Vilniaus Universitetas
EKONOMIKOS IR VERSLO ADMINISTRAVIMO FAKULTETAS

STRATEGINIŲ INFORMACINIŲ SISTEMŲ VALDYMO MAGISTRO PROGRAMA

VILIUS PEČIULIS
I kurso studentas

Įmonės kibernetinis saugumas: metodikų ir veiksnių, turinčių įtakos mokymo efektyvumui palyginamasis tyrimas

MAGISTRO DARBAS

Darbo vadovas: Doc., Dr. Mindaugas Krutinis

Vilnius, 2024

Turinys

Lentelių turinys

Paveiksliukų turinys

Įvadas

Šiuolaikinėje verslo aplinkoje, kur informacijos srautai ir privatumo gynimas tapo ne mažiau svarbūs nei korporacijų fizinių išteklių valdymas, kibernetinis saugumas tampa lemiamu veiksniu, siekiant užtikrinti tiek įmonės stabilumą, tiek jos reputaciją. Technologijos, besivystančios eksponentiniais tempais, reikalauja ne tik lanksčios, bet ir strategiškai pagrįstos kibernetinio saugumo sistemos, kuri būtų vienu metu ir atspari, ir dinamiškai pritaikoma prie kintančiu grėsmių. Todėl šio darbo tikslas – patobulinti organizacijos kibernetinio saugumo strategiją – išryškina šiandienos rinkos poreikius, taip pat atveria galimybę žengti žingsnį tolyn tiek teorinėje, tiek praktiškai taikomoje saugumo srityje (Shea, Gillis ir Clark, 2023).

Šio darbo metu bus įgyvendinti rūpestingai apgalvoti uždaviniai, kurių esmė – detaliai išnagrinėti, palyginti įvairias kibernetinio saugumo vertinimo metodikas, kurios pilnai atskleidžia organizacijų gebėjimą atsispirti informacijos technologijų pasaulio iššūkiams. Be to, bus svarstoma metodikų specifika, išryškinant kiekvienos jų naudą ir ribotumus, kad galėtume pateikti subalansuotą ir nuoseklų vertinimą, pasitelkiant įvairius atvejų tyrimus ir mokslinę literatūrą (Joseph,2022).

Darbo tikslas

Patobulinti organizacijos kibernetinio saugumo strategiją.

Darbo temos aktualumas

Kibernetinis saugumas dabar - tai ne šių dienų prabanga, o būtinybė. Vis daugiau įmonių, nepriklausomai nuo jų dydžio, privalo susidurti su elektroninius išteklius ir duomenis gresiančiomis grėsmėmis. Kaip kadaise buvo svarbu užrakinti biuro duris paliekant po darbo, taip dabar svarbu tinkamai apsaugoti kompiuterių sistemas nuo virtualių įsilaužėlių. Įmonėms, kurios gyvuoja ir klesti dėl interneto platumų, kibernetinio saugumo vertinimas yra tas žingsnis, kuris padeda ne tik atpažinti galimus nesklandumus, bet ir veiksmingai kovoti su jais (Irwin, 2022).

Reguliarus įmonių apsaugos būklės patikrinimas ir atnaujinimas daro didžiulę įtaką visam verslui: saugo kritinę informaciją, palaiko darbo tęstinumą ir mažina finansinį nuostolį, kurį gali lemti kibernetiniai incidentai (Drenik, 2022). Todėl šis tyrimas būtų netik aktualesnis, bet ir be galo reikalingas bet kuriai įmonei, norinčiai išsilaikyti ir pasisekti šiuolaikinėje informacinėje visuomenėje, kur kompiuteriniai tinklai yra kasdieninio gyvenimo dalis.

Darbo problematika

Kibernetinio saugumo tyrimo metu organizacijoms tenka spręsti daugybę iššūkių, kad užtikrintų patikimus ir tikslius tyrimo rezultatus. Iškylančios problemos gali žymiai paveikti tyrimo eigą ir jo išvadas, todėl labai svarbu į jas atsižvelgti ir ieškoti sprendimo būdų:

Pirma, išteklių stoka – tai realybė daugeliui įmonių, kurios varginasi suderinti ribotas finansines ir laiko galimybes su aukštos kokybės kibernetinio saugumo reikalavimais. Tam prisideda biudžeto apribojimai, kas apsunkina tinkamų saugumo priemonių įgyvendinimą ir kompetentingų specialistų samdymą.

Antras iššūkis – žinių ir kompetencijos trūkumas. Ne visos įmonės turi pakankamai išsilavinusią ir patyrusią darbuotojų komandą, kad galėtų atlikti kompleksinį kibernetinio saugumo vertinimą. Šis kompetencijos stygius gali sukelti paviršutiniškas analizes, o tai savo ruožtu veda prie netikslių arba nepakankamai išsamų organizacijos saugumo būvio įvertinimų.

Trečias iššūkis – kintanti ir sudėtinga grėsmių aplinka, dėl kurios įmonėms sunku išlikti atnaujintoms ir pasirengusioms galimiems naujiems iššūkiams. Greitas kibernetinių grėsmių evoliucijos tempo palaikymas reikalauja nuolatinės informacijos aktualizacijos ir sistemų atnaujinimo.

Ketvirta, matomumo ir skaidrumo trūkumas įmonės sistemose gali apsunkinti tikslų organizacijos kibernetinio saugumo padėties įvertinimą. Be aiškaus įsitraukimo ir atskaitomybės visuose lygiuose, negali būti užtikrinta veiksminga duomenų apsauga.

Penkta, organizacijos gali naudoti fragmentuotus ar nenuoseklius kibernetinio saugumo vertinimo metodus, o tai skaldo bendrą įmonės saugumo suvokimą ir trukdo efektyviai sumažinti rizikas.

Siekti, kad šie iššūkiai būtų sėkmingai įveikti, reiškia aiškiai atpažinti juos darbo pradžioje, kaip ir numatyta šio darbo tiksluose bei uždaviniuose. Kruopštus šių aspektų ištyrimas ir įvertinimas neabejotinai gali padėti organizacijoms sukurti patikimą, ilgalaikę ir atsparią kibernetinę saugumo strategiją (Embroker komanda, 2023).

Darbo uždaviniai

1. Išanalizuoti kibernetinio saugumo vertinimo metodikas ir būdus įmonėse
2. Palyginti kibernetinio saugumo vertinimo metodikas ir nustatyti trūkumus bei privalumus
3. Ištirti nuolatinio stiprinimo strategijų veiksmingumą gerinant darbuotojų sąmoningumą ir įsitraukimą į kibernetinį saugumą.

4. Įvertinti ilgalaikį darbuotojų informuotumo apie kibernetinį saugumą ir įsitraukimo tvarumą.
5. Nustatyti veiksnius darančius įtaką kibernetinio saugumo praktikų ilgalaikiam taikymui, siekiant sumažinti rizikas

Darbo objektas - kibernetinio saugumo vertinimo metodikų organizacijos viduje vertinimas ir palyginimas

Tyrimo metodai

1. Gyvi interviu: Šis metodas leidžia rinkti kokybinius duomenis, suteikiant galimybę gauti išsamesnius atsakymus.
2. Apklausa: Apklausa, kurioje yra tiek kiekybiniai (uždari klausimai ir Likerto skalės klausimai), tiek kokybiniai (atviras klausimas) tyrimo elementai, leidžia plačiau suprasti ir giliau išnagrinėti temą.

Duomenų apdorojimo metodai

1. Kokybiniai duomenys: Atsakymus į atvirus klausimus galima bus analizuoti naudojant teminę analizę, kurioje duomenys yra koduojami ir kategorizuojami pagal temas.
2. Kiekybiniai duomenys: Uždarųjų ir Likerto skalės klausimų atsakymus galima bus analizuoti naudojant statistinius metodus. O aprašomosios statistikos (vidurkis, mediana, moda, diapazonas) dėka bus galima apibendrinti duomenis.
3. Mišrūs metodai: Tai gali reikšti abiejų tipų duomenų integravimą siekiant suteikti išsamų tyrimo temos analizę.

1. MOKSLINĖS LITERATŪROS ANALIZĖ

Šiuolaikiniame skaitmeniniame amžiuje kibernetinis saugumas yra labai svarbus asmenims, organizacijoms ir vyriausybėms visame pasaulyje. Vis labiau pasikliaujant technologijomis ir internetu nuo komunikacijos ir pramogų iki bankininkystės ir prekybos, reikia apsaugoti jautrią informaciją ir sistemas nuo kibernetinių grėsmių, tokių kaip įsilaužimas, kenkėjiškos programos ir sukčiavimo atakos. Kibernetinis saugumas padeda užtikrinti duomenų ir sistemų konfidencialumą, vientisumą ir prieinamumą, būtinas pasitikėjimui palaikyti ir apsisaugoti nuo finansinės, reputacijos ir kitokio pobūdžio žalos. Be asmens ir organizacijos turto apsaugos, kibernetinis saugumas taip pat svarbus nacionaliniam saugumui ir pasauliniam stabilumui. Kibernetinės atakos gali turėti didelių pasekmių ir sutrikdyti esmines paslaugas, sugadinti svarbiausią infrastruktūrą ir pažeisti jautrią informaciją. Todėl svarbu, kad asmenys ir organizacijos imtųsi tinkamų priemonių, kad užtikrintų savo buvimą internete ir žinotų apie galimą riziką bei grėsmes, su kuriomis jie gali susidurti. Tai apima stiprių ir unikalių slaptažodžių naudojimą, programinės įrangos ir saugos protokolų atnaujinimą ir atsargumą bendraujant su nepažįstamomis svetainėmis ar asmenimis internete (Toohil, 2023). Kibernetinis saugumas itin svarbus visų dydžių ir pramonės šakų įmonėms. Šiuolaikinėje skaitmeninėje aplinkoje įmonės naudojasi technologijomis ir internetu, vykdydamos įvairią veiklą – nuo bendravimo ir bendradarbiavimo iki rinkodaros ir pardavimo. Dėl to jie yra pažeidžiami įvairių kibernetinių grėsmių, kurios gali pakenkti jautriai informacijai, sutrikdyti veiklą ir pakenkti jų reputacijai bei finansinei būklei.

1.1.1. Kibernetinio saugumo svarbos ir efektyvių vertinimo metodikų poreikio apžvalga

Kibernetinis saugumas yra praktika, skirta apsaugoti kompiuterius, serverius, mobiliuosius įrenginius, elektronines sistemas, tinklus ir duomenis nuo skaitmeninių atakų, vagysčių ir sugadinimo. Šios atakos gali pasireikšti kaip kenkėjiškos programos, išpirkos reikalaujančios programos, sukčiavimo atakos ir kiti metodai, galintys pakenkti sistemos ar jos duomenų konfidencialumui, vientisumui ir prieinamumui. Veiksmingos vertinimo metodikos yra svarbios nustatant sistemos pažeidžiamumą ir trūkumus bei įgyvendinant būtinus apsaugos nuo kibernetinių grėsmių kontrolę. Tai gali apimti tokius dalykus kaip skverbties bandymai, pažeidžiamumo vertinimai ir rizikos vertinimai. Reguliariai testuodamos ir vertindamos kibernetinio saugumo priemonių efektyvumą, organizacijos gali užtikrinti, kad jų sistemos yra saugios ir tinkamai reaguoti į bet kokius galimus incidentus. Kibernetinio saugumo svarbos negalima pervertinti, nes sėkmingos kibernetinės atakos pasekmės gali būti reikšmingos. Tai gali svyruoti nuo finansinių nuostolių ir žalos reputacijai iki jautrios informacijos praradimo ir net žalos asmenims. Didėjant priklausomybei nuo technologijų visuose mūsų gyvenimo aspektuose, svarbu imtis veiksmų, kad apsaugotume save ir

savo sistemas nuo kibernetinių grėsmių. Detalizuojant kibernetinio saugumo svarbą, svarbu paminėti ir darbuotojus, kurie dažniu atveju gali tapti silpniausią grandimi įmonėje, per kur gali ir įvykti įsilaužimas į vidinius įmonės duomenis, tad svarbu paminėti ne tik vidinių sistemų naujinimą ar stiprų kibernetinio saugumo skyrių, tačiau ir edukuoti ir dirbti su visais įmonės darbuotojais, kad pasiekti aukštą bendrą įmonės kibernetinio saugumo lygį (TBC komanda, 2021).

1.1.2. Kibernetinio saugumo svarba įmonėms: auganti reikšmė ir aktualumas

1. Skelbtinos informacijos apsauga: įmonės dažnai saugo ir apdoroja daug neskelbtinų duomenų, įskaitant asmeninę informaciją apie darbuotojus ir klientus, finansinius įrašus ir patentuotą verslo informaciją. Kibernetinis saugumas padeda apsaugoti šiuos duomenis nuo neteisėtos prieigos ar vagystės.

2. Operacijų palaikymas: kibernetinės atakos gali sutrikdyti įmonės veiklą, panaikindamos svetaines, išjungdamos sistemas arba pavogdamos svarbius duomenis. Dėl to gali sumažėti produktyvumas, pajamos ir klientų pasitikėjimas.

3. Finansinių nuostolių vengimas: dėl kibernetinių atakų įmonė gali patirti finansinių nuostolių dėl tiesioginių išlaidų, pvz., teisinių mokesčių ir ištaisymo išlaidų, taip pat netiesioginių išlaidų, tokių kaip verslo praradimas ir žala įmonės reputacijai.

4. Atitikties reikalavimų laikymasis: atsižvelgiant į pramonės šaką, įmonė gali reikalauti laikytis tam tikrų kibernetinio saugumo standartų ir taisyklių, kad būtų užtikrinta neskelbtinų duomenų apsauga. Šių reikalavimų nesilaikymas gali užtraukti baudas ir kitas nuobaudas.

Apskritai investuoti į kibernetinį saugumą yra labai svarbu įmonėms apsaugoti savo turtą, išlaikyti savo veiklą ir išvengti finansinės ir reputacijos žalos. Be galimo finansinio poveikio, įmonės taip pat teisiškai privalo apsaugoti tam tikros rūšies informaciją. Pavyzdžiui, įmonėms, kurios tvarko asmens duomenis, galioja tokie teisės aktai, kaip Bendrasis duomenų apsaugos reglamentas (BDAR) Europos Sąjungoje ir Kalifornijos vartotojų privatumo įstatymas (CCPA) Jungtinėse Valstijose, pagal kuriuos įmonės privalo įgyvendinti tinkamas saugumo priemones, kad apsaugotų asmeninius duomenis (Corallo, Lazoi ir Lezzi, 2022). Apskritai veiksmingas kibernetinis saugumas yra labai svarbus įmonėms, kad jos apsaugotų savo turtą, laikytųsi taisyklių ir išlaikytų klientų bei suinteresuotųjų šalių pasitikėjimą. Tai apima patikimų saugos protokolų įgyvendinimą, darbuotojų mokymą apie geriausią kibernetinio saugumo praktiką ir reguliarų sistemų testavimą bei atnaujinimą, siekiant užtikrinti, kad jos būtų saugios.

1.1.3. Rizikos ir grėsmių mažinimo strategijos: efektyvumo veiksniai

Siekiant sumažinti pavojų ar riziką įmonėje, dažnuose mokymuose yra nurodomos pagrindinės priemonės, kaip apsisaugoti nuo galimo duomenų nutekėjimo ar įsilaužimo į vidines

įmonės aplinkas, analizuojant skirtingus kibernetinio saugumo kursų pavyzdžius buvo galima atsižvelgti į dažniausiai pasikartojančias pastabas tiek darbuotojams, tiek įmonės kibernetinio saugumo specialistams, tad pagrindiniai veiksniai bus suskirstyti į lentelę ir sugrupuoti, pagal taip ar tai skirta įmonės visiems darbuotojams (įskaitant ir pačius kibernetinio saugumo specialistus) ar konkrečiai įmonės kibernetinio saugumo skyriui (1.1 lentelė).

1.1 lentelė. Pagrindiniai veiksniai, kurie turi būti taikomi įmonės darbuotojams, sudaryta darbo autoriaus

Taikyti visiems įmonės darbuotojams	Taikyti įmonės kibernetinio saugumo specialistams
Kibernetinio saugumo mokymai, padedantys atpažinti naujausias tendencijas ir atskirti silpniausias grandis, per kur įvyksta daugiausiai įsilaužimų	Filtrų diegimas elektroninio pašto dėžutėje, siekiant užblokuoti kiek įmanoma daugiau kenkėjiškus pranešimus
Reguliariai kurti atsargines duomenų kopijas ir talpint jas į kelias skirtingas, tačiau gerai apsaugotas laikmenas, jog atakos metu kopijas būtų galima greitai atkurti	Tvirta antivirusinė bei kenkėjiškų programų apsauga
Stiprių, unikalių slaptažodžių keitimas, bei dažnas jų keitimas	Reguliarus programinės įrangos atnaujinimas, sistemų taisymas, siekiant šalint visas rizikas ar žinomus pažeidžiamumus
Dviejų veiksnių autentifikavimas paskyroms apsaugoti	Reguliariai peržiūrėti ir atnaujinti įmonės kibernetinio saugumo politiką ir procedūras

1.1.4. Kibernetinio saugumo vertinimo ypatumai skirtingose ekonominėse srityse: sektorių analizė ir specifiniai iššūkiai

Skirtingų sektorių ar pramonės šakų kibernetinio saugumo vertinimo praktika ar politika gali skirtis, kadangi kiekvienas sektorius turi savitų savybių ar poreikių. Tokios paslaugos, kaip finansinės, sveikatos ar vyriausybinės įmonės saugo ypatingai daug svarbių duomenų, į kurias dažnai, yra bandoma įsilaužti ir nutekinti įmonių duomenų bazėse esama informaciją. Tad, šių įmonių ar sektorių reputacija analizuojant įsilaužimų apsaugą ar kibernetinio saugumo lygį turi būt nepriekaištinga, kadangi šių sektorių įmonės turi didžiausią riziką prarasti daug vartotojų bei nutekinti duomenis, informacija ar turtas turės besąlygiškai didelį nuostolį įmonės gerovei (Cavelty, 2013).

Šių dienų pasaulyje, kuomet vis daugėja kibernetinių išpuolių, atsirado labai svarbi ir pelninga sritis kurti stiprias ir geras kibernetinio saugumo programinės įrangas, kurios gali padėti užmaskuoti vartotojo interneto tikrąjį adresą, ar sukurti specialius interneto vartus, kurie sukurs lyg papildomą spyną, dėl kurios įsilaužti bus tik dar sunkiau. Kibernetinio saugumo pramonėje sukurti produktai, bei pačios įmonės turi turėti tokį pat nepriekaištingą lygį, kadangi bent menkiausia klaida galės padėti įsilaužti lengviau ar dar kitaip pakenkti vartotojui. Sukurta spraga kibernetinio saugumo programoje, galės ne tik padėti lengviau įsilaužti į programos kliento paskyrą, tačiau pridėti ir didžiulę baudą pačiai kibernetinio saugumo įmonei, kadangi prekiauja nepatikima saugumo sistema. Tad nepriklausomai nuo pramonės sektorių, kuriose yra vykdomos pinigų transakcijos ar pinigų laikymas, sveikatos priežiūros platformos, kuriose yra saugomos klientų sveikatos duomenis ar mažmeninės prekybos, kur yra talpinami ir saugomi kreditinių kortelių duomenis visose šiuose ir panašiose srityse yra vienas ir svarbus ir bendras dalykas, jog kibernetinio saugumo lygis turi būti nepriekaištingas, tad tokių įmonių savininkai ne tik turi investuoti į išmanias ir naujinamas pagalbines programas apsisaugoti ir saugoti duomenis, tačiau ir daug dėmesio skirti ir įmonės darbuotojams, juos edukuoti ir pritaikyti tinkamiausius mokymus ir pavyzdžius, kad darbo metu nepriartėtų prie nutekinimo ar įsilaužimo atakos.

