlari, qarz yig'uvchilar, notijorat kollejlari va Qo'shma Shtatlarda faoliyat yurituvchi boshqa moliyaviy kompaniyalar kiradi.

CIO (Chief Information Officer) – axborot texnologiyalari bo'yicha direktor. Tashkilotning butun IT strategiyasini ishlab chiqish va amalga oshirish, byudjetlarni boshqarish va barcha IT xodimlarini nazorat qilish uchun javobgardir. Ish barcha dasturiy ta'minot, apparat va infratuzilma, shuningdek, tashkilot ma'lumotlarini umumiy boshqarish uchun javobgarlikni o'z ichiga oladi.

CMMI (The Capability Maturity Model Integration) – Imkoniyatning yetuklik modeli integratsiyasi, bu tashkilotning jarayonlarini yaxshilash va ularning samaradorligini oshirishga mo'ljallangan model.

COSO (Committee of Sponsoring Organizations) – Homiy tashkilotlar qo'mitasi. Biznes uchun ichki nazorat, risklarni boshqarish va firibgarlikning oldini olishni baholash bo'yicha ko'rsatmalar ishlab chiqadigan tashkilotdir.

CRMP (Cyber Risk Management Program) – Kibertahdidlarni boshqarish dasturi – bu tashkilotning raqamli aktivlarini aniqlash, mavjud xavfsizlik choralari ko'rib chiqish va nima ishlashini davom ettirish yoki biznesga tahdid solishi mumkin bo'lgan xavfsizlik xatarlarini yumshatish uchun yechimlarni amalga oshirish jarayoni.

CRO (Chief risk officer) – tahdidlarni boshqarish bo'yicha bosh direktor. Korporativ boshqaruvchi bo'lib, korxona kapitali va daromadlariga jiddiy raqobatbardosh, tartibga soluvchi va texnologik tahdidlarni baholash va yumshatish vazifasini yuklaydi.

CRQ (Cyber risk quantification) – kibertahdidni miqdoriy baholash, bu muayyan kibertahdidning potensial moliyaviy ta'sirini baholash jarayonidir. Kiberxavflar miqdorini aniqlash aqlli qarorlar qabul qilishni qo'llab-quvvatlaydi va xavfsizlik bo'yicha mutaxassislarga qaysi tahdidlar va zaifliklarni birinchi navbatda hal qilish kerakligi haqida ongli qaror qabul qilishga yordam beradi.

CSA (Canadian Securities Administrators) – Kanada qimmatli qog'ozlar ma'murlari

CSO (Chief security officer) – xavfsizlik bo'limi boshlig'i, o'z tashkiloti xavfsizligining barcha jihatlarini uchun mas'ul bo'lgan rahbarlardir. Xavfsizlik bo'yicha bosh direktor kompaniyaning jismoniy va raqamli xavfsizligi uchun mas'ul bo'lgan C-suite ijrochi direktoridir. CSO ijroiya rahbariyatini ta'minlaydi va xavflarni aniqlash, baholash va ustuvorligini nazorat qiladi, tashkilot xavfsizligi bilan bog'liq barcha sa'y-harakatlarni boshqaradi.

CTO (Chief technology officer) – texnologiyalar bo'yicha bosh direktor. Butun axborot texnologiyalari bo'limini nazorat qiluvchi, biznes ehtiyojlari va talablarini IT rejalashtirish va operatsiyalariga integratsiya qilish uchun mas'ul bo'lgan yuqori darajadagi rahbar hisoblanadi.

CxO (Chief experience officer) – Mijozlar bilan ishlash bo‘lim boshlig‘i. Tashkilot mahsulotlari va xizmatlarining umumiy tajribasi uchun mas‘ul bo‘lgan ijrochi hisoblanadi.

Dark Web – maxsus brauzerlar orqali kiriladigan, oddiy qidiruv tizimlari tomonidan indekslanmaydigan Internetning yashirin qismi.

Ensemble learning – Jamoaviy o‘rganish, bu yaxshiroq bashoratlarni ishlab chiqish uchun ikki yoki undan ortiq modellarni (masalan, regressiya modellari, neyron tarmoqlari) birlashtiradigan mashinaviy o‘rganish usuli.

EQUIFAX – AQSHning Atlanta shahrida joylashgan ko‘p millatli iste‘mol kredit hisobotlari agentligi.

