Co-funded by the European Union

SME CYBER SECURITY CHANGE AGENTS OPPLÆRINGSBEHOV KARTLEGGINGSRAPPORT

CYBER AGENT 10.2023

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.cyberagents.eu

Arbeidspakke 2: CyberAgent tilnærming og strukturdesign

Leveranse 2.2: SME Cyber Security Change Agents Opplæringsbehov kartleggingsrapport

Leder av WP2 – Olemisen Balanssia ry
Leder av leveranse 2.2 – Olemisen Balanssia ry

INNHOLD

INTRODUKSJON

Denne prosjektrapporten tar sikte på å analysere og kartlegge opplæringsbehovene for å identifisere passende kompetanser som kreves for en SME Cyber Security Change Agent. Gjennom en omfattende gjennomgang av dagens utdanningstilbud og forståelse av små og mellomstore bedrifters preferanser angående cybersikkerhetsspørsmål, søker denne rapporten å bygge en bro over gapet mellom nåværende kompetanse og definere det ideelle ferdighetssettet som kreves.

Etter hvert som cybertruslene blir mer sofistikerte, er det et stort behov for små og mellomstore bedrifter å sikre at de har tilstrekkelig opplært personell for å bekjempe disse truslene. Endringsagenter innen cybersikkerhet spiller en avgjørende rolle i denne sammenhengen. Denne prosjektrapporten analyserer cybersikkerhetslandskapet gjennom ulike perspektiver: Utdanning og opplæring, kjønnsinkludering og den nåværende tilstanden i små og mellomstore bedrifter og skoleinstitusjoner.

1. METODIKK

For denne kartleggingsprosessen brukte vi en blandet tilnærming som kombinerer skrivebords- og feltforskning.

I skrivebordsforskningen ble det gjennomført en omfattende litteraturgjennomgang for å:

- Gjennomgå eksisterende og nye utdanningsbestemmelser på VET og HE-nivå innen cybersikkerhet i hvert av partnerlandene. Innhenting og sammenstilling av artikler, hvitbøker, forskning og rapporter relatert til opplæringsinnhold og behov for cybersikkerhet.
- Analysere VET og HE-kurs, deres læreplaner og deres relevans for virkelige cybersikkerhetsutfordringer.

Målene var å:

- Å identifisere gjeldende pensumkomponenter for cybersikkerhetskurs som tilbys på VET og HE-nivå i hvert land.
- Å vurdere hvordan disse læreplanene samsvarer med cybersikkerhetsutfordringer.
- Identifiser om det er spesifikke strategier eller program for å involvere flere kvinner i cybersikkerhetsstudier.

I løpet av feltforskningsfasen gjennomførte vi 2 undersøkelser. En utformet for lærere og instruktører fra både VET- og HE-kategorier fra hvert land for å forstå nyansene i dagens opplæringstilbud. Den andre ble skreddersydd for små og mellomstore bedrifter for å få et syn og en forståelse av situasjonen i selskaper angående cybersikkerhet: Hvordan ansatte er involvert og engasjert i disse temaene, utfordringene og behovene. Fokuset på denne feltforskningen var også for å kartlegge egenskaper, opplæringsbehov og læringspreferanser, spesielt fremheve behovene til kvinner i cybersikkerhet.

Vi oppnådde et betydelig antall svar for begge spørreskjemaene. 190 lærere og instruktører fra yrkesfag og høgskole og 176 fra ansatte i små og mellomstore bedrifter.

Undersøkelse 1: Kartlegging av opplæringsbehov for SME Cyber Security Change Agents - **VET og HEI undersøkelse.**

Type institusjon	**Svar**	**Kvinne**	**Mann**	**Vil helst ikke si**
HEI (høyere utdanningsinstitusjoner)	104	28	73	3
VET (yrkesrettet utdanning og opplæring)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Undersøkelse 2: Kartlegging av opplæringsbehov for SME Cyber Security Change Agents - **SMEs undersøkelse.**

Antall svar	**Antall**
Små og mellomstore bedrifter	176
Total	**176**

Spørreskjemaer og fullstendige data finnes i vedlegg C og D.

2. FORSKNING (ALLE PARTNERE)

2.1. GJELDENDE UTDANNINGS- OG OPPLÆRINGSTILBUD

Denne delen presenterer forskningen og gir innsikt fra skrivebordsforskningen og undersøkelsene, og fremhever styrker og hull i dagens utdannings- og opplæringsinfrastruktur i partnerlandene.

2.1.1. OVERSIKT OVER UTDANNING INNEN CYBERSECURITY I VET OG HEI

Vi oppnådde en bred analyse av utdanningslandskapet for cybersikkerhet i alle partnerland for å beskrive den nåværende tilstanden og utløse de relevante aspektene ved utdanning og opplæring innen cybersikkerhet.

I Litauen[1] avslørte et søk i AIKOS-databasen totalt seks formelle utdanningsprogrammer innen cybersikkerhet som tilbys av litauiske institusjoner, som omfatter både bachelor- og masternivå:

Studieretning	Program	Institusjon	STUDIEPOENG	Grad
Informatikk ingeniørfag	Informasjons- og informasjonsteknologisikkerhet[2]	Kaunas teknologiske universitet	120	Master i informatikk
Ledelse	Administrasjon av cybersikkerhet[3]	Mykolas Romeris-universitetet	90	Master of Business Management
Informatikk ingeniørfag	Informasjons- og informasjonsteknologisikkerhet[4]	Vilnius Gediminas tekniske universitet	120	Master i informatikk
Informatikk ingeniørfag	Informasjonssystemer og cybersikkerhet[5]	Universitetet i Vilnius	210	Bachelor i informatikk
Informatikk ingeniørfag	Teknologier for informasjonssystemer og cybersikkerhet[6]	Høgskolen i Marijampole	180	Profesjonell bachelor i informatikk
Informatikk ingeniørfag	Cybersystemer og sikkerhet[7]	Høgskolen i Kaunas	180	Profesjonell bachelor i informatikk

Cybersecurity-programmene på masternivå viser distinkte, men komplementære tilnærminger. Kaunas Universitet legger vekt på forskningsmetodikk, informasjonssikkerhetsmetoder og de juridiske aspektene ved elektronisk rom, med fokus på utvikling av sikker IT-systemdesign og implementeringsevner. Vilnius Gediminas tekniske universitet prioriterer å danne spesialister med en systematisk tilnærming til informasjonssikkerhetsspørsmål, blande vitenskapelig

[1] Nøkkelord som ble brukt på jakt etter programmer var *cyber, sikkerhet* og deres variasjoner. Kilde: https://www.aikos.smm.lt/Puslapiai/Pradinis.aspx https://www.aikos.smm.lt/Puslapiai/Pradinis.aspx
[2] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[3] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[4] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[7] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

kunnskap med metoder og teknologier for å sikre informasjonssikkerhet, sammen med å fremme kritisk tenkning og lederskap. Mykolas Romeris Universitet lener seg imidlertid tydelig mot ledelse innen cybersikkerhet, med fokus på å produsere spesialister som er flinke til å overvåke moderne IT-miljøer og komplekse cybersikkerhetsoppgaver, med sterk vekt på strategisk ledelse i dynamiske teknologiske sammenhenger.

Bachelor-nivå cybersecurity studieprogrammene deler et kjernefokus på å utvikle dyktige fagfolk innen informatikk og cybersikkerhet, men hver med forskjellige vektlegging. Vilnius Universitets program er orientert mot å gi et omfattende fundament i informatikk engineering, med fokus på analyse, design, utvikling og vedlikehold av sikre informasjonssystemer. Høgskolen i Marijampole, tar også sikte på å utdanne kompetente informatikkspesialister, men legger større vekt på praktiske aspekter som å opprette, vedlikeholde og administrere datanettverk og -systemer. Høgskolen i Kaunas skiller seg ut ved å fokusere på å forberede spesialister med evner, ikke bare i utforming og implementering av cybersystemer, men også i å lede lag, forståelse etiske, juridiske og sosiale implikasjoner, og å arbeide effektivt i flerkulturelle miljøer. Mens alle tre institusjonene tar sikte på å utstyre studentene med tekniske ferdigheter innen cybersikkerhet, varierer deres mål fra teknisk ferdighet (Vilnius Universitet), praktisk anvendelse og myk kompetanseutvikling (Høgskolen i Marijampole), til en blanding av tekniske, ledelsesmessige og etiske hensyn (Høgskolen i Kaunas)

Søket avslørte også fire registrerte ikke-formelle voksenopplæringsprogrammer innen cybersikkerhet, som alle fokuserer på ferdigheter som er avgjørende for å gjenkjenne, undersøke og forhindre cyberangrep, spesielt ved bruk av kryptografi. Selv om alle programmene deler dette kjernemålet, er deres tilnærminger og omfang forskjellige. Noen er konsentrert om cybersikkerhet og forebyggende strategier, mens andre tilbyr en bredere læreplan, inkludert programmering, som dekker områder som sosialteknikk, identitetsstyring og risikostyring. Spesielt begynner flere programmer med grunnleggende programmering og fremgang til avanserte cybersikkerhetsemner, egnet for nybegynnere. Ett bemerkelsesverdig program, i samarbeid med Cybint, henvender seg til de med begrenset IT-kunnskap, og tilbyr praktiske ferdigheter i både heltids- og deltidsformater. Disse programmene tar samlet sikte på å utvikle ulike cybersikkerhetskompetanser, alt fra grunnleggende programmering til grundig, applikasjonsfokusert læring.

Flere politiske tiltak for å styrke Finlands nasjonale sikkerhet og forsvar har påvirket utdanningsprogrammene knyttet til cybersikkerhet. Det har vært et økende antall forsknings- og utviklingsinitiativer, utdannings- og opplæringsprogrammer og sertifiserte fagfolk innen cybersikkerhet. Den finske strategien for cybersikkerhet (2019) (**https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/**) og utviklingsprogrammet for cybersikkerhet (2021) understreker viktigheten av å bygge nasjonal cybersikkerhetskompetanse gjennom utdanning og forskning. For skoleutdanningssystemet er målet å utstyre studentene med ferdigheter og kunnskaper for å navigere i den digitale verden trygt og bevissthet om cybertrusler og beskyttelsestiltak **Lehto-IWS-018.pdf (jyu.fi)**

I finsk yrkesopplæring (VET) fremheves ikke cybersikkerhet eksplisitt som et separat eller spesialisert fokus i de fleste materialer. Dette betyr imidlertid ikke nødvendigvis at cybersikkerhet er helt fraværende i VET-programmer. Gitt den økende betydningen av digital kompetanse og cybersikkerhet i alle sektorer, er disse emnene integrert i bredere IT- og tekniske utdanningsprogrammer. Det er viktig å merke seg at leverandører av yrkesrettet utdanning og yrkesfag i Finland har autonomi til å organisere utdanningstilbudene sine i henhold til regionale og feltspesifikke krav. Finsk yrkesopplæring har nylig gjennomgått den mest omfattende reformen på nesten 20 år. Målet med reformen i 2018 var å skape et mer effektivt og fleksibelt, kompetansebasert og kundeorientert yrkesfaglig system, effektivisere og bedre tilpasse kvalifikasjonene til arbeidsmarkedets behov. Dette gjøres hovedsakelig gjennom å redusere regulering og innføre mer autonomi og ansvar for yrkesfagleverandører. (Kilde: **https://www.cedefop.europa.eu/files/8133_en.pdf)** Dette betyr at noen institusjoner kan tilby mer spesialiserte moduler på områder som cybersikkerhet, avhengig av lokale bransjekrav og partnerskap. Basert på Lehtos forskning er cybersikkerhet ikke et eget emne, men integrert i forskjellige emner, spesielt i sammenheng med informasjons- og kommunikasjonsteknologi (IKT). Undervisningens ansvar er avhengig av lærerne for å innlemme cybersikkerhetsutdanning i sine emner. Denne tilnærmingen fører til en variasjon i hvordan dette implementeres på tvers av ulike skoler og klassetrinn, og fremhever behovet for mer strukturerte og konsistente tilnærminger til undervisning i cybersikkerhet, inkludert potensielt å gjøre det til et eget emne eller en mer fremtredende del av IKT-utdanningen.

På høyere utdanningsnivå (HE), tilbyr finske universiteter omfattende studieprogram innen cybersikkerhet. Disse programmene er utformet for å utstyre studentene med avansert kunnskap og ferdigheter innen ulike områder av cybersikkerhet. Mange tilbyr en mastergrad i informasjonssikkerhet og informasjonsteknologi, med fokus på de reelle konsekvensene og anvendelsene av disse konseptene. De er tilgjengelige på stedet og eksternt.

Cybersikkerhetssektoren i Belgia opplever en økt etterspørsel etter dyktige fagfolk, med omtrent 4,000 ledige stillinger innen cybersikkerhet (per november 2022 I erkjennelsen av at det haster med å tette dette gapet, er det innført ulike initiativer og utdanningsprogrammer for å utvikle landets kompetanse innen cybersikkerhet. En rekke institusjoner i Belgia som KU Leuven, Solvay Business School, Howest University of Applied Sciences, og mange andre har utviklet spesialiserte programmer på engelsk, fransk og nederlandsk, i stand til å nå et bredt publikum. Forskning utført av den belgiske organisasjonen Agoria, understreket imidlertid behovet for kontinuerlig opplæring også blant fagfolk som ikke lenger går på universitetet, for å holde dem oppdatert på cybersikkerhetsfeltet og dets trusler. Den belgiske cybersikkerhetsstrategien for årene 2021-2025 anerkjenner det høye nivået av integrering av cybersikkerhet i landets akademiske miljø og understreker den sentrale rollen som universiteter og andre utdanningsinstitusjoner spiller for å øke forsknings- og utviklingsinnsatsen på feltet. Ifølge CBBs (Centre for Cybersecurity Belgium) database, er det 33 kurs (bachelor, master og sertifiseringer) som tilbys av høyere utdanningsinstitusjoner, som legger opp til en rekke VET-programmer som tilbys i både offentlig og privat sektor i Belgia. CBB er organet som overvåker, koordinerer og overvåker implementeringen av den belgiske cybersikkerhetsstrategien, og utvikler for tiden en gratis opplæring i cybersikkerhet for belgiske ansatte for å spre kunnskap

om cybersikkerhet enda mer blant befolkningen. Samlet sett understreker den belgiske cybersikkerhetsstrategien viktigheten av å spre kunnskap og ferdigheter innen cybersikkerhet gjennom utdanning og forplikter seg til å utvide akademiske kurs, fremme forskning på feltet, oppmuntre til STEM-utdanning og gi praktiske opplæringsmuligheter for å takle den økende etterspørselen etter fagfolk i det belgiske cybersikkerhetslandskapet.

I Norge er ikke cybersikkerhet et hovedfag man kan studere på yrkesfaglig nivå. Elementer av programmet er inkludert i et VET-program kalt "Computer and Electronics". Det finnes ikke noe rammeverk for cybersikkerhet, bare nevnes i de generelle grunnleggende digitale ferdighetene for all utdanning at elevene skal kunne bruke og navigere i digitale ressurser i og utenfor nettverk og ivareta informasjon og datasikkerhet.

Nasjonal strategi for digital sikkerhetskompetanse påpeker 14.november 2023 viktigheten av at elever lærer om digital sikkerhet. For mange yrkesfag er dette svært relevant og viktig. Det er mangel på læringsmateriell om cybersikkerhet i yrkesfag, og lærerne mangler ferdighetene til å undervise, spesielt på områder som personvern, smarthusteknologi og IoT. Eksisterende programmer for cybersikkerhetsutdanning, som GenCyber og CyberFirst, adresserer ikke spesifikt behovene til dette yrkesprogrammet. (**Kilde 1 – 2**)

Gjennom et samarbeid mellom UiO, NTNU og lærere ved utvalgte yrkesfaglige skoler er planen å utvikle læringsmateriell for digital sikkerhet, som senere skal gjøres tilgjengelig på den nasjonale læringsplattformen **NDLA (Nasjonal digital læringsarena).**

Innenfor høyere utdanning finner du både årsstudium i digital sikkerhetskultur og bachelorprogram i cybersikkerhet. Emnet inngår også i en rekke masterprogrammer i Data Science and Informatics. Det finnes en rekke spesifikke cybersikkerhetsstudier som anvendt data- og informasjonsteknologi, bachelor i cybersikkerhet, bachelor i digital etterforskning, digital infrastruktur og cybersikkerhet, digital sikkerhetskultur og erfaringsbasert master i informasjonssikkerhet. Det finnes også studier der digital sikkerhet inngår som HMS-kultur og ledelse, kommunalt beredskapssamarbeid og styrearbeid i praksis og årsstudium i krisehåndtering.

For Polen har cyberstudier økt de siste årene. Flere og flere cyberkurs åpner på universitetene, samtidig som antall yrkesfag øker. Etterspørselen etter cyberyrker har økt i Polen de siste årene, og bevisstheten om cyber har også økt i den polske delegasjonen som fremmer selskaper til å ansette cybereksperter og beskytte informasjonen.
I Polen, som de fleste europeiske land, anses en akademisk grad som obligatorisk, og derfor er cyberkurs ofte et tilleggsstudium etter graden. Fordi de fleste av Akshmi-studiene er lengre, men på en teoretisk måte. Det er cyberkurs som er korte, men de fleste fokuserer på praktisk læring som forbereder studenten på ekte arbeidssituasjoner. Den store utfordringen for en student på cyberfeltet er at de fleste av de yrkesfaglige institusjonene ikke har egen finansiering, så det kreves en økonomisk løsning, og derfor er dette alternativet ikke alltid egnet for de som er interessert.

Selv om cybersikkerhet bør være en prioritet for alle aktivitetsområder, er VET-utdanningssystemet i Romania ennå ikke klar til å sikre at studentene er kompetente på dette feltet. I en analyse av læreplanen for den nedre syklusen av den videregående skolen - teknologisk felt - i et hvilket som helst domene av faglig opplæring, gir skoleplanen for teknisk kultur ikke enheter av læringsutbytte på cybersikkerhet. Noen spesifikke kompetanser på feltet finnes i læreplanen for generell kunnskap, i informasjons- og kommunikasjonsteknologidisiplinen, i læreplanen for 9. klasse. Disse er:

1. Beskrivelse og anvendelse av sikkerhetstiltak ved bruk av Internett:

- Smart bruk av Internett
- Betydningen av dataoverføringskryptering
- Bruk av digital signatur
- Måter å forsvare seg mot virus

2. Bruke chat-tjenesten:

- Presentasjon av samarbeidsapplikasjoner for videokonferanser
- Presentasjon av IRC-nettverksregler

For den øvre syklusen på videregående skole, 11. klasse, tilbyr bare feltet for profesjonell opplæring Elektronisk automatisering for spesialiseringene Telekommunikasjonstekniker, Dataoperatørtekniker, Telematikkoperatørtekniker, noe innhold om installering av sikkerhetsapplikasjoner. I 12. klasse, bare i spesialiseringen av datatekniker, inneholder den spesialiserte modulen innhold som:

- Grunnleggende prinsipper for sikkerheten til datasystemer og datanettverk
- Utvikling av sikkerhetspolitikk i nettverket
- Sikkerhetstrusler fra nettverk
- Beskyttelse mot nettlesing
- Virus og sikkerhetsapplikasjoner

Når det gjelder HEI, demonstrerer Transilvania Universitet i Brasov et sterkt engasjement for cybersecurity-utdanning, og tilbyr et omfattende masterprogram i Cybersikkerhet utført helt på engelsk. Universitetets dedikasjon til å fremme kompetanse på dette kritiske feltet er tydelig i den omfattende læreplanen som er gitt for programmet.

Dette masterprogrammet ved Transilvania Universitet er en utmerket mulighet for studenter som søker en helhetlig utdanning i cybersikkerhet innenfor en internasjonal akademisk setting. Kombinasjonen av en robust læreplan og engelskspråklig instruksjon posisjoneres kandidater for å lykkes i det dynamiske og utfordrende feltet cybersikkerhet.

Babes-Bolyai Universitet i Cluj-Napoca, gjennom Det matematisk-informatiske fakultet, har fra studieåret 2023-2024 initiert et masterprogram på engelsk i Cyber Security, med sikte på å forberede fremtidige spesialister på dette feltet av vital betydning i sammenheng med

overgangen til informasjonssamfunnet. Kursene i det nye programmet starter i oktober i år, sammen med studieåret 2023-2024, opptaket gir en konkurranse utover forventningene. Mer enn 40 studenter, inkludert fra utlandet, tatt opp til programmet vil bli spesialister innen Cybersikkerhet, kandidatene kan til og med velge å studere et studieår ved andre anerkjente universiteter i Europa.