1.1.5. Kibernetinio saugumo tyrimo spragos: būtinybės ir prioritetai tolesnei analizei

Analizuojant ir vertinant įvairius šaltinius galima atkreipti dėmesį į dažniausiai pasikartojančias rizikas ar grėsmes, kurios gali pakenkti organizacijų saugumo lygiui ar šių dienų pasaulyje yra susiduriama dažniausiai. Šiuo metu pati opiausia problema yra – Darbuotojų ne motyvacija domėtis kibernetiniu saugumu ar neefektyvus mokymų kursai, kurie nepadeda įmonėms pakelti ar užtikrinti aukštą kibernetinį saugumą įmonėje.

Darbuotojų ne noras mokytis ypač juntamas, kadangi trūksta suinteresuotumo ir sąmoningumo apie kibernetinės saugos svarbą. Tai sukelia paviršutinišką požiūrį bendrai į saugos politiką ar procedūras, nes tokie darbuotojai nelaiko kibernetinio saugumo esminiu savo darbo aspektu. Tokie scenarijai dažnai vyrauja tarp žmonių, kurie neturi nieko bendro su informacinių technologijų išsilavinimu, nes nėra plačiai pasidomėję, kokią didelę grėsmę gali sukelti vienas ar kitas atmestinai perskaitytas ar atidarytas elektroninis laiškas iš nepažįstamo adresato. Tačiau ši opi problema gali būti sudaryta iš kitos ne ką šiuo metu mažiau svarbios problemos – neefektyvus ir neaiškūs mokymų kursai įmonės darbuotojams. Mokymų kursai, kurie nesugeba pritraukti darbuotojų dėmesio ar neatsižvelgia į darbuotojų įvarius lygius ar poreikius, gali būti mažai naudingi. Tai sukelia žemą mokymų įsisavinimą ir pritaikymą praktikoje kasdieniniame gyvenime. Taip pat, šių dienų įmonėse pastebima tendencija, kuomet į kibernetinį saugumą yra investuojama ne tik laiko, bet ir lėšų tik įvykus kibernetiniam įsilaužimui, o iki tol niekas nesistengia ir nekreipia dėmesio į galbūt jau pasenusią ir programinę įranga įmonėje. Nenaudojimas naujausių saugumo įrankių ar dažnų atnaujinimų nedarymas gali palikti sistemas ir darbuotojus pažeidžiamus prieš naujausias kibernetines grėsmes. Pasenusi programinė įranga gali neturėti būtinų saugumo patobulinimų, kurie reikalingi siekiant išvengti naujų atakos metodų ir tipų (Dilmegani, 2023).

Tad, siekiant mažinti kibernetinio saugumo spragas ar rizikas, būtina atkreipti dėmesį į įmonės programinę įrangą, tačiau tuo labiau į darbuotojų informatyvumą ir ištirti kibernetinį saugumą įmonėse. Būtina kurti patrauklius ir prasmingus mokymus, bei skirti lėšų ne tik po įvykusios kibernetinės atakos, o reguliariai naujinti ir prižiūrėti įmonės programinę įrangą.

1.2. Pagrindiniai metodai tiriant kibernetinį saugumą įmonėse

Detalizuojant ir norint tirti kibernetinį saugumą įmonėje, tai galima padaryti keliais skirtingais būdais. Pats populiariausias ir dažniausiai taikomas praktikoje yra apklausos ir atvejų analizės metodas.

Apklausos ir atvejų analizės metodas apima duomenų rinkimą iš įmonės darbuotojų pasitelkiant apklausą ir interviu. Apklausos gali padėti surinkti informaciją apie bendrą situaciją įmonėje ar siekiant patikrinti kaip kiekvienas įmonės darbuotojas vertina savo žinias, požiūrį ar procedūras kibernetinio saugumo klausimais. Interviu galėtų būt skirtas konkrečiai pačios įmonės

specialistams, kurie yra atsakingi už įmonės kibernetinį saugumą. Taip būtų pritaikomas atvejo analizės metodas, kuriame pasitelkiami duomenis iš jau sudaryto klausimyno ir pasitelkiant duomenis iš jau atsakytų apklausos atsakymų sukurti ir vykdyti diskusiją, taip siekiant iki galo suprasti ir įvertinti įmonės kibernetinio saugumo lygį.

Dar vienas būdas įvertinti įmonės kibernetinio saugumo lygį yra pasitelkiant eksperimentą ar modelio diegimo metodas. Įmonės atstovas, kuriam priklauso vertinti įmonės saugumo lygį, gali atlikti eksperimentą, kad patikrintų skirtingų saugumo priemonių efektyvumą arba suprastų, kaip darbuotojai reaguoja į skirtingas kibernetinio saugumo mokymo programas. Modeliavimas gali būt naudojamas nustatant skirtingų saugumo priemonių efektyvumui patikrinti. Įdiegus specialų modelį įmonėje ar pritaikius eksperimentą yra atliekama nuodugni analizė ir vertinimas įmonės, taip nustatomi saugumo priemonių efektyvumas, nustatomas pažeidžiamumas bei darbuotojų reakciją į naują modelį ar mokymo programas.

1.2.1. Apklausos ir interviu modelis

Apklausų ir interviu metodas kibernetinio saugumo srityje suteikia galimybę giliai pažvelgti į darbuotojų suvokimą ir elgesį, atliekant vertingą kibernetinio saugumo rizikos ir sąmoningumo analizę. Tiesioginiai pokalbiai ir struktūrizuotos apklausos patenka į išsamių atsakymų sferą, kur negali nuskaityti automatizuotos sistemos ar algoritmai. Pagrindiniai privalomai nurodyti straipsniuose yra aprašyti lentelėje (1.2 lentelė).

1.2 lentelė. Pagrindiniai privalumai apklausos ir interviu metodo, sudaryta darbo autoriaus

Privalumas	Paaiškinimas
Tiesioginis Atsiliepimų Surinkimas	Pateikia detalių duomenų apie darbuotojų požiūrį ir elgesį
Operatyvumas	Greita reakcija į grėsmes leidžia nedelsiant įgyvendinti saugumo pakeitimus
Lankstumas	Klausimų pritaikymas pagal organizacijos poreikius leidžia nagrinėti specifinius rizikos aspektus
Ekonomiškumas	Įgyvendinimo kaštai yra mažesni, palyginti su kitomis, daugiau resursų reikalaujančiomis metodikomis

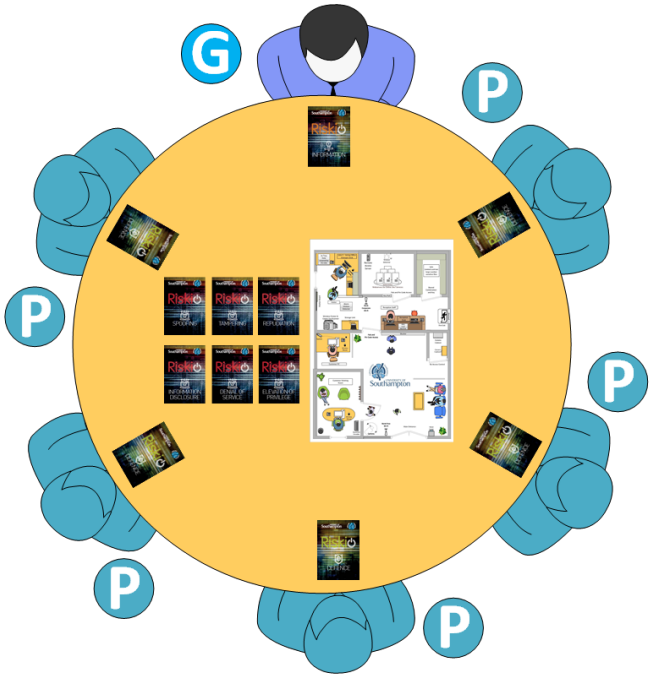
Mokslinėje literatūroje apklausų ir interviu metodas yra plačiai pripažintas ir naudojamas įmonės kibernetinio saugumo įvertinimui. Pavyzdžiui, straipsnis "Human Factors in Phishing Attacks: A Systematic Literature Review " (Desolda, Ferro, Marella, Tiziana ir Costabile, 2021) per interviu metodus parodė, kaip darbuotojų suvokimas apie sukčiavimo atakas ir jų reakcijos į sociotechnines schemas gali būti pagrindinis veiksnys formuojant efektyvias gynybos strategijas. Tokie tyrimai ne tik patvirtina apklausų ir interviu metodų svarbą identifikuojant organizacinius saugumo iššūkius, bet taip pat pateikia patikimus duomenis, kurie gali padėti organizacijoms geriau suprasti ir spręsti kibernetinio saugumo problemas.

1.2.2. Apklausos ir interviu modelio išvados

Apklausų ir interviu metodas pripažintas kaip vienas iš labiausiai informacinės įžvalgos teikiančių metodų įmonės kibernetinio saugumo vertinimui. Šis metodas, remiantis moksliniais šaltiniais, ne tik kad efektyvus, bet ir suteikia organizacijoms galimybę operatyviai tobulinti savo saugumo būklę, atsižvelgiant į asmeninę darbuotojų patirtį ir požiūrį. Todel apklausų ir interviu metodas rekomenduojamas kaip pirmenybinis įrankis saugumo spragų identifikavimui ir strateginių sprendimų formavimui remiantis tikrovės atkartojimu.

1.2.3. Eksperimento ir modeliavimo modelis

Modeliavimo metodas yra vertingas įrankis įmonės kibernetinio saugumo vertinimui, kadangi leidžia sistemingai analizuoti ir suprasti saugumo rizikas bei procesus. Jis gali būti įgyvendintas per įvairias formas, tokias kaip "Riskio" stalo žaidimas, kuris yra sukuriamas siekiant šviesti darbuotojus apie rizikos valdymą per interaktyvią ir įtraukiančią patirtį, taip pat padedant jiems suprasti saugumo svarbą ir imtis konkrečių veiksmų jų darbo aplinkoje (Hart, Margheri, Paci ir Sassone, 2020) (1.1 paveikslas).



1.1 pav. „Riskio“ stalo žaidimo pavyzdys, pagal Hart, Margheri, Paci ir Sassone, 2020

Eksperimento metodas, panaudojant "Kirkpatrick‘s“ vertinimo modelį, taip pat yra svarbus kibernetinio saugumo mokymų efektyvumo įvertinimui. Šis modelis padeda vertinti ir tobulinti saugumo mokymų programas, analizuodamas keturis lygius: reakcija, mokymasis, elgesys ir rezultatai (1.2 lentelė), kas suteikia aiškią mokymo programų grąžos viziją. Be to, įrodymais grįstos kenkėjiškų programų ataskaitos gali padėti stiprinti įmonės darbuotojų sugebėjimus ir sąmoningumą,

pateikiant jiems realias grėsmes ir skatinant laikytis saugumo praktikų (Khan, Ikram, Murtaza ir Javed, 2022).

1.3 lentelė. „Kirkpatrick“ vertinimo modelio planas, pagal Ivan Andreev, 2023

„Kirkpatrick“ vertinimo modelis		
Lygis	Procesas	Aprašymas
Pirmas lygis	Reakcija	Šis lygis matuoja besimokančiojo reakciją į mokymą, įskaitant bendrą pasitenkinimą ir įsitraukimą į medžiagą
Antras lygis	Mokymas	Šis lygis įvertina tai, ko praktikantas išmoko per mokymus, įskaitant žinias ir įgūdžius
Trečias lygis	Elgesys	Šis lygis įvertina, ar stažuotojas pritaikė tai, ko išmoko per mokymus, savo darbe ir ar dėl to pasikeitė jo elgesys
Ketvirtas lygis	Rezultatai	Šis lygis įvertina mokymo poveikį mokinio darbui ir visai organizacijai. Tai apima tokias priemones kaip našumas, kokybė ir klientų pasitenkinimas

Tačiau analizuojant ir vertinant šiuos vertinimo modelius, pastebėtos tokios pat grėsmės ar trūkumai, dėl kurių šie metodai nėra visais vertinimo atvejais patys tiksliausi. Lentelėje yra nurodomi pagrindiniai iššūkiai ir trūkumai.

1.4 lentelė. Pagrindiniai trūkumai eksperimentinio ir modelialiavimo modelių, sudaryta darbo autoriaus

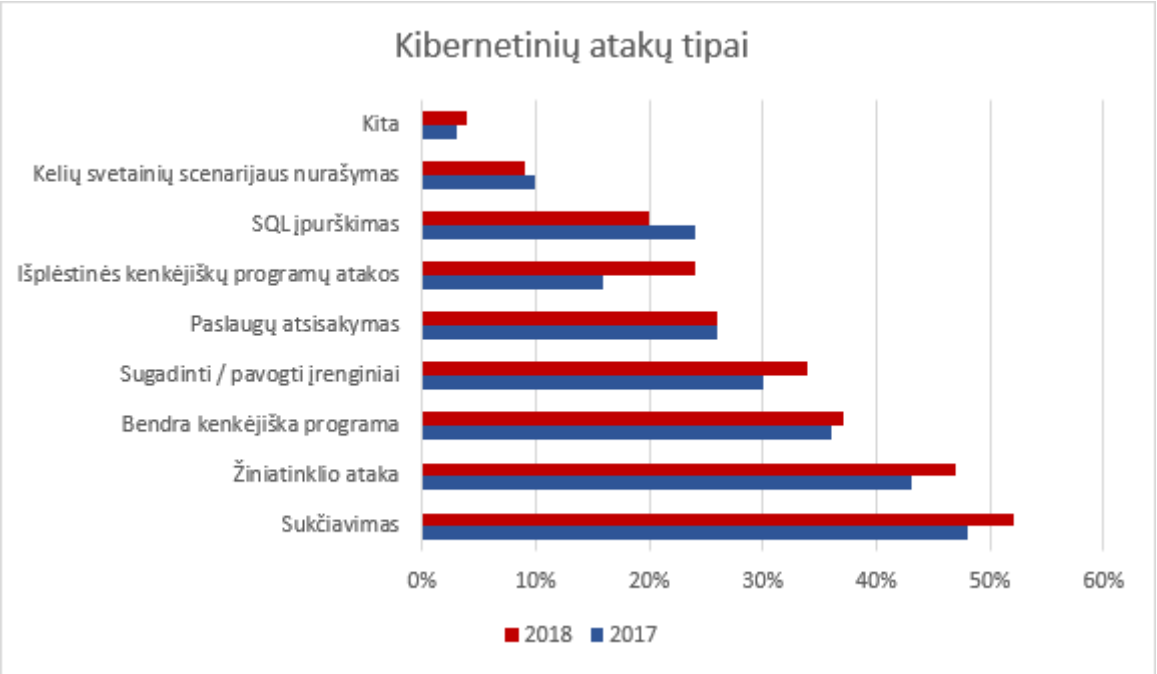
Trūkumas	Paaiškinimas
Laiko ir išteklių sąnaudos	Gali būti reikalingos didelės investicijos į šių metodų diegimą ir palaikymą
Praktiškumo trūkumas	Kartais sudėtinga tiksliai atkartoti realias grėsmes naudojant modeliavimo scenarijus
Kintamųjų kontrolė ir elgesio pokyčiai	Realiose situacijose susiduriama su daugybe nepastovumų, o eksperimentiniai metodai gali nesuteikti akivaizdžių ir išmatuojamų elgesio pokyčių
Bendravimo apribojimai	Dalis mokymų gali neleisti darbuotojams tiesiogiai bendrauti su saugumo ekspertais, kurie galėtų suteikti reikiamą pagalbą

1.2.4. Eksperimento arba modeliavimo metodo išvados

Lyginant šiuos du skirtingus įmonės kibernetinio saugumo vertinimo metodus, šiuo metu pranašesnis ir naudingesnis yra apklausos ir atvejų analizės metodas. Atvejo analizės metodai apima nuodugnią konkretaus asmens, grupės ar organizacijos analizę, siekiant ištirti konkrečią problemą ar reiškinį. Taikant tiek apklausos, tiek atvejo analizės metodus tame pačiame tyrime galima gauti išsamesnį ir nuodugnesnį tyrimo problemos supratimą. Pavyzdžiui, apklausa galėtų būti naudojama duomenims iš didesnės imties asmenų ar organizacijų rinkti, o atvejo analizė galėtų būti naudojama norint išsamiau išnagrinėti konkretų kontekstą ir konkrečios organizacijos iššūkius. Svarbu atidžiai sudaryti klausimyną ir tyrimo tikslus sprendžiant, kokius metodus naudoti, ir užtikrinti, kad metodai būtų tinkami ir papildytų vienas kitą. Taip pat svarbu aiškiai aprašyti ir pagrįsti kelių metodų naudojimą straipsnio tyrimo planavimo ir metodologijos skyriuose. Šių metodų naudojimas įmonėse parodė, kad jie teigiamai veikia darbuotojų požiūrį ir sąmoningumą apie kibernetinį saugumą, tačiau prie jų taip pat susiję tam tikri apribojimai. Modeliavimas ir eksperimentai suteikia svarbią pradinę platformą saugumo supratimo didinimui, tačiau ne visada yra patys efektyviausi. Palyginus su apklausų ir interviu metodu, pastarieji leidžia gauti greitą ir tikslią dabartinės situacijos įmonėje vaizdą. Jie yra ekonomiškai efektyvesni, leidžia operatyviai reaguoti į atsiradusius saugumo iššūkius ir yra labai tinkami individualizuotų saugumo strategijų kūrimui. Apklausos ir interviu gali būti efektyvesnis pasirinkimas, suteikiantis gilesnį įsivardijimą ir leidžiantis greičiau pradėti būtinus organizacinės saugumo patobulinimus.

1.3. Mažų arba vidutinių įmonių kibernetinis atakavimas

Mokslininkai Hayesas ir Bodhani yra nustatę, kad mažos ir vidutinės įmonės (MVĮ) vis dažniau susiduria su kibernetinėmis grėsmėmis dėl jų pažeidžiamumo. Kibernetiniai nusikaltėliai, įskaitant tuos, kurie yra nauji ir mažiau patyrę, dažnai taikosi į lengvus taikinius, įskaitant MVĮ (Hayes ir Bodhani, 2013). Remiantis „Verizon“ 2020 m. ataskaita, kibernetinės atakos yra plačiai paplitusios ir paveikia visas organizacijas, nepaisant jų dydžio, pramonės ar sektoriaus. Tačiau sveikatos priežiūros paslaugų tiekėjai ir su finansais susijusios įmonės yra labiausiai orientuotos visame pasaulyje. Akademinės bendruomenės ir pramonės ataskaitos rodo, kad dažniausiai MVĮ susiduriama su kibernetinėmis atakomis: socialinė inžinerija (pvz., sukčiavimas), įsilaužimas (pvz., pavogti kredencialai, duomenų vagystės), kenkėjiškos programos (pvz., išpirkos reikalaujančios programos), piktnaudžiavimas (pvz., piktybinė prekyba viešai neatskleista informacija), interneto atakos, ir el. pašto tiekimo grandinės atakų (Pritam, 2020). Kibernetinių atakų tikslesnė statistika yra nurodomo paveiksle 1.2, kuriame galima atkreipti dėmesį į tų metų ryškiausias tendencijas.



1.2 pav. Mažų-vidutinių įmonių atakų statistika, pagal „Verizon“ 2020 statistika

Duomenų pažeidimo atveju IT ištekliai visame pasaulyje ir visose organizacijose sutelkiami į taikomųjų programų serverius, ypač dėl to, kad vis dažniau naudojamos žiniatinklio programos ir debesies platformos. Kitas dažniausiai naudojamas turtas yra vartotojų staliniai ir nešiojamieji kompiuteriai, el. pašto serveriai, duomenų bazių serveriai ir patys galutiniai vartotojai. Kai kurie mokslininkai nustatė, kad mobilieji įrenginiai ir kiti daiktų interneto (IoT) įrenginiai yra ypač pažeidžiami mažų ir vidutinių įmonių aplinkoje, nes jie gali būti pažeisti ir naudojami neteisėtai prieigai prie tinklo. Neapsaugoti internetiniai įrenginiai taip pat gali būti ginkluoti siekiant pradėti sudėtingas atakas prieš kitas organizacijas, pavyzdžiui, priverstinai prisijungti prie botnetų ir dalyvauti internetinėse paskirstytose paslaugų atsisakymo (DDoS) atakose. Remiantis ataskaitomis, 70 % pastarojo meto pasaulinių duomenų pažeidimų įvykdė išorės veikėjai, t. y. užpuolikai iš išorės. Beveik pusė šių išpuolių buvo susiję su įsilaužimu arba neteisėtos prieigos gavimu. Didžioji dauguma (86 %) šių išpuolių buvo finansiškai motyvuoti, tačiau duomenų pažeidimus ir kibernetinius incidentus taip pat gali lemti kiti veiksniai, tokie kaip ideologija, pyktis, šnipinėjimas, valstybės rėmimas ir žmogiškosios klaidos (Zorabedian, 2023).