ESMA (European Securities and Markets) – Yevropa qimmatli qog‘ozlar va bozorlar boshqarmasi.

FAA (The Federal Aviation Administration) – Amerika Qo‘shma Shtatlari Milliy aviatsiya ma‘muriyati.

FAIR (Factor Analysis of Information Risk) – Axborot tahdidlarni omilli tahlil qilish.

FCA (Financial Conduct Authority) – Moliyaviy xulq-atvor nazorati boshqarmasi.

FINMA (Swiss Financial Market Supervisory Authority) – Shveysariya moliya bozorini nazorat qilish organi.

FINRA (Financial Industry Regulatory Authority) – Moliya sanoatini tartibga soluvchi vakolatli idora.

Fishing attack – fishing hujumi, bu tashkilot yoki jismoniy shaxsning shaxsiy ma‘lumotlari yoki moliyaviy ma‘lumotlarini o‘g‘irlash uchun elektron pochta, xabarlar yoki veb-saytlar kabi soxta aloqa usullaridan foydalanish.

FTC (Federal Trade Commission) – Federal savdo komissiyasi. Amerika Qo‘shma Shtatlari hukumatining mustaqil agentligi bo‘lib, uning asosiy vazifasi fuqarolik (jinoiy bo‘lmagan) monopoliyaga qarshi qonunlarni qo‘llash va iste‘molchilar huquqlarini himoya qilishni rag‘batlantirishdir.

GDPR (General Data Protection Regulation) – Ma‘lumotlarni himoya qilish umumiy reglamenti.

GRC (Governance, Risk, and Compliance Program) – Boshqaruv, tahdid va muvofiqlik dasturi. ATni biznes maqsadlariga muvofiqlashtirish, xavflarni boshqarish hamda barcha sanoat va hukumat qoidalariga rioya qilishning tuzilgan usulidir. U tashkilotni va risklarni boshqarishni texnologik innovatsiyalar va joriy etish bilan birlashtirish uchun vositalar va jarayonlarni o‘z ichiga oladi.

ID: IM (Identify improvement) – ijobiy o‘zgarishni aniqlash.

ID: RA (Identify risk assessment) – tahdidlarni baholashni aniqlash.

IIA (The Institute of Internal Auditors) – Ichki auditorlar instituti.

IOSCO (International Organization of Securities Commissions) – Qimmatli qog'ozlar komissiyalari xalqaro tashkiloti.

IoT (Internet of Things) – Internet orqali boshqa qurilmalar va tizimlar bilan ma'lumotlarni ulash va almashish uchun sensorlar, dasturiy ta'minot va boshqa texnologiyalar bilan o'rnatilgan jismoniy obyektlar tarmog'ini ifodalaydi.

IPO (initial public offering) – birlamchi ommaviy taklif, bu – kompaniyaning o'z aksiyalarini birjada birinchi marta ommaga taklif qilish orqali ochiq kompaniyaga aylanish jarayoni.

ISO (International Organization for Standardization) – Xalqaro standartlashtirish tashkiloti. Mustaqil, nodavlat, xalqaro standartlarni ishlab chiqish tashkiloti bo'lib, u a'zo mamlakatlarning milliy standartlar tashkilotlari vakillaridan tashkil topgan.

JFSA (Japan Financial Services Agency) – Yaponiya moliyaviy xizmatlar agentligi.

KPI (A key performance indicator) – asosiy samaradorlik ko'rsatkichlari. KPilar tashkilot yoki u ishtirok etayotgan muayyan faoliyat (masalan, loyihalar, dasturlar, mahsulotlar va boshqa tashabbuslar) muvaffaqiyatini baholaydi. KPI strategik va operatsion takomillashtirishga qaratilgan, qaror qabul qilish uchun tahliliy asos yaratadi va diqqatni eng muhim narsaga qaratishga yordam beradi.

KRI (key risk indicators) – asosiy xavf ko'rsatkichlari, bu boshqaruvda xavf darajasini ko'rsatish uchun ishlatiladigan o'lchovdir.

M2M (Machine-to-machine communication) – har qanday aloqa kanalidan foydalanadigan qurilmalar o'rtasida to'g'ridan to'g'ri aloqa.

Malicious insiders – zararli insayder – bu kompaniyaning maxfiy ma'lumotlarini qasddan tarqatish yoki suiiste'mol qilish uchun imtiyozli kirish huquqidan foydalanadigan xodim, pudratchi yoki biznes sherik.