Ved fakultetet for matematikk og informatikk tilbys masterprogrammet *Internet Technologies* (på engelsk) også i andre semester av det første året, et kurs i *kryptografi og systemsikkerhet*, som introduserer studentene til feltet cybersikkerhet og de spesifikke metodene for datakryptering.

Videre tilbyr masterprogrammet Modern Technologies in Software System Engineering i tredje semester et valgfritt emne kalt IT-systemsikkerhet, sentrert rundt de viktigste utfordringene i cybersikkerhet.

Begge kursene tillater masterstudenter ved Det matematisk-informatiske fakultet å få innsikt og kompetanse i dette emnet, som i den faktiske internasjonale konteksten er av avgjørende betydning, og å bli klar over utfordringene med kryptering og sikkerhet i moderne systemer.

Universitetet i Bucuresti, Det matematisk-filosofiske fakultet og informatikk, tilbyr et masterprogram Sikkerhet og anvendt logikk (på engelsk), som tilbyr en rekke emner dedikert til kryptografi og systemsikkerhet. Studentene kan tilegne seg kunnskap innen operativsystemsikkerhet, kryptografi, nettverkssikkerhet og cybersikkerhet, og er dermed forberedt på å møte utfordringene på dette feltet.

I Spania er de fleste studiene i cybersikkerhet på høyere utdanningsnivå, grader eller mastergrad. Ifølge dataene som er gjenopprettet av National Cybersecurity Institute of Spain, er det:

- Rundt 87 mastergrader i cybersikkerhet som tilbys av offentlige og private universiteter og andre høyere utdanningsinstitusjoner.
- 4 spesialiseringer, for det meste spesialiseringer i dataetterforskning.
- 3 universitetsgrader, alle tilbys av privat sektor.

Når det gjelder opplæring på VET-nivå, er det rundt 60 kurs tilgjengelig på spanske yrkesopplæringsinstitutter. Alle er regulert av samme læreplan, godkjent av utdanningsdepartementet i mai 2020 gjennom *kongelig dekret 479/2020, av 7. april, som etablerer spesialiseringskurset i cybersikkerhet i informasjonsteknologimiljøer*.

Til tross for de eksisterende programmene, er det erkjennelse av behovet for ytterligere innsats. Spania har implementert ulike planer, inkludert National Digital Skills Plan, SME Digitalization Plan 2021-2025 og Spain Digital 2025 Plan, med hovedfokus på å skape nye talenter for å møte den økende etterspørselen etter digitale ferdigheter, spesielt innen cybersikkerhet.

I Tyrkia har behovet for cybersikkerhet økt raskt og blitt veldig viktig, så vel som over hele verden, spesielt de siste årene. Samtidig med den teknologiske utviklingen har cyberrisiko og

trusler også endret seg i samme tempo og blitt komplekse. Cyberrisiko og trusler har nådd potensialet til å forårsake mye mer omfattende og negative konsekvenser enn fysiske angrep. Med sektorer som finans, elektronisk kommunikasjon, energi, transport og luftfart som leverer tjenester i et sikkert digitalt miljø, har det å sikre nasjonal cybersikkerhet blitt en av de viktigste prioriteringene for Tyrkia. I denne sammenheng fortsetter studier å spre cybersikkerhetsopplæring i yrkesopplæring og høyere utdanning i tråd med sektorens behov og utvikler og beriker opplæringsinnhold.

Innenfor rammen av disse studiene i yrkesutdanning: Cyber security grunnleggende kurs i nettverksoperasjon innen informasjonsteknologi. Innen cybersikkerhet, grunnleggende programmering, systemsikkerhet, nettverksteknologi, sikker programvareutvikling, penetrasjonstesting og respons på cyberhendelser, dataetterforskning, etc. Kursprestasjoner blir gitt til studenter.

I høyere utdanning, "Cyber Security Analyst and Operator" knytte studium i cyber security yrkesskoler, Forensic datateknikk lavere program ved universiteter og relevante masterstudier tilbys ved universiteter.

I tillegg gir videreutdanningssentre for universiteter, offentlige utdanningssentre i kommuner, offisielle institusjoner som TÜBİTAK, TSE og private utdanningsinstitusjoner også opplæring i cybersikkerhet.

2.1.2. CYBERSIKKERHETSUTFORDRINGER OG INDUSTRIENS BEHOV

Basert på en grundig litteraturgjennomgang har vi listet opp cybersikkerhetsutfordringene som små og mellomstore bedrifter står overfor i landene i prosjektet. I det utviklende landskapet for cybersikkerhet står små og mellomstore bedrifter (SMB) i Litauen overfor flere cybersikkerhetsutfordringer. Etter hvert som disse virksomhetene i økende grad er avhengige av digital teknologi for sin virksomhet, blir de mer sårbare for et spekter av cybertrusler, noe som krever en omfattende forståelse og strategisk tilnærming for å håndtere disse risikoene effektivt.

I studien fra 2022 ble, Bukauskas et al.[8] ulike typer organisasjoner basert på deres modenhet og kompetansebehov innen cybersikkerhet. Små organisasjoner, ifølge studien, er sammenlignbare med enkeltpersoner i samfunnet, da hovedparameteren for digital arbeidsplasssikkerhet er nivået på cyberhygiene, som påvirkes av den generelle forståelsen av cybersikkerhetstrusler. I dette nivået koordineres cybersikkerhet internt i organisasjonen, noe som fører til potensielle sikkerhetsbrudd i forretningsprosesser. I mellomstore bedrifter er styring og regulering av cybersikkerhet også svakt koordinert. Respons på hendelser eller andre cybersikkerhetsaktiviteter er heller ikke vektlagt i organisasjonen. Med tanke på at små bedrifter i Litauen utgjør 97% av alle selskaper, konkluderte Bukauskas et al. (2022) med at det er et betydelig behov for IT-spesialister som tilbyr IT-tjenester, konsulterer brukere og hvis

[8] Bukauskas, L., Brilingaitė, A., Lepaitė, D., Juozapavičius, A., Ikamas, K., 2022. 'Projekto "Kibernetinio saugumo kompetencijų žemėlapio kūrimas" ataskaita', Vilniaus universitetas Informatikos institutas. Tilgjengelig på: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf [Besøkt 12. januar 2024]. DOI: https://doi.org/10.15388/CIBERSEK.2022.

jobbfunksjoner inkluderer å sikre grunnleggende cybersikkerhetsprinsipper. De fremhevet også at en bemerkelsesverdig mangel er observert i trusseletterretning og vitenskapelig forskning, og et synlig behov for cybersikkerhetsspesialister innen sikkerhetsteknikk og systemlivssyklus.

Noen år tidligere organiserte "Create for Lithuania" -programmet, i samarbeid med departementet for nasjonalt forsvar, en offentlig høring om å øke bevisstheten om cybersikkerhet blant små og mellomstore bedrifter[9]. Initiativet konkluderte også med at det er tydelig at bevissthetsnivået om cybersikkerhet blant små og mellomstore bedrifter i Litauen ikke er høyt, og at små bedrifter ikke har oppnådd et tilstrekkelig nivå av cybermotstandskraft på grunn av manglende forståelse av de digitale risikoene. Videre bemerket initiativ at mer enn halvparten (57%) av bedriftsledere uttalte at de enten mangler eller er usikre på om de har nok kunnskap til å velge cybersikkerhetsløsninger, og over tre fjerdedeler av de ansatte var enige i at de mangler lett forståelig informasjon.

Ved å sammenligne funnene til Bukauskas et al. (2022) og det tidligere initiativet "Create for Lithuania" (2019), er det tydelig at situasjonen angående cybersikkerhet blant små og mellomstore bedrifter i Litauen har vist begrenset fremgang. Begge studiene understreker en vedvarende mangel på grunnleggende kunnskap om cybersikkerhet og beredskap i disse virksomhetene. Til tross for økt avhengighet av digital teknologi, fortsetter små og mellomstore bedrifter å vise sårbarheter på grunn av utilstrekkelig cybermotstandskraft og en generell mangel på forståelse av digitale risikoer. Denne pågående utfordringen understreker det akutte behovet for forbedret bevissthet om cybersikkerhet og opplæring blant små og mellomstore bedrifter, en kritisk sektor som utgjør størstedelen av Litauens forretningslandskap.

I Finland fremhevet en studie av ETLA (Elinkeinoelämän tutkimuslaitos), Economic Research Institute of Finland, at antall datainnbrudd i finske selskaper, inkludert små og mellomstore bedrifter, hadde doblet seg over to år. Finske selskaper rapporterte datainnbrudd tre ganger mer enn det europeiske gjennomsnittet i 2019, med de fleste hendelser relatert til svindel, phishing-angrep, datainnbrudd, skadelig programvare og sårbarheter. Denne studien fremhever også mangelen på dyktige fagfolk i cybersikkerhet som en hovedutfordring for finske små og mellomstore bedrifter. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

National Cyber Security Centre Finland (NCSC-FI) (https://www.kyberturvallisuuskeskus.fi/en**https://www.kyberturvallisuuskeskus.fi/en**) er et initiativ ledet av den finske regjeringen. Det opererer som en del av det finske transport- og kommunikasjonsbyrået (Traficom), som er et statlig organ som er ansvarlig for regulering av kommunikasjons- og transportsektorer i Finland. De gir informasjon om den nåværende tilstanden til cybersikkerhet og tilbyr veiledning og verktøy for både enkeltpersoner og organisasjoner for å forbedre deres cybersikkerhetspraksis. Senteret engasjerer seg også i nasjonale cybersikkerhetsinitiativer, for eksempel sårbarhetsvarsler, og fremmer bevissthet og beredskap mot cybertrusler.

[9] Opprett for Litauen og Ministry of National Defense, 2019. SVV Kibernetinio Saugumo Apklausos Apžvalga. [På nett] Tilgjengelig på: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

Deres ukentlige gjennomganger gir et godt innblikk i utfordringene små og mellomstore bedrifter står overfor. Vi får vite at finske små og mellomstore bedrifter, som mange andre, har stått overfor de samme sikkerhetsproblemene som er beskrevet av ETLA-instituttet ved å bli målrettet av mange phishing- og svindelmeldinger. Disse inkluderer forsøk på å utgi seg for å være legitime tjenester som Suomi.fi for å phiske etter legitimasjon eller annen sensitiv informasjon. Små og mellomstore bedrifters økonomiske ressurser kan være en begrensning for å distribuere moderne cybersikkerhetsløsninger for å forsvare seg mot cybertrusler. På samme side har allerede utstyrte små og mellomstore bedrifter problemer med å holde seg oppdatert mot nye cybersikkerhetstrusler.

I vårt forsøk på å forstå cybersikkerhetssituasjonen som små og mellomstore bedrifter i Belgia står overfor, gjennomførte vi en grundig undersøkelse. Vi fant det imidlertid utfordrende å skaffe omfattende data eller kilder som adresserer dette kritiske problemet. Denne mangelen på informasjon gjør det vanskelig å skape effektive strategier og løsninger som kan hjelpe små og mellomstore bedrifter med å beskytte sine digitale eiendeler mot cybertrusler.

Vi var i stand til å nå ut til fagfolk som er aktivt involvert innen cybersikkerhet i Belgia, takket være det omfattende nettverket til Women4Cyber Foundation. Disse ekspertene ga oss viktig innsikt og perspektiver som hjalp oss med å forstå de ulike utfordringene små og mellomstore bedrifter står overfor innen cybersikkerhet. Vi fikk innsikt fra Iva Tasheva, et bemerkelsesverdig medlem av Women4Cyber Belgium, som delte sin omfattende erfaring og kunnskap om utfordringene som små og mellomstore bedrifter står overfor når de prøver å beskytte sin digitale infrastruktur mot cybertrusler.

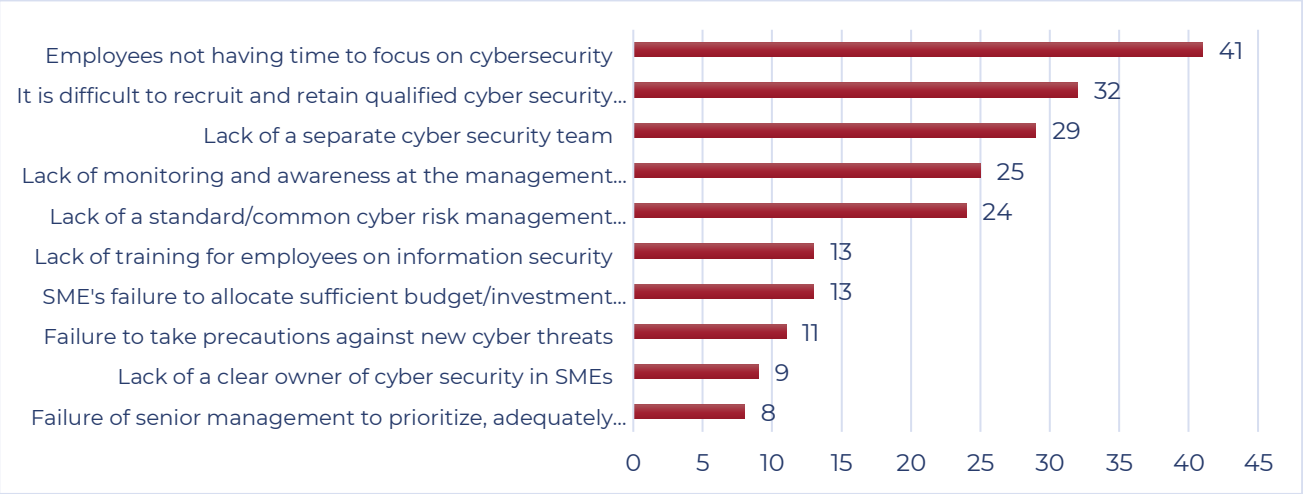
Små og mellomstore bedrifter står overfor flere cybersikkerhetsutfordringer, for eksempel vanskeligheter med å få tilgang til ad hoc-støtte, mangel på opplæring i identitets- og tilgangsadministrasjon for personellet og begrenset forståelse av skytjenesteroller og ansvar. I tillegg har små og mellomstore bedrifter begrenset tilgang til rimelige løsninger for sårbarhetsskanning og overvåkingsverktøy, noe som gjør dem mer sårbare for cybertrusler. Den gjennomgripende hypertilkoblingen i forretningsmiljøer utsetter små og mellomstore bedrifter for identitetstyveri og uredelige aktiviteter, mens phishing og svindel utgjør pågående risiko. For å møte disse utfordringene må små og mellomstore bedrifter iverksette proaktive tiltak, implementere robuste sikkerhetsprotokoller og gi omfattende opplæring av ansatte for å styrke ferdighetene sine og beskytte mot potensielle brudd og økonomiske tap.

Cybersikkerhet har blitt en av de viktigste prioriteringene for bedrifter i Spania, inkludert små og mellomstore bedrifter (SMB). Økningen i fjernarbeid og online klasser har ført til utbredt bruk av eksterne skrivebordsfunksjoner, cloud computing og samarbeidsverktøy, blant annet, økende risiko og dataangrep. Rapporten fra National Cryptologic Centre (CCN-CERT) knytter økningen i fjernarbeid og bruk av teknologi til økningen i disse risikoene. De hyppigste angrepene som selskaper har lidd er ransomware og angrep på eksterne tilgangssystemer. Økningen i cybertrusler har ført til at selskaper har økt antall personer som er tildelt cybersikkerhetsteam, enten internt eller eksternt. Til tross for dette outsourcer selskaper fortsatt rundt 50% av disse funksjonene.

I tillegg er det fortsatt 21% av selskapene i Spania som ikke har Security Operations Centers (SOC) for å behandle hendelser. Når det gjelder utdanning innen cybersikkerhet i forretningsmiljøet, fremhever Deloittes analyse at i 2022 økte timene med nettbasert opplæring i cybersikkerhet for ansatte i de analyserte organisasjonene med nesten 30% sammenlignet med dataene for 2021. Imidlertid har nesten 50% av selskapene i Spania ingen sertifisering innen cybersikkerhet, noe som er en klar utfordring for fremtiden.

Likevel er den største utfordringen for spanske selskaper fortsatt mangelen på talent innen cybersikkerhet. I følge rapporten "Analyse og diagnose av cybersikkerhetstalent i Spania" utarbeidet av ObservaCiber, hadde Spania i 2021 et talentgap estimert til 24.119. I 2024 anslås det at Spania vil kreve mer enn 83.000 eksperter, noe som øker talentgapet til 57,5%.

Det ser ut til at det svakeste leddet som får små og mellomstore bedrifter til å møte cybersikkerhetsutfordringer er den "menneskelige" faktoren. Den største utfordringen for små og mellomstore bedrifter er at personellet som er ansvarlig for cybersikkerhet ikke kan sette av nok tid til cybersikkerhet fordi de har ansvar på mer enn ett område. I tilknytning til dette er mangelen på et eget cybersikkerhetsteam nummer tre på listen over vanskeligheter som små og mellomstore bedrifter opplever innen cybersikkerhetsadministrasjon. Små og mellomstore bedrifter har problemer med å rekruttere og beholde kvalifiserte cybersikkerhetsansatte.



Skikkelse 1 - SMB-utfordringer - Türkiye-forskning.

I Romania gir Internett nye forretningsmuligheter og forbindelser som kan hjelpe små og mellomstore bedrifter med å utvikle seg, men det inneholder også mange risikoer.

Cybersikkerhet er ikke lenger en fortelling, det er en realitet i Romania også, selv om vi til nå ikke har hatt et stort cyberangrep.

Kilden til informasjonen som brukes er VERIZON-RAPPORTEN om cybertrusler i 2023 - de viktigste nøkkelpunktene for små og mellomstore bedrifter (DATA BREACH INVESTIGATIONS

REPORT - DBIR), basert på 16 312 sikkerhetshendelser, hvorav 5 199 ble bekreftet som brudd på datasikkerheten.

Interessepunkter for små og mellomstore bedrifter:

- Angrepsflatene for små og mellomstore bedrifter og selskaper er like, fordi de bruker skybasert programvare. Uautorisert inntrengning i systemet, sosialtekniske teknikker og grunnleggende webapplikasjonsangrep representerer 92% av de totale typene angrep for brudd registrert av små og mellomstore bedrifter (85% for selskaper).
- Ransomware 24% av tilfellene (data blir stjålet før de blir kryptert)
- Uautorisert inntrengning i systemet - komplekse angrep basert på skadelig programvare og / eller hacking for å nå sine mål.
- Eksterne angripere representerer den største trusselen som forårsaker 83% av dagens sikkerhetsbrudd, og når 94% i tilfelle SMB-angrep. 94% av aktørene som er involvert i spredning av trusler er eksterne, sammenlignet med 89% for store organisasjoner, og 98% av bruddene er økonomisk motiverte, sammenlignet med 97% for selskaper.
- Den økonomiske motivasjonen er nummer én i 95% av alle tilfeller, prosentandelen øker til 98% i tilfelle angrep på små og mellomstore bedrifter. Bare 1% er motivert av spionasje.
- Ansatte representerer det svakeste leddet i sikkerhetskjeden - 74% av alle tilfeller (dårlig bevissthet om cybertrusler). Den viktigste metoden for inntrenging kan skyldes bruk av stjålet legitimasjon - 49% og phishing - 12% eller andre metoder, for eksempel feilkonfigurasjon eller feilaktig sending av sensitive data.
- Kompromitterende forretnings-e-post - offeret blir lurt til å overføre store pengesummer til angripernes kontoer.

I Norge står små og mellomstore bedrifter (SMB) overfor betydelige utfordringer innen cybersikkerhet. Mange mangler en dyp forståelse av risikoen som er involvert, noe som fører til potensielle sårbarheter. Det er et merkbart gap i effektiv opplæring av ansatte om cybersikkerhet, noe som gjør menneskelige feil til en vanlig risikofaktor. Små og mellomstore bedrifter, spesielt de som rapporterer å ha begrensede ressurser, sliter ofte med å investere i avanserte cybersikkerhetstiltak og dyktig personell. De må også navigere i komplekse databeskyttelseslover, noe som øker kompleksiteten ved å sikre samsvar samtidig som sensitiv informasjon beskyttes. Økningen i phishing-angrep og sosial manipulering viser ytterligere deres sårbarhet, det samme gjør utilstrekkelig nettverkssikkerhet og risikoen for interne trusler. Håndtering av disse risikoene er avgjørende, men små og mellomstore bedrifter opplever ofte effektiv risikovurdering og -håndtering som utfordrende. I tillegg introduserer avhengighet av tredjepartsleverandører et nytt lag med kompleksitet, som potensielt utsetter små og mellomstore bedrifter for ytterligere cybersikkerhetstrusler.

2.2. KVINNER I CYBERSIKKERHET

Vi analyserte opplærings- og støttebehovene for kvinner, de eksisterende kvalifikasjonene og kompetansene til kvinner innen cybersikkerhet og anbefalinger for å involvere flere kvinnelige ansatte i cybersikkerhetsutfordringer.