Kibernetinio saugumo įmonės naudojasi pažangiomis technologijomis ir patirtimi, kad apsaugotų MVĮ nuo daugybės grėsmių. Šių įmonių siūlomos paslaugos apima pažeidžiamumo vertinimą, valdomas saugos paslaugas, darbuotojų mokymo ir informavimo programas, reagavimo į incidentus planavimą ir patikimų kibernetinio saugumo sistemų, tokių, kaip rekomenduoja NIST kibernetinio saugumo sistema, diegimą, bet tuo neapsiribojant (Dawkins ir Jacobs, 2023).

Be to, kibernetinio saugumo įmonės taip pat daug dėmesio skiria įperkamų ir keičiamo dydžio sprendimų kūrimui, kurie gali patenkinti ribotą MVĮ biudžetą nepakenkiant saugumo priemonių

veiksmingumui. Tai apima debesies pagrindu veikiančias saugos platformas, kurios siūlo realiojo laiko grėsmių žvalgybą ir automatinio reagavimo galimybes. Teikdamos aktyvių gynybos mechanizmų ir reaktyvaus incidentų valdymo derinį, kibernetinio saugumo įmonės padeda MVĮ ugdyti atsparumą kibernetinėms grėsmėms.

Pavyzdžiui, kaip pranešė „Verizon“ savo 2020 m. duomenų pažeidimo tyrimų ataskaitoje, kibernetinių atakų pažeidžiamos ne tik didelės įmonės, bet ir visų dydžių organizacijos. Tai paskatino kibernetinio saugumo įmones diegti naujoves ir kurti visapusiškus saugos sprendimus, galinčius aptarnauti platų klientų ratą. Be to, dirbtinio intelekto (AI) ir mašininio mokymosi (ML) naudojimas padidina šių įmonių gebėjimą greičiau ir tiksliau nei bet kada anksčiau aptikti grėsmes ir į jas reaguoti.

1.3.2. Kibernetinio saugos sistemos

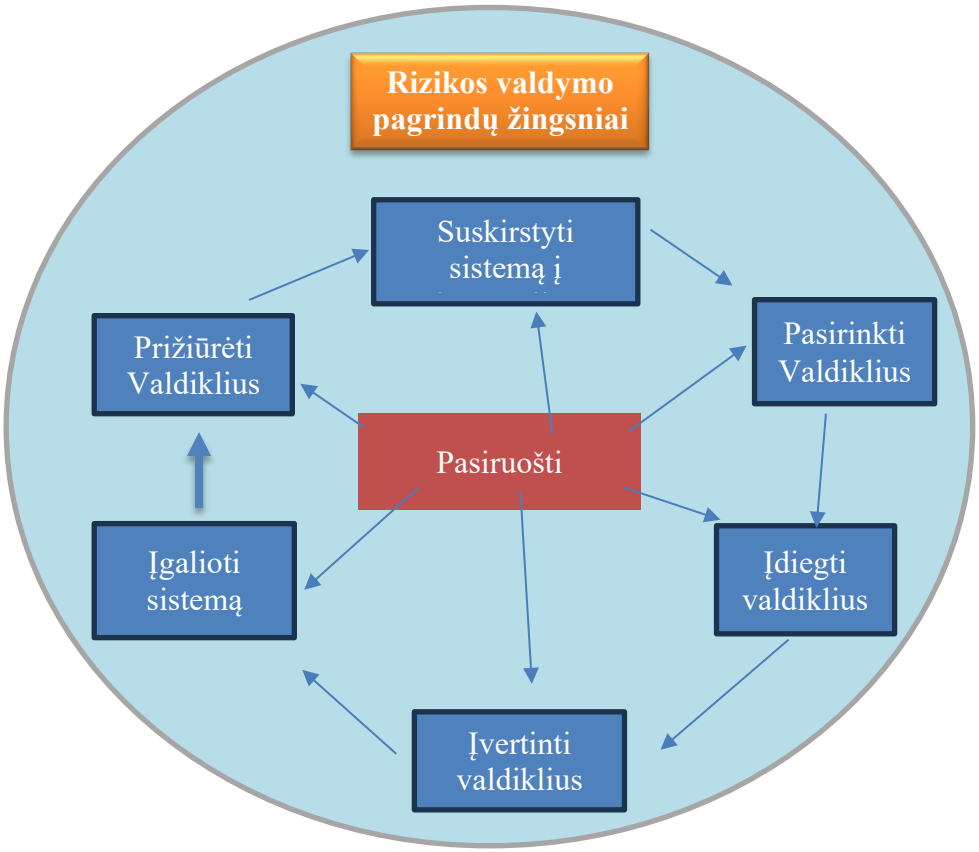
Kibernetinio saugumo sistemos yra technologijų, procesų ir praktikos rinkinys, skirtas apsaugoti tinklus, įrenginius ir duomenis nuo kibernetinių grėsmių. Šios grėsmės gali būti kenkėjiškos programos, išpirkos reikalaujančios programos, sukčiavimo atakos ir kitos elektroninių nusikaltimų formos. Kibernetinio saugumo sistemos yra skirtos užkirsti kelią šioms grėsmėms arba jas sušvelninti ir gali apimti įvairius komponentus. Yra daugybė skirtingų sistemų ir standartų, kuriais organizacijos gali vadovautis kurdamos ir įgyvendindamos savo kibernetinio saugumo sistemas. NIST yra pagrindinė įranga, kurios pagalba galima užtikrinti įmonėje aukštą kibernetinio saugumo lygį. Nacionalinis standartų ir technologijų institutas (NIST) turi daugybę modelių metodų, kurie naudojami įvairioms sistemoms ir procesams reprezentuoti ir analizuoti (Polk, 2017) . Kai kurie NIST modelio metodų pavyzdžiai:

1. NIST Kibernetinio saugumo sistema (CSF) yra modelis, suteikiantis bendrą kalbą ir požiūrį į kibernetinio saugumo pavojų supratimą ir valdymą. Tai apima standartų, gairių ir praktikos, kurias organizacijos gali naudoti vertindamos ir patobulindamos savo kibernetinio saugumo laikyseną, rinkinį. Plačiau lentelėje apačioje (1.5 lentelė).

1.5 lentelė. NIST CSF modelio detalus planas, pagal NIST 2014

Gebėjimas	Apibūdinimas
Identifikuoti	Kokį procesą ir turtą reikia apsaugoti?
Apsaugoti	Įgyvendinti atitinkamas apsaugos priemones, užtikrinančias įmonės turto apsaugą
Aptikti	Įdiegti tinkamus mechanizmus kibernetinio saugumo incidentams nustatyti
Atsakyti	Sukurti kibernetinio saugumo įvykių poveikio mažinimo metodus
Atsigauti	Įdiegti atitinkamus procesus, kad arkurti pajėgumus ir paslaugas, sutrikusias dėl kibernetinio saugumo įvykių

2. NIST rizikos valdymo sistema (RMF) yra modelis, nubrėžiantis informacinių sistemų ir duomenų rizikos vertinimo, prioritetų nustatymo ir mažinimo procesą. Tai apima veiksmų, kuriuos organizacijos gali atlikti, kad nustatytų, įvertintų ir sumažintų savo informacinių sistemų riziką, rinkinį, platesnis modelis nurodytas paveiksle 1.3.



1.3 pav. NIST detalus RMF modelis, pagal NIST 2022

3. NIST Kibernetinio saugumo darbo jėgos sistema (NCWF) yra modelis, suteikiantis bendrą kalbą ir struktūrą, skirtą suprasti ir tobulinti kibernetinio saugumo darbo jėgą. Tai apima standartų, gairių ir praktikos, kurias organizacijos gali naudoti vertindamos ir tobulindamos savo kibernetinio saugumo darbo jėgą, rinkinį.
4. NIST kompiuterių saugos išteklių centras (CSRC) yra išteklių centras, kuriame yra įvairių įrankių ir išteklių, padedančių organizacijoms pagerinti kibernetinio saugumo laikyseną, įskaitant pavyzdinius saugumo rizikos vertinimo metodus, reagavimo į incidentus planavimą ir kt.

   NIST CSF yra sistema, kuri suteikia bendrą kalbą ir požiūrį į kibernetinio saugumo pavojų supratimą ir valdymą. Tai apima standartų, gairių ir praktikos, kurias organizacijos gali naudoti vertindamos ir patobulindamos savo kibernetinio saugumo laikyseną, rinkinį. CSF sukurtas taip, kad būtų lankstus ir pritaikomas, ir gali būti pritaikytas, kad atitiktų organizacijos poreikius ir rizikos profilį. NIST RMF yra procesas, padedantis organizacijoms įvertinti, nustatyti prioritetus ir sumažinti jų informacinių sistemų ir duomenų riziką. Tai apima veiksmų, kuriuos organizacijos gali atlikti, kad nustatytų, įvertintų ir sumažintų savo informacinių sistemų riziką, rinkinį. RMF sukurtas naudoti kartu su kitais rizikos valdymo standartais ir gairėmis, pvz., ISO 27001 ir CSF, siekiant pateikti visapusišką rizikos valdymo metodą. NIST NCWF yra sistema, kuri suteikia bendrą kalbą ir

struktūrą, skirtą suprasti ir tobulinti kibernetinio saugumo darbo jėgą. Tai apima standartų, gairių ir praktikos, kurias organizacijos gali naudoti vertindamos ir tobulindamos savo kibernetinio saugumo darbo jėgą, rinkinį. NCWF sukurta siekiant padėti organizacijoms nustatyti žinias, įgūdžius ir gebėjimus, kurių turi turėti jų kibernetinio saugumo darbuotojai, ir pateikti gaires, kaip sukurti ir išlaikyti kvalifikuotą ir veiksmingą kibernetinio saugumo darbo jėgą. NIST CSRC yra išteklių centras, teikiantis įvairių įrankių ir išteklių, padedančių organizacijoms pagerinti kibernetinio saugumo padėtį. Tai apima daugybę išteklių, tokių kaip rekomendaciniai dokumentai, įrankiai ir geriausios praktikos pavyzdžiai, skirti padėti organizacijoms įvertinti ir pagerinti savo kibernetinio saugumo padėtį. CSRC taip pat teikia informaciją apie NIST kibernetinio saugumo tyrimų ir plėtros programas ir yra informacijos apie kibernetinio saugumo standartus, gaires ir praktikos centras.

1.3.3. Mažo-vidutinio ir didelių didžių įmonių palyginimas

Kibernetinės grėsmės nediskriminuoja pagal organizacijos dydį, o tai reiškia, kad mažos ir vidutinės įmonės (MVĮ) yra tokios pat pažeidžiamos šių grėsmių kaip ir didelės organizacijos. Nors didelės įmonės gali turėti didesnį atakų plotą ir daugiau išteklių kontrolės priemonėms įgyvendinti, joms taip pat gali būti sunku veiksmingai valdyti kibernetinę riziką, nes sunku aiškiai išreikšti, priartėti ir veikti. Be to, jiems gali būti sunku šviesti ir mokyti savo darbuotojus kibernetinio saugumo klausimais. MVĮ pranašumas gali būti, kad yra mažos ir judrios, turi lankstesnes IT priemones, tačiau jos taip pat linkusios mažiau investuoti į kibernetinį saugumą ir gali patirti proporcingai didesnes išlaidas sėkmingos kibernetinės atakos atveju. Tyrimai parodė, kad kibernetinė rizika kelia susirūpinimą tiek didelėms, tiek mažoms organizacijoms ir kad abiem gali būti sunku veiksmingai valdyti šią riziką. Šalyse, kuriose mažos įmonės vaidina svarbų vaidmenį ekonomimoje, pvz., Australijoje, didelių visuomenės sluoksnių finansinei gerovei gali turėti įtakos kibernetinės atakos prieš verslo sektorių, pakertančios pasitikėjimą elektronine prekyba, prekyba ir apskritai ekonomika.

1.4. Mažų arba vidutinių įmonių kibernetinio saugumo vertinimas

Mažų ir vidutinių įmonių (MVĮ) kibernetinio saugumo įvertinimas yra svarbi užduotis, nes MVĮ dažnai susiduria su kibernetinėmis grėsmėmis ir gali būti pažeidžiamos dėl duomenų pažeidimų ir kitų saugumo incidentų. Šios yra iš mažiausiai subrendusių ir labiausiai pažeidžiamų kibernetinio saugumo rizikos ir atsparumo požiūriu.

Moksliniame straipsynje „Calculated risk? A cybersecurity evaluation tool for SMEs“ aprašė metodiką, remiantis Nacionalinio Standartų Ir Technologijų Instituto (NIST) kibernetinio saugumo sistemą (CSF), tačiau ši neatitinka visų poreikių, tad buvo sukurta novatoriška MVĮ kibernetinio saugumo vertinimo įrankį (CET), kuri yra internetinė apklausa, sudaryta iš 35 klausimų, kuri buvo

išsiųsta 50 IT lyderių, daugiausia architektūros, inžinerijos ir statybos organizacijų MVĮ, kurios dažnai bendradarbiauja su pramonės tendencijomis. (Benz ir Chatterjee, 2020).

Visi 35 klausimai buvo sugrupuoti pagal keturias pagrindines NIST sistemos kategorijas:

1. Kur mūsų įmonė susiduria su rimta kibernetinio saugumo rizika?
2. Koks yra priimtinas rizikos lygis?
3. Kaip mes lyginame su kitais savo industrija?
4. Ką galime padaryti, kad patobulintume tose srityse, kuriose mes neatitinkame standartų?

Bendradarbiaujant su MVĮ organizacijomis yra susiduriama su daug problemų, vieną iš jų yra tą, jog ne visos vertinimo sistemos yra tinkamos. Daugelį būdų yra sunku interpretuoti ar net per brangu jas įdiegti. Tad remiantis šiomis priežastimis yra suprantama, kad ne visi vertinimo metodai yra leistini ir naudingi MVĮ tipo įmonėmis. Šiame straipsnyje autoriai pristatė tvirtą pagrindą turinčia vertinimo bei rekomendacijų sistemą. Vertinimas buvo sudarytas iš trijų skirtingų etapų. Pirmame buvo išsiunčiama apklausa internetu ir tikimąsi gauti atsakymus iš visų IT lyderių. Surinkus visus atsakymus buvo sukurta vertinimo sistema, kurioje autorius paskaičiavo visų vidutinį brandos balą, o pamačius spragas-buvo papildomai pridėta ir rekomendacija. CET metodika ir įrankis pateikia veiksmingų rekomendacijų dėl kiekvieno galimo spraga. Šios rekomendacijos yra pagrįstos 10 metų MVĮ IT saugumo patirtimi, literatūros apžvalga ir kibernetinio saugumo pramonės bei akademinės bendruomenės ekspertų atsiliepimais. Siekdamas gauti didžiausią naudą iš CET rekomendacijų ataskaitos, IT vadovas turi įvertinti nustatytas rizikas ir siūlomas rekomendacijas bei sudaryti planą, kaip nustatyti prioritetus ir įgyvendinti tinkamiausius patobulinimus. Ši metodika ne tik padės nustatyti stipriąsias ir silpnąsias puses, bet ir pateiks geriausios praktikos rekomendacijas, kaip veiksmingai pašalinti saugumo spragas.

Įdiegus šią vertinimo sistemą IT vadovai greit gali sužinoti ir įvertinti:

1. Nustatyti didžiausius jų pažeidžiamumus;
2. Palyginkite jų brandą su bendraamžių branda dėl standartinių priemonių rinkinio;
3. Pasirinkite vertingiausias tobulinimo pastangas.

Nors ir apklausa buvo paprasta ir lengvai prieinama visiems išsiustiems vadovams, tačiau atlikus kelių tyrimų analizę buvo galima pastebėti, kad apklausos retu atveju gauna didelį susidomėjimą iš įmonių. Pavyzdžiui Šios apklausos metu buvo išsiųsta kvietimų virš 50, tačiau apklausoje dalyvavo tik 52% vadovų iš kurių tik 16 rodė didelį susidomėjimą apklausos rezultatais ir rekomendacijas pritaikė darbinėje aplinkoje, kurias pasiūlė CET ataskaita. Tad iš to galime spręsti,

jog nors ir MVĮ yra labiausiai pažeidžiamos ir joms ypač nepatartina ilgai delsti, norint apsaugoti gerai esamą įmonę, tačiau apklausos / interviu tipo vertinimas yra mažai kam aktualus ir įdomus.

Toliau tiriant MVĮ galima pastebėti, kad tendencija nesikeičia ir išlieka tą pati „A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations“ mažų ir vidutinių įmonių kibernetinio saugumo tyrinėtojai, rinkdami duomenis, dažnai remiasi literatūros apžvalgomis ir dažnai taiko kokybinius metodus. Tai rodo, kad šioje srityje trūksta originalių tyrimų, tokių kaip eksperimentai, kuriuose naudojami įvairūs duomenų rinkimo būdai, įskaitant klausimynus, interviu, turinio analizę ir stebėjimus. Nors šioje jautrioje srityje atlikti originalius tyrimus gali būti sunku, pageidautina giliau suprasti problemas ir geresnius sprendimus. Mokslininkams taip pat gali būti sudėtinga atlikti literatūros apžvalgas, kai trūksta atitinkamos literatūros, ypač vietiniame kontekste. Remiantis autoriaus išvadomis, daug tyrimų buvo sutelkta į mažų ir vidutinių įmonių (MVĮ) saugumo strategijas ir politiką, tačiau atrodo, kad trūksta tyrimų apie praktinį šių priemonių įgyvendinimą, aptikimą, reagavimą ir atkūrimą. strategijos. Tai dar labiau padeda suprasti, jog MVĮ tipo organizacijomis reikia dažno mokymo, eksperimentų diegimų, kadangi nors ir apklausoje dalyvauja vadovų, tačiau nieks nepasisemia žinių ir nepritaiko jų darbinėje aplinkoje (Chidukwani, Zander ir Koutsakis, 2022).

Visi NIST modeliai pradedami nuo įvairių įmonės apklausų ir interviu, kurios metu yra stengiamasi kuo įmanoma išgauti daugiau informacijos ir ieškoti problemų ir lūžio taškų, kuriuos reiktų stiprinti. Ypač tiriant mažų-vidutinių įmonių kibernetinį saugumą, pastebima problema, kuomet NIST dažniausia įdiegia jau į esamą sistemą patobulinimus, todėl jeigu įmonėje kibernetinio saugumo lygis yra tragiškoje situacijoje, tai gali užimti be galo daug laiko bei pinigų. Analizuojant mažų-vidutinių įmonių kibernetinio saugumo lygį pasitelkiant / diegiant NIST susiduriama su problema, kuomet nors ir NIST pagalba yra pasiekiami sprendimo būdai bei situacijos valdymas, tačiau niekas nekalba apie kasdieninį darbuotojų ugdymą bei įsitraukimą į kibernetinį saugumą. Kaip ir šiek tiek anksčiau pateiktoje analizėje iš 50 išsiųstų apklausų NIST siūlomus pakeitimus panaudojo aplinkoje tik apie 16 IT vadovų.

Išanalizavus ir kitus NIST metodus išryškėja pagrindinės problemos, tokios kaip: sudėtingumas, išteklių apribojimai, informuotumo trūkumas, standartizacijos trūkumas, kultūrinės kliūtys.