MFA (multifactor authentication) – Ko'p omilli autentifikatsiya, ushbu autentifikatsiya ikki bosqichli tekshirish jarayonini talab qiladi, bu nafaqat foydalanuvchi nomi va parolni, balki faqat foydalanuvchi biladigan ma'lumotni ham talab qiladi.

ML (machine learning) – Mashinali o'qitish – bu sun'iy intellekt nazariyasining bir bo'limi, kompyuter sun'iy intellekt yordamida hal qilish jarayoni va usullarini izlashdan iborat.

Monte Carlo Simulation – Monte-Karlo usuli noma'lum qiymatni taxmin qilish uchun tasodifiy tanlab olishdan foydalanadigan statistik usuldir.

CxO (Chief experience officer) – Mijozlar bilan ishlash bo‘lim boshlig‘i. Tashkilot mahsulotlari va xizmatlarining umumiy tajribasi uchun mas‘ul bo‘lgan ijrochi hisoblanadi.

Dark Web – maxsus brauzerlar orqali kiriladigan, oddiy qidiruv tizimlari tomonidan indekslanmaydigan Internetning yashirin qismi.

Ensemble learning – Jamoaviy o‘rganish, bu yaxshiroq bashoratlarni ishlab chiqish uchun ikki yoki undan ortiq modellarni (masalan, regressiya modellari, neyron tarmoqlari) birlashtiradigan mashinaviy o‘rganish usuli.

EQUIFAX – AQSHning Atlanta shahrida joylashgan ko‘p millatli iste‘mol kredit hisobotlari agentligi.

ESMA (European Securities and Markets) – Yevropa qimmatli qog‘ozlar va bozorlar boshqarmasi.

FAA (The Federal Aviation Administration) – Amerika Qo‘shma Shtatlari Milliy aviatsiya ma‘muriyati.

FAIR (Factor Analysis of Information Risk) – Axborot tahdidlarni omilli tahlil qilish.

FCA (Financial Conduct Authority) – Moliyaviy xulq-atvor nazorati boshqarmasi.

FINMA (Swiss Financial Market Supervisory Authority) – Shveysariya moliya bozorini nazorat qilish organi.

FINRA (Financial Industry Regulatory Authority) – Moliya sanoatini tartibga soluvchi vakolatli idora.

Fishing attack – fishing hujumi, bu tashkilot yoki jismoniy shaxsning shaxsiy ma‘lumotlari yoki moliyaviy ma‘lumotlarini o‘g‘irlash uchun elektron pochta, xabarlar yoki veb-saytlar kabi soxta aloqa usullaridan foydalanish.

FTC (Federal Trade Commission) – Federal savdo komissiyasi. Amerika Qo‘shma Shtatlari hukumatining mustaqil agentligi bo‘lib, uning asosiy vazifasi fuqarolik (jinoiy bo‘lmagan) monopoliyaga qarshi qonunlarni qo‘llash va iste‘molchilar huquqlarini himoya qilishni rag‘batlantirishdir.

GDPR (General Data Protection Regulation) – Ma‘lumotlarni himoya qilish umumiy reglamentlari.

GRC (Governance, Risk, and Compliance Program) – Boshqaruv, tahdid va muvofiqlik dasturi. ATni biznes maqsadlariga muvofiqlashtirish, xavflarni boshqarish hamda barcha sanoat va hukumat qoidalariga rioya qilishning tuzilgan usulidir. U tashkilotni va risklarni boshqarishni texnologik innovatsiyalar va joriy etish bilan birlashtirish uchun vositalar va jarayonlarni o‘z ichiga oladi.

ID: IM (Identify improvement) – ijobiy o‘zgarishni aniqlash.

ID: RA (Identify risk assessment) – tahdidlarni baholashni aniqlash.

IIA (The Institute of Internal Auditors) – Ichki auditorlar instituti.

IOSCO (International Organization of Securities Commissions) – Qimmatli qog'ozlar komissiyalari xalqaro tashkiloti.

IoT (Internet of Things) – Internet orqali boshqa qurilmalar va tizimlar bilan ma'lumotlarni ulash va almashish uchun sensorlar, dasturiy ta'minot va boshqa texnologiyalar bilan o'rnatilgan jismoniy obyektlar tarmog'ini ifodalaydi.

IPO (initial public offering) – birlamchi ommaviy taklif, bu – kompaniyaning o'z aksiyalarini birjada birinchi marta ommaga taklif qilish orqali ochiq kompaniyaga aylanish jarayoni.