Microsoft gjorde en undersøkelse, på tvers av 35 europeiske land, færre enn 1 av 5 informatikkutdannede var kvinner. Interessen for realfag, teknologi, ingeniørfag og matematikk (realfag) faller altfor tidlig. Faktisk viser OECDs Programme for International Student Assessment (PISA) at gutter er langt mer sannsynlige enn jenter til å forestille seg selv som IKT-fagfolk, forskere eller ingeniører. (Microsoft, 2017).

Når vi ser på kvinneandelen blant sysselsatte IKT-spesialister, var det i EU27 i 2020 bare 18,5 % av alle IKT-spesialister kvinner. De største andelene kvinner var i Bulgaria – 28,2 %, Hellas – 26,6 % og Romania – 26,2 % (se figur 5 (Women go tech, 2021)). Landene fra den nordisk-baltiske regionen lå også stort sett nær toppen av listen, med unntak av Norge, som lå mer midt på landrangeringen. (Kvinner går tech, 2021).

Ifølge statistikkavdelingen i Republikken Litauen var antall ansatte i informasjons- og kommunikasjonskategorien i fjerde kvartal 2022 29,4 tusen menn og 21,5 tusen kvinner. I første kvartal 2023 var det 34,6 tusen menn og 20,7 tusen kvinner. For andre kvartal 2023 var det 36,8 tusen menn og 14,8 tusen kvinner, og i tredje kvartal 2023 var tallene 34,5 tusen menn og 18,0 tusen kvinner. Det er en merkbar nedgang i antall kvinnelige ansatte fra Q1 til Q2 2023, etterfulgt av en økning i Q3 2023 (Rodiklių Duomenų Bazė - Oficialiosios Statistikos Portalas, n.d.).

Med opptil 11% av kvinnene som jobber med cybersikkerhet, ble det gjennomført en undersøkelse for å finne ut publikums syn på kvinners perspektiver på dette feltet. I tvistene svarte 44,4% av respondentene at antall kvinner innen cybersikkerhet burde være mellom 30 og 60%. Den største andelen av respondentene svarte at kvinner bør utgjøre mellom 30 og 60% av de kvinnelige fagfolkene (35,2%). Ved å analysere svarene etter kjønn og aldersgruppe, kan man se at kvinner, spesielt de yngre (under 25 og 25-45), oftest mener at antall kvinner bør være rundt halvparten. Unge menn (under 25 år) mener at opptil 30% av kvinnene bør være kvinner. Det kan sees at kvinner selv har en tendens til å se et mye høyere antall kvinner innen cybersikkerhet enn det som er tilfelle i markedet. Dette er gode nyheter, da det å tiltrekke kvinner til feltet ikke bare vil bidra til å løse mangelen på fagfolk, men også øke sikkerheten til organisasjonene selv. (Bukauskas et al., 2022).

I Finland, som i mange europeiske land, er det en felles forståelse av kjønnsubalansen i cybersikkerhet og IT-feltet generelt. Initiativer og innsats for å støtte kvinner innen cybersikkerhet og for å fremme deres engasjement i å takle cybersikkerhetsutfordringer har økt. De fleste av dem støttes av ideelle organisasjoner.

Cybersecurity-feltet har sett flere initiativer for å utvikle utdannings- og karriereveier, treningsprogrammer og nettverksarrangementer. Strategien er også basert på å fremme

rollemodeller ved å fremheve vellykkede kvinners karrierevei innen cybersikkerhet og dele sine historier for å inspirere flere kvinner til å forfølge karrierer innen dette feltet. Women4Cyber og de oppførte initiativene understreker viktigheten av mangfold og inkludering for ikke bare å adressere ubalanse mellom kjønnene, men også for å bidra til den generelle styrken og motstandskraften til cybersikkerhetssektoren. Offentlige og private institusjoner støtter også denne strategien ved å inkludere denne likestillingsdimensjonen som en topp prioritet i alle sine initiativer.

Women4Cyber Finland (W4CFI)

W4CFI ble etablert i august 2021 og er en ideell organisasjon som har som mål å øke antall kvinner ansatt i den finske cybersikkerhetsindustrien. Det er en del av det større EU-omfattende Women4Cyber-initiativet og fokuserer på å støtte en mer mangfoldig og inkluderende industri i Finland. W4CFI er involvert i ulike aktiviteter, inkludert veiledning, utveksling av kunnskap og bevisstgjøring for å øke og støtte kvinners engasjement i cybersikkerhet. **Women4Cyber Finland.**

Det finske samferdselsdepartementet og Aalto-universitetsprosjektet

Det finske samferdselsdepartementet, i samarbeid med Aalto-universitetet, utvikler en utdanningspakke for å gjøre cybersikkerhet til en samfunnsferdighet over hele EU. Dette initiativet fremhever den økende betydningen av cybersikkerhet i hverdagen og behovet for bevissthet og ferdigheter blant alle borgere, inkludert kvinner. Det understreker utdanningsinstitusjonenes rolle i å tilby tilgjengelig utdanning og opplæring innen cybersikkerhet, noe som er avgjørende for å styrke kvinner i feltet. Finland øker utdanningen i cybersikkerhetsferdigheter i EU. **Plattform for digitale ferdigheter og jobber** (europa.eu).

"Mimmit koodaa" (Women Code) bevegelse

Dette initiativet tilbyr workshops, opplæring, nettverksmuligheter, webinarer og karrierestøtte. Den fokuserer på å utfordre stereotyper og oppmuntre flere kvinner til å utforske karrierer innen teknologi, inkludert cybersikkerhet. Denne organisasjonen tar sikte på å skape veier for kvinner å komme inn og utmerke seg i cybersecurity-feltet. **Mimmit koodaa**

I det belgiske cybersikkerhetslandskapet representerer kvinner 19% av arbeidsstyrken ifølge den første sosioøkonomiske studien om cybersikkerhetssektoren i Belgia utgitt av Agoria i 2022. Med koordinering av det belgiske økonomidepartementet (FPS Belgium) har kompetente politiske aktører i Belgia utarbeidet en femårsplan for kvinner i digital kalt "Women in Digital - National and Intersectional Strategy 2021-2026." Femårsplanen inneholder en felles og tverrsektoriell strategi basert på fem strategiske mål som er nyttige for å bekjempe fordommer og for å takle strukturelle hindringer som hindrer kvinner i å delta i den digitale økonomien. De fem målene er følgende:

1. Sikre at flere kvinner uteksamineres i den digitale sektoren; 2. Stimulere alle kvinner til å delta i det digitale arbeidsmarkedet og/eller den digitale sektoren. 3. Forbedre opprettholdelsen av kvinner i den digitale sektoren; 4. Opprette nye bilder for å fremme kvinners rolle i feltet (på og utenfor skjermen); 5. Tette kjønnsgapet mellom spesifikke målgrupper (**lenke til strategien**).

Women4Cyber Foundation, basert i Brussel, organiserer og støtter et bredt spekter av aktiviteter rettet mot kvinner som jobber eller starter sin karriere innen cybersikkerhet i Belgia og i Europa. I Belgia støtter og samarbeider stiftelsen med den belgiske nasjonalavdelingen (**Women4Cyber Belgium**) i disse aktivitetene. Den belgiske nasjonalavdelingen teller rundt 20 aktive medlemmer som jobber med initiativene. Aktivitetene, arrangementene og programmene som organiseres av kapittelet er, for eksempel: nettverksmøter og arrangementer (virtuelle og personlige) som "virtuell kaffe" der W4C Belgium Chapter inviterer eksperter på ulike felt relatert til cyber- og informasjonssikkerhet til å snakke; webinarer og info økter; mentorprogrammer som tar sikte på å hjelpe kvinner med å forbedre sine ferdigheter og fremme sine cybersikkerhetskarrierer på alle nivåer; prosjekter og arrangementer i samarbeid med den belgiske cybersikkerhetskoalisjonen (for eksempel organiseringen av **den internasjonale kvinnedagen 2023**); markedsføring av stipend for cyberrelaterte utdanningsprogrammer som de som er organisert av Solvay Brussels School of Economics og Management.

I Norge er det avgjørende å adressere kjønnsgapet i cybersikkerhet for å bygge en motstandsdyktig og mangfoldig arbeidsstyrke. Kvinneandelen i IT er bare 29%. Det lave tallet henger i stor grad sammen med at det er flere kvinner som velger matematiske og tekniske på videregående nivå.

Opplærings- og støttebehov og anbefalinger for å involvere kvinner

Det er behov for skreddersydde cybersikkerhetsprogrammer spesielt utviklet for å oppmuntre kvinners deltakelse. Disse programmene bør balansere tekniske aspekter med organisatoriske og menneskesentriske cybersikkerhetsproblemer. Det er flere tekniske videreutdanninger på feltet, mens videreutdanningstilbud i de fleste typiske kvinneyrker (pedagogisk – helseyrker) ikke har slike tilbud, og utvikling av kortere opplæringstilbud innen cybersikkerhet knyttet til disse yrkene vil kunne nå flere kvinner. Dette støttes også av sektoren selv, som uttalte at mangfold kan gi unike perspektiver til cybersikkerhetsutfordringer. Økende bevissthet om interne cybersikkerhetskarrierer blant kvinner kan skje gjennom workshops, seminarer og målrettede oppsøkende programmer på skoler og universiteter kan inspirere flere kvinner til å komme inn på dette feltet.

En annen tilnærming foreslått av mange av de nominerte topp 50 norske kvinnelige tech-kvinnene 2022 er å etablere mentorprogrammer og nettverksmuligheter for kvinner i cybersikkerhet for å gi viktig veiledning og støtte, og hjelpe dem med å navigere og avansere på dette feltet.

Cybersikkerhetssektoren foreslår selv at organisasjoner bør implementere inkluderende ansettelsespraksis og retningslinjer som aktivt oppmuntrer til rekruttering og oppbevaring av kvinner i cybersikkerhetsroller. 32 prosent av kvinner i tekniske roller er ofte «den eneste kvinnen i rommet» på jobb, ifølge McKinsey-rapporten «Women in the Workplace 2022.

Til slutt kan det å fremme kvinner i lederstillinger innen cybersikkerhet gi rollemodeller og inspirere andre kvinner til å gå lignende veier, som for eksempel **Mia Landsem**.

I Romania er cybersikkerhet fortsatt en av de mest dynamiske og spennende teknologisektorene. Denne sektoren trenger imidlertid en systemisk endring i kvinners representasjon og kompensasjon. Til tross for den økte interessen for cybersikkerhet, fortsetter kjønnsforskjellen. Kvinner er fortsatt sterkt underrepresentert, mens de fleste jobbene er overveiende mannlige. Fremtiden for cybersikkerhet påvirkes av evnen til å tiltrekke, beholde og fremme flere cyberfagfolk, inkludert flere kvinner.

Det ble gjort mange studier for å vise hvor underevaluerte kvinnene er rundt om i verden, men også for å få alle til å forstå viktigheten av kvinner på alle områder, og spesielt innen cybersikkerhet. Den ekstreme kjønnsforskjellen blant de ansatte i cybersikkerhet indikerer at andre krefter på jobb ikke er like i det hele tatt. Kvinner utgjør 39% av den totale arbeidsstyrken. De utgjør 38% av arbeidstakere i STEM-jobber, men bare rundt 25% av arbeidsstyrken innen cybersikkerhet, ifølge Cybersecurity Ventures.

Det er ulike barrierer som holder kvinner utenfor cybersikkerhet. Ifølge en undersøkelse fra (ISC)2, en ideell organisasjon som fokuserer på opplæring og sertifisering av cybersikkerhet, rapporterer flertallet av kvinner som har jobbet i feltet kjønnsbasert diskriminering. Nesten alle kvinner (87%) rapporterte å ha opplevd ubevisst diskriminering, mens 19% sa at de hadde blitt utsatt for åpen diskriminering. Kvinner siterte også uforklarlige forsinkelser i karriereutvikling (53%) og overdrevne svar på feil (29%).

Diskriminering manifesterer seg også i et lønnsgap. (ISC)2-forskning viser at 32 % av menn som jobber med cybersikkerhet tjener i gjennomsnitt $50.000 til $ 100.000 årlig, mens bare 18 % av kvinnene i cybersikkerhet opptar samme inntektsgruppe. Og 25% av mennene mot 20% av kvinnene tjener $100.000 til $500.000 årlig.

Det er sterke argumenter for å øke antall kvinner i cybersikkerhet, for eksempel fordelene med mangfold, innovasjon, emosjonell empati og et objektivt perspektiv, som alle er verdifulle ferdigheter for cybersikkerhetsarbeidsplassen.

Styremedlem Jay Koehler i Women in Cybersecurity ga en annen innsikt: «Kvinner dropper ut fordi det er en 'gutteklubb', og det er lav følelse av tilhørighet.» Dette problemet kan løses gjennom engasjement og ansvarlighet for å gi psykologisk trygghet og en kjønnsvennlig arbeidsplass og ved å skape kvinnenettverk.

Det er håp om at cybersikkerhet ikke lenger vil være et "mannsdominert yrke", men fullt av talentfulle mennesker av alle kjønn og bakgrunner.

Litteraturen om kvinners deltakelse i cybersikkerhet i Spania er knapp. Det meste av eksisterende litteratur viser en markant kjønnsubalanse i det bredere vitenskapelige samfunnet, inkludert STEM-disipliner, med en merkbar nedgang i kvinners progresjon til høyere karrierestadier, ofte betraktet som et "pipeline-fenomen". Når det gjelder høyere utdanning, er kjønnsforskjellen fortsatt uttalt, og bare 18% av de som fullfører studier i disse fagene er kvinner. Kvinner ansatt av små og mellomstore bedrifter for stillinger relatert til I + D er fortsatt svært lave, når ikke engang 30% ifølge dataene fra National Statistics Institute. Når det gjelder kvinnelige forskere innen cybersikkerhet for høgskolene i Spania, er det svært få av dem som

viser en balansert stab når det gjelder kjønn. Av de 31 HElene som er gjennomgått av *Fundación Alternativas*, har 11 av dem ingen kvinner som deltar i deres forskerteam, og bare 5 av dem viser en mer egalitær arbeidsstyrke. Som svar på disse utfordringene identifiserer analysen av opplærings- og støttebehov viktige forbedringsområder. Initiativer bør utvikles for å oppmuntre flere kvinner til å forfølge doktorgradsstudier og sikre en balansert representasjon gjennom hele utdanningsløpet. Adresseringen av skjevheter i karriereutviklingsprosesser er avgjørende, og mentorprogrammer kan spille en sentral rolle i å veilede kvinner gjennom vanskelighetene med cybersikkerhetsfeltet. Videre anbefales samarbeid med private bransjeorganisasjoner for å undersøke karrierebaner og stimulere kvinners engasjement i cybersikkerhetsroller i private næringer. Evalueringen av kvalifikasjoner og kompetanser understreker betydningen av tilpassede opplæringsprogrammer, med vekt på spesifikke cybersikkerhetsferdigheter og kompetanser.

2.3. ANALYSE AV ESCO YRKER

Vi tolker den eksisterende ESCO-klassifiseringen (European multilingual classification of Skills, Competences and Occupations) angående de identifiserte læringsutbyttene, inkludert kunnskap, ferdigheter og kompetanse. Målet er å:

- Analysere eksisterende ESCO-yrker knyttet til cybersikkerhet.
- Kartlegge identifisert læringsutbytte til ESCO-yrker når det gjelder kunnskap, ferdigheter, kompetanse, etc.

For hvert yrke er det et sett med kompetanser, ferdigheter og kunnskaper. Nedenfor er definisjoner og eksempler på kompetanse, ferdigheter, kunnskap og verdi.

Kompetanse refererer til en persons evne til å utføre en bestemt oppgave eller jobb effektivt. Den omfatter en kombinasjon av kunnskaper, ferdigheter og atferd som brukes for å forbedre ytelsen. Eksempel: Å være kompetent i prosjektledelse innebærer en kombinasjon av organisatoriske ferdigheter, kunnskap om prosjektledelsesprosesser og evnen til å kommunisere effektivt med teammedlemmer.

Ferdigheter er spesifikke evner eller evner som er oppnådd gjennom praksis, trening eller erfaring som gjør det mulig for en person å utføre oppgaver. Eksempel: Ferdigheter for penetrasjonstesting, evne til å bruke cybersikkerhetsverktøy og programvare, programmeringsferdigheter og evnen til å analysere og reagere på trusler i sanntid.

Kunnskap refererer til fakta, informasjon og forståelse lært gjennom utdanning eller erfaring. Det omfatter den teoretiske forståelsen av fakta og prinsipper knyttet til et bestemt felt. Eksempel: Forstå hvordan ulike typer cyberangrep utføres (f.eks. phishing, ransomware, DDoS-angrep) eller kunnskap om ulike krypteringsmetoder og kjennskap til de nyeste trendene og utviklingene innen cybersikkerhet.

Denne analysen er delt inn i 2 faser:

Fase 1: Gjennomgang og valg av ESCO-yrker

Konsultasjon på ESCO-portalen for å filtrere yrker knyttet til cybersikkerhet og dokumentere i neste avsnitt hver yrke, med spesiell oppmerksomhet til de oppførte ferdighetene, kompetansene, kunnskapene.

ESCO Yrke Tittel	Kunnskap	Ferdigheter	Kompetanse
3512.3 - IKT-sikkerhetstekniker	• IKT-nettverk • Vektorer for maskinvareangrep • Mottiltak mot cyberangrep • Operativsystemer Anskaffelse av IKT • Nettverksutstyr • Web-applikasjon • Sikkerhetstrusler	• adressere problemer kritisk • analysere IKT-systemet • Sikre riktig dokumenthåndtering • utføre programvaretester identifisere svakheter i IKT-systemet	• integrere systemkomponenter • gi teknisk dokumentasjon • løse problemer med IKT-systemet • Bruk programvare for tilgangskontroll
Implementeringsstandard 2529.1 - IKT-sikkerhetssjef - Omfatter personer som utfører sikkerhetsfunksjoner.	• Sikkerhetsrisikoer knyttet til IKT-nettverk • Regelverket for IKT-sikkerhet • Standarder for IKT-sikkerhet • angrepsvektorer • revisjon teknikker • Mottiltak mot cyberangrep • Cyber-sikkerhet • Personvern • Beslutningsstøttesystemer • Informasjon konfidensialitet • Strategi for informasjonssikkerhet • Retningslinjer for intern risikostyring • Organisatorisk motstandskraft	• Opplyse om datakonfidensialitet • sikre etterlevelse av organisatoriske IKT-standarder • sikre overholdelse av lovkrav • sikre samarbeid på tvers av avdelinger • Sikre personvern • identifisere IKT-sikkerhetsrisikoer • implementere styring av IKT-risiko • implementere retningslinjer for IKT-sikkerhet • implementere eierstyring og selskapsledelse	• lede katastrofegjenopprettingsøvelser • opprettholde plan for kontinuitet i driften • administrere overholdelse av IT-sikkerhet • Administrere planer for nødgjenoppretting • følge utviklingen i fagfeltet • overvåke teknologitrender utnytte beslutningsstøttesystem
2529.2 - Digital Forensics Expert - henter og analyserer informasjon fra datamaskiner og andre typer datalagringsenheter; undersøker digitale medier som kan ha blitt skjult, kryptert eller skadet, på en rettsmedisinsk måte med sikte på å identifisere, bevare, gjenopprette, analysere og presentere fakta og meninger om den	• Sikkerhetsrisikoer knyttet til IKT-nettverk • Standarder for IKT-sikkerhet • datamaskin rettsmedisin • Mottiltak mot cyberangrep • Informasjon konfidensialitet • Verktøy for penetrasjonstesting • Spørrespråk	• Bruk omvendt utvikling • utvikle strategi for informasjonssikkerhet • Opplyse om datakonfidensialitet • samle inn data for rettsmedisinske formål • identifisere IKT-sikkerhetsrisikoer • identifisere svakheter i IKT-systemet	• administrere overholdelse av IT-sikkerhet • Administrer data for juridiske saker • utføre kriminaltekniske konserveringer av digitale enheter