Apibendrinant galima teigti, nors ir daugelis mažo – vidutinio dydžio kompanijų naudojasi NIST metodais, tačiau išsamiau atlikus analizę galima pastebėti nemažai trūkumų. Vienas iš pagrindinių trūkumų yra, jog į interviu ar apklausos metodus pasitelkiant NIST yra įtraukiami tik vadovai, nors kibernetinis saugumas turi būt aktualus visiems darbuotojams nesvarbu kokias pareigas

jie užimtų. Taip pat, pastebima didžiulė žinių stoka, darbuotojams nėra didelės motyvacijos mokytis ir gilintis žinias pasitelkiant tradicinius mokymo būdus apie kibernetinį saugumą įmonėje.

1.5. Didelių įmonių kibernetinio saugumo vertinimas

Daugelis didelių įmonių naudoja Nacionalinį standartų ir technologijų institutą (NIST) kibernetinio saugumo sistemą (CSF) ir kitus NIST išteklius, kad padėtų pagerinti savo kibernetinio saugumo padėtį. NIST CSF yra sistema, kuri suteikia bendrą kalbą ir požiūrį į kibernetinio saugumo pavojų supratimą ir valdymą. Tai apima standartų, gairių ir praktikos, kurias organizacijos gali naudoti vertindamos ir patobulindamos savo kibernetinio saugumo laikyseną, rinkinį.

Taip pat , didelės įmonės taip pat gali naudoti kitus NIST išteklius, pvz., NIST rizikos valdymo sistemą (RMF) ir NIST kibernetinio saugumo darbo jėgos sistemą (NCWF), siekdamos pagerinti savo kibernetinio saugumo laikyseną. Daugelis didelių kompanijų taip pat dalyvauja NIST tyrimų ir plėtros programose ir gali naudoti NIST rekomendacijas bei geriausią praktiką informuodamos apie savo kibernetinio saugumo strategijas.

Vienas iš pagrindinių skirtumų tarp būdo, kuriuo MVĮ ir didelės įmonės naudoja NIST, yra išteklių ir patirties lygis, kurį jos gali panaudoti. Didelės įmonės dažnai turi daugiau išteklių, įskaitant personalą, biudžetą ir technines žinias, skirtas kibernetinio saugumo pastangoms. Jie taip pat gali turėti sudėtingesnę IT aplinką ir gali susidurti su įvairesnėmis kibernetinio saugumo grėsmėmis. Dėl to didelės įmonės gali labiau naudoti NIST išteklius visapusiškiau ir nuodugniau ir gali būti labiau linkusios siekti sertifikavimo pagal NIST standartus. RMF yra labai orientuotas į sistemą ir nesprendžia organizacinių klausimų, o tai reiškia, kad jame nenumatytas holistinis požiūris į informacijos saugumo rizikos valdymą. Todėl NIST RMF gali būti labiau tinkamas didelėms vyriausybinėms organizacijoms ir mažiau taikomas mažesnėms organizacijoms (Ebad ir Shouki, 2021).

Nepaisant to, jog didelėse įmonėse galimybės turėti aukštesnį kibernetinio saugumo lygį yra ženkliai didesnės, tačiau atlikus mokslinių šaltinių analizę, galima teigti, jog išryškinamos tos pačios pagrindinės problemos, kaip ir mažų-vidutinių dydžio įmonėse.

1.6. Mažo-vidutinio bei didelių įmonių saugumo vertinimo išvados

Išanalizavus mokslininkų straipsnius kuriuose buvo taikomas NIST metodas įvairaus dydžio įmonėse, galima teigti, jog didelės apimties organizacijos dėl savųjų didelių resursų gali geriau panaudoti NIST siūlomą metodiką, nes yra užtektinai finansų įkurti atskirą komandą, kuri bus atsakinga už įmonės kibernetinio saugumo įvedimą bei užtikrinimą. Šis skyrius galėtų dirbti vien tik su NIST metodo siūlomais sprendimo būdais, siekiant užtikrinti saugesnį įmonės gyvavimą. NIST rizikos valdymo sistema (RMF) visų pirma skirta naudoti vyriausybinėms agentūroms ir jų

rangovams Jungtinėse Valstijose ir yra orientuota į šių organizacijų IT sistemų sertifikavimą ir akreditavimą. Tai riboja jo naudojimą ne JAV ir nevyriausybinėse organizacijose. Tiriant visų dydžių įmonių kibernetinį saugumą galima pastebėti ir panašumų, lentelėje apačioje yra pateikiamos pagrindinės problemos, kurios galioja visų dydžių įmonėms.

1.6 lentelė. Mažų-vidutinių bei didelių įmonių bendros problemos, sudaryta darbo autoriaus

Problema	Aprašymas
Sudėtingumas	CSF yra išsami sistema, apimanti daugybę standartų, gairių ir praktikos, o ją įgyvendinti gali būti sudėtinga
Išteklių apribojimai	CSF įgyvendinimas gali pareikalauti daug išteklių, todėl gali tekti skirti personalo, laiko ir biudžeto
Informuotumo trūkumas	Kai kurios organizacijos gali būti nesusipažinusios su CSF arba nesuprasti jos vertės, todėl gali būti sunku gauti dalyvavimo ir paramos jo įgyvendinimui
Standartizacijos trūkumas	CSF sukurtas taip, kad būtų lankstus ir pritaikomas, tačiau dėl to organizacijoms gali būti sunku standartizuoti savo požiūrį į kibernetinį saugumą
Kultūrinės kliūtys	Organizacijos požiūrio į kibernetinį saugumą pakeitimas gali būti kultūrinis pokytis, todėl gali reikėti pakeisti požiūrį ir elgesį. Kai kurioms organizacijoms tai gali būti sunku pasiekti

1.6.2. Teorinės dalies išvados

Nors apklausos ir interviu metodas ne visada yra dėmesio centre, jis išsiskiria kaip efektyviausia ir operatyviausia priemonė įvertinti kibernetinį saugumą įmonėje arba darbuotojų supratimą apie tai. Pažymėtina, kad mažos ir vidutinės įmonės (MVĮ) šiandieninėje rinkos aplinkoje tampa labiausiai pažeidžiamomis įmonėmis. Įvairaus dydžio įmonėms neužtenka vien diegti pažangiausias sistemas, tokias kaip NIST, kad užkirstų kelią didėjančiam kibernetinių atakų kiekiui. Šis neadekvatumas ypač išryškėja įvertinus bendrą darbuotojų kibernetinio saugumo žinių trūkumą.

Atsižvelgiant į NIST analizę, atvejo ir apklausos, būtina įtraukti visus darbuotojus į kibernetinių atakų prevenciją tampa ypač ryškus šiuolaikiniame pasaulyje. NIST, nors ir padeda nustatyti įmonės trūkumus ir siūlyti praktines alternatyvas, neužtikrina visų darbuotojų įsitraukimo ir tobulėjimo siekiant aukšto kibernetinio saugumo įvertinimo.

Apibendrinant galima teigti, kad apklausos ir atvejų tyrimai paprastai sulaukia minimalaus susidomėjimo, sunaudoja daugiau laiko ir atskleidžia kibernetinio saugumo spragas po ilgesnio laiko. Priešingai, eksperimentinis požiūris įtraukia visus darbuotojus greitai, suteikia greitų įžvalgų per neformalų švietimą, leidžia nedelsiant nustatyti spragą ir inicijuoti aktyvų mokymosi procesą. Tai savo ruožtu palengvina patikimesnį įmonės kibernetinio saugumo vertinimą.

2. EMPIRINIO TYRIMO METODIKA

Įvadas

Kibernetinis saugumas šiandien yra vienas kritiškiausių iššūkių, su kuriais susiduria organizacijos, siekdamos apsaugoti duomenis ir informacijos sistemas. Mūsų tyrimo tikslas orientuotas į kibernetinio saugumo vertinimo iššūkius, metodų analizę ir tolesnio veiksmingumo gerinimo rekomendacijas. Tai aktualu, nes nuolatos kintanti grėsmių aplinka reikalauja nuolatinio dėmesio ir naujų požiūrių į saugumo praktikas.

Mes siekiame suprasti, kaip organizacijoje atliekama kibernetinio saugumo mokymai ir vertinimai. Tyrimas apima apklausas bei interviu, leidžiančias atskleisti darbuotojų požiūrį ir subalansuotą saugumo padėtį. Taip pat planuojame tikrinti mūsų iškeltas hipotezes, kurios susijusios su bendradarbiavimo, nuolatinių stiprinimo strategijų įtaka įsitraukimui bei organizacinių veiksnių reikšme saugumo išlaikymui.

Techninių aspektų supratimas yra svarbus, tačiau dažnai yra ignoruojamas efektyvus bendravimas su įvairių kompetencijų turinčiais darbuotojais, kas ne mažiau kritiška užtikrinant visapusį saugumą. Todėl siūlome inovatyvius mokymo metodus, tokius kaip žaidimai ar realaus gyvenimo incidentų analizė, kad padėtume visiems darbuotojams giliau suprasti ir įsitraukti į kibernetinio saugumo procesus.

Analizuodami skirtingas saugumo vertinimo praktikas, mūsų tikslas – atrasti tai, ką įmonės gali daryti geriau. Tyrime naudosime įvairias duomenų rinkimo metodus, teikiant rekomendacijas, kurios galėtų būti integruotos į esamas vertinimo sistemas. Per šį tyrimą tikimės naujai pažvelgti į komunikacijos reikšmę saugumo vertinimuose ir suteikti organizacijoms įrankius, kaip pagerinti saugumo supratimą.

Šiuolaikinėje kibernetinių grėsmių eroje būtina pateikti saugumo mokymus patraukliai ir suprantamai, todėl šis tyrimas – tai mūsų įnašas į šią svarbią misiją, kuriant naujas saugumo kultūros pamatas.

Pagrindinė idėja

Šio tyrimo esmė yra nustatyti kibernetinio saugumo mokymų veiksmingumą organizacijoje. Praktinėje dalyje, siekdami gilinti supratimą apie šią sritį, pasitelksime mišrų metodą. Tai reiškia, kad duomenys bus renkami tiek iš anksto sudarytų darbuotojų apklausų, tiek iš gilesnių ekspertų interviu. Analizuosime, kaip darbuotojai supranta ir taiko kibernetinio saugumo principus, kokias reakcijas keliantys mokymai ir jų siūlomi patobulinti.

Ekspertų interviu metu sieksime atskleisti šiuolaikinį kibernetinių strategijų veiksmingumą, identifikuoti klaidingai taikomas praktikas, aptarti galimus patobulinimus bei ieškoti būdų kaip geriau informuoti ir įtraukti darbuotojus į saugumo procesus.

Atliktame tyrime išbandysime tris pagrindines hipotezes, siekdami suprasti, kaip funkcinis bendradarbiavimas, stiprinimo strategijos ir organizacinės aplinkybės veikia saugumo mokymų efektyvumą. Remdamiesi gautais rezultatais, galėsime pateikti praktinius patarimus, kurie padės stiprinti kibernetinę saugumo kultūrą organizacijoje ir efektyviau organizuoti mokymų programas.

Tikslas

Tikslas - išanalizuoti kibernetinio saugumo vertinimo iššūkius ir metodus bei pateikti rekomendacijas kibernetinio saugumo praktikai ir mokymų rezultatams tobulinti.

Tyrimo uždaviniai

1. Suprasti esamą kibernetinio saugumo protokolų ir mokymų organizacijoje būklę
2. Atlikti apklausą ir interviu
3. Surinkti tiesioginius duomenis iš darbuotojų
4. Atsakyti į tyrimo klausimus ir paneigti arba patvirtinti hipotezes

Darbo analizės vienetas

2.1 lentelė. Darbo analizės vienetų išsamus aprašymas

Analizės vienetas	Aprašymas
Kibernetinio saugumo vertinimo metodikos	Šis vienetas išnagrinės ir palygins įvarias metodikas, skirtas įvertinti organizacijos kibernetinio saugumo laikyseną
Nuolatinio stiprinimo strategijos	Šis vienetas tirs strategijų, naudojamų darbuotojų informuotumu ir įsitraukimui į kibernetinį saugumą didinti, efektyvumą
Organizaciniai veiksniai, darantys įtaką kibernetinio saugumo praktikai	Šis vienetas tirs, kaip įvairūs organizaciniai veiksniai įtakoja kibernetinio saugumo praktikos išsaugojimą ir taikymą po mokymų

Hipotezės

1 hipotezė: „Organizacijos funkcinių padalinių bendradarbiavimas padidina kibernetinio saugumo mokymo efektyvumą“.

Ši hipotezė reiškia, kad už kibernetinį saugumą atsakingas ne tik IT skyrius, bet ir kitos funkcijos, tokios kaip žmogiškieji ištekliai, finansai, rinkodara ir kt. Bendradarbiaudami įvairiose srityse, darbuotojai gali dalytis žiniomis, įgūdžiais ir geriausia praktika, kad pagerintų savo veiklą. kibernetinio saugumo supratimas ir elgesys. Efektyvumą galima įvertinti pagal tai, kaip darbuotojai kasdieniame darbe taiko kibernetinio saugumo principus ir politiką, pvz., naudoja stiprius slaptažodžius, vengia sukčiavimo el. laiškų, praneša apie incidentus ir pan.

2 hipotezė: „Nuolatinės stiprinimo strategijos didina darbuotojų įsitraukimą į kibernetinį saugumą“.

Ši hipotezė rodo, kad kibernetinio saugumo mokymai turėtų būti ne vienkartinis įvykis, o nuolatinis procesas, sustiprinantis ir atnaujinantis darbuotojų žinias ir įgūdžius. Sustiprinimo strategijos gali apimti žaidimus, viktorinas, grįžtamąjį ryšį, atlygį ir kt. Įtraukimas gali būti matuojamas pagal tai, kaip dažnai ir nuosekliai darbuotojai naudojasi kibernetinio saugumo praktika, kurią išmoko mokymuose.

3 hipotezė: „Organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlaikymui“.

Ši hipotezė rodo, kad organizacijos kontekstas ir kultūra vaidina svarbų vaidmenį, kaip darbuotojai išlaiko ir perima kibernetinio saugumo praktikas po mokymo. Organizaciniai veiksniai gali apimti vadovavimo įsipareigojimą, bendravimą, paskatas, išteklius ir kt. Šie veiksniai gali palengvinti arba trukdyti darbuotojų motyvacijai ir gebėjimui laikytis kibernetinio saugumo gairių ir procedūrų.

Šiame tyrime hipotezėms patikrinti ir analizuoti bus naudojamos apklausos ir interviu. Apklausų metu bus renkami kiekybiniai duomenys apie tai, kaip dalyviai supranta, įsitraukia ir suvokia žaidimo efektyvumą, ir realūs kibernetinio saugumo vertinimo pavyzdžiai. Apklausos taip pat bus skirtos asmenims, turintiems žemo kompiuterinio raštingumo, siekiant užfiksuoti jų nuomonę ir patirtį.

Interviu metu bus išsamiau nagrinėjamos dalyvių įžvalgos ir patirtis. Pokalbių metu bus kibernetinio saugumo specialistai ir darbuotojai, turintys skirtingą kompiuterinio raštingumo lygį. Interviu pagrindinis dėmesys bus skiriamas jų nuomonei apie žaidimą ir realaus gyvenimo pavyzdžiams, taip pat jų dalyvavimui kibernetinio saugumo mokymuose ir informavimo programose. Interviu metu bus gauti kokybiniai duomenys apie dalyvių požiūrį, motyvaciją ir galimą šių metodų poveikį jų saugumo praktikai.

Apklausos ir interviu duomenys bus detaliai išanalizuoti. Apklausos atsakymai bus analizuojami naudojant statistinius metodus, tokius kaip aprašomoji statistika, koreliacinė analizė ir

hipotezių tikrinimas. Ši analizė įvertins, kaip žaidimas ir realūs pavyzdžiai yra susiję su dalyvių supratimu ir įsitraukimu į kibernetinio saugumo vertinimą.

Interviu duomenys bus perrašomi ir koduojami, kad būtų galima nustatyti temas, modelius ir pagrindines įžvalgas. Su žaidimu ir realaus gyvenimo pavyzdžiais susijusioms išvadoms išgauti ir interpretuoti bus naudojama teminė analizė. Ši analizė padės geriau suprasti, kaip šie metodai veikia dalyvių informuotumą ir supratimą apie saugumo praktiką.

Duomenų analizė pateiks empirinius įrodymus hipotezėms pagrįsti arba atmesti. Rezultatai patvirtins žaidimo ir realaus gyvenimo pavyzdžių veiksmingumą gerinant informuotumą apie kibernetinį saugumą ir mažo kompiuterinio raštingumo asmenų įsitraukimą. Rezultatai taip pat atskleis šių metodų privalumus, trūkumus ir pasekmes tobulinant kibernetinio saugumo vertinimo metodikas.

Apklausos ir interviu duomenys vaidins labai svarbų vaidmenį vertinant hipotezes ir suteikiant vertingų įžvalgų apie žaidimo naudą bei realius kibernetinio saugumo mokymų pavyzdžius.

Teorinis pagrindas

Šiame tyrime atlikta mokslinės literatūros analizė suteikė vertingų įžvalgų apie skirtingų požiūrių efektyvumą didinant darbuotojų sąmoningumą ir supratimą apie kibernetinį saugumą. Nustatyta, kad realių problemų pavyzdžių panaudojimas ir žaidimais pagrįstų mokymų bei programų įtraukimas gali būti veiksmingos strategijos, padedančios tobulinti kibernetinio saugumo žinias ir įgūdžius (Ben-Asher ir González, 2015). Pateikdami informaciją įtraukiančiai ir interaktyviai, darbuotojai labiau išsaugos žinias ir efektyviai jas pritaikys kasdieniame darbe. Tai gali žymiai pagerinti bendrą įmonės kibernetinio saugumo padėtį. Literatūros apžvalgos išvados rodo, kad tradiciniai mokymo metodai, tokie kaip nuobodūs mokymai, gali būti ne tokie veiksmingi siekiant patraukti darbuotojų dėmesį ir skatinti supratimą. Vietoj to, naudojant realius problemų pavyzdžius ir žaidimo metodus, darbuotojai gali įgyti praktinės ir įtraukiančios mokymosi patirties, o tai paskatins didesnį įsitraukimą ir žinių išsaugojimą.

Tyrimo metodika

Šiame tyrime pasirinkome dirbti su įmone „*A*“, toliau ją vadinsime tiesiog *A*, kibernetinio saugumo įmonės, kurios pagrindinis dėmesys skiriamas humanizuotų privatumo ir saugumo sprendimų kūrimui, darbuotojų apklausa. Įmonė *A* siūlo daugybę produktų, kurie padeda užtikrinti saugumą kompiuteryje bei internete. Turėdama daugiau nei 300 darbuotojų, *A* yra ideali aplinka mokymosi efektyvumui ir realaus gyvenimo pavyzdžiams tirti kibernetinio saugumo mokymų kontekste. Kadangi teorinėje dalyje buvo išskiriama mažo – vidutinio dydžio įmonės, kaip vienas iš rizikingiausių ir galinčių patirti didžiausias problemas kibernetinių atakų metų, todėl būtent tokia įmonė ir buvo pasirinkta.

Pagrindinė apklausa bus skirta darbuotojams iš skirtingų įmonės padalinių, o interviu bus atliekami tik su saugumo skyriaus specialistais. Šis skirstymas leidžia mums suvokti platų visos organizacijos darbuotojų požiūrį ir gauti konkretesnių įžvalgų iš saugumo ekspertų. Derindami kiekybinius ir kokybinius tyrimo metodus, siekiame visapusiškai suprasti tyrimo temą.