ISO (International Organization for Standardization) – Xalqaro standartlashtirish tashkiloti. Mustaqil, nodavlat, xalqaro standartlarni ishlab chiqish tashkiloti bo'lib, u a'zo mamlakatlarning milliy standartlar tashkilotlari vakillaridan tashkil topgan.

JFSA (Japan Financial Services Agency) – Yaponiya moliyaviy xizmatlar agentligi.

KPI (A key performance indicator) – asosiy samaradorlik ko'rsatkichlari. KPIlar tashkilot yoki u ishtirok etayotgan muayyan faoliyat (masalan, loyihalar, dasturlar, mahsulotlar va boshqa tashabbuslar) muvaffaqiyatini baholaydi. KPI strategik va operatsion takomillashtirishga qaratilgan, qaror qabul qilish uchun tahliliy asos yaratadi va diqqatni eng muhim narsaga qaratishga yordam beradi.

KRI (key risk indicators) – asosiy xavf ko'rsatkichlari, bu boshqaruvda xavf darajasini ko'rsatish uchun ishlatiladigan o'lchovdir.

M2M (Machine-to-machine communication) – har qanday aloqa kanalidan foydalanadigan qurilmalar o'rtasida to'g'ridan to'g'ri aloqa.

Malicious insiders – zararli insayder – bu kompaniyaning maxfiy ma'lumotlarini qasddan tarqatish yoki suiiste'mol qilish uchun imtiyozli kirish huquqidan foydalanadigan xodim, pudratchi yoki biznes sherik.

MFA (multifactor authentication) – Ko'p omilli autentifikatsiya, ushbu autentifikatsiya ikki bosqichli tekshirish jarayonini talab qiladi, bu nafaqat foydalanuvchi nomi va parolni, balki faqat foydalanuvchi biladigan ma'lumotni ham talab qiladi.

ML (machine learning) – Mashinali o'qitish – bu sun'iy intellekt nazariyasining bir bo'limi, kompyuter sun'iy intellekt yordamida hal qilish jarayoni va usullarini izlashdan iborat.

Monte Carlo Simulation – Monte-Karlo usuli noma'lum qiymatni taxmin qilish uchun tasodifiy tanlab olishdan foydalanadigan statistik usuldur.

MRB (Model risk management) – model xavfini boshqarish, qaror qabul qilish uchun yetarli darajada aniq bo'lmagan modellardan foydalanish natijasida zarar ko'rish xavfini boshqarish.

NACD (National Association of Corporate Directors) – Korxona direktorlari milliy uyushmasi.

NCSC (National Cyber Security Centre) – Milliy kiberxavfsizlik markazi.

NIST CSF (Cybersecurity Framework of National Institute of Standards and Technology) – Standartlar va texnologiyalar milliy instituti kiberxavfsizlik asoslari.

NISTIR (National Institute of Standards and Technology Interagency or Internal Reports) – Standartlar va texnologiyalar milliy instituti idoralararo yoki ichki hisobotlari.

NLP (natural language processing) – tabiiy tilni qayta ishlash – bu Alning kichik to'plami bo'lib, u kompyuterlar va mashinalarga inson tilini tushunish, izohlash, manipulyatsiya va muloqot qilish imkonini beradi.

NYSE (New York Stock Exchange) – Nyu York fond birjasi.

Pen (penetration) testing – Pentest, tarmoq yoki dasturga xakerlik hujumiga o'xshash jarayonlarni amalga oshiruvchi test tizimi hisoblanadi. Pentestning maqsadi tizim yoki dasturning qanday himoyalanganini o'rganishdir.

PMI (Project Management Institute) – Loyihani boshqarish instituti

Ransomware – jabrlanuvchining kompyuterini ishlashga yaroqsiz holga keltiradigan troyan ot tipidagi zararli dastur hisoblanadi.

SC (System and Communications Protection) – Tizim va aloqa himoyasi. Tarmoqqa asoslangan zararli kodlar va zararli veb-saytlarni tashqi zararli kodlarni identifikatsiyalash usullari bilan faol ravishda aniqlash, virtualizatsiya yordamida aniqlangan har qanday zararli kod tashkilot tizimlariga zarar bermasligiga ishonch hosil qilish.

SEBI (Securities and Exchange Board of India) – Hindiston Qimmatli qog'ozlar va birja kengashi.