digitale informasjonen.	• Spørrespråk for rammeverk for ressursbeskrivelse	• implementere diagnoseverktøy for IKT-nettverket • gi IKT-rådgivning • Sikre sensitiv kundeinformasjon • Bruke skriptprogrammering • bruke programvare for databevaring • utføre testing av IKT-sikkerhet	
2529.3 - Embedded systems Security Engineer - fokus for de innebygde systemene Security Engineers er på tilkoblede produkter og deres støttenettverk, og mindre på organisatorisk sikkerhet som med IKT-sikkerhetsingeniøren.	• Sikkerhetsrisikoer knyttet til IKT-nettverk • Standarder for IKT-sikkerhet • Tingenes internett • Dataprogrammering • Mottiltak mot cyberangrep • Innebygde systemer • Strategi for informasjonssikkerhet • Uregelmessigheter i programvaren	• analysere IKT-systemet • Opprette flytskjemadiagram • Definere sikkerhetspolicyer • utvikle driver for IKT-enheter • utvikle programvare prototype • Utfør programvaretester • identifisere IKT-sikkerhetsrisikoer • identifisere svakheter i IKT-systemet • tolke tekniske tekster • gi IKT-rådgivning • utføre testing av IKT-sikkerhet • gi teknisk dokumentasjon	• Hold deg oppdatert på de nyeste informasjonssystemløsningene • administrere overholdelse av IT-sikkerhet • Overvåk systemytelsen • utføre risikoanalyse • Rapporter testfunn ved bruk av programvaredesignmønstre • Bruk programvarebiblioteker • benytte dataassisterte programvareutviklingsverktøy • definere tekniske krav
2529.4 - etisk hacker - utfører sikkerhetssårbarhetsvurderinger og penetrasjonstester i samsvar med bransjeaksepterte metoder og protokoller; Analyserer systemer for potensielle sårbarheter som kan skyldes feil systemkonfigurasjon, maskinvare- eller programvarefeil eller driftssvakheter.	• angrepsvektorer • datamaskin rettsmedisin • Mottiltak mot cyberangrep • etikk • lovkrav til IKT-produkter • Verktøy for penetrasjonstesting • Uregelmessigheter i programvaren • verktøy for automatisering av IKT-tester • Sikkerhetstrusler mot webprogrammer	• utføre testing av IKT-sikkerhet • gi teknisk dokumentasjon • Utvikle kodeutnyttelser • utføre IKT-revisjoner • Utfør programvaretester • identifisere IKT-sikkerhetsrisikoer • identifisere svakheter i IKT-systemet	• adressere problemer kritisk • analysere konteksten til en organisasjon • Overvåk systemytelsen
2529.5 - IKT resilience manager - forsker, planlegger og utvikler	• IKT-gjenopprettingsteknikker	• utvikle beredskapsplaner for nødsituasjoner	• analysere forretningsprosesser • analysere konteksten til

modeller, retningslinjer, metoder, teknikker og verktøy som forbedrer en organisasjons cybersikkerhet, motstandskraft og katastrofegjenoppretting	• Intern cybersikkerhet • Retningslinjer for risikostyring • Organisatorisk motstandskraft • Beste praksis for sikkerhetskopiering av systemet	• utvikle strategi for informasjonssikkerhet • utføre IKT-revisjoner • identifisere IKT-sikkerhetsrisikoer • implementere IKT-gjenvinningssystem • implementere styring av IKT-risiko	en organisasjon • overholde lovbestemmelser • lede katastrofegjenopprettingsøvelser • administrere overholdelse av IT-sikkerhet • Administrere planer for nødgjenoppretting • Administrere systemsikkerhet • utføre testing av IKT-sikkerhet
2529.6 - IKT-sikkerhetsansvarlig - planlegger og gjennomfører sikkerhetstiltak for å beskytte informasjon og data mot uautorisert tilgang, bevisst angrep, tyveri og korrupsjon.	• Sikkerhetsrisikoer knyttet til IKT-nettverk • Tingenes internett • Mottiltak mot cyberangrep • Verktøy for databaseutvikling • Styring av Internett • Administrasjon av mobilenheter • Operativsystemer • Organisatorisk motstandskraft • Metoder for kvalitetssikring • Beste praksis for sikkerhetskopiering av systemet	• identifisere svakheter i IKT-systemet • tolke tekniske tekster • vedlikeholde IKT-identitetsforvaltningen • Oppretthold databasesikkerheten	• Bruk firmapolicyer • ivareta kvaliteten i IKT-systemene • Sikre riktig dokumenthåndtering • administrere IKT-dataarkitektur • administrere overholdelse av IT-sikkerhet • utføre IKT-feilsøking • løse problemer med IKT-systemet
2529.7 - IKT-sikkerhetsingeniør - rådgiver og implementerer løsninger for å kontrollere tilgang til data og programmer og sikrer beskyttelse av organisasjonens oppdrag og forretningsprosesser.	• Regelverket for IKT-sikkerhet • Standarder for IKT-sikkerhet • angrepsvektorer • Forretningsanalyse • Mottiltak mot cyberangrep • Cyber-sikkerhet • Fremvoksende teknologier • Informasjonsarkitektur • Strategi for informasjonssikkerhet • Operativsystemer • Organisatorisk motstandskraft • Risikostyring • Ustrukturerte data	• utvikle strategi for informasjonssikkerhet • Opplyse om datakonfidensialitet • Ivareta informasjonssikkerheten • utføre IKT-revisjoner • Utfør programvaretester • identifisere IKT-sikkerhetsrisikoer • identifisere svakheter i IKT-systemet • implementere styring av IKT-risiko • gi IKT-rådgivning • analysere IKT-systemet • Definere	• Definere kriterier for datakvalitet • definere tekniske krav • Føre oppgaveoppføringer • Hold deg oppdatert på de nyeste informasjonssystemløsningene • administrere overholdelse av IT-sikkerhet • Administrere planer for nødgjenoppretting • Overvåk systemytelsen • utføre dataanalyse • utføre risikoanalyse • Rapporter testfunn feilsøke • verifisere formelle IKT-

		sikkerhetspolicyer	spesifikasjoner
2529.8 - IKT-sikkerhetssjef - foreslår og implementerer nødvendige sikkerhetsoppdateringer; gir råd, støtter, informerer og gir opplæring og sikkerhetsbevissthet og iverksetter direkte tiltak på hele eller deler av et nettverk eller system.	• IKT problemhåndtering teknikker • IKT-prosjektledelse • Kvalitetspolitikk for IKT • Standarder for IKT-sikkerhet • Krav til IKT-systemets brukere • Tingenes internett • angrepsvektorer • datamaskin rettsmedisin • Strategi for informasjonssikkerhet • Retningslinjer for intern risikostyring • Styring av Internett • lovkrav til IKT-produkter	• Definere sikkerhetspolicyer • utvikle strategi for informasjonssikkerhet • etablere en plan for forebygging av IKT-sikkerhet • implementere styring av IKT-risiko	• lede katastrofegjenopprettingsøvelser • vedlikeholde IKT-identitetsforvaltningen • administrere overholdelse av IT-sikkerhet • Administrere planer for nødgjenoppretting • løse problemer med IKT-systemet
2529.9 - kunnskapsingeniør - integrerer strukturert kunnskap i datasystemer (kunnskapsbaser) for å løse komplekse problemer som normalt krever et høyt nivå av menneskelig kompetanse eller kunstig intelligens metoder.	• Forretningsintelligens • Modellering av forretningsprosesser • Verktøy for databaseutvikling • Uttrekk av informasjon • Informasjonsstruktur Naturlig språkbehandling • Prinsipper for kunstig intelligens • Spørrespråk for rammeverk for ressursbeskrivelse • Livssyklus for systemutvikling • Systemteori • Algoritmisering av oppgaver • Web-programmering	• Bruke et programspesifikt grensesnitt • Bruke databaser • Bruk markeringsspråk	• analysere forretningskrav • anvende IKT-systemteori • vurdere IKT-kunnskap • Opprette semantiske trær • definere tekniske krav • administrere semantisk integrasjon med IKT • administrere forretningskunnskap • Behandle database

Fase 2: Kartlegging av ESCO Yrke og læringsutbytte

Med forrige tabell analyserte vi de dokumenterte yrkene og identifiserte læringsutbyttet knyttet til hver rolle. Vi brukte ESCO-rammeverket til å kategorisere disse resultatene i kunnskap, ferdigheter og kompetanse.

Et læringsutbytte er et klart og konkret utsagn som beskriver hva studentene forventes å lære og være i stand til når en undervisningsperiode er avsluttet. Uttalelsen inneholder kunnskaper, ferdigheter og holdninger.

I ESCO yrkes-klassifiserer seksjonen er fagfolk innen Informasjons- og kommunikasjonsteknologi delt opp i to underseksjoner: 'Programvare- og applikasjonsutviklere'

og 'analyse og database og nettverksfagfolk'. Den siste består av fire grupper: 'Database og nettverk', 'systemadministratorer', 'datanettverk og database' og 'nettverk ikke andre steder klassifisert'. Alle cybersikkerhetsyrker presentert i tabellen ble funnet i denne enhetsgruppen. For eksempel inkluderer gruppen sikkerhetsspesialister innen informasjons- og kommunikasjonsteknologi.

I slike tilfeller vil oppgaver omfatte:

a) utvikle planer for å sikre datafiler mot utilsiktet eller uautorisert endring, ødeleggelse eller offentliggjøring og for å oppfylle nøddatabehandlingsbehov.

(b) opplæring av brukere og fremme sikkerhetsbevissthet for å sikre systemsikkerhet og for å forbedre server- og nettverkseffektiviteten.

(c) snakke med brukere for å diskutere spørsmål som datatilgangsbehov, sikkerhetsbrudd og programmeringsendringer.

(d) overvåke gjeldende rapporter om datavirus for å avgjøre når virusbeskyttelsessystemer skal oppdateres.

(e) endre datasikkerhetsfiler for å innlemme ny programvare, rette feil eller endre individuell tilgangsstatus.

(f) overvåke bruken av datafiler og regulere tilgangen til å beskytte informasjon i datafiler.

(g) utføre risikovurderinger og utføre tester av databehandlingssystem for å sikre at databehandlingsaktiviteter og sikkerhetstiltak fungerer.

(h) kryptere dataoverføringer og opprette brannmurer for å skjule konfidensiell informasjon når den overføres, og for å holde skjemte digitale overføringer ute.

Beskrivelse av læringsutbytte for hvert yrke:

Yrke	Læringsutbytte
IKT-sikkerhetstekniker (3512.3)	• Demonstrere omfattende forståelse av IKT-nettverk, maskinvareangrepsvektorer, mottiltak mot cyberangrep og operativsystemer. • Kritisk analysere og diagnostisere sårbarheter i IKT-systemer for å forbedre systemsikkerheten. • Implementer og administrer robuste dokumenthåndteringsstrategier som overholder IKT-sikkerhetsprotokoller. • Utvikle og gjennomføre detaljerte programvaretestplaner for å identifisere og rette opp programvaresårbarheter. • Integrer systemkomponenter og bruk programvare for adgangskontroll for å bygge sikre og effektive IKT-systemer.
Sjef for IKT-sikkerhet (2529.1)	• Forstå og analysere IKT-nettverkssikkerhetsrisiko, lovgivning og

	standarder for å beskytte organisasjonsinformasjon. • Utvikle og implementere informasjonssikkerhetsstrategier og interne risikostyringspolitikker. • Lede katastrofegjenopprettingsøvelser og opprettholde operasjonelle kontinuitetsplaner. • Lær opp ansatte i datakonfidensialitet og sikre samarbeid på tvers av avdelinger for forbedret sikkerhetspraksis.
Ekspert på digital kriminalteknikk (2529.2)	• Analyser og test sikkerheten til innebygde systemer, spesielt i Tingenes Internett-miljøet (IoT). • Utvikle og utføre programvare prototyper og tester og utnytte dataassistert software engineering verktøy. • Administrer IT-sikkerhetssamsvar og utfør risikoanalyse og overvåking av systemytelse. • Definer og implementer sikkerhetspolicyer og tekniske krav for innebygde systemer.
Sikkerhetstekniker for innebygde systemer (2529.3)	• Analyser og test sikkerheten til innebygde systemer, spesielt i Tingenes Internett-miljøet (IoT). • Utvikle og utføre programvare prototyper og tester og utnytte dataassistert software engineering verktøy. • Administrer IT-sikkerhetssamsvar og utfør risikoanalyse og overvåking av systemytelse. • Definer og implementer sikkerhetspolicyer og tekniske krav for innebygde systemer.
Etisk Hacker (2529.4)	• Utfør sikkerhetssårbarhetsvurderinger og penetrasjonstesting ved hjelp av bransjeaksepterte metoder. • Identifiser og utnytt potensielle sårbarheter i systemer for å forbedre sikkerhetstiltak. • Utvikle kodeutnyttelser og utføre IKT-revisjoner for å sikre systemintegritet. • Analyser konteksten til en organisasjon for å skreddersy sikkerhetsstrategier effektivt
Leder for IKT-motstandsdyktighet (2529.5)	• Utvikle og implementere beredskapsplaner og informasjonssikkerhetsstrategier for nødscenarier. • Implementere og administrere IKT-gjenopprettingssystemer og risikostyringsprosesser. • Lede katastrofegjenopprettingsøvelser og administrere systemsikkerhet under kriser. • Analyser forretningsprosesser for å forbedre

	organisatorisk motstandskraft og overholdelse av lovbestemmelser.
Administrator for IKT-sikkerhet (2529.6)	• Planlegge og implementere sikkerhetstiltak for å beskytte data og administrere IKT-identitetssystemer. • Opprettholde databasesikkerheten og sikre systemets integritet og robusthet. • Løse IKT-systemproblemer og utføre feilsøkings- og kvalitetssikringsmetoder. • Administrer dataarkitektur og følg organisasjonspolicyer for databeskyttelse.
IKT-sikkerhetsingeniør (2529.7)	• Gi råd om og implementere løsninger for å kontrollere tilgangen til data og beskytte forretningsprosesser. • Analysere IKT-systemer og definere sikkerhetspolitikk og datakvalitetskriterier. • Utfør dataanalyse og risikoanalyse og administrer IT-sikkerhetssamsvar og planer for nødgjenoppretting. • Hold deg oppdatert med nye teknologier og informasjonssystemløsninger
Leder for IKT-sikkerhet (2529.8)	• Foreslå og implementere sikkerhetsoppdateringer og administrere IKT-sikkerhet på tvers av ulike prosjekter. • Lede katastrofegjenopprettingsøvelser og etablere planer for forebygging av IKT-sikkerhet. • Vedlikeholde og administrere IKT-identitetsstyringssystemer og løse komplekse systemproblemer. • Utvikle og implementere informasjonssikkerhetsstrategier og administrere katastrofegjenopprettingsplaner.
Kunnskapsingeniør (2529.9)	• Integrer strukturert kunnskap i datasystemer ved hjelp av avanserte verktøy som RDF-spørringsspråk og webprogrammering. • Administrer semantisk integrering og databasesystemer for å forbedre virksomhetens kunnskapshåndtering. • Analyser forretningskrav og bruk IKT-systemteori for å utvikle effektive kunnskapsbaser. • Lag semantiske trær og vurder IKT-kunnskap for å løse komplekse problemer ved hjelp av AI-metoder.

3. ANALYSE OG FUNN

3.1. ANALYSE AV FELTFORSKNINGEN

Feltundersøkelsesanalyse for yrkesfag og HEI

Undersøkelsesdataene fra "Mapping the Training Needs for SME Cyber Security Change Agents" inneholder en rekke spørsmål som fokuserer på opplæring i cybersikkerhet i sammenheng med yrkesutdanning og opplæring (VET) og høyere utdanningsinstitusjoner (HEI). Vi samlet inn data om emner som inngår i opplæring i cybersikkerhet, undervisningsmetoder, kjønnsinklusivitet og respondentenes demografi.

Målet med denne studien er å analysere svarene for å forstå den nåværende tilstanden til opplæring i cybersikkerhet, metodene som brukes, og oppfatningene rundt inkludering og effektivitet innen dette feltet.

Svaranalysen vil være basert på følgende nøkkelstruktur:

- Demografi
- Pensum, opplæringsbehov og læringspreferanser
- Kompetansekrav og fremtidige ferdigheter
- Kjønnsspesifikk innsikt

Demografi:

Kjønnsfordelingen blant respondentene i undersøkelsen mellom yrkesopplæringsinstitusjoner og høyere utdanningsinstitusjoner (HEI) er som følger:

Totalt antall respondenter per institusjonstype

Type institusjon	Svar	Kvinne	Mann	Vil helst ikke si
HEI (høyere utdanningsinstitusjoner)	104	28	73	3
VET (yrkesrettet utdanning og opplæring)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Mens det er en kjønnsubalanse i både HEI- og VET-institusjoner, er gapet mindre i yrkesfaglige institusjoner. For å gi et klarere bilde av kjønnsrepresentasjonen i forhold til totalt antall svar fra hver institusjon og justere resultatene med hensyn til antall svarskjevheter, har vi beregnet andelen av hvert kjønn innenfor begge institusjonstypene.

Fordeling av respondenter per institusjonstype

Type institusjon	Kvinne %	Mann %	Foretrekker å ikke si%	Total
HEI (høyere utdanningsinstitusjoner)	27	70	3	**100%**
VET (yrkesrettet utdanning og opplæring)	42	56	2	**100%**

Analysen justert for svarskjevhet bekrefter at selv om begge institusjonstypene har en høyere andel mannlige respondenter, er gapet mellom mannlig og kvinnelig representasjon fortsatt mindre i institusjonene. Årsaken kan være mangfoldig (f.eks. kulturelle, strukturelle eller politiske faktorer som påvirker kjønnsmangfold i cybersikkerhetsutdanning på tvers av disse institusjonstypene). Den høyere andelen kvinnelige respondenter i yrkesfagene antyder potensielle områder for videre undersøkelse av praksiser som støtter et mer kjønnsinkluderende miljø i yrkesopplæringen sammenlignet med høyere utdanning.

Pensum, opplæringsbehov og læringspreferanser

Emner som inngår i HEI og VET eksisterende cybersikkerhetsopplæringer

Emne	Svar	HEI	VET
Grunnleggende cybersikkerhet	151	90	61
Nettverkssikkerhet	123	72	51
Trusselanalyse og -håndtering	99	65	34
Kryptografi	92	57	35
Respons på hendelser	82	49	33
Risikostyring	77	43	34
Lover og retningslinjer for cybersikkerhet	73	42	31
Avanserte trusselreduserende teknikker	54	33	21

Det ser ut til at grunnleggende kunnskap og ferdigheter og nettverkssikkerhet er en prioritet. Trusselanalyse og -håndtering, Kryptografi and Respons på hendelser antyder en omfattende dekning av cybersikkerhetstrusler i opplæringene. Risikostyring og cybersikkerhetslover og retningslinjer til tross for å peke på en bevissthet om behovet for en helhetlig tilnærming som inkluderer å forstå den juridiske konteksten og håndtere risiko effektivt, er ikke alltid valgt. Det er interessant å merke seg at avanserte trusselreduserende teknikker er mindre inkludert i treninger.

For å gi resultatene uten skjevheten introdusert av antall respondenter fra hver type institusjon (HEI og VET), ble dataene normalisert av totalt antall svar for hver institusjonstype. Denne tilnærmingen lar oss se andelen institusjoner som inkluderer hvert emne i opplæringsprogrammene for cybersikkerhet.

Emner	HEI Andel	VET-andel
Grunnleggende cybersikkerhet	15.76%	15.48%
Nettverkssikkerhet	12.61%	12.94%
Trusselanalyse og -håndtering	11.38%	8.63%
Kryptografi	9.98%	8.88%
Respons på hendelser	8.58%	8.38%
Risikostyring	7.53%	8.63%
Lover og retningslinjer for cybersikkerhet	7.36%	7.87%
Avanserte trusselreduserende teknikker	5.78%	5.33%

Interessant nok er det lignende prioriteringer med små variasjoner. Både HEI- og VET-institusjoner legger betydelig vekt på "Grunnleggende cybersikkerhet" og "Nettverkssikkerhet". Dette indikerer at disse temaene er anerkjent som kritiske komponenter i utdanning innen cybersikkerhet. Proporsjonene er tett matchet, med "Grunnleggende cybersikkerhet" litt mer vektlagt i HEIs sammenlignet med VETs og "Nettverkssikkerhet" som viser et lignende mønster, men med et smalere gap.

Det er en merkbar variasjon i vektleggingen av mer spesialiserte emner som "Trusselanalyse og-håndtering", "Kryptografi" og "Avanserte trusselreduserende teknikker." HEI-er har en tendens til å tildele en litt høyere andel av treningsprogrammene sine til disse emnene sammenlignet med yrkesfag. Det kan forklares med at høgskolenes fokus er på å gi en mer omfattende, teoribasert forståelse av cybersikkerhet, som ofte inkluderer et bredere spekter av spesialiserte. Institusjoner for yrkesrettet utdanning kan derimot, selv om de fortsatt dekker et bredt spekter av emner, prioritere praktiske anvendelser og umiddelbar jobb-beredskap.