Kiekybinėje tyrimo dalyje bus naudojamos apklausos, kad būtų renkami duomenys iš didesnės dalyvių imties. Apklausos anketa bus skirta surinkti kiekybinius duomenis apie dalyvių supratimą, įsitraukimą ir suvokiamą žaidimais pagrįsto mokymosi efektyvumą bei realaus gyvenimo pavyzdžius kibernetinio saugumo mokymuose. Apklausą sudarys struktūrizuoti ir standartizuoti uždarojo tipo klausimai, leidžiantys efektyviai rinkti ir analizuoti duomenis. Apklausos metu gauti kiekybiniai duomenys bus analizuojami statistiniais metodais, leidžiančiais daryti kiekybines įžvalgas ir daryti apibendrinamas išvadas.

Papildant kiekybinį komponentą, kokybinis tyrimo aspektas apims giluminius interviu. Pusiau struktūruoti interviu bus atliekami su mažesne imtimi dalyvių, kurie savo kibernetinio saugumo mokymuose patyrė žaidimais pagrįstą mokymąsi ir realius pavyzdžius. Šie interviu suteiks galimybę išsamiau ištirti dalyvių patirtį, požiūrį ir suvokimą. Dalyvaudami atvirose diskusijose siekiame surinkti turtingus kokybinius duomenis, apimančius dalyvių pasakojimus, įžvalgas ir kontekstinę informaciją, kurios neįmanoma lengvai kiekybiškai įvertinti. Teminė analizė bus naudojama analizuojant kokybinius interviu duomenis, nustatant bendras temas, modelius ir unikalias perspektyvas, siekiant sukurti kokybines įžvalgas ir pagilinti mūsų supratimą apie dalyvių patirtį. Apklausos atsakymai bus sudaryti pagrindine iš šių atsakymų:

1. „Taip“ arba „Ne“.
2. „Sutinku“ arba „Nesutinku“.
3. Nuo 1 iki 5 balų vertinimas.

2.2. Apklausos ir interviu klausimynai

1. Ar per pastaruosius metus dalyvavote kibernetinio saugumo mokymo programose? Taip/Ne

2. Jeigu taip, ar po dalyvavimo mokymuose esate įsitikinęs(-usi) skalėje nuo 1 (Nesitiki) iki 5 (Labai įsitikinęs(-usi)), kad išmoktas praktikas galite pritaikyti atliekant kasdienes užduotis?

3. Kaip įvertintumėte savo dabartinį supratimą apie kibernetinio saugumo protokolus organizacijoje pagal skalę nuo 1 (labai prastai) iki 5 (puikiai)?

4. Kaip dažnai jūsų organizacija dalyvauja tarpžinybiniame bendradarbiavime kibernetinio saugumo klausimais skalėje nuo 1 (niekada) iki 5 (visada)?

5. Kiek padalinių bendradarbiavimas turi įtakos kibernetinio saugumo mokymų efektyvumui organizacijoje skalėje nuo 1 (visiškai ne) iki 5 (reikšmingai)?

6. Ar jūsų skyrius taiko nuolatinę stiprinimo strategiją, kad padidintų informuotumą apie kibernetinį saugumą?

7. Jei taip, kiek šios strategijos yra veiksmingos, siekiant išlaikyti kibernetinio saugumo praktiką skalėje nuo 1 (neveiksminga) iki 5 (labai efektyvu)?

8. Kiek organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlikimui po mokymų? (1 = jokios įtakos, 2 = mažai įtakos, 3 = šiek tiek įtakos, 4 = didelę įtaką, 5 = labai didelę įtaką)

9. Kaip dažnai sąmoningai taikote išmoktas kibernetinio saugumo praktikas kasdienėse užduotyse skalėje nuo 1 (niekada) iki 5 (visada)?

10. Kaip jaučiatės pasirengę(-usi) spręsti su nuotoliniu darbu susijusius saugumo iššūkius skalėje nuo 1 (nepasiruošęs(-usi)) iki 5 (labai pasiruošęs(-usi))?

11. Ar esate įsitikinęs(-usi), kad nustatote galimas grėsmes saugumui ir pranešate apie jas, tokias kaip sukčiavimo atakos ir išpirkos reikalaujančios programos, skalėje nuo 1 (Nepasitiki) iki 5 (Labai pasitikintis(-i))?

12. Kaip dažnai saugos naujinimai ir pataisos yra taikomi jūsų skyriaus sistemoms skalėje nuo 1 (niekada) iki 5 (visada)?

13. Ar jūsų skyrius turi specialių kibernetinio saugumo protokolų, kurie skiriasi nuo bendrųjų organizacijos protokolų?

14. Jei galėtumėte pakeisti vieną dalyką apie dabartinius kibernetinio saugumo mokymus ar praktiką jūsų organizacijoje, kas tai būtų? (Atviras)

Pokalbio metodas skirtas tik organizacijos saugos komandos nariams:

1. Ar galite apibūdinti atvejį, kai tarp funkcinis bendradarbiavimas turėjo teigiamos įtakos kibernetinio saugumo mokymų įgyvendinimui?

2. Kaip tarpžinybinis bendradarbiavimas veikia kibernetinio saugumo mokymų efektyvumą pagal jūsų patirtį?

3. Ar galėtumėte pateikti nuolatinio stiprinimo strategijų, naudojamų jūsų organizacijoje, siekiant padidinti informuotumą apie kibernetinį saugumą, pavyzdžių?

4. Kaip manote, ar šios strategijos yra veiksmingos skatinant įsitraukti į kibernetinio saugumo praktiką?

5. Ar Jūsų organizacija yra kūrusi sąmoningumo programas remiantis NIST saugumo mokymų rekomendacijomis?

6. Ar galite paliudyti, kaip organizacija naudoja NIST CSF, kad identifikuoti, įvertinti ir valdyti kibernetines rizikas?

7. Kaip nuotolinio darbo saugumo politikos ir praktikos yra kuriamos ir įdiegiamos remiantis NIST CSF valdymo rekomendacijomis?

8. Ar galėtumėte pasidalinti strategijomis, kurios buvo veiksmingos nustatant galimas grėsmes saugumui ir apie jas pranešant, pvz., sukčiavimo atakas ir išpirkos reikalaujančias programas?

2.3. Duomenų analizė

Apklausos metu gauti duomenys bus analizuojami statistiniais metodais. Uždarojo tipo klausimai pateiks kiekybinius duomenis, kuriuos galima analizuoti siekiant nustatyti modelius, tendencijas ir koreliacijas. Bus apskaičiuojama aprašomoji statistika, pvz., priemonės, dažniai ir procentai, siekiant apibendrinti atsakymus ir pateikti dalyvių supratimo, įsitraukimo ir suvokto žaidimu pagrįsto mokymosi bei realaus gyvenimo pavyzdžių veiksmingumo apžvalgą.

Kokybiniams duomenims, surinktiems per interviu, bus atlikta teminė analizė. Tai apima pasikartojančių temų, modelių ir unikalių perspektyvų nustatymą dalyvių pasakojimuose. Interviu duomenys bus perrašomi ir koduojami, o tada kodai bus sugrupuoti į temas. Nagrinėdami dalyvių temas, taip bus įgyta gilesnių įžvalgų apie patirtį, požiūrį ir efektyvumo bei iššūkių, susijusių su žaidimu pagrįstu mokymusi ir realaus gyvenimo pavyzdžius, suvokimą. Svarbu paminėti, kad teorinėje dalyje aprašyta NIST CSF strategijos modelis / įrankis padedantis pagerinti kibernetinio saugumo lygį įmonėje taip pat yra įtrauktas į klausimyną, bei interviu metu bus naudojami nurodyti klausimai, tačiau tam tikrais atvejais bus kuriama diskusija.

2.4. Praktinis įgyvendinimas

Duomenų analizės išvados gali turėti praktinių pasekmių tiek organizacijai, tiek kibernetinio saugumo mokymų sričiai. Rezultatai gali padėti kurti ir tobulinti kibernetinio saugumo mokymo programas žemo kompiuterinio raštingumo darbuotojams. Nustatydamos esamų mokymo programų stipriąsias ir silpnąsias puses, tokios organizacijos kaip *A* gali pagerinti savo kibernetinio saugumo mokymų pristatymą ir turinį, kad pagerintų mokymosi rezultatus.

Apklausos atsakymų analizė gali išryškinti konkrečias sritis, kuriose darbuotojai mano, kad reikia tobulinti kibernetinio saugumo mokymus. Ši informacija gali padėti organizacijai kurti tikslines

intervencijas ir papildomas temas, skirtas pašalinti nustatytas spragas. Pavyzdžiui, jei apklausa atskleidžia, kad darbuotojams sunku atpažinti sukčiavimo el. laiškus, organizacija gali sutelkti dėmesį į mokymo modulių, skirtų konkrečiai šiai problemai spręsti, kūrimą.

Pokalbiuose su saugumo specialistais gautos įžvalgos gali padėti praktikoje įgyvendinti kibernetinio saugumo vertinimus ir tobulinimo iniciatyvas organizacijoje. Jų atsakymų analizė gali nustatyti dabartinių kibernetinio saugumo priemonių iššūkius, pažeidžiamumą ir tobulinimo sritis. Ši informacija gali padėti organizacijai paskirstyti išteklius, įgyvendinti saugos kontrolę ir šalinti nustatytas spragas, siekiant pagerinti bendrą kibernetinio saugumo padėtį.

Be to, tyrimų rezultatai gali prisidėti prie platesnės kibernetinio saugumo mokymo srities. Jie gali suteikti įžvalgų apie geriausias praktikas, gerinančius žemo kompiuterinio raštingumo asmenų supratimą ir sąmoningumą. Šiomis išvadomis galima dalytis su kitomis organizacijomis ir tyrėjais, kad būtų galima informuoti apie geriausios praktikos ir įrodymais pagrįstų kibernetinio saugumo mokymo metodų kūrimą.

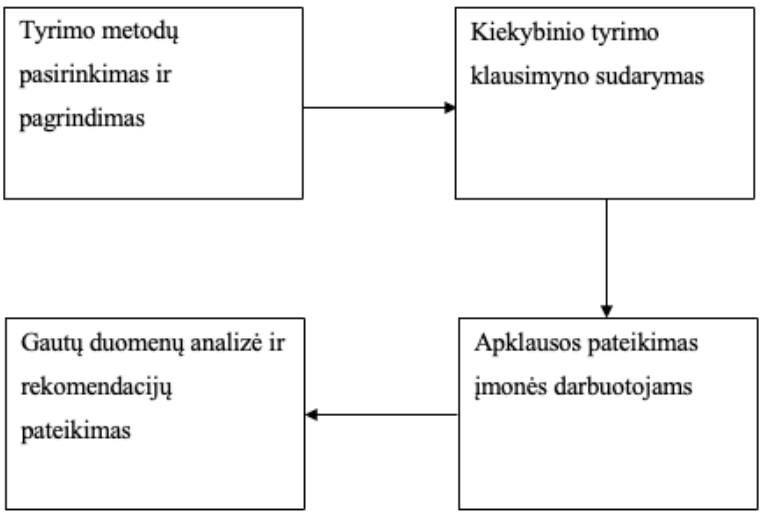
Apskritai, duomenų analizė ir praktinis tyrimų išvadų įgyvendinimas gali padėti patobulinti kibernetinio saugumo mokymo programas, pagerinti darbuotojų sąmoningumą ir elgesį bei sustiprinti kibernetinio saugumo kultūrą organizacijoje. Pašalinusios nustatytas spragas ir iššūkius, organizacijos gali geriau apsaugoti savo sistemas, duomenis ir tinklus nuo kibernetinių grėsmių.

3. EMPIRINIŲ REZULTATŲ ANALIZĖ

Apklausos tikslas - apklausa skirta surinkti kiekybinius duomenis iš didelio dalyvių skaičiaus. Tai leidžia įvertinti darbuotojų supratimą, požiūrį ir elgesį, susijusį su kibernetinio saugumo protokolais ir mokymu jūsų organizacijoje. Struktūrizuotas apklausos formatas leidžia lengviau analizuoti ir statistiškai palyginti atsakymus.

3.1.1. Kiekybinio tyrimo detalus planas

Pagal pateiktą paveikslą apačioje bus vykdomas planas, kurio pabaigoje bus pateikiamos rekomendacijos įmonei. Nurodytas planas galioja tik kiekybiniui tyrimui, kadangi planas pagal kurį vyks kokybinis tyrimas skirsis ir bus šiek tiek detalesnis. Kadangi teorinėje dalyje, buvo aprašyta ir ištirta, kad sujungus kiekybinius ir kokybinius tyrimų rezultatus galima gauti geriausias rekomendacijas, todėl būtent praktinėje dalyje tokius metodus ir pasirinkta taikyti.



3.1 pav. Kiekybinio tyrimo išsamus planas, sudaryta darbo autoriaus

3.1.2. Kiekybinio tyrimo klausimų sudarymo planas

Pagrindinis uždavinys rengiant klausimyną apklausai įmonės darbuotojams buvo, sukurti tokius klausimus, kurie kuo įmanoma geriau pateiktų dabartinę situaciją įmonę, kuomet yra tiriamas kibernetinis saugumas įmonėje. Kaip ir jau ir buvo minėta, dažnu atveju buvo pasiremta „Likerto“ skale, kurios dėka galima sužinoti kiek įmanoma tikslesnį lygį įmonėje. Taip pat, kiekvienas klausimas turi būt susijęs su vieną iš trijų iškeltų hipotezių ar darbo uždavinių ir tai taip pavyks pateikti tikslias rekomendacijas ir analizes pačiai įmonei. Tad, kiekvienas apklausos klausimas skirtas patikrinti vieną ar kelias hipotezes. Pavyzdžiui:

– 3 klausimai apklausoje yra susiję su 1 hipoteze, nes jais matuojamas kibernetinio saugumo mokymų efektyvumas ir išmoktos praktikos taikymas.

- 3 klausimai apklausoje yra susiję su 2 hipoteze, nes jais vertinamas nuolatinio stiprinimo strategijų naudojimas ir efektyvumas.

– 4 klausimai apklausoje yra susiję su 3 hipoteze, nes juose nagrinėjama organizacinių veiksnių įtaka kibernetinio saugumo praktikai.

Taip pat, prie 11-ikos privalomų prisidėjo ir keli neprivalomi ir netaikomi visiems, kadangi keli yra priklausomi ar respondentas atsakė į prieš tai buvusį klausimą „Taip“, o kitas atviras tačiau taip pat niekam neprivalomas klausimas.

3.1.3. Kiekybinio tyrimo analizė

Kiekybinio tyrimo metu dalyvavo per 100 respondentų iš visiškai skirtingų skyrių ir departamentų, tačiau nei vienas respondentas nebuvo susijęs su kibernetinio saugumo specialybę. Atlikus tyrimą buvo galima pastebėti panašias tendencijas ir įvertinti bendrą vaizdą įmonės kibernetinio saugumo srityje.

Siekiant išgryninti stiprų ir efektyvų kibernetinio saugumo mokymų, strategijų ir praktikų veiksmingumą mūsų organizacijoje, parengėme kruopštų klausimyną. Kiekvienas klausimas yra ruoštas su minčių įvertinti ir patikrinti mūsų iškeltas hipotezes. Bus nagrinėjama, kaip bendradarbiavimas, pastovios stiprinimo strategijos ir organizaciniai veiksniai prisideda prie mokymų efektyvumo, darbuotojų įsitraukimo į saugumo užtikrinimą bei visapusės saugumo praktikos išlaikymo. Šios apklausos rezultatai leis mums suprasti, kur yra mūsų stiprybės ir silpnybės, bei kurti strategijas, kurios dar labiau stiprintų mūsų organizacijos kibernetinį saugumą.

3.1 lentelė. Kiekybinio klausimų prilyginamas iškeltom hipotezėm

Klausimas	**Hipotezė**
Pirmas apklausos klausimas: Ar per pastaruosius metus dalyvavote kibernetinio saugumo mokymo programose? Taip/Ne	Organizacijos funkcinių padalinių bendradarbiavimas padidina kibernetinio saugumo mokymo efektyvumą
Ketvirtas apklausos klausimas: Kaip dažnai jūsų organizacija dalyvauja tarpžinybiniame bendradarbiavime kibernetinio saugumo klausimais skalėje nuo 1 (niekada) iki 5 (visada)?	Organizacijos funkcinių padalinių bendradarbiavimas padidina kibernetinio saugumo mokymo efektyvumą
Penktas apklausos klausimas: Kiek padalinių bendradarbiavimas turi įtakos kibernetinio saugumo mokymų efektyvumui organizacijoje skalėje nuo 1 (visiškai ne) iki 5 (reikšmingai)?	Organizacijos funkcinių padalinių bendradarbiavimas padidina kibernetinio saugumo mokymo efektyvumą
Šeštas apklausos klausimas: Ar jūsų skyrius taiko nuolatinę stiprinimo strategiją, kad padidintų informuotumą apie kibernetinį saugumą?	Nuolatinės stiprinimo strategijos didina darbuotojų įsitraukimą į kibernetinį saugumą
Septintas apklausos klausimas: Jei taip, kiek šios strategijos yra veiksmingos, siekiant išlaikyti	Nuolatinės stiprinimo strategijos didina darbuotojų įsitraukimą į kibernetinį saugumą

kibernetinio saugumo praktiką skalėje nuo 1 (neveiksminga) iki 5 (labai efektyvu)?	
Devintas apklausos klausimas: Kaip dažnai sąmoningai taikote išmoktas kibernetinio saugumo praktikas kasdienėse užduotyse skalėje nuo 1 (niekada) iki 5 (visada)?	Nuolatinės stiprinimo strategijos didina darbuotojų įsitraukimą į kibernetinį saugumą
Trečias apklausos klausimas: Kaip įvertintumėte savo dabartinį supratimą apie kibernetinio saugumo protokolus organizacijoje pagal skalę nuo 1 (labai prastai) iki 5 (puikiai)?	Organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlaikymui
Aštuntas apklausos klausimas: Kiek organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlikimui po mokymų? (1 = jokios įtakos, 2 = mažai įtakos, 3 = šiek tiek įtakos, 4 = didelę įtaką, 5 = labai didelę įtaką)	Organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlaikymui
Dvyliktas apklausos klausimas: Kaip dažnai saugos naujinimai ir pataisos yra taikomi jūsų skyriaus sistemoms skalėje nuo 1 (niekada) iki 5 (visada)?	Organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlaikymui
Tryliktas apklausos klausimas: Ar jūsų skyrius turi specialių kibernetinio saugumo protokolų, kurie skiriasi nuo bendrųjų organizacijos protokolų?	Organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlaikymui

Nepaminėti lentelėje klausimai yra bendro pobūdžio ir gali padėti išgauti duomenis, kurie gali padėti susidaryti papildomą kontekstą tiriant įmonę pagal iškeltas hipotezes. Tokie klausimai kaip antras, dešimtas ar vienuoliktas, taip pat gali padėti atskleisti darbuotojų subjektyvų patyrimą ir požiūrį į savo saugumo kompetencijas, bei sąveiką su mokymais ar jų taikymą.

Svarbu paminėti, jog nors paskutinis apklausos klausimas buvo neprivalomas ir atviras, tačiau dažnas respondentas pasidalino savo įžvalgomis ir pasidalino savo nuomonę apie pokyčius, kurie yra reikalingi norint padidint ir pagerinti situaciją organizacijoje saugumo kontekste.