SEC (Securities and Exchange Commission) – Qimmatli qog'ozlar va birjalar komissiyasi, Amerikaning qimmatli qog'ozlar bozorini nazorat qiluvchi va tartibga soluvchi asosiy organi.

SI (System and Information Integrity) – Tizim va axborot yaxlitligi. Tizim va ma'lumotlarning yaxlitligi xato xabarlarini yaratish orqali ta'minlanadi, ular to'g'rilash uchun zarur bo'lgan ma'lumotlarni ishlatadigan ma'lumotlarni oshkor qilmasdan va faqat bu xabarlarni vakolatli xodimlar yoki rollarga oshkor qiladi.

SLA (service-level agreements) – xizmat ko‘rsatish darajasi shartnomasi, bu xaridor bilan taqdim etiladigan xizmatlarni belgilaydigan aniq (ichki yoki tashqi) kelishuv.

SOC (Security Operations Center) – xavfsizlik operatsiyalari markazi. Tashkilotni kibertahdidlardan himoya qilish uchun javobgardir. SOC tahlilchilari tashkilot tarmog‘ining kecha-yu kunduz monitoringini amalga oshiradilar va har qanday mumkin bo‘lgan xavfsizlik hodisalarini tekshiradilar.

Tahdid eskalatsiyasi (Risk escalation) – tahdidning kuchayishi – bu tahdid uchun javobgarlikni tashkilot ichidagi vakolatli shaxslarga o‘tkazish.

VPN (virtual private network) – virtual xususiy tarmoq. Bu shaxsiy tarmoqni (masalan, umumiy Internet bo‘lmagan har qanday kompyuter tarmog‘i) ishonchsiz bo‘lgan bir yoki bir nechta boshqa tarmoqlar bo‘ylab virtual ravishda kengaytirish uchun tarmoq arxitekturasini.

WEF (World Economic Forum) – Jahon iqtisodiy forumi. Xalqaro nodavlat notijorat tashkiloti va tahlil markazi bo‘lib, asosi Shveysariyaning Jeneva kantoni, Kyolni shahrida joylashgan. Maqsadi global, mintaqaviy va sanoat kun tartibini shakllantirish uchun biznes, siyosiy, akademik va jamiyatning boshqa rahbarlarini jalb qilish orqali dunyo holatini yaxshilash.

Brayan Allen muhim infratuzilmaga ega bo'lgan Time Warner Cable kompaniyasida bosh xavfsizlik xodimi bo'lib ishlagan. U EY kompaniyasida CRMP rahbari sifatida faoliyat yuritib, ba'zi yirik global tashkilotlarning boshqaruv kengashlari va C darajadagi rahbarlari oldida taqdimotlar qilgan. Hozirda Brayan Bank siyosati institutida kiberxavfsizlik va texnologiya bilan bog'liq tahdidlarni boshqarish bo'yicha katta vitse-prezident sifatida ishlaydi, u bank rahbarlari bilan ishlab, sanoatni nazorat organlari, qonun chiqaruvchilar, huquqni muhofaza qiluvchi organlar va razvedka jamoalari oldida himoya qiladi. B.Allen bir nechta sanoat va hukumat tomonidan muvofiqlashtirilgan muhim infratuzilma guruhlarida, jumladan, Comm-ISAC va Comm-SEC va aloqa sohasini muvofiqlashtirish kengashida ishlagan.

U Federal aloqa agentligi (FCC¹⁴⁹) raisi tomonidan kiberxavfsizlik tamoyilini ishlab chiqishda NIST bilan hamkorlik qilishda kommunikatsiya sanoati vakili etib tayinlangan.

Janob Allen korxona xavfsizlik riskini boshqarish bo'yicha 2 ta kitob muallifi, Konnektikut universiteti MBA dasturi Moliyaviy tahdidlarni boshqarish dasturi professori, kiberxavfsizlik va korxona tahdidlarini boshqarish tushunchalarini o'rgatadi va butun dunyo bo'ylab ushbu mavzu bo'yicha ma'ruzalar bilan ishtirok etadi. Janob Allen ko'plab sanoat sertifikatlariga ega va Nyu York shtati advokatlar assotsiatsiyasi a'zosi.

Brendon Bapst EY kompaniyasining kiberxavfsizlik amaliyot bo'limida kibertahdidlar bo'yicha maslahatchi sifatida ishlaydi. U ijrochi rahbarlar, CSO va CISolar bilan yaqindan ishlaydi hamda yetuk CRMP ishlab chiqishda yordam beradi. Brendon taktik xavfsizlik dasturlarini ma'lumotlar va texnologiyalar tahliliga asoslangan korxona xavfsizligi uchun tahdidlarni boshqarishning kompleks metodlariga o'zgartirish uchun Global Fortune 100 ro'yxatidagi kompaniyalar bilan ishlagan. Brendon sertifikatlangan axborot tizimlari xavfsizligi bo'yicha mutaxassis, sertifikatlangan axborot xavfsizligi menejeri (CISM¹⁵⁰) va sertifikatlangan axborot tizimlari auditori (CISA¹⁵¹).

Terry Allan Hiks uzoq yillik biznes va texnologiya yozuvchisi bo'lib, asosan moliyaviy xizmatlar, axborot xavfsizligi va korporativ boshqaruv bilan bog'liq sohalarida yozadi. U, dunyoning yetakchi AT tadqiqot va maslahat firmasi bo'lgan Gartnerda yigirma yildan ortiq yetakchi yozuvchi sifatida ishlagan. Shuningdek, Terry Allan Hiks yigirmadan ortiq kitoblarni muallifi.

¹⁴⁹ FCC (Federal Communications Commission) – Federal aloqa agentligi.

¹⁵⁰ CISM (Certified Information Security Manager) – sertifikatlangan axborot xavfsizligi menejeri.

¹⁵¹ CISA (Certified Information Systems Auditor) – sertifikatlangan axborot tizimlari auditori.

MUNDARIJA

Kibertahdidlarni boshqarish dasturining yaratilishi	3
Kirish	5

I BOB. RAQAMLI TEXNOLOGIYALAR ASRIDA KIBERXAVFSIZLIK: DUNYO TAHDID OSTIDA

To'rtinchi sanoat inqilobi	14
Kiberxavfsizlik – tahdid bilan bog'liq amaliyot	18
Kibertahdidlarni boshqarish nazorati va javobgarligi	20
Raqamli texnologiyalar va CRMPni takomillashtirish	21
Kiberxavfsizlik shunchaki “xavfsizlik” muammosi emas	21
CRMP: Korxonaning dolzarb muammosi	25
Kitobning yo'l xaritasi	26
Yakuniy xulosa	27

II BOB. KIBERTAHDIDLARNI BOSHQARISH DASTURI (CRMP)

SEC gapiradi – butun dunyo tinglaydi	28
Noxush hodisalarning oshkor qilinishi (“Amaldagi ma'lumotlarning oshkor qilinishi”)	29
Tahdidlarni boshqarish, strategiya va boshqaruvga oid ma'lumotlarning oshkor qilinishi (“Ma'lumotlarning davriy oshkor qilinishi”)	30
CRMP tamoyillari	31
CRMP: Asosiy harakatlantiruvchi omillar	33
Vazifa va majburiyatlarni bajarish	36
Tahdidlarni boshqarish to'liq muvaffaqiyatsizlikka uchraganda: Boeing 737 MAX samolyoti halokatlari	37
Boeing samolyoti halokatlarida qo'llanilgan tahdidlarni boshqarish dasturi	40
“Jiddiy va o'ta muhim”: Boeing ishi	42
Favqulodda vaziyatlarda xavfsizlik dasturining afzalliklari	43
1-afzallik: Xavfsizlikka tahdid funksiyasining strategik tan olinishi	45
2-afzallik: Kibertahdidlarga qarshi kurash bo'linmasining samarali byudjetini ta'minlash	46

3-afzallik: Tahdidlar bo'yicha qaror qabul qiluvchi shaxslar uchun himoya	46
Tizimli, ammo tahdiddan mutlaq xoli bo'lmagan CRMP	47
Kengashning mas'uliyati va yuridik javobgarligi	48
Boeing kompaniyasi ishi bo'yicha sud qarori va kibertahdid nazorati bo'yicha javobgarlik	51
Axborot xavfsizligi boshqarmasi boshliqlari javobgarlik uchun tanqid ostida	53
Yakuniy xulosa	55

III BOB. MOSLASHUVCHAN BOSHQARUV

Moslashuvchan boshqaruv ta'rifi	57
Uber kompaniyasi tomonidan xakerlik hujumining yashirilishi	58
Samarali boshqaruv qanday bo'ladi?	59
Korxonani boshqaruv strategiyasi bilan muvofiqlashtirish	61
Moslashuvchan boshqaruvning yetti tamoyili	64
1-tamoyil: Siyosat va jarayonlarni joriy etish	64
2-tamoyil: "Uch chiziqli himoya modeli" doirasida boshqaruv, vazifalar va majburiyatlarni o'rnatish	65
3-tamoyil: Boshqaruv amaliyotlarini mavjud tahdidlarni boshqarish tizimi bilan muvofiqlashtirish	68
4-tamoyil: Direktorlar kengashi va rahbariyat qamrov doirasini belgilaydi	70
5-tamoyil: Direktorlar kengashi va yuqori bo'g'in rahbarlari nazoratni amalga oshiradilar	71
6-tamoyil: Boshqaruv jarayonlari auditi	73
7-tamoyil: Resurslarni belgilangan vazifa va majburiyatlarga muvofiqlashtirish	74
Yakuniy xulosa	75

IV BOB. TAHDID HAQIDAGI MA'LUMOTLARGA ASOSLANGAN TIZIM

Nega tahdid haqidagi ma'lumotlar juda muhim?	77
Tahdid va tahdid to'g'risidagi ma'lumotlar ta'rifi	78
Tahdidlar haqidagi ma'lumotlarga asoslangan tizimning besh tamoyili	81

1-tamoyil: Tahdidlarni baholash tizimi va metodologiyasini aniqlash	82
2-tamoyil: Tahdid darajalarini aniqlash metodologiyasini ishlab chiqish	84
3-tamoyil: Tahdidga asoslangan ehtiyojlar tushunchasini shakllantirish	87
4-tamoyil: Tahdidlarni baholash muddati bo'yicha kelishib olish	89
5-tamoyil: Hisobot jarayonlarini yo'lga qo'yish	91
Yakuniy xulosa	93

V BOB. TAHDIDGA ASOSLANGAN STRATEGIYA VA UNING IJROSI

ChatGPT biznes dunyosini larzaga solmoqda	97
AI bilan bog'liq tahdid: Ikki qudratli texnologiya kompaniyalari ikki xil yo'lni tanlaydi	98
"Uoll-strit" gazetasi: Tez harakat qiling, aks holda sizning o'rningizni boshqalar egallaydi	100
Dunyoni o'zgartiruvchi raqamli texnologiyalar paydo bo'lishda davom etmoqda	101
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	103
Tahdidlarni baholashga asoslangan strategiya va uni amalga oshirishning olti tamoyili	104
1-tamoyil: Maqbul tahdid chegaralarini aniqlash	105
2-tamoyil: Strategiya va byudjetni maqbul tahdid chegarasi bilan muvofiqlashtirish	107
3-tamoyil: Maqbul tahdid chegaralari doirasida ijro	110
4-tamoyil: Doimiy ravishda nazorat qilish	112
5-tamoyil: Tahdidning chegaraviy darajalariga nisbatan audit tekshiruvi	113
6-tamoyil: Tahdidlarni bartaraf etish rejasiga uchinchi tomonlarni kiritish	114
Yakuniy xulosa	115

VI BOB. TAHDIDLAR ESKALATSIYASI VA MA'LUMOTLARNING OSHKOR ETILISHI

SEC va tahdid haqidagi ma'lumotlarning oshkoraligi	119
Butunjahon tartibga soluvchi organlari tahdidga oid ma'lumotlarni oshkor qilishni talab qiladi	120
Tahdidlar eskalatsiyasi	122
Kibertahdid tasnifi	124

Tahdidlar eskalatsiyasi va ma'lumotlarning oshkoraligi – faqatgina xavfsizlikka oid hodisalar emas	126
Ma'lumotlarni oshkor qilish – korxonalar uchun majburiy talab	127
Ekvifaks (Equifax) mojarosi	128
Bir nechta tahdidlar birlashib, jiddiy tahdidga aylanganda	130
SECning muhimlik haqidagi mezonlari	131
CRMP bilan ERMni muvofiqlashtirish	133
Tahdidlar eskalatsiyasi va ma'lumotlarni oshkor qilishning besh tamoyili	134
1-tamoyil: Eskalatsiya jarayonlarini o'rnatish	135
2-tamoyil: Barcha korxonalar uchun ma'lumotlarni oshkor qilish jarayonlarini yo'lga qo'yish	137
3-tamoyil: Ochiq aksiyadorlik jamiyatlari uchun ma'lumotlarni oshkor qilish jarayonlarini o'rnatish	139
4-tamoyil: Eskalatsiya va ma'lumotlarni oshkor qilish jarayonlarini sinovdan o'tkazish	142
5-tamoyil: Eskalatsiya va ma'lumotlarni oshkor qilish jarayonlarini tekshirish	144
Yakuniy xulosa	145

VII BOB. CRMPNI JORIY ETISH

Kibertahdidlarni boshqarish jarayonlari	147
Kibertahdidlarni boshqarish jarayonini boshlash	149
CRMPni joriy etish	151
Moslashuvchan boshqaruv	151
Moslashuvchan boshqaruv bilan bog'liq umumiy muammolar	153
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim	155
Tahdidlar haqidagi ma'lumotlarga asoslangan tizim bilan bog'liq umumiy muammolar	157
Tahdidlarni baholashga asoslangan strategiya va uning ijrosi	166
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	169
Dasturni sotish	173
Yakuniy xulosa	177

VIII BOB. AMALIY XAVF-XATAR VA BARQARORLIKKA NISBATAN QO'LLANILADIGAN CRMP

Korxonaning operatsion barqarorlik bilan bog'liq va uning o'sishiga yordam beradigan vazifalari	182
Zararli dasturiy ta'minot hujumi sababli Maersk kompaniyasining butun dunyo bo'ylab tizimlari ishdan chiqdi	184
CRMPning to'rt asosiy komponenti yordamida operatsion barqarorlikni ta'minlash bo'yicha ko'rsatma	187
Moslashuvchan boshqaruv	187
Tahdid haqidagi ma'lumotlarga asoslangan tizim	188
Tahdidlarga asoslangan strategiya va uning ijrosi	189
Tahdidlar eskalatsiyasi va ma'lumotlarning oshkor etilishi	189
Yakuniy xulosa	190

IX BOB. AI VA BOSHQALAR: RAQAMLASHTIRILGAN DUNYODA TAHDIHLARNI BOSHQARISHNING KELAJAGI

AI ta'rifi	192
AI: Butunlay yangi, xavfli dunyo	194
Tortishuvli mashinali o'qitish (AML): NISTning taksonomiyasi va terminologiyasi	197
Sun'iy intellektdan foydalanish bilan bog'liq tahdidlarni boshqarish tizimlari	198
Alni joriy etishning asosiy tushunchalari va asoslari	201
Aldan tashqari: raqamli texnologiyalar hech qachon rivojlanishdan to'xtamaydi	205
Yakuniy xulosa	207
Ilova: CRMP tizimi v 1.0	209
Glossariy	218
Mualliflar haqida	224

Brayan Allen, Brendon Bapst, Terri Allan Xiks

KIBERTAHDIDLARNI BOSHQARISH DASTURINI YARATISH

Raqamli texnologiyalar asrida xavfsizlik tizimini takomillashtirish

Muharrir
Badiiy muharrir
Texnik muharrir
Sahifalovchi

T. Mirzayev
D. Mulla-Axunov
R. Ahmedov
G. Ahmedova

Noshirlik faoliyati to'g'risidagi xabarnoma
6.11.2023-yil qabul qilingan, tasdiqnoma № 156149.
Bosishga 2025-yil 11-aprelda ruxsat etildi.
Bichimi 70x100 $\frac{1}{16}$. Bosma tabog'i 14,5. Adadi 50.
Buyurtma № 016/O-25.

“Donishmand ziyosi” MChJ nashriyotida nashrga tayyorlandi.
Toshkent shahar, Navoiy ko'chasi, 30-uy.

“Kamalak-PRESS” MChJ bosmaxonasida chop etildi.
Toshkent shahar, Navoiy ko'chasi, 30-uy.

1066,556

Ushbu xorijiy o'quv adabiyoti o'zbek tiliga ilk marotaba tarjima qilinganligi munosabati bilan nashriyot va tarjimonlar tomonidan ayrim kamchilik va xatoliklarga yo'l qo'yilgan bo'lishi mumkin. Kamchiliklarni bartaraf etish maqsadida fikr-mulohazalaringizni quyidagi manzil va telefon raqamlari orqali qabul qilamiz.

Manzil: Toshkent shahar, Navoiy ko'chasi, 30-uy.

Telefon raqami 71-244-15-53.