Undervisnings- og læringsformer

Undervisnings- og læringsformer	HEI Andel	VET-andel
Casestudier	60.91%	39.09%
Gruppeprosjekter	58.95%	41.05%
Praktiske oppgaver	59.02%	40.98%
Forelesninger	56.97%	43.03%
Omvendt undervisning	34.78%	65.22%
Online simuleringer	51.35%	48.65%

Case Studies, Gruppeprosjekter, Praktiske oppgaver, Forelesninger metoder er mye brukt på tvers av begge institusjonstyper, med en preferanse i HEI enn i VET. Når det gjelder omvendt klasserom-metoden, er den mer utbredt i VET (65,22%) enn i HEI (34,78%), noe som indikerer en tilbøyelighet til interaktiv læringsmodell i yrkesopplæring. Omvendte klasserom prioriterer aktiv læring og studentengasjement, som stemmer godt overens med den praktiske og ferdighetsbaserte tilnærmingen som er karakteristisk for VET.

Effektivitet av undervisningsmetoder

Undervisnings- og læringsform	Antall svar
Praktiske treningsøkter	141
Personlige workshops	134
Interaktive simuleringer	104
Kurs på nett	100
Opplæringsvideoer	73
Webinarer	68

Denne oversikten fremhever et mangfold i foretrukne undervisningsmetoder, men med klar vekt på praktiske, interaktive og fleksible læringsopplevelser. Praktiske praksisøkter og personlige workshops er høyt verdsatt siden de gir en interaktiv og praktisk læringsopplevelse. Interaktive simuleringer og online kurs fikk også betydelig omtale som viser viktigheten av tilgjengelige læringsmodaliteter.

Utfordringer som skoleinstitusjonene står overfor.

På spørsmål om de viktigste utfordringene skoleinstitusjonene står overfor, oppsummerer vi de mest tilbakevendende temaene:

- **Mangfold av deltakerferdigheter og erfaring**: Undervisere står overfor vanskeligheter på grunn av variert bakgrunn og kompetansenivå blant deltakerne. Å skreddersy opplæringen til å passe hele gruppen og sikre at både tekniske og ikke-tekniske personer kan dra nytte av øktene er utfordrende.
- **Holde kursmaterialet oppdatert**: Den raske utviklingen av cybersikkerhetstrusler krever kontinuerlige oppdateringer av opplæringsmateriell og undervisningsmetoder for å sikre relevans.
- **Praktiske opplæringsbegrensninger**: Det er en betydelig utfordring å gi praktisk erfaring. Begrensninger inkluderer utilstrekkelige laboratoriefasiliteter, mangel på virkelige simuleringsevner og vanskeligheten med å skape realistiske cyberangrepsscenarier for praksis.
- **Ressursbegrensninger**: Trenere må ofte håndtere begrensede økonomiske ressurser, mangel på kvalifisert personell, utdatert studiemateriell og utilstrekkelige maskinvare- og programvareverktøy som er nødvendige for effektiv trening.
- **Studentengasjement og motivasjon**: Det er vanskelig å opprettholde studentenes oppmerksomhet og motivere dem til å delta aktivt i læringen, spesielt med behovet for å dekke komplekst og noen ganger tørt teknisk innhold.
- **Læreplan og utdanningsstruktur**: Det er behov for omfattende, tverrfaglige læreplaner som dekker alle aspekter av cybersikkerhet. Videre er det fortsatt en betydelig utfordring å innlemme cybersikkerhet i læreplanen, spesielt på videregående nivå.
- **Tilgang til oppdaterte verktøy og teknologier**: Å gi studentene tilgang til de nyeste cybersikkerhetsverktøyene og teknologiene for praktisk læring er ofte utfordrende, noe som er avgjørende for praktisk forståelse.
- **Språk- og lokaliseringsproblemer**: Cybersikkerhets-ressurser er kanskje ikke alltid tilgjengelige på studentenes morsmål, noe som legger til et lag med kompleksitet til opplæring i ikke-engelsktalende regioner.
- **Bransje- og utdanningstilpasning: Det** er en utfordring å balansere behovet for å undervise de teoretiske fundamentene med de praktiske ferdighetene som samsvarer med

industriens behov. Det er også en nødvendighet å forberede studentene på arbeidsmarkedet med relevante ferdigheter.

- **Lærerkapasitet og utvikling**: Å sikre at lærere har oppdatert kunnskap og er i stand til effektivt å formidle komplekse konsepter er avgjørende, men utfordrende.

Tilpasning til små og mellomstore bedrifters spesifikke behov

Alternativ for svar	Antall svar
Nøytral	82
Samkjørt	67
Litt samkjørt	19
Svært samkjørt	17
Ikke samkjørt	5

Flertallet av svarene indikerer en nøytral tilpasning, noe som tyder på at det er rom for forbedringer på dette punktet. Et betydelig antall respondenter vurderte programmene sine som samkjørt, mens svært få lærere mener at programmene deres er svært samkjørte eller ikke i tråd med industriens behov. Svarene i den nedre enden av skalaen (Ikke samkjørt og litt samkjørt) gjenspeiler bekymringer eller utfordringer med å tilpasse pedagogisk innhold fullt ut med den utviklende naturen til cybersikkerhet i bransjen. Denne fordelingen av svar viser at utfordringen med å sikre cybersikkerhetsutdanning, tilpasset bransjetrender og krav, fortsatt er relevant. Det fremhever relevansen av CyberAgent-prosjektet som tar sikte på å gi kontinuerlige pensumoppdateringer, bransjepartnerskap og praktiske opplæringsmuligheter for å forbedre tilpasningen av opplæringsprogrammer for cybersikkerhet med behovene til cybersikkerhetsindustrien.

Spesifikke emner for små og mellomstore bedrifter

Emne/ferdighet	Antall svar
Grunnleggende cybersikkerhet for små og mellomstore bedrifter	91
Databeskyttelse og personvern for små og mellomstore bedrifter	75
Ingen små og mellomstore bedrifters spesifikke emne eller ferdigheter er inkludert i programmet	**64**
Hendelsesrespons for små og mellomstore bedrifter	58
Risikovurdering og styring i SMB-sammenheng	53
Utvikling av retningslinjer for cybersikkerhet for små og mellomstore bedrifter	46

Det legges stor vekt på grunnleggende cybersikkerhetsprinsipper og databeskyttelse. De hyppigst nevnte emnene, Grunnleggende cybersikkerhet for små og mellomstore bedrifter og databeskyttelse og personvern for små og mellomstore bedrifter, indikerer at lærere prioriterer å utstyre små og mellomstore bedrifter med kunnskapen for å beskytte dataene sine og forstå grunnleggende cybersikkerhetskonsepter. Antall svar på "Ingen små og mellomstore bedrifters spesifikke emne eller ferdigheter er inkludert i programmet" er en indikasjon på et gap i noen opplæringsprogrammer for cybersikkerhet angående skreddersydd innhold for små og mellomstore bedrifter (SMB). Det fremhever et kritisk område for forbedring av opplæring i

cybersikkerhet, spesielt med tanke på utfordringene og truslene som små og mellomstore bedrifter står overfor.

Små og mellomstore bedrifter opererer ofte med begrensede ressurser og har kanskje ikke tilgang til spesialisert cybersikkerhetsekspertise, noe som gjør dem spesielt sårbare for cybertrusler. Fraværet av SMB-spesifikt innhold i opplæringsprogrammer for cybersikkerhet antyder at disse programmene kanskje ikke fullt ut imøtekommer de forskjellige behovene til små og mellomstore bedrifter, noe som potensielt etterlater et gap i deres forberedelse og motstandskraft mot nettangrep. Å adressere dette gapet krever integrering av emner og ferdigheter som er spesielt utviklet for å møte cybersikkerhetsbehovene til små og mellomstore bedrifter, for eksempel risikovurdering skreddersydd for mindre forretningsdrift, kostnadseffektiv cybersikkerhetspraksis og strategier for å utvikle en effektiv cybersikkerhetspolitikk med begrensede ressurser.

Kompetanseunderskudd hos SMB-ansatte

Ferdighet/emne	Antall svar
Oppdagelse og respons på trusler	103
Ekspertise på skysikkerhet	87
Hendelsesrespons og gjenoppretting	69
Datasikkerhet og beskyttelse	67
Risikostyring og analyse	63
Nye teknologier	58
Nettverkssikkerhet	41
Kunnskap om samsvar og regelverk	36

Analysen viser at de ansatte mangler kompetanse på sentrale områder, med trusseldeteksjon og respons som den hyppigst nevnte. Dette fremhever viktigheten av å forberede studentene til å identifisere og svare på cybersikkerhetstrusler som en viktig evne i feltet. Ekspertise innen skysikkerhet er nummer to, og viser tillit til skyteknologier og behovet for spesialisert kunnskap for å sikre skymiljøer fra de ansatte. Hendelsesrespons og gjenoppretting, personvern og beskyttelse, og risikostyring og analyse verdsettes også. Det vurderes at når det gjelder nye teknologier, er behovet for å holde seg oppdatert med de siste fremskrittene i feltet ikke et område med underskudd. Samme for nettverkssikkerhet som er et grunnleggende område som er en del av de fleste opplæringsprogrammer for cybersikkerhet. Det viser effektiviteten av treningene angående det punktet.

Trusler

Trusler	Antall svar
AI-drevne cyberangrep	117
Ransomware-angrep	96
Phishing og sosial manipulering	87
Sikkerhetsbrudd i skyen	82
IoT-sårbarheter	75

Deepfake-trusler	51
Innsidetrusler	25

Analysen avslører et betydelig fokus på AI-drevne cyberangrep som den hyppigst nevnte nye cybersikkerhetstrusselen, noe som indikerer en bekymring over raffinement og kompleksitet av cybertrusler drevet av kunstig intelligens. Ransomware-angrep og phishing og sosial manipulering rangerte også høyt og viste tilstedeværelsen av disse angrepsvektorene for små og mellomstore bedrifter. Skysikkerhetsbrudd og IoT-sårbarheter fremhever bekymringer knyttet til sikkerheten til skytjenester og det voksende tingenes internett, noe som gjenspeiler utfordringene med å beskytte mangfoldige og distribuerte teknologiske økosystemer for små og mellomstore bedrifter. Deepfake-trusler og Insider-trusler anses ikke som store trusselvektorer. Et opplæringsprogram som dekker de 5 beste emnene, kan bedre utstyre studenter og SMB-ansatte til å takle truslene som står overfor.

Nye trender

Område	**Antall svar**
AI og maskinlæring i cybersikkerhet	160
Digital identitet og personvern	96
Etisk hacking og defensive ferdigheter	82
Trusler om kvantedatabehandling	67
Desentraliserte sikkerhetssystemer (f.eks.	52
Fokus på myke ferdigheter og tverrfaglig opplæring	47

Det legges stor vekt på AI og maskinlæring i cybersikkerhet som det hyppigst nevnte området, noe som gjenspeiler viktigheten av disse teknologiene for å forbedre cybersikkerhetstiltak og behovet for fagfolk som er dyktige på disse områdene. Digital identitet og personvern er et annet viktig fokus som fremhever viktigheten av å beskytte digitale identiteter og sikre personvern. Etisk hacking og defensive ferdigheter score indikerer en etterspørsel etter praktiske, håndfaste ferdigheter som gjør det mulig for fagfolk å identifisere sårbarheter og forsvare seg mot angrep effektivt. Quantum Computing trussler, desentraliserte sikkerhetssystemer, som blockchain-teknologi og myke ferdigheter og tverrfaglig opplæring ble ikke ansett som nye trender. Distribusjonen av svar fremhever mangfoldet i cybersecurity-feltet og viktigheten av å forberede fagfolk med et mangfoldig sett med ferdigheter og kunnskaper for å takle nåværende og fremtidige utfordringer. Men AI-emnet stoler på toppen av listen.

Likestilling

Andel kvinner	**Antall svar**
Mindre enn 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
Mer enn 75%	3

Andelen kvinner i opplæringsprogrammer for cybersikkerhet avslører en forskjell i kjønnsmangfold, med flertallet av svarene som viser lav kvinnelig deltakelse. I detaljer plasserte 79 svar kvinners deltakelse mellom 10% og 25%, og 57 svar indikerte at det var mindre enn 10%. Et moderat nivå av kjønnsmangfold er foreslått i noen programmer, med 43 respondenter som anslår kvinners deltakelse til å være mellom 26% og 50%. Imidlertid er programmer med en høy andel kvinnelige deltakere spesielt sjeldne, dokumentert av bare 8 svar som indikerer et område på 51% til 75%, og en minimal telling av 3 svar som estimerer mer enn 75%. Disse dataene understreker utfordringen med å oppnå kjønnsmangfold innen opplæringsprogrammer for cybersikkerhet, og fremhever et betydelig gap i kvinnelig deltakelse på tvers av de fleste rapporterte programmer.

Initiativ for kjønn

Svar	Antall svar
Ja	30
Nei	160

Dataene indikerer at et betydelig flertall av respondentene, 160 totalt, ikke bruker spesifikke tiltak eller strategier for å oppmuntre kvinners deltakelse i opplæring i cybersikkerhet. Kun 30 respondenter bekreftet gjennomføringen av slike tiltak. Dette antyder at mens det er en viss bevissthet og innsats mot å øke kvinnelig deltakelse i opplæring i cybersikkerhet gjennom målrettede tiltak, kan det hende at flertallet av programmene ennå ikke prioriterer eller implementerer spesifikke strategier for å adressere kjønnsmangfold. Denne mangelen på målrettede tiltak kan bidra til den lave andelen kvinners deltakelse som nevnt i svarene på det forrige spørsmålet.

Kjønnsinkluderende opplæring

Svar	Antall svar
Ja	47
Nei	44
Usikker	72
Ikke relevant for meg	27

Resultatene antyder en delt mening blant respondentene om tilgjengeligheten av kjønnsinkluderende opplæringsmoduler innen cybersikkerhet. Den største gruppen, bestående av 72 respondenter, uttrykte usikkerhet ("Usikker"), noe som indikerte mangel på klar konsensus eller kunnskap om tilstedeværelsen av kjønnsinkluderende materiale. Det er en nesten jevn fordeling mellom de som mener det er nok kjønnsinkluderende moduler (47 svar) og de som ikke gjør det (44 svar). I tillegg vurderte 27 respondenter spørsmålet som ikke relevant for deres erfaring eller kontekst.

Denne inndelingen gjenspeiler den pågående debatten og varierte oppfatninger om inklusiviteten til opplæringsinnhold for cybersikkerhet. Det høye antallet usikre svar fremhever

et potensielt gap i bevissthet eller tilgjengelighet av kjønnsinkluderende opplæringsressurser innen økosystemet for utdanning og opplæring innen cybersikkerhet.

Barrierer mot kjønnsinkludering

Barriere	Antall svar
Stereotyper eller kulturelle normer	107
Manglende bevissthet om muligheter innen cybersikkerhet	86
Mangel på mentorskap eller rollemodeller	74
Utfordringer med balansen mellom arbeid og privatliv	60
Opplevd kjønnsskjevhet i bransjen	58

De viktigste hindringene for kvinners deltakelse i cybersikkerhet, slik de oppfattes av respondentene, er stereotyper eller kulturelle normer (107 antall svar) og mangel på bevissthet om muligheter innen cybersikkerhet (86 antall svar). Disse to barrierene antyder at samfunnsmessige oppfatninger og utilstrekkelig informasjon om karriereveier betydelig hindrer kvinners inntreden i cybersikkerhetsfeltet. Mangel på mentorskap eller rollemodeller og utfordringer med balanse mellom arbeid og privatliv er også betydelige barrierer, og understreker viktigheten av støttenettverk og fleksible arbeidsmiljøer for å oppmuntre kvinners deltakelse. I tillegg peker oppfattet kjønnsskjevhet i bransjen på et behov for kulturelle og systemiske endringer innen feltet for å gjøre det mer innbydende og rettferdig for kvinner.

Spesifikt program for å fremme mangfold og inkludering

Svar	Antall svar
Ja	44
Nei	85
Er ikke sikker	61

Dataene avslører at en betydelig del av de undersøkte institusjonene, med 85 svar, ikke har spesifikke retningslinjer eller programmer på plass for å fremme mangfold og inkludering for kvinner i opplæring i cybersikkerhet. I mellomtiden indikerte 44 respondenter at deres institusjoner implementerer slike tiltak, og fremhever en tilnærming til å adressere kjønnsmangfold i feltet. Imidlertid er et betydelig antall respondenter, 61, usikre på om deres institusjoner har slike retningslinjer eller programmer, og peker på en potensiell mangel på kommunikasjon eller bevissthet om eksisterende mangfolds- og inkluderingsarbeid. Denne blandede responsen antyder også at mens noen institusjoner gjør skritt mot inkludering i opplæring i cybersikkerhet, gjenstår et betydelig gap, både i implementeringen av mangfoldsprogrammer og i bevisstheten om slike initiativer blant fakultet, ansatte og studenter.

Forslag til forbedringer

Forslag	Antall svar
Økt synlighet av vellykkede kvinnelige cybersikkerhetsfagfolk	95
Flere kvinnelige cybersikkerhetsinstruktører eller opplæringspersonell	89
Tilby stipend eller insentiver	81
Muligheter for mentorskap	49
Opplæringsinnhold som unngår kjønnsforstyrrelser	33
Oppdater policyer regelmessig for å støtte inkludering	31
Kjønnsinkluderende casestudier og scenarier	24
Skreddersydde treningsprogrammer	21
Flere treningsøkter kun for kvinner	18

Analysen av svarene, angående forslag for å gjøre opplæring i cybersikkerhet mer kjønnsinkluderende, avslører en sterk konsensus om viktigheten av flere viktige strategier. Det mest støttede forslaget, med 95 omtaler, er den økte synligheten til vellykkede kvinnelige cybersikkerhets-fagfolk. Dette understreker den kritiske rollen som rollemodeller og ambisiøse figurer i å inspirere kvinner til å forfølge karrierer innen cybersikkerhet. Like bak, med 89 omtaler, er oppfordringen til flere kvinnelige cybersikkerhetsinstruktører eller opplæringspersonale, og fremhever behovet for representasjon i den pedagogiske arbeidsstyrken. Å tilby stipend eller insentiver, som mottar 81 omtaler, er identifisert som avgjørende for å gjøre feltet mer økonomisk tilgjengelig og attraktivt for kvinner. Mentorskapsmuligheter, bemerket av 49 respondenter, understreker viktigheten av veiledning og støtte fra erfarne fagfolk på feltet. Behovet for opplæringsinnhold som unngår kjønnsskjevheter og regelmessig oppdaterte retningslinjer for å støtte inkludering, peker mot en nødvendighet for læreplan- og policyjusteringer som gjenspeiler og fremmer mangfold.

SMBs feltundersøkelsesanalyse

Demografi:

Undersøkelsen fikk svar fra partnerlandene. Romania har flest respondenter (28), etterfulgt av Norge (23), og deretter Litauen, Spania og Belgia, hver med 21 respondenter. Finland og Tyrkia har også et betydelig antall svar, med 20 hver, og Polen er hakk i hæl med 19 respondenter.

Næringslivet

Selskapssektoren	Antall svar
IT	18
Utdannelse	6
Bygg	4
Rådgivning	4
Cybersikkerhet	4

Dataene indikerer en sterk representasjon fra IT-sektoren, med 18 respondenter som identifiserer sitt selskap som opererer innenfor denne sektoren. Utdannings-, konstruksjons-,

konsulent- og cybersikkerhetssektorer har også bemerkelsesverdige representasjoner, hver med teller fra 4 til 6. Utover topp fem er det en lang hale av sektorer med færre antall, noe som illustrerer undersøkelsens brede tilnærming på tvers av ulike bransjer.

Respondentens profil

Stilling i selskapet	Antall svar
Direktør	48
Leder/eier	35
Teknisk (ingeniør/utvikler/analytiker)	27
Annen	25
Koordinator/administrator	8
Salg/markedsføring	8
Spesialist/ekspert	8
Arbeidstaker	8
Konsulent	3
Utdanning/undervisning	2
Økonomi/regnskap	1
Prosjektledelse	1
HR	1
Total	**175**

Det er et bredt utvalg av jobbtitler med et mangfoldig faglig publikum og et stort panel av stillinger som "Ansatt" og "Direktør" som indikerer et bredt spekter av respondenter, som spenner over ulike nivåer innen organisasjonshierarkier. Cybersikkerhet er et tverrgående problem som engasjerer enkeltpersoner på tvers av ulike roller og ansvar i selskaper.

Kjønn

Kjønnsfordelingen blant respondentene i undersøkelsen viser en høyere representasjon av menn (102) sammenlignet med kvinner (69), med en liten andel av respondentene (4) som foretrekker å ikke oppgi kjønn. Denne fordelingen antyder et kjønnsgap i feltet som undersøkelsen representerer, noe som gjenspeiler bredere trender innen cybersikkerhet og teknologisektorer der mannlig dominans ofte rapporteres. Det betydelige antallet kvinnelige respondenter indikerer imidlertid en meningsfull deltakelse av kvinner i feltet, og peker mot pågående endringer i sektorens kjønnsmangfold. Mens kjønnsgapet er tydelig, peker mangfoldet i svarene også mot et gradvis skiftende landskap innen cybersikkerhet.