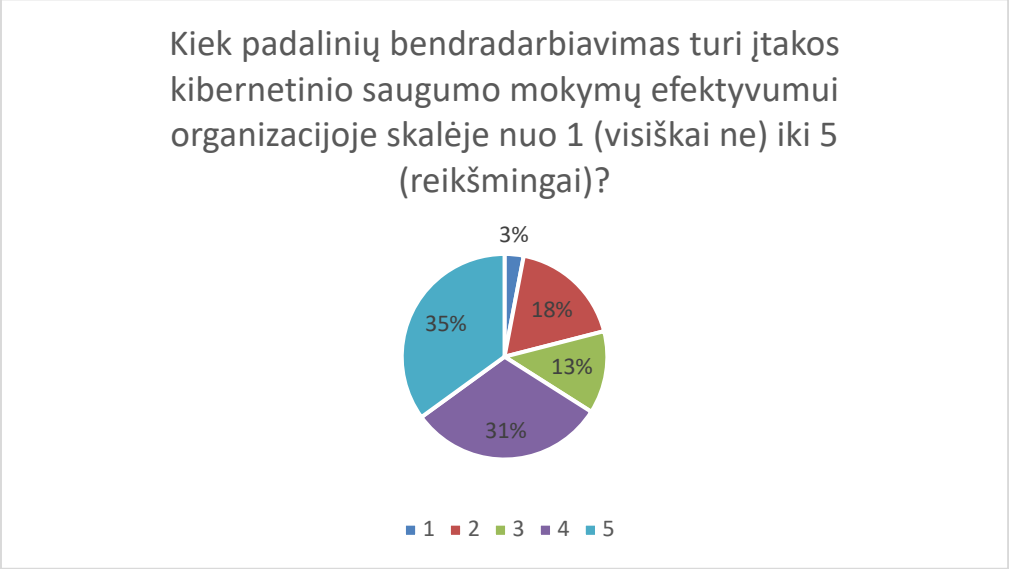
3.1.4. Organizacijos funkcinių padalinių bendradarbiavimas padidina kibernetinio saugumo mokymo efektyvumą

Informuotumas apie kibernetinio saugumo protokolus: vidutinis 3,61 balo iš 5 rodo gana aukštą darbuotojų informuotumo lygį. Tai rodo, kad mokymo programos yra veiksmingos suteikiant žinias apie kibernetinio saugumo protokolus.

Išmoktos praktikos taikymas: Vidutinis 3,37 balo iš 5 rodo, kad nors darbuotojai taiko išmoktas praktikas, balas nėra toks aukštas, koks galėtų būti, lyginant su informuotumo balu. Tai rodo, kad darbuotojai po mokymų gali nepasitikėti savo žiniomis ir ne visais atvejais pritaikyti įgytas teorines žinias.

Bendradarbiavimas tarp padalinių: Vidutinis įvertinimas 3,87 iš 5 rodo teigiamą poveikį kibernetinio saugumo mokymų efektyvumui, kai vyksta bendradarbiavimas tarp padalinių. Tai galėtų pagerinti kibernetinio saugumo politikos ir protokolų derinimą ir koordinavimą skirtinguose skyriuose.

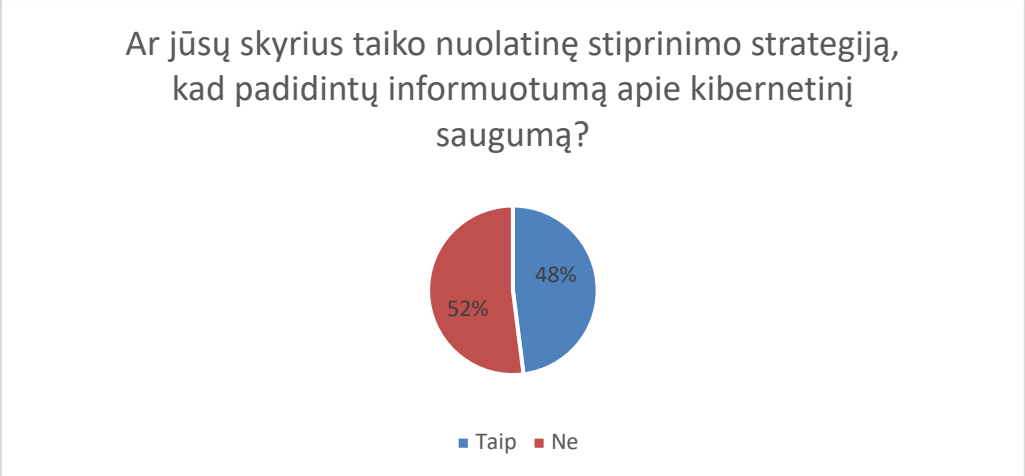
Atsižvelgiant į tai galima daryti preliminarią išvadą, kad nors kibernetinio saugumo supratimas yra aukštas ir vertinamas tarpžinybinis bendradarbiavimas, išmoktos praktikos taikymas nėra toks aukštas, koks galėtų būti. Norint tai išspręsti, gali būti naudinga skatinti bendravimą ir teikti pagalbą, kad darbuotojai jaustųsi patogiai prašydami saugos specialistų pagalbos, kai susiduria su problemomis, o ne bandydami išspręsti incidentus patys.



3.2 pav. Darbuotojų nuomonė, kaip reiškminga yra padalinių bendradarbiavimas rezultatai

3.1.5. Nuolatinės stiprinimo strategijos didina darbuotojų įsitraukimą į kibernetinį saugumą

Sustiprinimo strategijų buvimas: 48–49 % respondentų nurodė, kad jų skyrius taiko nuolatinę stiprinimo strategiją, skirtą informuotumui apie kibernetinį saugumą didinti, tai rodo, kad maždaug pusė departamentų aktyviai dirba siekdami palaikyti kibernetinio saugumo supratimą. (3.3 paveikslas).



3.3 pav. Ar darbuotojo skyrius taiko nuotalinę stiprinimo strategija rezultatai

Stiprinimo strategijų veiksmingumas: vidutinis 3,75 balo įvertinimas (skalėje nuo 1 iki 5) šių strategijų efektyvumui palaikant kibernetinio saugumo praktikas rodo teigiamą poveikį. Tai rodo, kad nuolatinės stiprinimo strategijos iš tiesų stiprina dalyvavimą kibernetinio saugumo srityje. (3.4 paveikslas)

3.4 pav. Jeigu darbuotojo padalinys taiko nuolatinę stiprinimo strategiją, koks didelis jos veiksmingumas rezultatai

Atsižvelgiant į šiuos duomenis, galima daryti preliminarią išvadą, kad nors tik pusė įmonės padalinių taiko nuolatinio saugumo stiprinimo strategiją, mūsų duomenimis, ji yra efektyvi. Tai galėtų būti įtikinamas pavyzdys kitiems skyriams. Įdomu, tai ,kad departamentai, kurie netaiko nuolatinių stiprinimo strategijų yra labiau pažeidžiami net iki 22%, tiek procentais dažniau įvyksta kibernetinio saugumo incidentų skyriuose, kurie nuolat nesirenka stiprinti saugumo strategijos. Tai rodo, kad nors šios strategijos yra veiksmingos, visada yra kur tobulėti ir prisitaikyti prie nuolat besikeičiančios kibernetinio saugumo grėsmių. Todėl labai svarbu, kad visi skyriai ne tik diegtų, bet ir nuolatos atnaujintų bei tobulintų savo kibernetinio saugumo strategijas.

3.1.6. Organizaciniai veiksniai turi įtakos kibernetinio saugumo praktikos išlaikymui

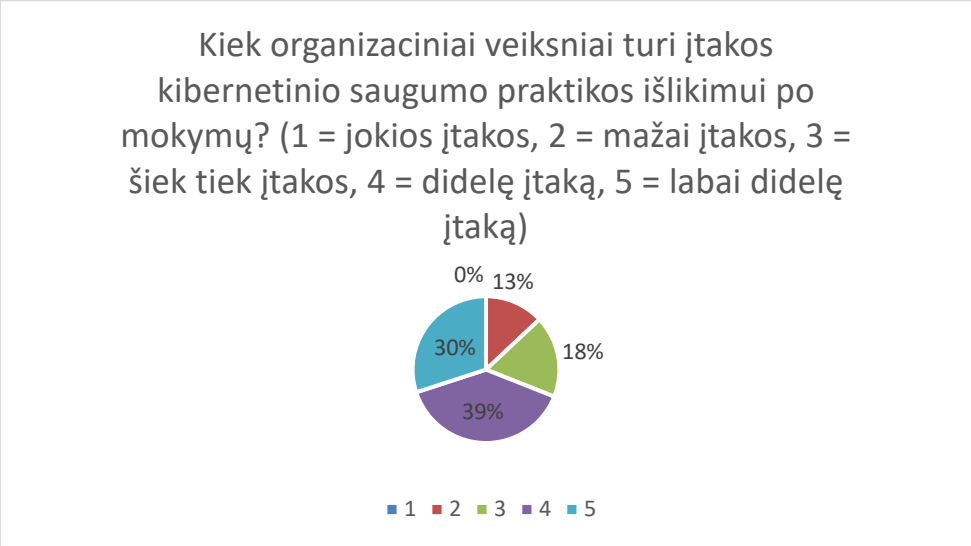
Tarpžinybinis bendradarbiavimas: vidutinis 3,37 balo iš 5, kaip dažnai organizacija dalyvauja tarpžinybiniame bendradarbiavime kibernetinio saugumo klausimais, rodo vidutinį bendradarbiavimo lygį. Tai galėtų pagerinti dalijimąsi informacija ir geriausia praktika kibernetinio saugumo srityje.

Organizaciniai veiksniai: vidutinis 3,87 balo iš 5 įvertinimas, kiek organizaciniai veiksniai įtakoja kibernetinio saugumo praktikos išlaikymą po mokymų, rodo reikšmingą poveikį. Tai rodo, kad tokie veiksniai kaip organizacijos kultūra, struktūra, bendravimas ir lyderystė vaidina svarbų

vaidmenį palaikant darbuotojų sąmoningumą ir elgesį kibernetinio saugumo klausimais (3.5 paveikslas).

Saugos naujinimai ir pataisos: vidutinis 3,84 balo iš 5 įvertinimas, kaip dažnai departamentų sistemoms taikomi saugos naujinimai ir pataisos, rodo aukštą atitikimo kibernetinio saugumo standartams lygį. Tai rodo, kad organizacija aktyviai rūpinasi savo sistemų saugumu ir atnaujinimu.

Apibendrinant galima teigti, kad nors tarpžinybinė komunikacija išlieka vidutinio lygio, ji darbuotojų vertinama teigiamai ir labai aukštai. Tai rodo, kad šioje srityje yra galimybių tobulėti. Didinant tarpžinybinį bendradarbiavimą, gali būti įmanoma išlaikyti aukštą kibernetinio saugumo praktikos laikymosi lygį visoje organizacijoje.



3.5 pav. Kaip smarkiai organizaciniai veiksniai turi įtakos kibernetinio saugumo išlikimui po mokymų rezultatai

3.1.7. Atviras klausimas - Jei galėtumėte pakeisti vieną dalyką apie dabartinius kibernetinio saugumo mokymus ar praktiką jūsų organizacijoje, kas tai būtų?

Apklausos pabaigoje, kaip ir buvo minėta buvo pateiktas neprivalomas, tačiau atviras klausimas, kur kiekvienas respondentas turėjo teisę palikti pastabą ar savo nuomonę kalbant apie konkretų dalyką kurį norėtų pakeisti ar patobulinti, kuomet yra kalbama apie saugumo mokymus ar praktiką organizacijoje. Net 36% apklaustųjų pateikė savo įžvalgas šiuo klausimu ir analizuojant kiekvieną atsakymą detaliai ir vėliau juos palyginus su kitais atsakymais, buvo galima dažnus atsakymus priskirti į grupės, kur kiekviena grupė priklauso būdo dalykui, kurio būtent trūksta įmonėje kuomet yra analizuojamas įmonės kibernetinio saugumo mokymai, visi nurodyti lentelėje apačioje (3.2 lentelė).

3.2 lentelė. Pagrindiniai dalykai, kurių yra trūkumas įmonėje

Būdo dalykas	Paaiškinimas
Interaktyvumas	Daugelis respondentų minėjo, kad reikia daugiau interaktyvių mokymų. Tai gali apimti praktinius pratimus, atvejų analizę ir net imituojamus sukčiavimo išpuolius
Dažnumas	norisi dažniau atlikti praktines užduotis. Tai rodo, kad dabartiniai mokymai gali būti nepakankamai reguliarūs, kad kibernetinis saugumas būtų svarbiausias
Praktiškumas	Respondentai nori daugiau praktinių ir teorinių pavyzdžių bei realios gerosios praktikos dokumentacijos. Tai galėtų padėti jiems geriau suprasti ir taikyti kibernetinio saugumo principus
Svarbumo supratimas	Kai kurie respondentai mano, kad ne visi supranta kibernetinio saugumo svarbą, o tai rodo, kad reikia geriau informuoti apie jo aktualumą
Mokymo trūkumas	Keli respondentai paminėjo, kad trūksta mokymų, o tai rodo, kad kai kurios organizacijos gali neturėti oficialios kibernetinio saugumo mokymo programos
Veiksmingumas	Respondentai nori, kad mokymai būtų veiksmingesni ir jų turinys būtų gilesnis, o tai rodo, kad dabartiniai mokymai gali neatitikti jų poreikių

Šią analizę buvo atliktą skaitant ir analizuojant kiekvieną anketą ir taip išskiriant pagrindinius procesus, kuriuos labiausiai pabrėždavo savo atsakymuose respondentai. Apačioje pateiktoje lentelėje (3.3 lentelė) yra kiekvienai citatai priskirta po vieną būdo dalyką, kurio trūksta ar reiktų padidinti įmonėje.

3.3 lentelė. Respodentų citatos prilyginamos su būdo dalykais, kurių įmonėje yra trūkumas

Citata	**Būdo dalykas**
„<..>Toks mokymas nevyksta, todėl iš pradžių jis turėtų būti įvestas <..>“	Mokymų trūkumas: šis atsakymas aiškiai rodo, kad esamų mokymų nepriteklių.
„<..> Daugiau praktinių pavydžių <..>“	Praktiškumas: šio atsakymo dėka, galima atkreipti dėmesį į įmonėje praktinių pavyzdžių ir užduočių nepriteklių.
„<..>Padidinti mokymų skaičių (kartą kas pusmetį) ir daryti juos interaktyviai, o ne tiesiog skaityti tekstą ir po “paskaitos“ prašyti pasirašyti už dalyvavimą <..>“	Dažnumas: šis atsakymas parodo pačio darbuotojo motyvaciją ir norą, kad mokymai vyktų dažniau ir su daugiau praktinių užduočių.
„<..> Reiktų daryti juos interaktyvesnius, leisti patiems tapti užpuolikais, kad geriau suprast atakų prasmę ir kaip jas vykdyti <..>“	Interaktyvumas: atsakymas pabrėžia interaktyvesnių mokymų metodų poreikį įmonėje.

3.1.8. Kiekybinio tyrimo rekomendacijos

Remiantis tyrimo rezultatais, mūsų rekomendacijos įmonei – tai ne tik dažniau organizuoti ir praturtinti mokymus interaktyviomis užduotimis, bet ir žiūrėti į kibernetinio saugumo ugdymą kaip į

nuolatinį vidinės kultūros aspektą. Būtina nuolatos atnaujinti mokymus atsižvelgiant į besikeičiančią kibernetinių grėsmių aplinką ir skatinti visų organizacijos lygių įsitraukimą. Darbuotojų pasiūlymai yra vertinga informacija, rodanti, kur galime tobulėti ir kaip galime geriau įtraukti asmenis į saugumo procesus.

3.1.9. Kiekybinio tyrimo išvados

Kiekybinio tyrimo duomenų analizė mums atvėrė pro langą pažvelgti į įmonės kibernetinio saugumo mokymų, strategijų ir praktikų veiksmingumą iš vidinės perspektyvos. Šie duomenys rodo, kad nors darbuotojai įgijo solidų pagrindą kibernetinio saugumo protokolams suprasti, jų įgyvendinimas kasdienėje praktikoje kiek svyruoja ir reikalauja papildomo dėmesio. Bendradarbiavimas tarp skirtingų organizacijos padalinių teigiamai įtakoja mokymo efektyvumą, tačiau ši veikla įgyvendinama nevienodai visose įmonės dalyse. Organizaciniai veiksniai, tokie kaip komunikacija ir vadovų įsitraukimas, taip pat vaidina svarbų vaidmenį palaikant ir skatinant saugumo sąmoningumą.

Svarbu pažymėti, kad šios išvados ir rekomendacijos yra paremtos tik kiekybiniu tyrimo aspektu. Darbo pabaigoje visos išvados ir rekomendacijos bus atidžiai išnagrinėtos ir derinamos su kokybinio tyrimo data. Taip galėsime palyginti, susieti bei sukurti visapusiškesnę ir nuoseklesnę darbo tyrimo analizę, kuri leis mums suteikti aiškesnę bendrą organizacijos kibernetinio saugumo vaizdą. Su visapusišku tyrimo įžvalgų supratimu bus galima parengti išbaigtas ir struktūruotas rekomendacijas, kurios leis organizacijai stiprinti kibernetinio saugumo veiksmingumą ir tvarumą.

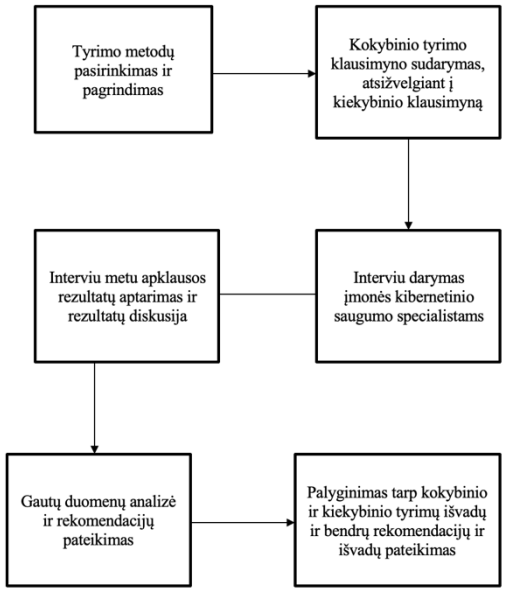
3.2. Kokybinio tyrimo eiga ir rezultatai

Interviu tikslas – interviu skirta surinkti kokybinius duomenis iš riboto kiekio žmonių, kadangi interviu bus skirtas tik įmonės kibernetinio saugumo specialistams. Pokalbio metu atsakymai padės įvertinti įmonės sąmoningumą kibernetinio saugumo klausimais, požiūrį ar elgesį bei pridėjus išvadas kiekybinio tyrimo, prieiti bendrą išvadą bei rekomendacijas, kurios bus pristatytos įmonei. Interviu bus paimtas iš 80% įmonės kibernetinio saugumo specialistų.

3.2.1. Kokybinio tyrimo detalus planas

Pagal apačioje sudaryta lentelę yra sudarytas planas, kurio reikia laikytis norint pasiekti geriausių rezultatų. Planas prasidėjo jau teorinėje dalyje, kurioje buvo išskiriamos sistemos, bei vertinimo aplinkos kurių pagalbą, galima tiksliausiai įvertinti kibernetinį saugumą įmonės bei pateikti geriausias rekomendacijas. Sudarius klausimyną bei sulaukus pirmųjų apklausos rezultatų bus pradėta kokybinio tyrimo eiga. Visi interviu vyks gyvai ir bus vadovaujamasi jau paminėtais klausimais, savaime suprantama tam tiktų interviu metu tikėtina, kad įvyks diskusija ir atsiras papildomų klausimų ar atsakymų.

Kuomet bus surinkti tyrimo duomenis, bus atlikta analizė, kurios metu bus ieškoma pasikartojantys dalykai, tai reiškia – procesai ar sąvokos / raktiniai žodžiai kurie dažniausiai kartosis per interviu. Taip turint rezultatus ir juos susisteminus, bus galima pateikti rezultatus ir sujungti juos su kiekybinio tyrimo rezultatais ir išvadomis bei apjungus pateikti geriausias ir praktiškiausias rekomendacijas.



3.6 pav. Detalus kokybinio tyrimo planas, sudaryta darbo autoriaus

3.2.2. Kokybinio tyrimo klausimų sudarymo planas

Kokybiniame tyrime kuriant klausimyną svarbu neatitolti nuo apklausos klausimyno, kadangi tai gali papildyti bendrą analizę ir sujungus abiejų tyrimo rezultatus galima prieiti bendrų išvadų ar rekomendacijų. Interviu turi būt planuojamas taip, kad būtų galima interpretuoti apklausos duomenis ir diskutuojant su kibernetinio saugumo specialistus panagrinėti giliau ir aptarti subjektyvias darbuotojų įžvalgas, kurias vėliau būtų galima sistemingai lyginti su kiekybinės analizės rezultatais.

Interviu klausimai yra svarbus tyrimo etapas, leidžiantis giliau įsigilinti į klausimus ir atsakymus, gautus per apklausą. Jie leidžia užduoti atviresnius, detaliais pavyzdžiais paremtus klausimus, o tai padeda suvokti ir išgryninti dalyvių patirtis bei požiūrius. Kiekvienas pradinis klausimas turės savo tikslą ar bus savaip susijęs su pagrindinės hipotezėmis ar apklausos klausimais, tad tai ir yra aprašoma lentelėje apačioje (3.4 lentelė).

3.4 lentelė. Kiekvieno interviu klausimo tikslas, sudaryta darbo autoriaus

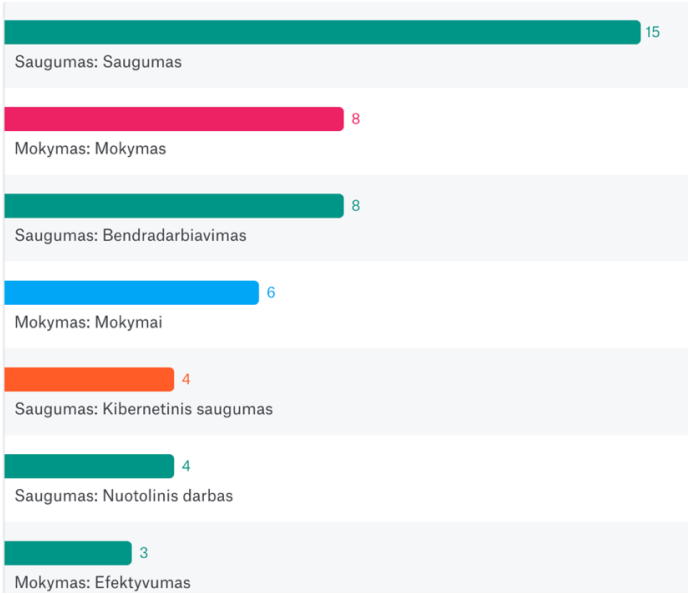
Interviu klausimas arba klausimai	Paaiškinimas ar klausimo ar klausimų tikslas
Ar galite apibūdinti atvejį, kai tarp funkcinis bendradarbiavimas turėjo teigiamos įtakos kibernetinio saugumo mokymų įgyvendinimui?	Ieškoma tikroviškų pavyzdžių, kurie iliustruotų pirmąją hipotezę apie organizacijos funkcinių padalinių bendradarbiavimo poveikį kibernetinio saugumo mokymo veiksmingumui. Tai padės tirti, kaip konkretūs bendradarbiavimo atvejai atitinka

	anketos rezultatus, susijusius su funkcinių padalinių bendradarbiavimu ir mokymų efektyvumu.
Kaip tarpžinybinis bendradarbiavimas veikia kibernetinio saugumo mokymų efektyvumą pagal jūsų patirtį?	Padės aptarti tarpžinybinio bendradarbiavimo veiksmingumą, o tai tiesiogiai sietina su pirmąja hipoteze. Respondentams suteikiama galimybė dalintis asmeninėmis patirtimis.
Ar galėtumėte pateikti nuolatinio stiprinimo strategijų, naudojamų jūsų organizacijoje, siekiant padidinti informuotumą apie kibernetinį saugumą, pavyzdžių? Kaip manote, ar šios strategijos yra veiksmingos skatinant įsitraukti į kibernetinio saugumo praktiką?	Šie du klausimai yra susiję su antrąją hipoteze, susijusia su nuolatinės stiprinimo strategijų veiksmingumu. Respondentams leidžiama išsamiai nusakyti naudojamas strategijas, pateikti konkrečias situacijas ir įvertinti jų poveikį.
Ar Jūsų organizacija yra kūrusi sąmoningumo programas remiantis NIST saugumo mokymų rekomendacijomis? Ar galite paliudyti, kaip organizacija naudoja NIST CSF, kad identifikuoti, įvertinti ir valdyti kibernetines rizikas?	Šie du klausimai yra susiję su organizaciniais veiksniais ir NIST saugumo mokymų rekomendacijomis, kurie gali turėti įtaką kibernetinio saugumo praktikos išlaikymui, t.y., trečiąją hipotezę. Padės interviu metu gilintis į tai, kaip organizacijos politikos ir procedūros naudoja NIST standartus.
Kaip nuotolinio darbo saugumo politikos ir praktikos yra kuriamos ir įdiegiamos remiantis NIST CSF valdymo rekomendacijomis? Ar galėtumėte pasidalinti strategijomis, kurios buvo veiksmingos nustatant galimas grėsmes saugumui ir apie jas pranešant, pvz., sukčiavimo atakas ir išpirkos reikalaujančias programas?	Šių dviejų klausimų tikslas yra ištirti, kaip įmonės kuria ir taiko politiką bei praktikas, orientuotas į nuotolinį darbą ir grėsmių valdymą, ypač į nuotolinio darbo saugumo pasiruošimo ir grėsmių valdymo temas.

Svarbu paminėti, kad čia yra pradiniai klausimai, kurie sudaro pagrindą interviu metu, tačiau tyrimo eigoje kalbant su įmonės kibernetinio saugumo vadovu bus panaudoti ir papildomi klausimai diskusijai dėl tam tikrų apklausos ir interviu atsakymų.

3.2.3. Kokybinio tyrimo analizė

Kokybinio tyrimo prielaidos buvo susijusios su hipotezėmis kurios buvo pristatytos jau ankščiau, bei dauguma klausimų buvo susiję su apklausos klausimyne esančiais klausimais, kurie išvadų ir rekomendacijų metu galės papildyti vienas kitą. Kiekvienas interviu vyko gyvai ir visi atsakymai buvo vedami į kompiuterio užrašinę. Gauti interviu atsakymai į pagrindinius klausimus, buvo analizuojami pasitelkiant „Atlas.ti“ įrankį, kuriame įkelti visi klausimai ir respondentų atsakymai automatiškai leido suskirstyti visus atsakymus į „kodus“, kurių pagalbą buvo galima matyti, kaip respondentai minėjo tam tikras sąvokas ar žodžius, kurių pagalba buvo galima lengviau ir grupuoti ar analizuoti atsakymus. Įrankio metu buvo pastebėta ir sukurta virš 20 kodų, kurie turi bent kelis panaudojimus įkeltame dokumente. Kitais žodžiais tariant, buvo aptikta virš 20 skirtingų frazių ar sąvokų, kurios buvo paminėtos bent jau keliuose skirtinguose pokalbiuose. Labiausiai respondentų minėtas žodis buvo „saugumas“ net 15 kartų, taip pat „mokymas“ arba „bendradarbiavimas po 8 kartus ar “nuotolinis darbas” 4 kartus. Platesnis sąrašas pateiktas lentelėje apačioje (3.7 paveikslas).



3.7 pav. „Atlas.ti“dažniausiai pasikartojančių žodžių sąrašas interviu metu

Suprantama, jog interviu metu sąvoka „saugumas“ buvo panaudota daugiausiai, nes aplink tai ir buvo visi klausimai užduodami. Tačiau daug respondentų užsiminė apie bendradarbiavimo bei mokymų svarbą siekiant pagerint įmonės kibernetinį saugumo lygį.

Kibernetinio saugumo specialistai pokalbio metu dažniausiai išskyrė bendradarbiavimo svarbą, kuomet buvo kalbama apie tarp funkcinį bendradarbiavimą ir kaip sėkmingas tarp funkcinio bendradarbiavimas gali būt priežastis ir priedas kalbant apie efektyvius mokymus.

Pavyzdžiui, pateiktoje lentelėje yra nurodyti net 4 atsakymai, kurie yra skirtingų specialistų, tačiau bendra vyraujanti nuomonė apie sėkmingą tarp funkcinį bendradarbiavimą (3.5 lentelė).

3.5 lentelė. Respondentų citatos susijusios su tarp funkciniu bendradarbiavimu

Respondentas	Citata susijusi su tarp funkciniu bendradarbiavimu
R01	„<..>Tarp funkcinis bendradarbiavimas mūsų organizacijoje paskatino tikslingesnius ir veiksmingesnius kibernetinio saugumo mokymus. Įtraukdami įvairius skyrius, galėjome pašalinti konkrečias pažeidžiamumas ir atitinkamai pritaikyti mokymus.<..>“
R02	„<..>Tokio bendradarbiavimo rezultate išgryninamos aktualios temos, vietos, konkretūs neapibrėžtumai <..>”
R03	„<..>Tarp funkcinis bendradarbiavimas buvo labai svarbus mūsų organizacijos kibernetinio saugumo mokymuose. Tai leido sukurti išsamesnę ir veiksmingesnę mokymo programą.<..>”
R04	„<..>Šis sinergijos pavyzdys skatino darbuotojus dalyvauti ir aktyviau įsisavinti mokymo medžiagą, nes mokymai buvo tiesiogiai susiję su jų kasdienėmis funkcijomis.<..>“

Siekiant detaliau išnagrinėti interviu metu išryškintas tarpfunkcinio bendradarbiavimo pranašumus, svarbu paminėti, kad atvira komunikacija tarp skirtingų organizacijos padalinių prisideda prie kibernetinio saugumo stiprinimo. Specialistai akcentavo, jog ši bendradarbiavimo dimensija leidžia permąstyti standartinius mokymų programas ir orientuoti jas ne tik į saugumo teoriją, bet ir praktines kasdienio darbo situacijas. Šis individualizuotas požiūris į mokymus kuria asmens atsakomybės jausmą ir gerina gebėjimus taikyti mokytas procedūras tikrose darbo aplinkose. Daug respondentų taip pat išskyrė tarpžinybinio bendradarbiavimo naudą, priimant sprendimus ir planuojant saugumo politikas. Tai reiškia, jog mokymų kokybė ir prieinamumas yra neatsiejami nuo komunikacijos efektyvumo ir skyrių vadovų iniciatyvumo. Būtina atkreipti dėmesį, kad tarpusavio ugdymas ir žinių mainai tarp skirtingų padalinių yra neįkainojama vertybė, leidžianti organizacijai veiksmingai reaguoti į nuolatiniai kibernetinės aplinkos kaitą. Tačiau tik dėl laiko trūkumo ir šio tyrimo apimties dar nebuvo įmanoma giliai analizuoti visų tarp funkcinių bendradarbiavimo aspektų.

Kitas, tikrai ne mažiau reikšmingas terminas, kurį dažnai pabrėžė interviu metu specialistai, yra „mokymai“ ir „mokymų efektyvumas“. Ankstesnėje analizėje jau yra aptarta, kaip sėkmingas skirtingų departamentų tarp funkcinis bendradarbiavimas gali būti laikomas puikiu mokymų pasekmių pavyzdžiu. Toks bendradarbiavimas leidžia skirtingų padalinių darbuotojams drąsiai keistis informacija, užduoti klausimus kibernetinio saugumo specialistams bei kartu sumažinti riziką įmonės gerovei. Tačiau svarbu sužinoti, kokios kitos sudedamosios dalys lemia efektyvius ir naudingus mokymus. Atlikta analizė parodo, kad efektyvūs kibernetinio saugumo mokymai turėtų jungti teorines žinias su praktiniais užsiėmimais, kurie padeda saugumo principus įgyvendinti praktiškai. Susistemintų organizacijų atsakymai rodo, kad nuolatinė mokymosi kultūra yra gyvybiškai svarbi ilgalaikių saugumo praktikų palaikymui ir stiprinimui. Esminę efektyvių mokymų dalį sudaro informacijos atnaujinimas ir nuolatinė mokymų organizacija. Vienas iš respondentų išskyrė, kad: „<..>Kiekvieną savaitę siunčiami laiškai apie kibernetines naujienas, naujas grėsmes, taip pat darbuotojai pasirinktinai kviečiami į savanoriškus mokymus apie saugumą<..>“. Ši pastaba pabrėžia, kad nuolatinis sąmoningumo palaikymas yra kritinis mokymų efektyvumo veiksnys. Analizuojant mokymų programą, kitas respondentas paminėjo, kad organizacija įgyvendina „nuolatinę kibernetinio saugumo informavimo programą“, kuri suteikia darbuotojams reikalingas žinias ir įrankius, siekiant stiprinti saugumą, akcentavo aktyvų įsitraukimą ir patirties dalijimąsi kaip svarbų mokymosi aspektą. Respondentų atsakymų analizė taip pat atskleidžia, kad organizaciniai veiksniai, tokie kaip vadovybės palaikymas, techninė kontrolė, stebėsena, reguliarūs atnaujinimai ir kultūra, kuri įvertina saugumą labai svarbūs siekiant išlaikyti kibernetinio saugumo praktiką. Dar vienas specialistas minėjo, kad: „<..> Keletas organizacinių veiksnių turi įtakos kibernetinio saugumo

praktikos išlaikymui po mokymų <..>“. Tai rodo, kad saugumo praktikos sėkmingam taikymui reikalingas visas organizacinis palaikymas.

Interviu metu atsakymai aiškiai parodo tarpfunkcinio bendradarbiavimo reikšmę ir neatskyrimą nuo kibernetinio saugumo mokymų veiksmingumo. Lyginamoji duomenų analizė yra neįkainojama: ji leidžia nustatyti, ar tarp funkcinis bendradarbiavimas yra tik saugumo specialistų pabrėžiamas elementas, ar tai yra universalus ir viso darbuotojų rato pripažintas reiškinys. Interviu metu išryškėjusios įžvalgos ne tik atitinka modernius kibernetinio saugumo standartus, bet ir suteikia tvirtą pagrindą tolesniam mokslinių tyrimų vystymui ir praktinių mokymų programų tobulinimui. Šios įžvalgos padeda organizacijoms ir darbuotojams ne tik pakelti saugumo kultūros lygį, bet ir geriau suprasti naujausias grėsmes bei efektyvius būdus į jas reaguoti.

Išvadoje būtina pabrėžti, kad mokymų veiksmingumas yra maksimaliai didinamas, kai jie yra integruoti į organizacijos kultūrą, o mokymų turinys yra reguliariai atnaujinamas ir pritaikytas praktiniam pritaikymui. Svarbus yra ne tik mokymų pritaikymas prie konkrečių darbo funkcijų, bet ir kiekvieno darbuotojo aktyvus įsitraukimas į saugumo procesus, leidžiantis kibernetiniam saugumui tapti kasdienio darbo dalimi. Ypatingas dėmesys turėtų būti skiriamas reguliariems priminimams, interaktyviems mokymams ir realių incidentų analizei, kurie, kaip minėjo respondentai, yra kritiškai svarbūs skatinant darbuotojų sąmoningumą ir paruošimą tinkamai reaguoti į esamas bei potencialias grėsmes.

3.2.4. Interviu metu papildomai užduoti klausimai

Interviu metu buvo kalbinami skirtingų rangų specialistai nuo jaunesniojo specialisto kibernetinio saugumo klausimais iki asmens, kuris yra atsakingas už visos įmonės kibernetinį saugumą (CSO). Būtent interviu metu, kuomet buvo kalbama su įmonės kibernetinio saugumo vadovu, tam tikri klausimai buvo papildyti rezultatais iš apklausos ir taip sukurti keli papildomai klausimai, norint iki galo suprasti, kodėl tam tikri procesai yra prašomi iš darbuotojų pusės ir kokia nuomonė asmens, kuris yra už tai atsakingas. Keliant diskusiją buvo iškelti keli svarbiausi aspektai, tokie kaip: Tarp funkcinis bendradarbiavimas, NIST platformos pagalba ir taikymas įmonėje bei apklausos metu gauti atsakymai į atvirą klausimą, kuriame reikėjo pabrėžti, ką reiktų keisti įmonėje.

Lentelėje apačioje yra nurodyti tikslūs klausimai, bei išsamūs kibernetinio saugumo vadovo atsakymai (3.6 lentelė).

3.6 lentelė. Papildomi klausimai užduoti įmonės CSO, sudaryta darbo autoriaus

Diskusijos klausimas	Kibernetinio saugumo vadovo atsakymas
„Apklausiant įmonės darbuotojus dažnas atsakovas išskyrė, jog tarp funkcinis bendradarbiavimas įmonėje yra labai svarbus, tačiau klausime: „Kaip dažnai jūsų organizacija dalyvauja tarpžinybiniame	„Tiesa, kad interviu metu pabrėžtas tarp funkcinis bendradarbiavimas, ir mes jį laikome Iškilia organizacijos vertybe. Mes galime stebėti vidutinį rezultatą 3.38 tarpžinybinio bendradarbiavimo

bendradarbiavime kibernetinio saugumo klausimais skalėje nuo 1 (niekada) iki 5 (visada)?“ Įmonės darbuotojai vidutiniškai rinkdavosi 3.38, kodėl net ir kiti kibernetinio saugumo specialistai įvertina tokia svarba tarp funkcinio bendradarbiavimo, tačiau jisai ne iki galo yra pritaikytas ir naudojamas įmonėje?“	skalėje ir tai atspindi realybę, jog, nors šis bendradarbiavimas yra vertinamas, jis dar nėra visapusiškai įsisąmonintas ar įgyvendintas. Tai gali atsirasti dėl įvairių priežasčių, tokių kaip struktūros silpnybės, neadekvačios komunikacijos strategijos ar tiesiog kasdienės veiklos iššūkių. Mūsų tikslas – ugdyti tokią kultūrą, kurioje tarpfunkcinio bendradarbiavimas būtų natūralus ir nuolatinis procesas, o ne „ad hoc“ iniciatyva. Tai pasiekus, kibernetinio saugumo efektyvumas ženkliai padidėtų.“
„Kadangi Jūs esat CSO, manau jus geriausiai galėtume pakomentuoti esama situacija įmonėje pasitelkiant NIST CSF -> Ar Jūsų organizacija yra kūrusi sąmoningumo programas remiantis NIST saugumo mokymų rekomendacijomis?“	„Taip, mes kuriame ir tobuliname sąmoningumo programas vadovaudamiesi NIST rekomendacijomis. Tai yra mūsų saugumo ugdymo pagrindas. Mes taip pat ieškome būdų, kaip adaptuoti šias rekomendacijas pagal mūsų specifinius poreikius ir kibernetinio saugumo bendrąjį vaizdą. Mūsų tikslas yra ne tik atitikti standartus, bet ir užtikrinti, kad mokymai būtų gerai įsimintini mūsų darbuotojams, taip formuojant tvirtą saugumo pajautą.“
„Apklausiant įmonės darbuotojus, dažnas išskyrė šias pastabas, kuomet buvo kalbama apie pokyčius, kuriuos jie norėtų matyti įmonėje kalbant apie kibernetinio saugumo mokymus, pastabos buvo visokios nuo paprasčiausio mažo kiekio iki veiksmingumo trūkumo mokymuose ar mažo interaktyvumo, kaip jūs vertinate tai ir ar bus imtasi kažkokių pokyčių ir atsižvelgiama į darbuotojų pastabas?“	„Šie respondentų atsakymai yra labai informatyvūs ir juos vertinu kaip vertingą grįžtamąjį ryšį. Aišku, kad reikalingas mokymų patobulinimas ir personalizavimas, kad jie taptų dar efektyvesni. Interaktyvūs mokymai, dažnesnė praktika, pavyzdžių ir atlikimų įtraukimas, taip pat aiškesnis ir gilesnis suvokimas apie kibernetinio saugumo svarbą – visa tai liudija apie mūsų darbuotojų norą mokytis ir tobulėti. Planuojame įtraukti šias rekomendacijas į mūsų esamas ir būsimas mokymų programas, siekiant užtikrinti, kad mūsų darbuotojai ne tik žinotų apie saugumą, bet ir sugebėtų veiksmingai taikyti šias žinias realiame gyvenime.“

3.2.5. Kokybinio tyrimo rekomendacijos

Remiantis interviu metu gautais duomenimis, organizacijai yra pateikiamas rekomendacijų planas, kuris apima kelias kertines sritis. Pirmiausia, reiktų puoselėti ir sistemiškai stiprinti tarp funkcinį bendradarbiavimą, įtraukiant darbuotojus iš skirtingų padalinių į saugumo procesus ir svarbių sprendimų priėmimą, taip stiprinant visos įmonės saugumo pajėgumus. Tęsti darbą su NIST saugumo standartais, šių standartų ir rekomendacijų integravimą bei adaptaciją prie specifinių organizacijos poreikių, siekiant pagerinti mokymų programų atitikimą darbuotojų lūkesčiams ir užtikrinti jų efektyvumą praktinėje aplinkoje.