Kjønnsfordeling etter land

Land	Kvinnelig	Mannlig	Vil helst ikke si
Belgia	10	10	1
Finland	9	11	0
Litauen	9	12	0
Norge	8	15	0
Polen	8	9	2
Romania	12	16	0
Spania	6	14	1
Tyrkia	7	13	0

Tabellen viser kjønnsfordelingen mellom ulike land. Det er flere mannlige respondenter enn kvinnelige respondenter i alle land, i samsvar med den generelle kjønnsfordelingen som ble diskutert tidligere. Gapet varierer imidlertid fra land til land, der enkelte land, som Belgia, har like mange mannlige og kvinnelige respondenter (10 hver) og Polen har en tettere fordeling mellom menn (9) og kvinner (8), med et lite antall respondenter som foretrekker å ikke si kjønn (2). Land som Romania og Norge har et høyere antall respondenter generelt og opprettholder et høyere forhold mellom menn og kvinner. Denne kjønns-landsfordelingen gir en nyansert forståelse av den demografiske sammensetningen av respondentene, og fremhever både kjønnsforskjellene og det geografiske mangfoldet innen cybersikkerhetsfeltet.

Selskapets størrelse

Selskapets størrelse	Antall svar
Opptil 10 ansatte	64
11-50	60
51-250	51

Svarene fra undersøkelsen indikerer et betydelig antall små og mellomstore bedrifter blant deltakerne. Den største gruppen er bedrifter med inntil 10 ansatte (64 respondenter), tett fulgt av bedrifter med 11 til 50 ansatte (60 respondenter), og deretter av bedrifter med 51 til 250 ansatte (51 respondenter).

Overvekten av mindre selskaper blant respondentene fremhever viktigheten av skreddersydde cybersikkerhetsløsninger som adresserer de spesifikke behovene og begrensningene til små og mellomstore bedrifter.

Kunnskapsnivå

Kunnskapsnivå om cybersikkerhet	Antall svar
Viderekommen	85
Nybegynner	64
Avansert	26

Svarene fra undersøkelsen indikerer at flertallet av respondentene vurderer sine ansattes nåværende nivå av cybersikkerhetskunnskap som "Viderekommen" (85), etterfulgt av de som

vurderer det på et "nybegynnernivå" (64), og en mindre del ser sine ansatte som å ha "avansert" cybersikkerhetskunnskap (26).

Denne fordelingen antyder et betydelig potensial for vekst og utvikling i cybersikkerhetsferdigheter i organisasjonene som er representert. Flertallet av "Viderekommen" og "Nybegynner" nivåer peker på nødvendigheten av pågående opplærings- og utdanningsinitiativer for å heve kunnskapsbasen om cybersikkerhet for disse ansatte. Det fremhever en mulighet for målrettede opplæringsprogrammer for cybersikkerhet som imøtekommer forskjellige kunnskapsnivåer, og sikrer at grunnleggende prinsipper for cybersikkerhet blir godt forstått av nybegynnere.

Tilstedeværelsen av ansatte med avansert kunnskap, men færre, er oppmuntrende, da det indikerer et grunnleggende lag av cybersikkerhetskompetanse i noen organisasjoner.

Kunnskapsnivå basert på selskapets størrelse.

Selskapets størrelse	Avansert	Nybegynner	Viderekommen
Opptil 10 ansatte	6	25	33
11-50	10	20	30
51-250	10	19	22

Tabellen viser hvordan kunnskapsnivåene for cybersikkerhet (avansert, nybegynner, viderekommen) er fordelt på ulike selskapsstørrelser. Små bedrifter (opptil 10 ansatte) viser en tilbøyelighet til "Viderekommen" nivå av cybersikkerhet kunnskap, etterfulgt av "Nybegynner". Dette antyder at selv om små bedrifter kan ha en viss forståelse av cybersikkerhet, er det fortsatt en betydelig del på nybegynnernivå, noe som indikerer rom for forbedring og behovet for mer grunnleggende opplæring. Mellomstore bedrifter (11-50 ansatte) har en balansert fordeling på tvers av kunnskapsnivåene, med en liten preferanse for "middels" kunnskap. Dette kan gjenspeile en mer strukturert tilnærming til opplæring i cybersikkerhet i litt større organisasjoner, men indikerer på samme måte tilstedeværelsen av både avansert forståelse og grunnleggende læringsbehov. Større SMB-er (51-250 ansatte) følger et lignende mønster som mellomstore bedrifter, med like mange avanserte og nybegynnere og et litt lavere antall mellomkunnskaper.

På tvers av alle selskapsstørrelser er det "viderekommende" nivået av kunnskap om cybersikkerhet mest vanlig.

Ansatte som arbeider med cybersikkerhetsoppgaver

Antall ansatte	Antall svar
1-5	88
0	22
6-10	17
21+	12
11-20	5

Utvalg av ansatte innen cybersikkerhet	Antall svar
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Tabellene viser fordelingen av antall ansatte som utfører arbeid knyttet til cybersikkerhet på tvers av ulike virksomheter. Det gir en klarere oversikt over hvordan cybersikkerhetsansvar er fordelt på ulike områder av antall ansatte. De aller fleste svarene faller innenfor 0-4-området, noe som indikerer et stort antall organisasjoner med svært små cybersikkerhetsteam eller til og med ingen dedikert spesielt til cybersikkerhet. Det er en betydelig nedgang i frekvens når vi beveger oss til høyere områder, med en viss gjenoppblomstring i organisasjoner som har over 100 ansatte dedikert til cybersikkerhet. Det forklares av det faktum at disse selskapene jobber i cybersikkerhetsdomenet som hovedbeskjeftigelse.

I detaljer antyder dataene et bredt spekter i størrelsen på cybersikkerhetsteam, der den vanligste størrelsen er en enkelt ansatt, etterfulgt av ingen dedikerte cybersikkerhetsansatte, noe som indikerer at mange organisasjoner i liten grad eller ikke i det hele tatt har dedikert cybersikkerhetspersonell. Det er en merkbar nedgang i frekvens etter hvert som teamstørrelsen øker.

Distribusjonen fremhever et potensielt gap i bemanning av cybersikkerhet, der et betydelig antall små og mellomstore bedrifter (SMB) kanskje ikke har tilstrekkelige ressurser dedikert til cybersikkerhet, noe som utsetter dem for større risiko. Tilstedeværelsen av større team i noen organisasjoner antyder en anerkjennelse av viktigheten av cybersikkerhet i visse sektorer eller større selskaper.

Kvinner i cybersikkerhet

Utvalg av kvinner i cybersikkerhet	Antall svar
0	78
1-5	57
6-10	8
11-15	4
16-20	1

Resultatene av spørsmålet "Hvor mange av disse ansatte er kvinner?" fremhever et betydelig kjønnsgap i cybersikkerhetsarbeidsstyrken innen små og mellomstore bedrifter. Den mest slående observasjonen er at et flertall av selskapene, 78 totalt, rapporterte at de ikke hadde noen kvinner i sine cybersikkerhetsroller. Dette indikerer et utbredt problem med underrepresentasjon av kvinner i dette kritiske området på tvers av de undersøkte små og mellomstore bedriftene. En gradvis nedgang i antallet er notert ettersom antall kvinner i cybersikkerhetsroller øker, med 31 selskaper som har en kvinne i en slik stilling.

Tilstedeværelsen av noen få selskaper med 10 eller flere kvinner i cybersikkerhetsroller, selv om det er positivt, forblir et unntak snarere enn normen. Disse tilfellene kan representere organisasjoner med større cybersikkerhetsteam eller de som har satt et spesifikt fokus på kjønnsmangfold i arbeidsstyrken innen cybersikkerhet. Det understreker behovet for initiativer som tar sikte på å oppmuntre og støtte kvinner i å forfølge karrierer innen cybersikkerhet. Det betydelige antallet selskaper uten kvinner i cybersikkerhetsroller fremhever et kritisk område for intervensjon for å fremme kjønnsmangfold og inkludering i sektoren. Å bygge bro over dette kjønnsgapet kan bidra til mer mangfoldige perspektiver for å takle cybersikkerhetsutfordringer.

Bruk av eksterne tjenester

Svar	Antall svar
Nei	115
Ja	60

Svarene avslører et betydelig aspekt av hvordan små og mellomstore bedrifter tilnærmer seg cybersikkerhet. Et flertall av de undersøkte selskapene, 115 av 175, oppgir at de ikke leier inn eksterne tjenester til cybersikkerhetsarbeid. Dette antyder en preferanse eller nødvendighet for å håndtere cybersikkerhetsarbeid internt i et stort segment av SMB-befolkningen. Ulike faktorer kan drive denne trenden, for eksempel budsjettbegrensninger, oppfattet kontroll over cybersikkerhetspraksis eller troen på at deres eksisterende interne ressurser er tilstrekkelige til å møte deres cybersikkerhetsbehov. Denne situasjonen gjør CyberAgent-prosjektet svært relevant for å utstyre den ansatte med grunnleggende ferdigheter og kunnskaper.

60 selskaper rapporterte å ansette eksterne tjenester for cybersikkerhetsoppgaver. Denne gruppen anerkjenner sannsynligvis fordelene med outsourcing, for eksempel å få tilgang til spesialiserte ferdigheter, holde seg oppdatert med de nyeste cybersikkerhetstruslene og mottiltakene, eller supplere deres interne evner. Beslutningen om å ansette eksterne tjenester kan også gjenspeile en forståelse av kompleksiteten av cybersikkerhetstrusler, noe som kan være utfordrende å administrere helt internt, spesielt for små og mellomstore bedrifter med begrensede ressurser.

Denne splittelsen fremhever en forskjell i cybersikkerhetsstrategi blant små og mellomstore bedrifter, balansering mellom intern ledelse og ekstern outsourcing av cybersikkerhetsfunksjoner. Det understreker viktigheten av en skreddersydd tilnærming til cybersikkerhet, og anerkjenner at ulike organisasjoner kan ha varierte behov, evner og ressurser som påvirker deres beslutninger om å søke ekstern støtte til cybersikkerhetsarbeid.

Effektivitet av treningsprogrammer

Svar	Antall svar
1 (ineffektiv)	8
2	38
3	79
4	39
5 (veldig effektiv)	11

Svarene gir innsikt i oppfatninger om effektiviteten av dagens opplæringsprogrammer for å forberede studentene på virkelige cybersikkerhetsutfordringer i små og mellomstore bedrifter. Flertallet av respondentene, med 79 i antall svar, vurderte effektiviteten av dagens treningsprogrammer som en "3", noe som indikerer en nøytral eller moderat oppfatning av deres effektivitet. Dette antyder at mens det er en viss grad av tillit til disse programmene, er det også betydelig rom for forbedring. Svarene viser også en tendens til den nedre enden av skalaen, der «2» får 38 svar, noe som peker i retning av skepsis til effekten av disse treningsprogrammene. På ytterpunktene fikk '1' (ineffektiv) færrest svar (8 svar), og '5' (veldig effektiv) fikk litt mer (11 svar). Dette indikerer at svært få respondenter ser på dagens opplæringsprogrammer som enten helt ineffektive eller svært effektive for å forberede studentene på cybersikkerhetsutfordringer i små og mellomstore bedrifter. Det balanserte antallet svar for '4' (39 svar) antyder at et bemerkelsesverdig segment av deltakerne ser treningsprogrammene som relativt effektive, men ikke uten betydelige begrensninger. Mens nåværende opplæringsprogrammer gir en viss forberedelse for virkelige cybersikkerhetsutfordringer i små og mellomstore bedrifter, er det et gap mellom opplæringen som tilbys og industriens behov. Dette gapet kan skyldes flere faktorer, for eksempel utviklingstakten i cybersikkerhetstrusler, praktisk anvendelse av ferdigheter eller spesifisiteten til utfordringer som små og mellomstore bedrifter står overfor.

Topp 3 områder innen opplæring i cybersikkerhet

Kategori	Antall svar
Oppdagelse og respons på trusler	102
Risikostyring og analyse	81
Hendelsesrespons og gjenoppretting	72
Datasikkerhet og beskyttelse	68
Ekspertise på skysikkerhet	51
Nettverkssikkerhet	46
Kunnskap om samsvar og regelverk	31
Nye teknologier	24

Analysen av svarene avslører at "Trusseldeteksjon og respons" regnes som det mest avgjørende området i opplæring i cybersikkerhet, med 102 tellinger, noe som indikerer en sterk tro på dens betydning for å takle virkelige cybersikkerhetsutfordringer i små og mellomstore bedrifter. Dette området følges tett av "Risikostyring og analyse" og "Hendelsesrespons og gjenoppretting", med henholdsvis 81 og 72 tellinger, som understreker verdien av å forstå risiko og være i stand til å reagere effektivt på hendelser. "Datasikkerhet og beskyttelse" får også betydelig vekt som gjenspeiler den økende betydningen av databeskyttelseslover og behovet for å beskytte personlig og sensitiv informasjon i den digitale tidsalderen. «Skysikkerhetsekspertise» er identifisert som et nøkkelområde av 51 respondenter, sannsynligvis på grunn av den økende adopsjonen av skytjenester og de unike sikkerhetsutfordringene de presenterer. Nettverkssikkerhet, med 46 tiltalepunkter, er fortsatt en grunnleggende bekymring, og understreker behovet for sterkt forsvar mot nettverksbaserte trusler. "Kunnskap om samsvar og regelverk" og "Nye teknologier" blir sett på som mindre viktig.

Kompetanse og kunnskap

Kompetanse- og kunnskapsområde	Viktig (%)	Høyt behov (%)	Moderat behov (%)	Lavt behov (%)	Ikke nødvendig (%)
Datasikkerhet og beskyttelse	38.29	38.29	13.14	10.29	0.00*
Risikovurdering og styring	34.86	36.00	24.00	4.57	0.57
Hendelsesrespons og gjenoppretting	33.14	38.86	19.43	8.00	0.57
Kommunikasjonsevner	32.57	35.43	22.29	8.00	1.71
Teknisk kunnskap	30.29	32.00	26.29	8.57	2.86
Trusseletterretning og overvåking	29.71	37.14	24.00	8.57	0.57
Retningslinjeutvikling og implementering	24.00	37.14	24.00	12.57	2.29

*: "Ikke nødvendig" prosentandelen for "Data Privacy and Protection" er ikke tilgjengelig (NaN), noe som kan skyldes at alle respondenter vurderer dette området i det minste av noe behov, og kan derfor betraktes som 0%.

Tabellen viser gjennomsnittlig poengsum for hvert kompetanse- og kunnskapsområde, avledet fra undersøkelsessvar som rangerer deres betydning på en skala fra 1 (ikke nødvendig) til 5 (viktig). Disse poengsummene gir et kvantitativt innblikk i hvordan respondentene prioriterer ulike områder innenfor feltet.

Denne tabellen gir en klar oversikt over hvordan hvert kompetanse- og kunnskapsområde verdsettes av respondentene. Områder som "Datasikkerhet og beskyttelse" og "Risikovurdering og styring" har den høyeste prosentandelen av Viktig" rangeringer, noe som gjenspeiler deres kritiske betydning i feltet. I motsetning til dette viser "Retningslinjeutvikling og implementering" en bredere fordeling av svar, noe som indikerer en mer variert oppfatning av dens betydning. Resultatene fremhever en sterk vekt på teknisk kunnskap, trusselbevissthet og evnen til å reagere på hendelser, sammen med det avgjørende behovet for effektiv kommunikasjons- og databeskyttelsespraksis.

Nye cybersikkerhetstrusler

Fremvoksende cybersikkerhetstrussel	Antall svar
Phishing og sosial manipulering	105
AI-drevne cyberangrep	95
Ransomware-angrep	90
Sikkerhetsbrudd i skyen	60
Deepfake-trusler	57
IoT-sårbarheter	44
Innsidetrusler	31

Phishing og sosial manipulering regnes som de mest presserende truslene, med AI-drevne cyberangrep og ransomware-angrep som også får betydelig oppmerksomhet. Dette antyder en

sterk bevissthet blant små og mellomstore bedrifter om behovet for å beskytte seg mot både tradisjonelle og nye cybertrusler. Sikkerhetsbrudd i skyen og deepfake-trusler fremheves også, noe som gjenspeiler bekymringer for sikkerheten til skytjenester og potensielt misbruk av kunstig intelligens. IoT-sårbarheter og innsidetrusler identifiseres også, selv om de blir sett på som mindre overhengende enn de andre kategoriene. Spesielt er det svar som indikerer at noen respondenter er usikre på spesifikke trusler eller ikke har ideer på forretningsnivå, noe som tyder på et potensielt gap i bevissthet eller bekymring for spesifikke nye trusler blant noen små og mellomstore bedrifter.

Gap i kunnskap eller ferdigheter innen cybersikkerhet

Gap i kunnskap eller ferdigheter innen cybersikkerhet	Antall svar
Lavt nivå av trusselbevissthet	105
Lavt nivå av Cybersecurity Regular Trainings	88
Lavt nivå av sårbarhetsvurdering	80
Lavt nivå av tekniske ferdigheter	71
Lavt nivå av politikk og regelverksforståelse	50
Lavt nivå av myke ferdigheter	37

De viktigste hullene i kunnskap eller ferdigheter innen cybersikkerhet blant ansatte er trusselbevissthet, regelmessig opplæring i cybersikkerhet, sårbarhetsvurdering, tekniske ferdigheter og forståelse av retningslinjer og forskrifter. Hyppigheten av disse svarene fremhever et avgjørende behov for omfattende utdanning og opplæring innen cybersikkerhet som adresserer disse spesifikke områdene. Trusselbevissthet skiller seg ut som det viktigste gapet, noe som indikerer at ansatte kanskje ikke er fullt klar over cybersikkerhetstruslene som kan påvirke organisasjonen deres. Dette gapet understreker viktigheten av å styrke bevissthetsprogrammer og opplæring for å hjelpe ansatte med å gjenkjenne mulige trusler mer effektivt. Regelmessige cybersikkerhetstreninger blir også sett på som et gap, og peker på behovet for kontinuerlig utdanning og oppdateringer om de nyeste cybersikkerhetspraksisene og truslene, i stedet for engangsopplæringsøkter.

Nye trender

Nye trender innen opplæring i cybersikkerhet	Antall svar
AI og maskinlæring i cybersikkerhet	134
Digital identitet og personvern	108
Etisk hacking og defensive ferdigheter	86
Fokus på myke ferdigheter og tverrfaglig opplæring	54
Trusler om kvantedatabehandling	39
Desentraliserte sikkerhetssystemer (f.eks. Blockchain)	28

Analysen viser en klar vektlegging av AI og maskinlæring innen cybersikkerhet som den mest etterlengtede trenden de neste fem årene. Dette indikerer en økende anerkjennelse av rollen som avansert teknologi spiller for å styrke cybersikkerhetsforsvaret og utvikle nye sikkerhetsløsninger. Den høye frekvensen av svar i denne kategorien antyder at opplæringsprogrammer i økende grad vil trenge å inkludere AI- og

maskinlæringskomponenter for å forberede cybersecurity-fagfolk for fremtiden. Digital identitet og personvern fremstår som den nest mest etterlengtede trenden, og fremhever bekymringene rundt beskyttelse av personopplysninger og styring av digitale identiteter i en stadig mer online verden. Denne trenden antyder en etterspørsel etter opplæring som dekker kompleksiteten i personvernlover, databeskyttelsesteknikker og identitetsadministrasjonsløsninger. Etisk hacking og defensive ferdigheter er identifisert som den tredje nøkkeltrenden, noe som gjenspeiler viktigheten av proaktive forsvarsstrategier innen cybersikkerhet. Vektleggingen av etisk hacking viser et skifte mot trening som gjør det mulig for fagfolk innen cybersikkerhet å tenke som angripere for bedre å forsvare organisasjonene sine.