Be to, rekomenduojama didinti mokymuose interaktyvumo lygį, įtraukiant darbuotojus į daugiau praktinių užduočių, atvejų analizę ir imituojamus sukčiavimo išpuolius, siekiant sutvirtinti saugumo žinių taikymą ir užtikrinti ilgalaikį mokymosi poveikį. Taip pat, reguliariai atnaujinti

mokymus, atsižvelgiant į naujausias saugumo tendencijas ir grėsmių evoliuciją, taip užtikrinant, kad mokymo programos išliktų aktualios.

Galiausiai, svarbu paminėti organizacinės kultūros gerinimo svarbą, įskaitant vadovų įsipareigojimą ir nuolatinį įtraukimą į saugumo iniciatyvas. Šiuo palaikymu ne tik sustiprinama kibernetinio saugumo svarbos supratimą visame įmonės lygmenyje, bet ir palaikomas darbuotojų sąmoningumas bei atsakomybės jausmas. Šis holistinis požiūris yra gyvybiškai svarbus, siekiant sukurti galingą ir efektyvią saugumo strategiją, kuri sumaniai apjungia žmogiškąjį faktorių ir technologinius sprendimus.

3.2.6. Kokybinio tyrimo išvados

Interviu rezultatai atskleidė, jog tarpfunkcinio tipo bendradarbiavimas yra išties svarbus organizacijos saugumo kultūrai stiprinti ir mokymų efektyvumui užtikrinti. Tyrimo metu gautas akcentas - kad nors saugumo specialistai pripažįsta šio bendradarbiavimo svarbą, įmonėje jis dar nėra pilnai pritaikytas. Tai rodo, kad, nors egzistuoja tvirtas pagrindas, būtina toliau tobulinti bendradarbiavimo procesus, siekiant atitikti aukščiausius kibernetinio saugumo standartus.

Taikyti NIST saugumo mokymų standartus bei rekomendacijas į organizacijos sąmoningumo programas yra strategiškai svarbu, kaip pabrėžia tyrimo duomenys ir kibernetinio saugumo vadovo komentarai. Siekiama ne tik paisyti šių standartų, bet ir adaptuoti juos taip, kad maksimaliai atitiktų konkretų saugumo kraštovaizdį ir darbuotojų poreikius.

Darbuotojų grįžtamasis ryšys apie mokymus yra vertinamas kaip esminis mokymų patobulinimo aspektas. Organizacija turėtų suprasti interaktyvumo, praktikumo ir mokymų dažnio svarbą, o tai atspindi darbuotojų norą ir motyvaciją platesniu aspektu įsitraukti į saugumo procesus. Todėl tais atvejais, kai darbuotojai pažymi mokymų trūkumus ir siūlo jų patobulinimus - tai yra signalas, jog reikia imtis veiksmų, garantuojančių efektyvesnį mokymų turinį ir pristatymą.

Interviu ir apklausos duomenų sujungimas atneš išsamias išvadas ir leis sukurti visapusiškas rekomendacijas, atspindinčias darbuotojų nuomonę ir įmonės vadovų įžvalgas. Sutelkus dėmesį į šiuos susistemintus atsakymus, bus galima efektyviai tobulinti saugumo strategijas ir užtikrinti, kad organizacija ir toliau būtų saugi ir atspari kibernetinėms grėsmėms.

3.3. Kiekybinio ir kokybinio tyrimų rezultatų apibendrinimas

Sudėliojus gautų duomenų rezultatus iš kiekybinio ir kokybinio tyrimo, galima pastebėti, kad abu tyrinėjimo metodai ne tik papildo, bet ir stiprina vienas kitą, suteikdami pranašumą suprasti, kaip organizacijoje yra suvokiamas ir praktikuojamas kibernetinis saugumas. Kiekybiniame tyrime gauti darbuotojų pasireiškimai dėl mokymų dažnumo, interaktyvumo ir supratimo apie saugumo svarbą davė išsamų kokybinį atsaką, kuris toliau buvo gilinamas per kokybinį tyrimą, atskleidžiant

konkrečius pavyzdžius ir gyvas įžvalgas iš saugumo specialistų. Organizacijoje vykdyti tyrimai neabejotinai suteikė išsamų vaizdą apie kibernetinio saugumo supratimą ir praktikas. Analizė parodė, kad tiek darbuotojų apklausa, tiek interviu su saugumo specialistais dvejopai prisideda prie bendro suvokimo: vieni atskleidžia bendrą tendenciją, kiti gilina kontekstą ir pateikia praktinius pavyzdžius. Pavyzdžiui, kol apklausoje fiksuotas vidutiniškai teigiamas požiūris į tarp funkcinį bendradarbiavimą galimai atspindi tą svarbą, kuri vadovaujamajame lygyje jau yra suvokiama, kokybinių interviu metu kalbinti vadovai siūlo konkrečius sprendimus, kaip sėkmingai įgyvendinti ir tobulinti šią praktiką. Taip pat, apklausos metu gautas mokymų dažnumo ir interaktyvumo įvertinimas rodo, kad darbuotojai jaučia mokymų reikšmę ir nori dažniau bei aktyviau dalyvauti mokymuose. Kitapus, interviu metu vadovų pateikti konkretūs pasiūlymai dėl mokymų turinio praplėtimo ir simuliacijų įdiegimo rodo aiškų ketinimą šias lūkesčius įgyvendinti ir tobulinti esamas programas. Analizuojant duomenis iš abiejų tyrimų, tapo aišku, jog pavyzdžiui, tarpfunkcinio bendradarbiavimo svarba, kuri buvo vertinama apklausoje vidutiniškai 3.38 balais, interviu metu buvo praplatinta su CSO pateiktais konkrečiais veiksmų planais ir procesais, kurie gali sukurti struktūrizuotą ir tikslinį bendradarbiavimo modelį įmonėje. Tai rodo, kad vertinant vien iš kiekybinio tyrimo pusės, gauname bendrą vaizdą, o iš kokybinio - konkrečią, taikomą informaciją strategijoms tobulinti. Nuolatinės mokymų tobulinimo galimybės - kiekvienas tyrimas parodė poreikį šiuolaikinti ir kurti dinameškesnius mokymus. Apklausoje darbuotojai minėjo interaktyvumo trūkumą bei retus mokymus, o interviu metu kibernetinio saugumo specialistai pabrėžė, kad mokymai turėtų būti praktinių užduočių įtraukiami, bei rengiami dažniau, atliepiančius realias darbuotojų ir įmonės aplinkybes. Priešingai nei ankstesnėje proceso dalies ištrauka numanoma, kiekybinis tyrimas atskleidžia reikšmingus signalus, kuriuos patvirtina ar išplėtoja kokybinis tyrimas. Pavyzdžiui, noras padidinti mokymų skaičių buvo minėtas ne kartą, o CSO patvirtino, kad siekiama tapti lankstesniems prie naujovių, stiprinant mokymų programas bei mokyklų turį įmonėje. Toks duomenų derinys parodė kur reikia siekti pokyčių ir kaip tai įgyvendinti.

Visos šios sujungtos išvados nukreipia dėmesį į tris esminius mokymų aspektus: integravimą, praktiškumą ir nuolatinį atnaujinimą, kurie bus svarbus žingsniai organizacijai kuriant ne tik veiksmingas, bet ir darbuotojų poreikius atitinkančias saugumo mokymų programas. Įdiegiant šias rekomendacijas, organizacija taps geriau pasiruošusi įveikti kibernetinio saugumo iššūkius, sukuriant tvirtą saugumo kultūros pagrindą ir maksimaliai išnaudojant turimus išteklius.

4. IŠVADOS

1. Mokslinė literatūra atskleidžia, kad mažos ir vidutinės įmonės yra itin pažeidžiamos kibernetinių atakų, tvirtų saugos protokolų palaikymas ir reguliarus saugumo politikos ir praktikos atnaujinimas yra pagrindinis veiksnys mažinant šį pažeidžiamumą. Tolesni doktorantūros tyrimai galėtų ištirti ilgalaikį šių protokolų poveikį kibernetinei rizikai mažinti įvairiuose MVĮ kontekstuose.
2. Praktinė tyrimo dalis parodė, kad darbuotojų mokymas turi būt orientuotas į interaktyvumą bei pritaikytas prie realių kasdieninės veiklos situacijų, kas padės užtikrinti žinių ir gebėjimų pritaikymą praktikoje.
3. Tyrimas atskleidė tarpfunkcinio bendradarbiavimo svarbą veiksmingai kibernetinio saugumo praktikai. Labiau tikėtina, kad organizacijos, skatinančios dalytis žiniomis tarp padalinių, sukurs stiprią saugumo kultūrą. Papildomi moksliniai tyrimai doktorantūros lygmeniu galėtų gilintis į tokių bendradarbiavimo struktūrų mechanizmus ir rezultatus.
4. Organizacinės kultūros ir valdymo palaikymas kartu su nuolatiniu mokymo programų atnaujinimu sudaro ilgalaikio ir efektyvaus kibernetinio saugumo supratimo organizacijoje pagrindą. Vadovybės įsipareigojimas ne tik inicijuoti, bet ir palaikyti saugos praktiką yra labai svarbus siekiant puoselėti saugos kultūrą ir įtraukti komandą. Šis sudėtingas kultūros ir praktikos santykis, esminis kovojant su kibernetinėmis grėsmėmis, suteikia tolesnių tyrimų galimybių, kurias būtų galima ištirti doktorantūros studijų metu.

Literatūros šaltiniai

What is cybersecurity?. Iš

https://www.techtarget.com/searchsecurity/definition/cybersecurity (žiūrėta 2023 - 12 - 25)

How Businesses Can Fight Cybersecurity Risks in Today's Digital World. Iš

https://blog.smu.edu.sg/lb/ed/how-businesses-can-fight-cybersecurity-risks-in-todays-digital-world/ (žiūrėta 2023 - 12 - 25)

Top 5 Cyber Security Risks for Businesses. Iš

https://www.itgovernance.co.uk/blog/top-5-cyber-security-risks-for-businesses (žiūrėta 2023 - 12 - 25)

Cyber Risk Is Rising: Here Is How Companies Can Tackle Tomorrow's Threats Today. Iš

https://www.forbes.com/sites/garydrenik/2022/11/21/cyber-risk-is-rising-here-is-how-companies-can-tackle-tomorrows-threats-today/?sh=7f88b766dc3e (žiūrėta 2023 - 12 - 25)

The 21 Latest Emerging Cyber Threats to Avoid. Iš

https://www.aura.com/learn/emerging-cyber-threats (žiūrėta 2023 - 12 - 25)

CYBERSECURITY: AMONG THE TOP 3 RISKS TO BUSINESSES IN 2021. Iš

https://www.tbconsulting.com/cybersecurity-among-the-top-3-risks-to-business (žiūrėta 2023 - 12 - 25)

Cybersecurity trends: Looking over the horizon. Iš

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon (žiūrėta 2023 - 12 – 25)

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022, May 1). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry. Elsevier B.V. https://doi.org/10.1016/j.compind.2022.103614

Back, S., & Guerette, R. T. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. Journal of Contemporary Criminal Justice, 37(3), 427–451. https://doi.org/10.1177/10439862211001628

Myriam Dunn Cavelty, From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, International Studies Review, Volume 15, Issue 1, March 2013, Pages 105–122, https://doi.org/10.1111/misr.12023

10 Cybersecurity Best Practices for Corporations in 2023. Iš

https://research.aimultiple.com/cybersecurity-best-practices/ (žiūrėta 2023 - 12 - 25)

Luigi Gallo, Danilo Gentile, Saverio Ruggiero, Alessio Botta, Giorgio Ventre, The human factor in phishing: collecting and analyzing user behavior when reading emails, Computers & Security, 2023, 103671, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103671

Giuseppe Desolda, Lauren S. Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile. 2021. Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Comput. Surv. 54, 8, Article 173 (November 2022), 35 pages. https://doi.org/10.1145/3469886

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. Computers and Security, 95. https://doi.org/10.1016/j.cose.2020.101827

Naurin Farooq Khan, Naveed Ikram, Hajra Murtaza, Mehwish Javed, Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model, Computers & Security, Volume 125,2023,103049,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.103049. (https://www.sciencedirect.com/science/article/pii/S0167404822004412)

Hayes, J. & Bodhani, A.. (2013). Cyber security: small firms under fire [InformatIon Technology Professionalism]. Engineering & Technology. 8. 80-83. 10.1049/et.2013.0614.

Money makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report iš https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report (žiūrėta 2024 - 01 - 02)

What's new in the 2023 Cost of a Data Breach report Iš https://securityintelligence.com/posts/whats-new-2023-cost-of-a-data-breach-report/ (žiūrėta 2024 - 01 - 02)

Dawkins, S. and Jacobs, J. (2023), Phishing With a Net: The NIST Phish Scale and Cybersecurity Awareness, RSA Conference 2023: Human Element Track, San Francisco, CA, US, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936343

Polk, W. (2017), Enhancing Resilience of the Internet and Communications Ecosystem: A NIST Workshop Proceedings, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8192

NIST CYBERFRAMEWORK. Iš

https://www.nist.gov/cyberframework (žiūrėta 2024 – 01 – 02)

NIST CYBERSECURITY FRAMEWORK. Iš

https://www.balbix.com/insights/nist-cybersecurity-framework/ (žiūrėta 2024 – 01 – 02)

NIST RMF FRAMEWORK. Iš

https://csrc.nist.gov/projects/risk-management/about-rmf (žiūrėta 2024 – 01 – 02)

NIST FRAMEWORK CENTER. Iš

https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center (žiūrėta 2024 – 01 – 02)

NIST CET. Iš

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=861637 (žiūrėta 2024 – 01 – 02)

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons, 63(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Chidukwani, S. Zander and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," in IEEE Access, vol. 10, pp. 85701-85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

Ebad, Shouki. (2021). Security Assessment of Large-Scale IT Infrastructure. 22. 10.37575/b/cmp/0055.

Sánchez, L. E., Santos-Olmo, A., Fernández-Medina, E., & Piattini, M. (2010). Security culture in small and medium-size enterprise. In Communications in Computer and Information Science (Vol. 110 CCIS, pp. 315–324). https://doi.org/10.1007/978-3-642-16419-4_32

Ben-Asher, N., & González, C. (2015). Effects of cyber security knowledge on attack detection. Comput. Hum. Behav.. https://www.semanticscholar.org/paper/Effects-of-cyber-security-knowledge-on-attack-Ben-Asher-Gonz%C3%A1lez/923218d1201b12738aef735c131af036f69a847b

Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535, https://doi.org/10.1016/j.inffus.2023.101804.

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In Proceedings of the Annual Hawaii International Conference on System Sciences (Vol. 2019-January, pp. 6398–6407). IEEE Computer Society. https://doi.org/10.24251/hicss.2019.769

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. Journal of Intellectual Capital, 21(2), 203–213. https://doi.org/10.1108/JIC-05-2019-0112

ENTERPRISE CYBER SECURITY: A COMPARATIVE STUDY OF METHODOLOGIES AND FACTORS AFFECTING TRAINING EFFECTIVENESS

Vilius Pečiulis

Master Thesis

Strategic information system management programme

Vilnius University

Faculty of Economis and Business Administration

Supervisor – Assoc., Dr. Mindaugas Krutinis

Vilnius, 2024

SUMMARY

61 pages, 13 tables, 10 pictures, 33 literature sources.

The objective of the master's thesis: To improve the cyber security strategy of the organization. This will be done through a detailed analysis and comparison of various cyber security assessment methods and an examination of the factors affecting the effectiveness of training. **The master's thesis consists of two main parts and their description:** Literature analysis: this part includes a detailed review of scientific articles in order to determine the main characteristics and methods of assessing and determining the company's cyber security. The vulnerability of companies of different sizes and different sectors of the economy is also examined. Practical Part: In this part, the method chosen from the literature review is applied to a real-world scenario. This includes surveying and interviewing Company A to analyze its cybersecurity posture and identify ways to improve it. **Applied methods:** To achieve the objectives of the master's thesis and to answer the research questions, various methods were used, such as live interviews, surveys, literature sources.

The most important results of the master's thesis: The work identified several challenges of cyber security assessment, including limited resources, knowledge and competence gaps, and a rapidly changing and complex threat environment. Also, solutions to reduce this risk are proposed, including optimization of assessment methods, implementation of continuous improvement strategies

and raising employee awareness. These measures are designed to ensure the security of systems and data, thereby protecting the organization from potential cyber threats.

Keywords: Cyber security, Evaluation methods, Continuous improvement strategies, Employee awareness, Risk reduction.

ĮMONĖS KIBERNETINIS SAUGUMAS: METODIKŲ IR VEIKSNIŲ, TURINČIŲ ĮTAKOS MOKYMO EFEKTYVUMUI PALYGINAMASIS TYRIMAS

Vilius Pečiulis

Magistro baigiamasis darbas

Strateginio informacinių sistemų valdymo studijų programa

Vilniaus Universitetas

Ekonomikos ir verslo administravimo fakultetas

Darbo vadovas – Doc., Dr. Mindaugas Krutinis

Vilnius, 2024

SANTRAUKA

61 puslapis, 13 lentelių, 10 paveikslų, 33 literatūros šaltinių.

Magistro baigiamojo darbo tikslas: Tobulinti organizacijos kibernetinio saugumo strategiją. Tai bus padaryta išsamiai išanalizavus ir palyginus įvairius kibernetinio saugumo vertinimo metodus bei išnagrinėjus veiksnius, turinčius įtakos mokymų efektyvumui. **Magistro darbas susideda iš dviejų pagrindinių dalių ir jų aprašymo:** Literatūros analizė: ši dalis apima išsamią mokslinių straipsnių apžvalgą, siekiant nustatyti pagrindines įmonės kibernetinio saugumo vertinimo ir nustatymo ypatybes ir metodus. Taip pat nagrinėjamas įvairaus dydžio ir įvairių ekonomikos sektorių įmonių pažeidžiamumas. Praktinė dalis: šioje dalyje iš literatūros analizės pasirinktas metodas taikomas realaus pasaulio scenarijui. Tai apima apklausą ir interviu įmonėje A, siekiant išanalizuoti jos kibernetinio saugumo būklę ir nustatyti būdus, kaip ją pagerinti. **Taikomi metodai:** Magistro baigiamojo darbo tikslams pasiekti ir į tyrimo klausimus atsakyti buvo taikomi įvairūs metodai, tokie kaip gyvi interviu, apklausos, literatūros šaltiniai.

Svarbiausi magistro baigiamojo darbo rezultatai: Darbe nustatyti keli kibernetinio saugumo vertinimo iššūkiai, įskaitant resursų ribotumą, žinių ir kompetencijų spragas bei greitai kintančią ir sudėtingą grėsmių aplinką. Taip pat, siūloma sprendimų, kaip sumažinti šią riziką, įskaitant vertinimo metodų optimizavimą, nuolatinio stiprinimo strategijų įgyvendinimą ir darbuotojų

informuotumo didinimą. Šios priemonės skirtos užtikrinti sistemų ir duomenų saugumą, taip apsaugant organizaciją nuo galimų kibernetinių grėsmių.

Raktiniai žodžiai: Kibernetinis saugumas, Vertinimo metodai, Nuolatinio tobulėjimo strategijos, Darbuotojų sąmoningumas, Rizikos mažinimas.