Tilstrekkelighet av treningsprogrammer

Svar	Antall svar
Ja	81
Er ikke sikker	65
Nei	29

Analysen av spørsmålet som utforsket respondentenes syn på tilstrekkeligheten av dagens opplæringsprogrammer for cybersikkerhet, avslører et blandet syn blant deltakerne. En betydelig del, som representerer flertallet av respondentene, mener at dagens opplæringsprogrammer for cybersikkerhet er tilstrekkelige, som indikert av "Ja" -svarene. Dette antyder at en rekke individer føler at opplæringen som er tilgjengelig i dag oppfyller behovene til deres organisasjoner eller samsvarer med deres forventninger til hva opplæring i cybersikkerhet skal innebære. Imidlertid er et betydelig antall respondenter "Ikke sikre" på tilstrekkeligheten av nåværende opplæringsprogrammer, og fremhever en grad av usikkerhet eller mangel på informasjon om opplæringsalternativene som er tilgjengelige eller deres effektivitet når det gjelder å takle dagens cybersikkerhetsutfordringer. Denne usikkerheten kan tilskrives utviklingen av cybertrusler og vanskeligheten med å holde treningsprogrammer oppdatert med den siste utviklingen på feltet. "Nei" -svarene, selv om de representerer den minste gruppen, indikerer en klar bekymring for at eksisterende treningsprogrammer ikke er tilstrekkelige for å møte dagens cybersikkerhetsbehov. Denne gruppen kan oppfatte hull i opplæringens dekning av nye trusler, teknologier eller metoder.

Inkludering i treningsprogrammer

Svar	Antall svar
Ja	81
Er ikke sikker	65
Nei	29

Analysen av svarene indikerer et mangfoldig perspektiv på inklusiviteten til dagens opplæringsprogrammer for cybersikkerhet angående kjønn. Et flertall av respondentene føler at dagens opplæring er inkluderende og effektivt ivaretar behovene til alle kjønn, som indikert av "Ja" -svarene. Dette antyder at en betydelig del av cybersikkerhetssamfunnet mener at dagens opplæringsinnsats gjør fremskritt mot inkludering og likestilling. Imidlertid er et stort antall

respondenter "ikke sikre" på inklusiviteten til disse programmene, noe som indikerer en betydelig mengde usikkerhet eller mangel på bevissthet om kjønnsinklusiviteten til opplæring i cybersikkerhet. Dette svaret kan fremheve et kommunikasjonsgap mellom opplæringsleverandører og deltakere, eller antyde at inkluderingsarbeidet kanskje ikke er så synlig eller virkningsfullt som tiltenkt. Nei-svarene, som representerer den minste gruppen blant respondentene, fremhever likevel en kritisk bekymring for at dagens opplæring i cybersikkerhet ikke i tilstrekkelig grad ivaretar behovene til alle kjønn. Denne tilbakemeldingen peker på et gap i inklusivitetsarbeidet innen opplæringsprogrammer for cybersikkerhet, noe som tyder på at mer arbeid er nødvendig for å sikre at disse programmene er innbydende og skreddersydd for behovene til enkeltpersoner av alle kjønnsidentiteter.

3.2. TRENINGSPREFERANSER OG BEHOV

Basert på funnene fra feltforskningen, her er en beskrivelse av identifiserte egenskaper og opplæringsbehov, læringspreferanser, opplæring og støtte til kvinner involvert i cybersikkerhet

Opplæring trenger identifikasjon:

Område 1 - Grunnleggende kunnskaper og ferdigheter

En prioritet i utdanning innen cybersikkerhet. Spesielt temaer som grunnleggende cybersikkerhet og nettverkssikkerhet. Det er betydelige hull på områder som trusseldeteksjon og -respons, skysikkerhetsekspertise, hendelsesrespons og -gjenoppretting, personvern og beskyttelse av data, og risikostyring og analyse. Treningsprogrammer må adressere disse ferdighetsunderskuddene. Det er også et sterkt behov for cybersikkerhet for SMB-orientert innhold.

Område 2 - Spesialiserte emner

Dette er et behov for opplæring som dekker et bredt spekter av cybersikkerhetstrusler og mottiltak. Noen spesialiserte emner som trusselanalyse og -styring, kryptografi og avanserte trusselreduserende teknikker ble fremhevet. Opplæringen bør inneholde innhold om de hyppigst nevnte nye truslene, inkludert AI-drevne cyberangrep, ransomware-angrep, phishing og sosial manipulering, sikkerhetsbrudd i skyen og IoT-sårbarheter.

Område 3 - Praktisk anvendelse

Preferansen for undervisningsmetoder som praktiske laboratorier, casestudier og gruppeprosjekter fremhever viktigheten av praktisk, interaktiv og real-world applikasjon i cybersikkerhet-trening.

Gjeldende praksis:

Når det gjelder undervisningsmetoden, kan vi merke bruken av ulike praksiser som case-studier, gruppeprosjekter, praktiske laboratorier og forelesninger. Det er en blanding av teoretiske og praktiske tilnærminger i dagens treningsprogrammer.

Nåværende opplæringsprogrammer dekker en rekke cybersikkerhetsemner, med grunnleggende emner som prioriteres. Det er imidlertid et kjent fravær av SMB-spesifikt innhold i enkelte programmer.

Når det gjelder inkludering og kjønnsbalanse, har noen programmer iverksatt tiltak for å øke kvinnelig deltakelse og skape kjønnsinkluderende opplæringsmiljøer, selv om denne innsatsen ser ut til å være i mindretall.

Utfordringer:

Hovedutfordringene i utdanning innen cybersikkerhet er:

- Tilpasse opplæringen til å passe ulike bakgrunner og kompetansenivåer er utfordrende da det er et mangfold av ferdigheter og erfaring
- Holde kursmaterialet oppdatert for å takle den raske utviklingen av cybersikkerhetstrusler. Det krever kontinuerlig oppdatering av opplæringsmateriellet.
- Praktiske opplæringsbegrensninger på grunn av begrensninger i laboratoriefasiliteter, simuleringsfunksjoner i den virkelige verden og opprettelse av realistiske cyberangrepsscenarier for praksis
- Det er vanskelig å holde studentene engasjerte og motiverte, spesielt med komplekst teknisk innhold.
- Industri og pedagogisk tilpasning med balansering av teoretiske grunnlag med praktiske ferdigheter som samsvarer med industriens behov utgjør en utfordring.

Forslag til opplæringsutvikling:

- Tilpasse opplæringen til SMB-behov: integrering av emner og ferdigheter som er spesielt utviklet for å møte cybersikkerhetsbehovene til små og mellomstore bedrifter.
- Forbedre praktisk anvendelse ved å utvide bruken av praktiske, interaktive undervisningsmetoder for å forbedre praktiske ferdigheter og real-world beredskap.
- Innlemme nye trender som AI og maskinlæring, digital identitet og personvern og etisk hacking. De anses nå som nøkkelområder for fremtidig fokus i treningsprogrammer.
- Adressere ferdighetsunderskudd ved å fokusere på områder der ansatte mangler, for eksempel trusseldeteksjon og respons, skysikkerhet og hendelsesrespons, for bedre å forberede dem på å møte utfordringene og bli effektive og motstandsdyktige CyberAgent.
- Utvikle initiativer for kjønnsmangfold for å øke kvinnelig deltakelse gjennom målrettede tiltak, mentorskap og rollemodeller.

4. KVALIFIKASJONSPROFIL FOR EN SMB CYBER SECURITY CHANGE AGENT

Basert på funnene fra skrivebords- og feltforskning, her er et eksempel på CyberAgent forventet sett med kunnskaper, ferdigheter og kompetanser. Disse resultatene artikulerer de forventede prestasjonene til deltakerne på slutten av deres respektive opplæringsprogrammer for cybersikkerhet, og sikrer en utvikling fra grunnleggende kunnskaper og ferdigheter på EQF nivå 4/5 til en mer avansert og ledelsesorientert evne på EQF nivå 6.

CyberAgent kvalifiserings-profil	**Kunnskap**	**Ferdigheter**	**Kompetanse**
På EQF-nivå 4/5	**Grunnleggende om cybersikkerhet** - Grunnleggende konsepter for cybersikkerhet - Typer cybertrusler (phishing, ransomware, DDoS-angrep), angrepsvektorer - Viktigheten av cybersikkerhet for å beskytte organisatoriske eiendeler. **Cybersikkerhet juridiske- og datarammeverk** - Lovgivning, standarder og samsvarskrav for cybersikkerhet - Strategier og retningslinjer for informasjons-sikkerhet - Personvern - Retningslinjer for risikostyring	**Sikkerhet** - Identifiser potensielle cybersikkerhets-risikoer og sårbarheter - Bruk cybersikkerhets-verktøy og programvare for å beskytte mot cybertrusler - Fremme praktisk anvendelse av grunnleggende cybersikkerhets-praksis, sikker passord-oppretting, sikker surfing, e-postsikkerhet og sikker håndtering av sensitive data	**Risikostyring og risikoreduserende tiltak** - Vurder og reduser potensielle sikkerhetstrusler **Effektiv kommunikasjon om cybersikkerhets-spørsmål** - Evne til å kommunisere effektivt om cybersikkerhetsproblemer, - Rapportere trusler og brudd til de riktige kanalene i organisasjonen.

På EQF-nivå 6	**Avanserte cybersikkerhetskonsepter** - Forstå avanserte cybersikkerhets-prinsipper, inkludert sofistikerte cybertrusler og angrepsvektorer, - Bevissthet om de nyeste trendene innen cybersikkerhets-trusler og forsvars-mekanismer. **Lovgivning og overholdelse av cybersikkerhet** - Kunnskap om nasjonal og internasjonal lovgivning, standarder og krav til cybersikkerhet, og andre som er relevante for deres spesifikke bransje.	**Avansert risikovurdering og styring** - Evne til å gjennomføre omfattende risikovurderinger - Bruk av avanserte metoder og verktøy - Utforme og implementere effektive risikostyrings-strategier for å redusere identifiserte risikoer. **Ekspertise innen sikkerhetsarkitektur og nettverksforsvar** - Designe, implementere og evaluere sikre nettverks-arkitekturer, inkludert bruk av brannmurer, inntrengings-deteksjons-systemer (ID-er) og inntrengings-forebyggings-systemer (IPS). **Hendelsesrespons og gjenoppretting** - Evne til å forberede seg på, svare på og gjenopprette fra cybersikkerhets-hendelser, - Utvikle planer for gjenoppretting og forretnings-kontinuitet.	**Planlegging og politikkutvikling** - Evne til å utvikle og implementere strategiske retningslinjer og rammer for cybersikkerhet i tråd med organisasjonens mål og samsvars-forpliktelser. **Ledelse i cybersikkerhets-initiativer** - Lede og administrere cybersikkerhets-prosjekter og -team, inkludert evnen til å inspirere og veilede ansatte i implementeringen av cybersikkerhets-strategier. **Beslutninger** - Ta etiske beslutninger om cybersikkerhets-praksis

På EQF-nivå 4/5 kan mulige læringsutbytter være:

- Elevene vil lære de grunnleggende konseptene for cybersikkerhet, inkludert grunnleggende terminologi, typer cybertrusler som phishing, ransomware og DDoS-angrep, og deres respektive angrepsvektorer.
- Elevene vil kunne identifisere potensielle cybersikkerhetsrisikoer og sårbarheter, bruke relevante verktøy og programvare for å redusere disse risikoene, og implementere grunnleggende cybersikkerhetspraksis som sikker passordoppretting og sikker surfing.
- Elevene vil få kunnskap om lovgivning, standarder og krav til cybersikkerhet, sammen med strategier og retningslinjer for informasjonssikkerhet og risikostyring i en organisasjon.
- Elevene skal utvikle kompetansen til å vurdere og redusere potensielle sikkerhetstrusler effektivt og kommunisere cybersikkerhetsproblemer tydelig og effektivt i organisasjonen, inkludert rapportering av trusler og brudd til passende kanaler.

På EQF-nivå 6 kan mulige læringsutbytter være:

- Elevene skal utvikle en avansert forståelse av cybersikkerhetsprinsipper, inkludert evnen til å identifisere sofistikerte cybertrusler og angrepsvektorer og holde seg informert om de nyeste trendene innen cybersikkerhetsforsvar.
- Elevene skal tilegne seg omfattende kunnskap om nasjonal og internasjonal lovgivning, standarder og krav til cybersikkerhet, og skreddersy denne forståelsen til de spesifikke behovene i deres bransje.
- Elevene vil kunne gjennomføre detaljerte risikovurderinger ved hjelp av avanserte metoder og verktøy, og lage effektive risikostyringsstrategier for å redusere disse risikoene.
- Elevene skal designe, implementere og evaluere sikre nettverksarkitekturer, inkludert mestring av bruk av kritiske sikkerhetsteknologier som brannmurer, IDS og IPS.
- Elevene vil være dyktige i planlegging og gjennomføring av hendelsesrespons og gjenopprettingsstrategier, noe som sikrer organisatorisk motstandskraft gjennom effektive gjenopprettings- og forretningskontinuitetsplaner.
- Elevene skal demonstrere lederskap innen cybersikkerhet ved å utvikle strategiske retningslinjer, administrere cybersikkerhetsprosjekter og team, og ta informerte, etiske beslutninger under press.

5. VEDLEGG

5.1. VEDLEGG A: LISTE OVER LITTERATUR GJENNOMGÅTT

Oversikt over utdanning innen yrkesrettet utdanning innen cybersikkerhet

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=finne
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4qNukWMvDPXICf62FgF
14. Analyse og diagnose av cybersikkerhetstalent i Spania, mars 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competencias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Planlegg España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Cybersikkerhetsutfordringer og industriens behov

1. El estado de la ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (koord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la ciberseguridad en España: un país vulnerable, Telefónica **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/**
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 de Marzo de 2023 **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. Analyse og diagnose av cybersikkerhetstalent i Spania, mars 2022, Observaciber, **https://www.observaciber.es/**
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Panorama actual de la Ciberseguridad en España **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Planlegg España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**
10. **Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf**
11. **https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf**

12. http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28
13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Kvinner i cybersikkerhet

1. Microsoft. (2017, mars). Hvorfor Europas jenter ikke studerer realfag. Microsoft News. Hentet January 20, 2024, fra https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Kvinner går tech. (2021, september). IKT-arbeidsstyrken i Europa og dens kjønnsutfordring etter Covid-19. Women Go Tech. Hentet January 20, 2024, fra https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (ND) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius, og Lepaite. (2022, 5. august). Ataskaita Lietuvos kibernetinio saugumo kompetencijų žemelapis. Universitetet i Vilnius. Hentet January 20, 2024, fra https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (koord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres empleadas no ciencia y tecnología (reparto por sectores). España, UE-27 og UE-28. Serien 2019-2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. Analyse og diagnose av cybersikkerhetstalent i Spania, mars 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

5.2. VEDLEGG B: SPØRRESKJEMA

VET og HEI spørreskjema

Denne undersøkelsen er utformet for å samle innsikt i dagens tilstand og fremtidige behov for opplæring i cybersikkerhet og bidra til å forme et effektivt opplæringsprogram for cybersikkerhet skreddersydd for cybersikkerhetsutfordringene til små og mellomstore bedrifter (SMB).

Undersøkelsen er delt inn i 4 seksjoner:

- Demografi
- Pensum, opplæringsbehov og læringspreferanser
- Kompetansekrav og fremtidige ferdigheter
- Kjønnsspesifikk innsikt

Det tar ca. 8 minutter å gjennomføre undersøkelsen.

DEMOGRAFI

Hva er ditt land?
▫ Litauen
▫ Belgia
▫ Norge
▫ Tyrkia
▫ Finland
▫ Romania
▫ Spania
▫ Polen

I hvilken skoleinstitusjon underviser for tiden?
▫ Yrkesfag (yrkesfaglig utdanning og opplæring)
▫ HEI (høyere utdanning (HE) institusjon)

Hva er ditt kjønn?
▫ Mann
▫ Kvinne
▫ Vil helst ikke si

Hvor mange år har du vært involvert i opplæring i cybersikkerhet?
▫ Mindre enn 1 år
▫ 1-5 år
▫ 6-10 år
▫ Mer enn 10 år

PENSUM, OPPLÆRINGSBEHOV OG LÆRINGSPREFERANSER

Hvilke av følgende emner er inkludert i opplæringsprogrammet ditt for cybersikkerhet? (Velg alt som gjelder)

▫ Grunnleggende om cybersikkerhet
▫ Trusselanalyse og -håndtering
▫ Avanserte trusselreduserende teknikker
▫ Kryptografi
▫ Nettverkssikkerhet
▫ Lover og retningslinjer for cybersikkerhet
▫ Risikostyring
▫ Hendelsesrespons
▫ Annet: _____

Hvilke undervisningsmetoder bruker du primært i opplæringen i cybersikkerhet? (Velg alt som gjelder)

▫ Forelesninger
▫ Praktiske laboratorier
▫ Case Studies
▫ Gruppeprosjekter
▫ Online simuleringer
▫ Omvendt klasserom
Annen:_____

Hvilke læringsformater vil være mest effektive for opplæring i cybersikkerhet? (Velg alt som gjelder)

▫ Personlige workshops
▫ Online kurs
▫ Webinarer
▫ Interaktive simuleringer
▫ Video tutorials
▫ Praktiske øvingsøkter
▫ Annet: _____

Hva er de største utfordringene du står overfor når du skal levere effektiv opplæring i cybersikkerhet?

Åpent spørsmål

På en skala fra 1 til 5, hvor effektivt tror du de nåværende treningsprogrammene forbereder studentene på virkelige små og mellomstore bedrifters cybersikkerhetsutfordringer?

▫ Svært ineffektivt
▫ Noe ineffektivt
▫ Nøytral

▫ Noe effektivt
▫ Veldig effektiv

Hvor godt tror du den nåværende cybersikkerhetsopplæringen samsvarer med de spesifikke behovene til små og mellomstore bedrifter?
1 (Samsvarer ikke)
2 (Samsvarer litt)
3 (Samsvarer godt)
4 (Samsvarer mye)
5 (Samsvarer veldig mye)

Er det spesifikke emner eller ferdigheter du inkluderer i opplæringen din for å imøtekomme de unike cybersikkerhetsbehovene til små og mellomstore bedrifter? (Velg alt som gjelder)
▫ grunnleggende cybersikkerhet for små og mellomstore bedrifter
▫ Risikovurdering og styring i SMB-sammenheng
▫ Hendelsesrespons for små og mellomstore bedrifter
▫ Databeskyttelse og personvern for små og mellomstore bedrifter
▫ Utvikling av retningslinjer for cybersikkerhet for små og mellomstore bedrifter
▫ Annet: _____

Hvor ofte tilpasser du opplæringen i cybersikkerhet for å imøtekomme små og mellomstore bedrifter bedre?
▫ Alltid
▫ Ofte
▫ Noen ganger
▫ Sjelden
▫ Aldri

Mottar du tilbakemelding eller er du i kontakt med SMB-representanter eller fagfolk for å sikre at opplæringsinnholdet ditt er relevant for deres behov?
▫ Ja, regelmessig
▫ Av og til
▫ Sjelden
▫ Aldri

Basert på din erfaring, hvor effektiv tror du den nåværende cybersikkerhetsopplæringen er i å utstyre SMB-fagfolk til å håndtere cybersikkerhetsutfordringer?
▫ Svært ineffektivt
▫ Noe ineffektivt
▫ Nøytral
▫ Noe effektivt

▫ Veldig effektiv

Hvilke forslag har du for å forbedre relevansen og effektiviteten av cybersikkerhetsopplæring for små og mellomstore bedrifter?
Åpent spørsmål

KOMPETANSEKRAV OG FREMTIDIG KOMPETANSE

Etter din mening, hva er de beste ferdighetsunderskuddene i den nåværende SMB-cybersikkerhetsarbeidsstyrken? (Velg opptil tre)
▫ Oppdagelse og respons på trusler
▫ Sikkerhetsekspertise i skyen
▫ Kunnskap om samsvar og regelverk
▫ Hendelsesrespons og gjenoppretting
▫ Risikostyring og analyse
▫ Personvern og beskyttelse av data
▫ Nye teknologier
▫ Nettverkssikkerhet

Vennligst ranger, fra en skala fra 1 (ikke nødvendig) til 5 (svært nødvendig) kompetansen og kunnskapsbehovene:

	Vurdering				
Risikovurdering og styring Forstå typer risiko og innvirkning.					
Teknisk kunnskap Tekniske aspekter ved cybersikkerhet og kunnskap om operativsystemer, nettverk og databaseadministrasjon.					
Hendelsesrespons og gjenoppretting Identifisere, reagere på og gjenopprette etter sikkerhetsbrudd og hendelser.					
Politikkutvikling og implementering Utvikle og implementere effektiv sikkerhetspolitikk og praksis.					
Trusseletterretning og overvåking Hold deg oppdatert med de nyeste trendene, truslene og angrepsmetodene for cybersikkerhet.					
Kommunikasjonsevner Effektiv kommunikasjon med ansatte, ledelse og muligens kunder om cybersikkerhetsspørsmål.					
Datasikkerhet og beskyttelse Prinsipper for personvern og hvordan du beskytter sensitiv informasjon.					

Ser du noe relevant sett med ferdigheter og kunnskaper som ikke er oppført i forrige spørsmål, som kan være svært nødvendig for små og mellomstore bedrifter?

Åpent spørsmål

Hvilke nye cybersikkerhetstrusler tror du små og mellomstore bedrifter må være forberedt på de neste 5 årene? (Velg opptil tre)

▫ Ransomware-angrep
▫ IoT-sårbarheter
▫ sikkerhetsbrudd i skyen
▫ AI-drevne cyberangrep
▫ Innsidetrusler
▫ Annet: _____

Hva forutser du som de 3 beste nye trendene innen opplæring i cybersikkerhet de neste 5 årene? (Velg opptil 3 alternativer)

▫ AI og maskinlæring i cybersikkerhet
▫ Fokus på myke ferdigheter og tverrfaglig opplæring
▫ Trusler mot kvantedatabehandling
▫ Etisk hacking og defensive ferdigheter
▫ Digital identitet og personvern
▫ Desentraliserte sikkerhetssystemer (f.eks.
▫ Annet: _____

Er det noen spesielle treningsmetoder, verktøy eller plattformer som du mener er eksepsjonelt effektive for utdanning i cybersikkerhet?

Åpen tekst

Noen ytterligere kommentarer eller forslag til forbedring av opplæring i cybersikkerhet for små og mellomstore bedrifter?

Åpen tekst

KJØNNSSPESIFIKK INNSIKT

Hva er den estimerte prosentandelen kvinner blant deltakerne i treningsprogrammene dine for cybersikkerhet?

▫ Mindre enn 10 %
▫ 10% - 25%
▫ 26% - 50%
▫ 51% - 75%
▫ Mer enn 75%

Er det noen spesifikke initiativer eller strategier du bruker for å oppmuntre kvinners deltakelse i opplæring i cybersikkerhet?

▫ Ja

▫ Nei
Hvis ja, vennligst spesifiser: _____

Tror du det er nok kjønnsinkluderende opplæringsmoduler tilgjengelig innen cybersikkerhet?
▫ Ja
▫ Nei
▫ Usikker
▫ Ikke relevant for meg

Etter din erfaring, hva er de viktigste barrierene som hindrer kvinner i å delta eller avansere i opplæring og karriere innen cybersikkerhet? (Velg alt som gjelder)
▫ Manglende bevissthet om muligheter innen cybersikkerhet
▫ Stereotypier eller kulturelle normer
▫ Mangel på mentorskap eller rollemodeller
▫ Utfordringer med balanse mellom arbeid og privatliv
▫ Opplevd kjønnsskjevhet i bransjen
▫ Annet: _____

Har institusjonen din spesifikke retningslinjer eller programmer for å fremme mangfold og inkludering, spesielt for kvinner, i opplæring i cybersikkerhet?
▫ Ja
▫ Nei
▫ Ikke sikker

Hva kan gjøre opplæring i cybersikkerhet mer kjønnsinkluderende? (Velg opptil tre)
▫ Flere kvinnelige cybersikkerhetsinstruktører eller opplæringspersonell
▫ Tilby stipend eller insentiver
▫ Opplæringsinnhold som unngår kjønnsskjevheter
▫ Økt synlighet av vellykkede kvinnelige cybersikkerhets-fagfolk
▫ Flere treningsøkter kun for kvinner
▫ Kjønnsinkluderende casestudier og scenarier
▫ Skreddersydde opplæringsprogrammer
▫ Mentorskapsmuligheter
▫ Andre: _____

SMB-SPØRRESKJEMA

Denne undersøkelsen tar sikte på å kartlegge opplæringsbehovene for SMB Cyber Security Change Agents. Svarene dine vil bidra til å forstå det nåværende landskapet med kunnskap og ferdigheter om cybersikkerhet i ulike små og mellomstore bedrifter, identifisere hull i opplæring i cybersikkerhet og øke effektiviteten til fremtidige treningsprogrammer.

Undersøkelsen er delt inn i 3 seksjoner:

- Demografi
- Behov for opplæring
- Inkludering og kvinners behov for cybersikkerhet.

Det tar ca. 5 minutter å gjennomføre undersøkelsen.

DEMOGRAFI

Hva er ditt land?
▫ Litauen
▫ Belgia
▫ Norge
▫ Tyrkia
▫ Finland
▫ Romania
▫ Spania
▫ Polen

Hva er din nåværende stilling og avdeling i selskapet?
Posisjon:_____
Departement:_____

Hva er ditt kjønn?
▫ Mann
▫ Kvinne
▫ Vil helst ikke si

Hvor mange ansatte jobber i selskapet?
▫ opptil 10 ansatte
▫ 11-50
▫ 51-250

Hvordan vil du rangere ansattes nåværende nivå av kunnskap og ferdigheter innen cybersikkerhet?
▫ Nybegynner
▫ Middels
▫ Avansert

Hvor mange ansatte utfører arbeid relatert til cybersikkerhet?
Sett inn nummer: _____

Leier du inn eksterne tjenester for cybersikkerhetsarbeid?
▫ Ja
▫ Nei

OPPLÆRINGSBEHOV
På en skala fra 1 (ineffektiv) til 5 (veldig effektiv), hvor effektivt tror du de nåværende treningsprogrammene forbereder studentene på virkelige små og mellomstore bedrifters cybersikkerhetsutfordringer?
1- Ineffektiv
5- Veldig effektiv

Etter din mening, hva er de beste ferdighetsunderskuddene i den nåværende SMB-cybersikkerhetsarbeidsstyrken? (Velg opptil tre)

▫ Oppdagelse og respons på trusler
▫ sikkerhetsekspertise i skyen
▫ Kunnskap om samsvar og regelverk
▫ Hendelsesrespons og gjenoppretting
▫ Risikostyring og analyse
▫ Personvern og beskyttelse av data
▫ Nye teknologier
▫ Nettverkssikkerhet
▫ Annet: _____

Vennligst ranger, fra en skala fra 1 (ikke nødvendig) til 5 (essensiell) kompetansen og kunnskapsbehovene:

	Vurdering				
Risikovurdering og styring Forstå typer risiko og innvirkning.					
Teknisk kunnskap Tekniske aspekter ved cybersikkerhet og kunnskap om operativsystemer, nettverk og databaseadministrasjon.					
Hendelsesrespons og gjenoppretting Identifisere, reagere på og gjenopprette etter sikkerhetsbrudd og hendelser.					
Politikkutvikling og implementering Utvikle og implementere effektiv sikkerhetspolitikk og praksis.					
Trusseletterretning og overvåking Hold deg oppdatert med de nyeste trendene, truslene og angrepsmetodene for cybersikkerhet.					
Kommunikasjonsevner Effektiv kommunikasjon med ansatte, ledelse og muligens kunder om cybersikkerhetsspørsmål.					
Datasikkerhet og beskyttelse Prinsipper for personvern og hvordan du beskytter sensitiv informasjon.					

Ser du noe relevant sett med ferdigheter og kunnskaper som ikke er oppført i forrige spørsmål, som kan være svært nødvendig for små og mellomstore bedrifter?
Åpent spørsmål

Hvilke nye cybersikkerhetstrusler tror du små og mellomstore bedrifter må være forberedt på de neste 5 årene? (Velg opptil tre)

▫ Ransomware-angrep
▫ IoT-sårbarheter
▫ sikkerhetsbrudd i skyen
▫ AI-drevne cyberangrep
▫ Innsidetrusler
▫ Annet: _____

Hvilke spesifikke hull, om noen, føler du eksisterer i ansattes nåværende cybersikkerhetskunnskap eller ferdighetsstatus?

▫ Lavt nivå av tekniske ferdigheter
▫ Lavt nivå av myke ferdigheter
▫ Lavt nivå av sårbarhetsvurdering
▫ Lav forståelse av politikk og regelverk
▫ Lavt nivå av trusselbevissthet
▫ Lavt nivå av Cybersecurity regelmessige treninger
▫ Annet: _____

Hva forutser du som de 3 beste nye trendene innen opplæring i cybersikkerhet de neste 5 årene? (Velg opptil 3 alternativer)
▫ AI og maskinlæring i cybersikkerhet
▫ fokus på myke ferdigheter og tverrfaglig opplæring
▫ Trusler mot kvantedatabehandling
▫ Etisk hacking og defensive ferdigheter
▫ Digital identitet og personvern
▫ Desentraliserte sikkerhetssystemer (f.eks.
▫ Annet: _____

INKLUDERING OG KVINNERS BEHOV INNEN CYBERSIKKERHET

Føler du at dagens opplæring i cybersikkerhet er inkluderende og adresserer behovene til alle kjønn effektivt?
▫ Ja
▫ Nei
▫ Ikke sikker

Hvis du identifiserer deg som kvinne, har du møtt noen barrierer eller utfordringer med å få tilgang til eller delta i opplæring / studier innen cybersikkerhet?
▫ Ja
▫ Nei
▫ Vil helst ikke si
▫ Hvis ja, vennligst spesifiser: _____

Kjenner du til initiativer eller programmer i organisasjonen din som spesifikt støtter eller fremmer kvinners deltakelse i cybersikkerhet?
▫ Ja
▫ Nei
▫ Ikke sikker

Hvilke typer støtte eller ressurser vil oppmuntre flere kvinner i organisasjonen din til å delta i opplæring i cybersikkerhet? (Åpen)
Åpent spørsmål

Hvilke forbedringer eller innovasjoner vil du foreslå for å øke effektiviteten av opplæring i cybersikkerhet?
Åpent spørsmål

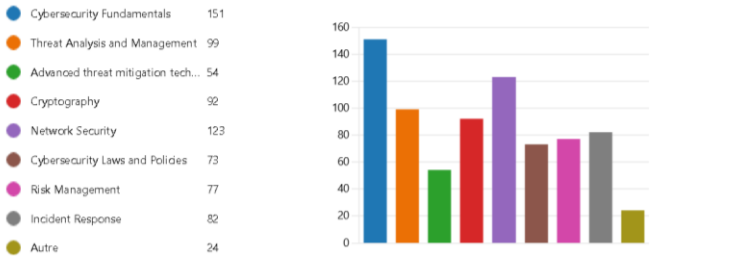
5.3. VEDLEGG C: RESULTATER FRA UNDERSØKELSEN

VET og HEI

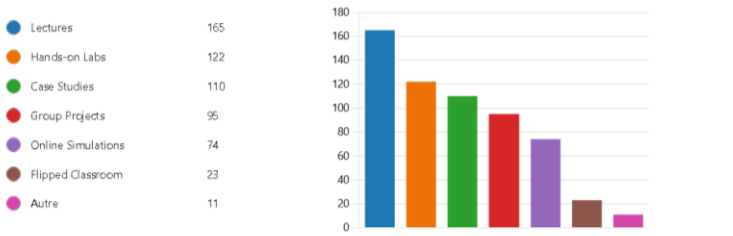
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

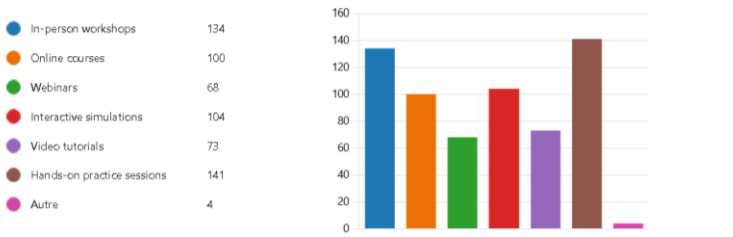
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

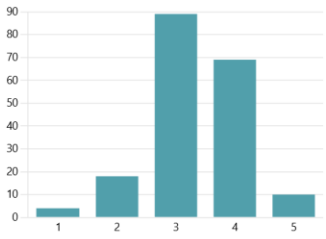
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

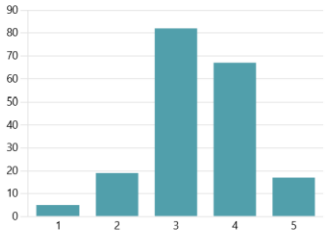
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



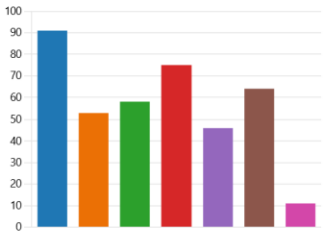
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

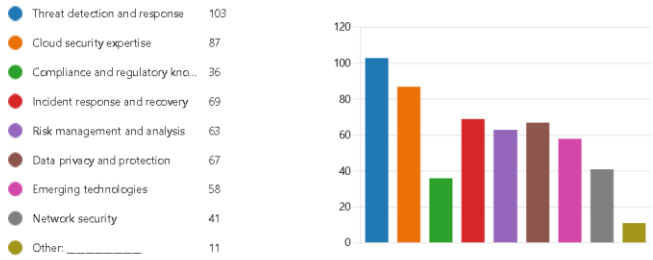
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

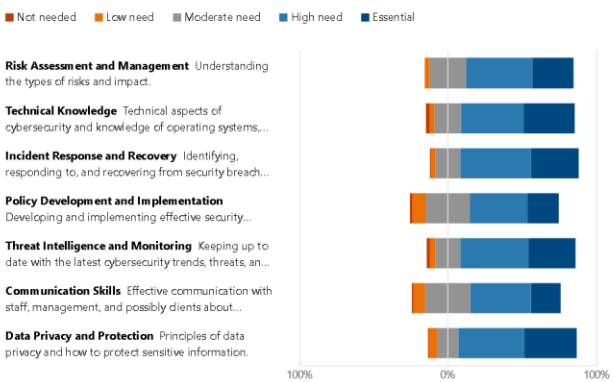
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

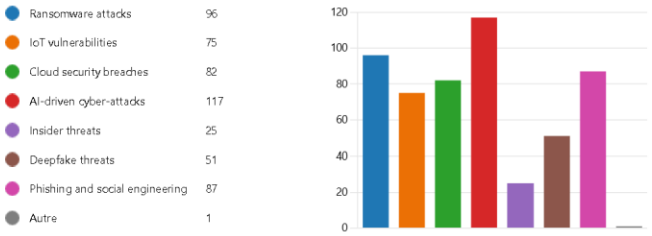
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

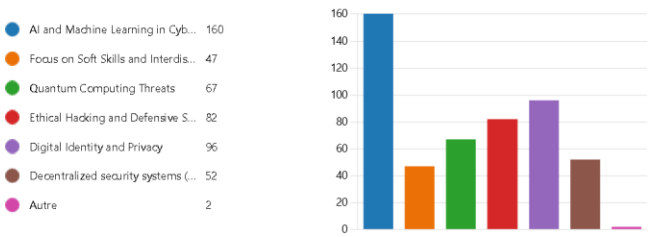
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

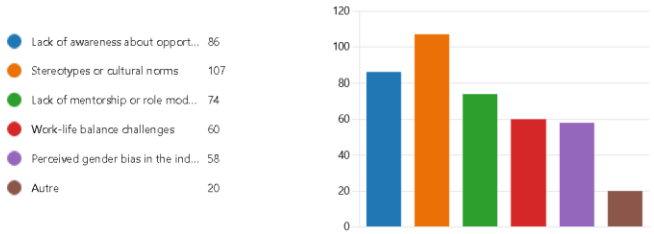
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

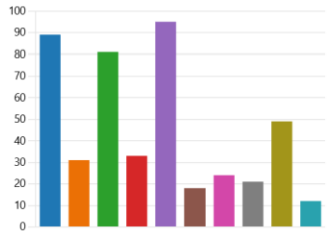
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

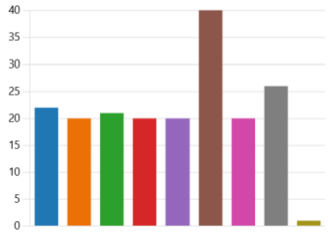
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

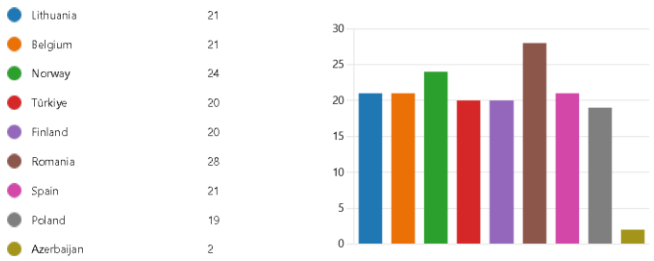
29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

Male	103
Female	69
Prefer not to say	4

5. **How many employees are working in the company?**

Up to 10 employees	64
11-50	60
51-250	52

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

Beginner	64
Intermediate	85
Advanced	27

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

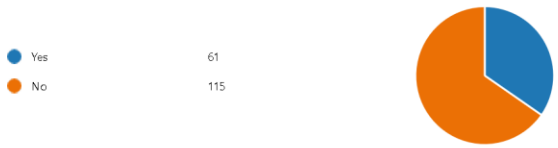
176
Réponses

Dernières réponses
"1"
"1"
"0"

Mettre à jour

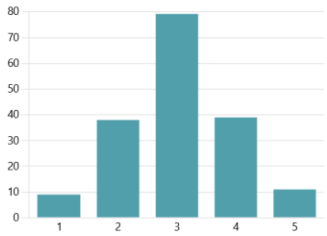
31 répondants (**18**%) répondu **1** pour cette question.

9. **Do you hire external services for cybersecurity work?**



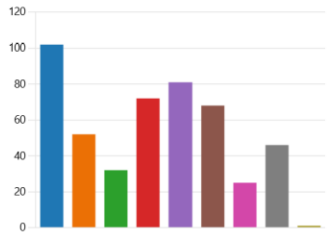
10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.03
Évaluation moyenne

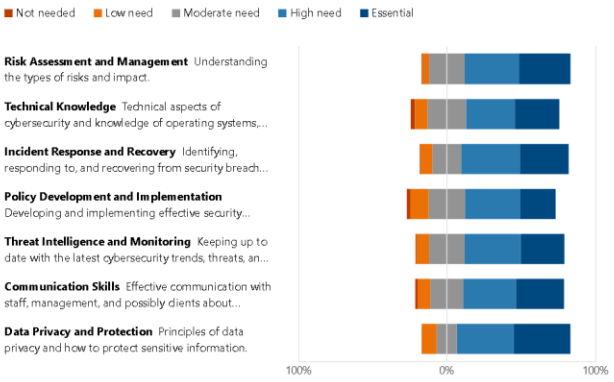


11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**

Threat detection and response	102
Cloud security expertise	52
Compliance and regulatory kno...	32
Incident response and recovery	72
Risk management and analysis	81
Data privacy and protection	68
Emerging technologies	25
Network security	46
Other: _____	1



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

Dernières réponses

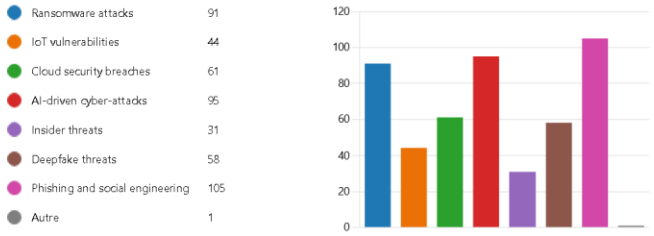
"My assumption is that Subject matter experts (SME's) in a big company are ...

"Cyber Security on all these topics arround Generative AI - which is complete...

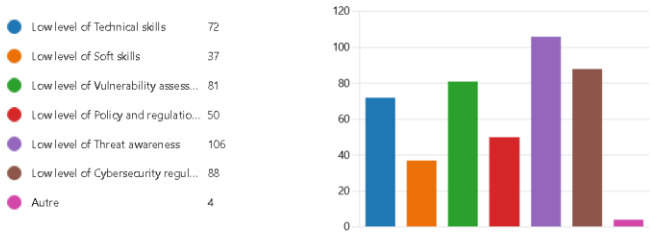
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

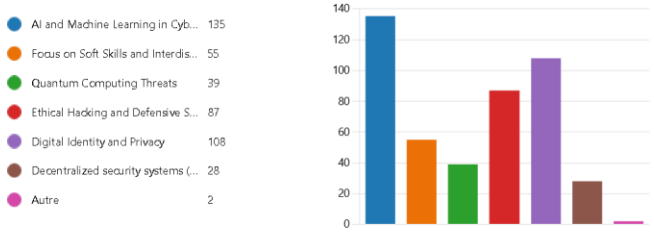
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**

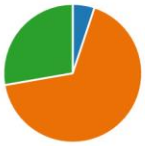


17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

Yes	82
No	29
Not sure	65

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**

Yes	7
No	92
Prefer not to say	38



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

Yes	18
No	158

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

5.4. VEDLEGG D: LISTE OVER ESCO-YRKER SOM ER GJENNOMGÅTT

Referanser:

2529,1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf
2529,2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf
2529,3 https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529,4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529,5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529,6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529,7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529,8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529,9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-agent-EU

@ CyberAgent.EU

@CyberAgentEU

@ Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau