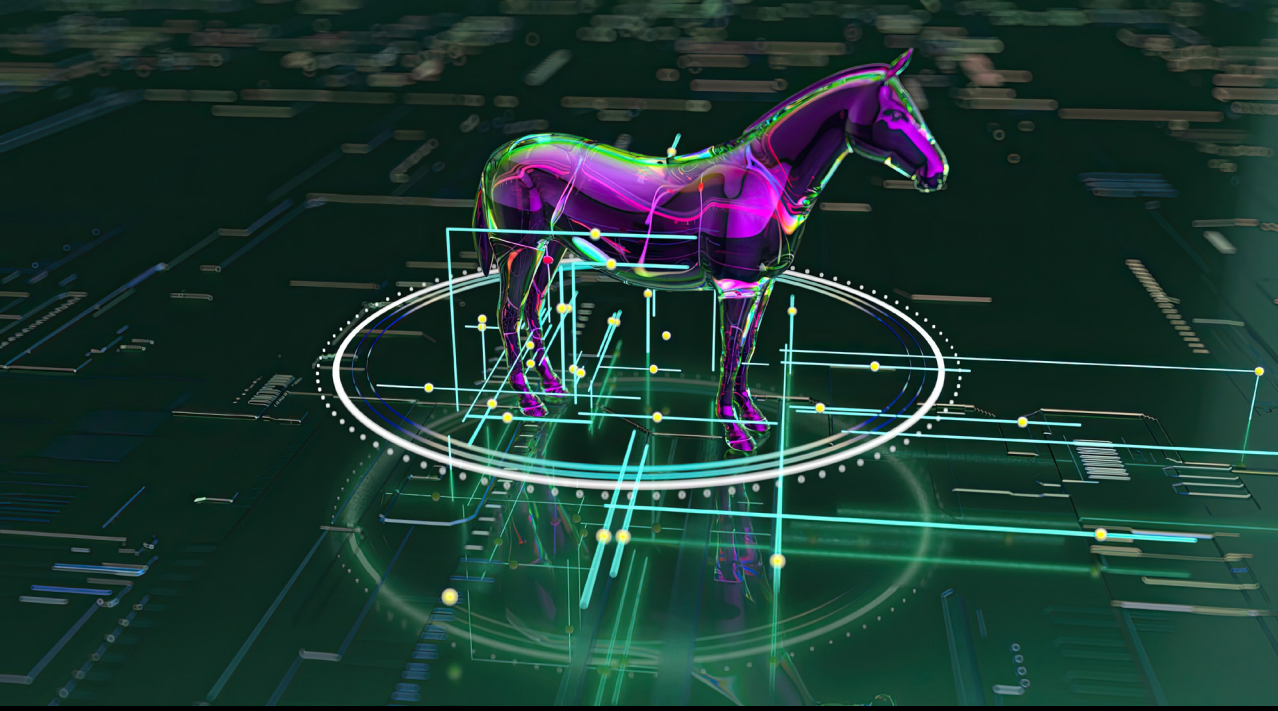


Inte mitt bord

Fördelning av ansvarstagande för cybersäkerhet på samhällsviktiga arbetsplatser

Mattias Svahn, Sebastian Cancino Montecinos, Alexander Melbi

FOI-R--5669--SE

Mars 2025

Mattias Svahn, Sebastian Cancino Montecinos, Alexander Melbi

Inte mitt bord

Fördelning av ansvarstagande för cybersäkerhet på samhällsviktiga arbetsplatser

Titel	Inte mitt bord – Fördelning av ansvarstagande för cybersäkerhet på samhällsviktiga arbetsplatser
Title	Not For Me – Distribution of Responsibility for Cybersecurity at Critical Workplaces.
Rapportnr	FOI-R--5669--SE
Månad	Mars
Utgivningsår	2025
Antal sidor	48
ISSN	1650-1942
Uppdragsgivare	FOI
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Operationer i cyberdomänen
Projektnr	A311031
Godkänd av	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild: Shutterstock/AI

Sammanfattning

Denna studie undersöker uppfattningar och förväntningar kring ansvarsfördelning för cybersäkerhet på samhällsviktiga arbetsplatser i Sverige. Undersökningen är kvantitativ och analyserar hur medarbetare och chefer uppfattar varandras kunskap och ansvar före, under och efter en cyberincident.

Resultaten visar en hög "gemensam verklighet" innan en incident, där både medarbetare och chefer uppfattar varandra som förberedda.

Under en pågående cyberincident uppstår skillnader; chefer tror att medarbetare har bättre koll än vad medarbetarna själva upplever, vilket antyder en potentiell övertro från ledningens sida.

Efter incidenten återfinns en gemensam syn på ansvar, där chefer förväntas leda återhämtningen. Studien belyser behovet av ökad tydlighet i förståelsen av cybersäkerhet, ökad gemensam förståelse samt klara policyer och rutiner för att motverka organisatoriska sårbarheter. Resultaten understryker vikten av en helhetssyn på cybersäkerhet, där tekniska och mänskliga faktorer vägs samman ör att stärka samhällskritiska arbetsplatsers resiliens.

Nyckelord: Förväntningar, cybersäkerhet, gemensam verklighet

Summary

This study examines expectations and responsibilities related to cybersecurity in societally important workplaces in Sweden. The quantitative survey and data analysis show how employees and managers perceive each other's knowledge levels and responsibilities before, during, and after a cyber-incident.

Findings indicate a high "shared reality" before an incident, with both employees and managers feeling prepared.

However, during an incident, managers believe employees are more competent than employees perceive themselves, suggesting possible overconfidence from leadership.

After the incident, there is mutual agreement on responsibility, with managers expected to lead recovery. The study highlights the need for enhanced clarity in cybersecurity training, shared understanding, and clear policies to mitigate organizational vulnerabilities.

Results emphasize the importance of a holistic approach to cybersecurity, incorporating technical and human factors to strengthen cyber resilience in societally critical functions.

Keywords: Förväntningar, cybersäkerhet, gemensam verklighet

Innehållsförteckning

1 Inledning 6
1.1 Bakgrund i samhällsutvecklingen 6
1.2 Syfte 7
1.3 Perspektiv på cybersäkerhet och cybersäkerhetsrelaterat arbete 7
2 Vad är ”cyber” och cybersäkerhet? 10
3 Teoretisk bakgrund 12
4 Metod 15
4.1 Deltagare 15
4.2 Enkätinstrumentet 16
4.3 Variablernas struktur 17
5 Analys och tolkning 19
5.1 Analys av medelvärdesskillnader 20
6 Diskussion och slutsatser 25
6.1 Begränsningar 26
7 Tankar för kommande studier 27
7.1 Falsklarm och beslutsfattande under cyberincidenter 27
7.2 ”Dissonanstriangeln”: IT-avdelningen, chefer och medarbetare 27
7.3 Effekter av chefers optimism på medarbetares agerande under cyberincidenter 28
7.4 ”När ska vi trycka på knappen?”: Utveckling av beslutsstöd för incidentrapportering 28
7.5 Återkommande barometer för cybersäkerhet 29
7.6 Undersök CERT:ars roll och funktioner 29
8 Referenser 31
Appendix 1 – Beskrivning av statistiska analyser 35
Appendix 2a – Introduktion och bakgrundsinformation 37
Appendix 2b – Enkät 1 till medarbetare 40
Appendix 2c – Enkät 2 till medarbetare 43
Appendix 2d – Enkät till chefer 46

1 Inledning

De senaste decennierna har varit en tid av oavbruten digitalisering. Sedan 1990-talet har digitaliseringen präglat politiska målsättningar och omvandlat vardagliga rutiner som förut sköttes med penna och papper till att idag bara vara en enkel knapptryckning på våra mobila enheter, både privat och på jobbet. Den en gång tidskrävande uppgiften att slå upp okända ord i ett fysiskt lexikon ersattes först av sekundsnabba sökningar på sökmaskiner som t.ex. Google och nu av AI-chattbottar. Bankärenden som en gång krävde fysiska besök på kontor kan nu utföras dygnet runt via digitala plattformar på telefoner i våra fickor.

Denna omvälvande digitalisering har inte bara förändrat individens vardag utan också i många fall omformat samhällsviktiga funktioner till att bli mer effektiva, tillgängliga och innovativa. Men parallellt med de uppenbara fördelarna uppstår också utmaningar. Den hastiga teknikutvecklingen lämnar ofta säkerhetsluckor som angripare kan utnyttja för att få obehörig tillgång till systemen, eller störa deras funktion. Cybersäkerhet står idag på en central plats i samhällsdebatten och i den debatten finns en underförstådd förväntan på vad ”cybersäkerhet” ska kunna ge samhället.

Rapporten är en del av ett internt initiativ inom FOI där FOI tvärvetenskapligt utreder forskningsfrågeställningar inom ”cyber” ur ett samhällsvetenskapligt perspektiv.

Den tilltänkta målgruppen är personer med ansvar för, delaktighet i och intresse för, arbete med cybersäkerhet på arbetsplatser i allmänhet och på samhällsviktiga arbetsplatser i synnerhet (samhällsviktiga enligt MSB, 2023). Avsikten är att det inte ska krävas någon djupare teknisk förståelse om cybersäkerhet för att läsa rapporten.

1.1 Bakgrund i samhällsutvecklingen

Cybersäkerhet utgör en kritisk komponent för att skydda svenska samhällsviktiga arbetsplatser mot ständigt ökande hot. Det sker allt fler cyberattacker som syftar till att stjäla information och destabilisera verksamheter vilket kan få både nationella säkerhetsmässiga och ekonomiska konsekvenser. Denna utveckling har blivit alltmer akut. Ett exempel av många är hur Kalix kommun drabbades av en attack vid årsskiftet 2021/2022 (Kalix Kommun, 2022). Ett annat exempel är hur Tietoevry drabbades av en ransomware[1]-attack i början av 2024, vilket orsakade betydande problem för många myndigheter (Karlén, 2024; Tietoevry.com, 2024). Under 2024 har patientinformation stulits från sjukhus och spridits internationellt (Wiklund, 2024). Även Systembolagets leverantör Skanlog har drabbats av liknande cyberincidenter, vilket resulterade i störningar i alkoholleveranserna (Martin, 2024). Under hösten 2024 har det visats vara

[1] Ransomware (på svenska kanske ”*utpressningsprogram”)* krypterar filerna på datorn så att du inte kan komma åt dem utan en dekrypteringsnyckel. I utbyte mot dekrypteringsnyckeln krävs en summa pengar.

problem med cybersäkerhetsrutinerna hos Lantmäteriet (Aro, 2024). Till och med Integritetskyddsmyndigheten har rapporterats ha drabbats av cyberattacker från ryska hackergrupper (Palmborg, 2024). I början av 2025 drabbades Hallandstrafiken av en överbelastningsattack och hemsidan låg nere en vecka (SVT 2025). MSB:s Cybersäkerhetskollen visade i början av 2025 på brister i cybersäkerhetsarbetet hos en majoritet av de samhällsviktiga verksamheterna (MSB, 2025). Sådana händelser och den efterföljande debatten understryker behovet av att förstå och adressera de växande hoten mot digital säkerhet.

I ljuset av denna utveckling ifrågasätts också den tidigare idealiserade synen på det digitaliserade samhället. Det granskas nu istället för sina potentiella sårbarheter och risker (Bengtsson m.fl., 2023; Ingemarsdotter m.fl., 2020; Svahn m.fl., 2024). Dessa nämnda händelser belyser de ökande riskerna såväl från antagonistiska hackergrupper som från ren teknisk dysfunktionalitet och misstag i mänsklig hantering av cybersystemen på arbetsplatser.

Sist men inte minst kan det finnas risker i att grupper på samhällsviktiga arbetsplatser ser cybersäkerhet som någon annans ansvar, eller inte förstår sin egen roll för den.

1.2 Syfte

Syftet med denna studie är att undersöka uppfattningar om cybersäkerhetsrelaterat arbete hos organisationer som anses samhällsviktiga. Som en del av detta arbete kommer studien att inhämta chefers och medarbetares uppfattningar om olika aspekter av cybersäkerhetsrelaterat arbete såsom rutiner, risker, ansvarsfördelning, stöd från myndigheter och rapporteringskrav.

Studien är ämnad att undersöka följande frågeställningar:

1. I vilken utsträckning har chefer och medarbetare skilda uppfattningar om cybersäkerhetsrelaterat arbete?
2. Kring vilka aspekter av cybersäkerhetsrelaterat arbete har chefer och medarbetare skilda uppfattningar?

Utgående från frågeställning 1 och 2 diskuteras vad eventuella skilda uppfattningar kan få för konsekvenser för cybersäkerheten på arbetsplatser.

1.3 Perspektiv på cybersäkerhet och cybersäkerhetsrelaterat arbete

Cybersäkerhet diskuteras ofta med fokus på tekniska lösningar såsom brandväggar, kryptering, intrångsdetekteringssystem och hantering av sårbarheter (Heiding m.fl., 2023). Dessa lösningar utgör en viktig del av organisationers säkerhetsstrategier och syftar till att förhindra obehörig åtkomst och upptäcka hot. Brandväggar agerar som

barriärer och kontrollerar trafiken baserat på säkerhetsregler. Kryptering omvandlar data från ett läsbart till ett krypterat oläsbart format där endast auktoriserade användare med rätt krypteringsnyckel kan läsa den för att möjliggöra autenticitetskontroll (t.ex. med hashsummor) och för att signera i internetbanker. Intrångsdetekteringssystem övervakar nätverk och enskilda datorer för att upptäcka misstänkta aktiviteter och varna vid hot. Sårbarhetsskanning och patch-hantering identifierar och åtgärdar svagheter i programvara för att minska risken för attacker. Lösningar såsom de nämnda utgör delar av arbetsområdet cybersäkerhet men är inte heltäckande.

Psykologiska och sociologiska aspekter på cybersäkerhetsrelaterat arbete har relativt de tekniska aspekterna fått mindre uppmärksamhet inom forskningen. Frågor kring hur cybersäkerhetsrelaterat arbete påverkas av organisationsstrukturer, kommunikationsvägar och de anställdas beteenden och förväntningar på varandra är avgörande för att förstå och förbättra säkerheten i företag och myndigheter. (Edeh, 2023) genomförde en litteratursammanställning och fann endast 43 studier som behandlade mänskligt och sociologiskt beteende som en faktor i cybersäkerhet, vilket är att se som relativt få. Detta understryker behovet av ytterligare forskning på området.

Mänskligt beteende och förväntningar spelar en central roll i hur effektivt tekniska säkerhetslösningar implementeras och används, så som t.ex. (Pollini m.fl., 2022) lägger fram.

Incidenter inom cybersäkerhet kan ofta spåras till mänskliga fel eller brister i beteendet, anställda som inte följer säkerhetspolicyer eller inte är medvetna om ansvarsfördelningen mellan medarbetare och chefer som äventyrar säkerheten trots avancerade tekniska skyddsåtgärder.

Ett konkret exempel på hur mänskliga faktorer påverkar cybersäkerhetsrelaterat arbete är hanteringen av utbildning och medvetenhet kring cybersäkerhet inom organisationer. Ett exempel på hanteringen av utbildning och medvetenhet är det som på engelska kallas för *social engineering*, eller på svenska ”social manipulation”. Det är manipulationstekniker som utnyttjar mänsklig psykologi för att få individer att avslöja konfidentiell information eller att vidta åtgärder som försätter systemen i ett osäkert läge. Ett exempel är nätfiske, där angripare skickar falska e-postmeddelanden som ser ut att komma från betrodda källor och få användare att ge bort data, klicka på länkar som leder till skadlig kod, eller utföra andra åtgärder. (Karlzen & Sommestad, 2020) har gjort en sammanställning av dessa ämnen. En annan studie på området är Burda m.fl., (2024) som granskar social ingenjörskonst via en systematisk översikt av 169 studier med fokus på mänsklig kognition och attacker. De lyfter forskningsluckor, särskilt inom t.ex. multimodala attacker som utnyttjar hierarkiska barriärer och bristande internkommunikation inom organisationer.

Chefers inställning till cybersäkerhetsrelaterat arbete, utanför det som är arbetsplatsens kärnuppgift är avgörande för att skapa en cybersäkerhetsmedveten kultur. Det gäller också chefernas engagemang i att implementera och upprätthålla cybersäkerhetsarbete.

Chefer som prioriterar cybersäkerhet säkerställer att nödvändiga resurser och stöd finns för att upprätthålla en bra säkerhetskultur. Båda inkluderar att kommunicera ut och upprätthålla tydliga policyer, säkerställa att dessa förstås och efterlevs, samt främja en miljö där anställda känner sig bekväma med att rapportera cybersäkerhetsproblem utan rädsla för repressalier. I en studie Taib m.fl., (2019) läggs fram att en av de psykologiska aspekter som har högst risk för att leda till framgångsrik phishing-försök är anställda som bara vill passa in och inte ifrågasätta.

Den tidigare FOI-rapporten "Delat ansvar är ingens ansvar?" av Svahn m.fl., (2024) granskar hur lag, reglering och statlig styrning påverkar cybersäkerhetsarbetet på en makronivå, med betoning på vikten av tydliga riktlinjer och ansvarsområden på en makronivå i samhället för att effektivt hantera cybersäkerhetsrisker. Denna rapport behandlar en liknande diskussion men i ett individuellt perspektiv.

2 Vad är ”cyber” och cybersäkerhet?

Inom kommunikations- och diskursteori är det väl etablerat att en tydlig och produktiv diskussion kräver att alla parter har en gemensam förståelse av nyckelbegrepp (Sapienza m.fl., 2016). I Rapporten ”Delat ansvar är ingens ansvar?” av Svahn m.fl., (2024) presenteras hur detta gäller begreppet ”cyber”. Ett sådant behov av gemensam begreppsförståelse gäller i hög grad för studier som rör cybersäkerhetens mänskliga faktorer och särskilt för att kunna analysera cybersäkerhetsfenomenets mångbottnade natur. Ett sådant behov av gemensam begreppsförståelse kvarstår även vid författandet av denna rapport så den presentationen läggs fram även här.

Prefixet "cyber" har sitt ursprung i det grekiska ordet "kubernetes", som betyder styrman och är nära besläktat med "kubernesis", vilket refererar till konsten att styra eller leda. Fysikern André-Marie Ampère använde redan 1834 termen "cybernétique" för att beskriva studiet av styr- och reglersystem (Ampere, 1865). Detta utvecklades senare till begreppet "cybernetik", som populariserades av matematikern Norbert Wiener på 1940-talet (Wiener, 2000). Den tidiga cybernetikens har haft inflytande på dagens förståelse av digitala system, och lade grunden för dagens förståelse av cybersäkerhet.

William Gibson introducerade termen "cyberspace" på 1980-talet, vilket han beskrev som en datorgenererad hallucination (Popova, u.å.) och detta begrepp blev snabbt centralt inom diskussioner om den digitala världen. Samtidigt har begrepp som "cyber" fått en rad olika tolkningar, vilket kan skapa förvirring inom samhällsdebatten, särskilt i frågor som rör säkerhet i digitala miljöer. En rapport från FOI 2023 visade att olika tolkningar av prefixet "cyber" finns i analyser av cyberkrig i Ukraina, där "cyber" definieras som ett prefix för datorgenererade aktiviteter jfr. Nilsson, (2023).

Vid en läsning av diskussion om cybersäkerhet i ett bredare samhälleligt sammanhang är det lätt att stöta på relaterade begrepp såsom "informationssäkerhet" och "IT-säkerhet". Dessa begrepp är centrala inom digitaliserade verksamheter men skiljer sig i fokus. Enligt standarden SS-EN 27000[2] handlar informationssäkerhet om att bevara informationens konfidentialitet, riktighet och tillgänglighet samt andra egenskaper som autenticitet och ansvarsskyldighet jfr. Eidenskog m.fl., (2023). Cybersäkerhet saknar dock en entydig definition på grund av sitt breda tillämpningsområde. Enligt Europeiska unionens cybersäkerhetsbyrå Enisa är cybersäkerhet all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot som täcker allt från skydd mot cyberhot till säker hantering av information i digitala system (Europaparlamentets och rådets förordning (EU) 2019/881, 2019).

[2] https://www.sis.se/ [åtkomst 2024-12-09]

I denna studie väljer vi att använda begreppet ”cybersäkerhet” som åsyftandes säker hantering, av både teknologisk och mänsklig hantering av, de vardagliga digitala arbetsredskapen, - i samhällsviktiga jobb (MSB, 2023).

Vi använder begreppet ”cyberincident” om såväl antagonistiska angrepp och angreppsförsök som om oavsiktliga funktionsfel, såsom t.ex. hur det sommaren 2024 skedde en cyberincident med Crowdstrikes säkerhetsprogram (Wickström & Wiman, 2024).

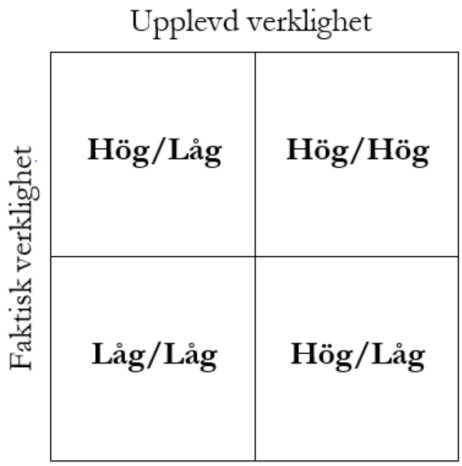
3 Teoretisk bakgrund

Teorin om ”gemensam verklighet” (eng. ”shared reality”) är en grundsten för denna studie. Teorins grundtes är att människor har en naturlig tendens att vilja få samförstånd med andra människor Higgins et al. (2021). Det kan antas att så även är fallet i ifråga om cybersäkerhet och förväntningar på beredskap inom cybersäkerhet. Denna studie tar avstamp i den teorin och utvecklar den för att söka en bakomliggande struktur kring missförstånd och förväntningar på cybersäkerhet i samhällsviktiga jobb.

Det mänskliga beteende som beskrivs i teorin har både individuella orsaker och sociala orsaker. Enligt teorin har människor en inneboende motivation att tolka och förstå världen så gott det går. Ett sätt att göra det är att stämma av med andra människor. Socialt sett är vi människor motiverade att knyta band med andra, vilket leder till att vi gärna vill se verkligheten, däribland även yrkesverkligheten via andras ögon. De nämnda förståelseprocesserna sker ofta instinktivt utanför människors kontroll och medvetande. När människor jobbar i grupper kan dessa processer påverka grupparbetet positivt eftersom det finns en vilja att förstå varandra och komma överens socialt jfr. Echterhoff m.fl., (2009).

Ett problem är att *förväntan* på en gemensam verklighet inte betyder att en individ faktiskt *har* en gemensam verklighet med medarbetaren eller chefen. Förväntningen på att det finns en gemensam verklighet kan alltså leda till falsk konsensus.

Det psykologiska fenomenet *gemensam verklighet* kan vara ett tveeggat svärd när det gäller beslutsfattande i grupper på samhällsviktiga arbetsplatser. Forskning visar att grupper som tenderar att fokusera för mycket på gemensam (snarare än icke-gemensam) verklighet, fattar ofta felaktiga beslut ((Stasser, 1999; Stasser & Titus, 1985).

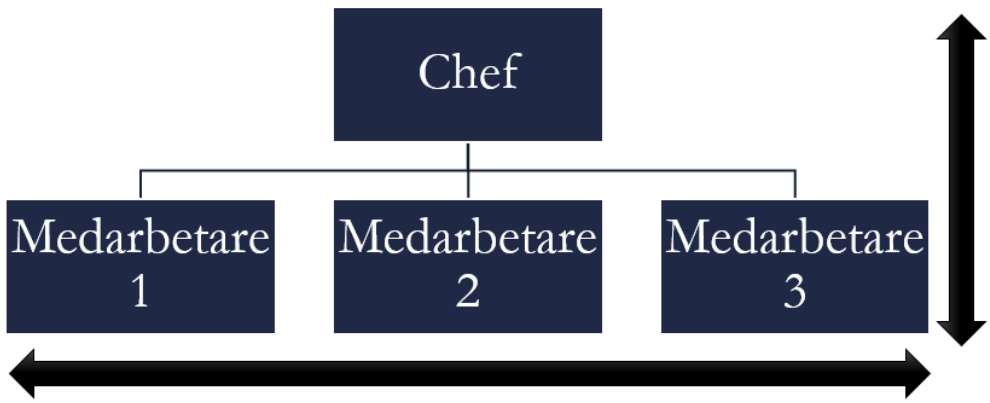


Figur 1. Teoretisk modell för studien

Fel! Hittar inte referenskälla. visar de olika utfallen som kan uppstå mellan upplevelsen av gemensam verklighet och den faktiska gemensamma verkligheten. Matrisen visar på en teoretisk struktur för vilka utfall som studien kan ge. I den vänstra kvadraten längst upp (Hög/Låg) föreligger en situation där en organisation faktiskt har en hög grad av gemensam verklighet men upplever att så inte är fallet. I den högra kvadraten längst upp (Hög/Hög) föreligger vad som kan framstå som idealsituationen, här finns en hög samstämmighet mellan upplevd och faktisk gemensam verklighet – där en organisation upplever hög gemensam verklighet och att upplevelsen återspeglar den faktiska situationen (dvs. verkligheten), då finns dock en risk för grupptänk.

Den vänstra kvadraten längst ned (Låg/Låg) visar också hög samstämmighet. I en sådan situation upplever inte parterna att de har någon gemensam verklighet, vilket också stämmer överens med den faktiska situationen. Parterna är med andra ord medvetna om situationen. Det råder dock liten risk för grupptänk. I den sista kvadraten i figuren, längst ned till höger (Låg/Hög) visas en situation där den faktiska gemensamma verkligen är låg men där upplevelsen av en gemensam verklighet är hög. Parterna tror alltså att situationen är bättre än vad den är. Detta utgör den potentiellt farligaste situationen.

Utöver skillnader mellan upplevelsen av verkligheten och den gemensamma verkligheten kommer det i en organisation alltid att finnas flera olika parter som kan uppleva gemensam verklighet i olika frågor ur olika perspektiv. Denna studie utgår från premissen att det är viktigt att undersöka både relationer i hierarkiskt vertikala led (chef–medarbetare) och i hierarkiskt horisontella led (medarbetare 1–2–3).



Figur 2. Illustration över jämförelserna mellan chef och medarbetare

Dessa relationer påverkar varandra ömsesidigt. Det betyder att både chefen och medarbetaren kan ha korrekta eller mindre korrekta verklighetsuppfattningar. När det gäller horisontella jämförelser kan situationer uppstå där medarbetare med olika grundkompetens sätts samman för att lösa en mer övergripande cybersäkerhetuppgift.

Här kan missförstånd (dvs. diskrepans mellan upplevd och faktiskt verklighet) uppstå på grund av medarbetarnas olika utgångspunkter i problemförståelsen och i förståelsen för varandras kompetenser och ansvarsområden.

Den uppåtgående kommunikationen **Figur 2** syftar på hur anställda kommunicerar med chefer Det är viktigt för cybersäkerheten att anställda förstår organisationens policyer för interaktion med varandra och med chefer. Det är också viktigt att ge personalen sätt att ta sina eventuella problem eller förslag kring cybersäkerhet och dela dem med högre rankade medlemmar i organisationen.

Nedåtgående kommunikation i organisationen sker när en chef eller högre tjänsteman kommunicerar med personal lägre i organisationsstrukturen. Syftet är att främja en tydlig kommunikation som bygger gemensam verklighet kring kompetensområden och ansvarsfördelning.

4 Metod

Studien använde en kvantitativ forskningsmetod med en explorativ ansats för att undersöka förväntningar på cybersäkerhet inom samhällskritiska verksamheter i Sverige. Den kvantitativa metoden valdes på grund av dess potential att generera generaliserbara resultat baserade på numeriska data. Den explorativa ansatsen möjliggjorde en fördjupning i ett relativt outforskat område, där teorin om gemensam verklighet tillämpades och utvecklades.

4.1 Deltagare

Datainsamlingen ägde rum under hösten 2024 via en webbenkät. Respondenterna rekryterades från en panel med tillgång till ett brett urval av yrkesverksamma.[3] Filterfrågor användes för att sortera fram individer som var yrkesverksamma inom vad Myndigheten för samhällsskydd och beredskap (MSB) definierar som samhällsviktiga arbeten (se MSB, 2023). Figur 3 visar på fördelningen av respondenter mellan olika kategorier av samhällsviktiga arbeten. Det är värt att notera att deltagarna kommer från ett brett urval av yrkeskompetenser inom samhällsviktiga arbeten, inte specifikt personer med särskild kompetens inom cybersäkerhet. De är personer som använder digitala redskap i sitt arbete, men inte specifikt har cybersäkerhet som en särskild arbetsuppgift.

Enkättjänstens panel levererade 206 svar från yrkesverksamma inom samhällsviktiga sektorer. Urvalet omfattade 48 chefer och 158 medarbetare, vilket möjliggjorde jämförelser mellan olika yrkesroller. Resultaten analyserades för att identifiera signifikanta skillnader i förväntningar mellan chefer och medarbetare (se Appendix 1 – Beskrivning av statistiska analyserför en komplett analys).

[3] www.netigate.se [åtkomst 2024-12-03]

1 Hälso- och sjukvård	90 (39%)
2 Räddningstjänst och säkerhet	9 (4%)
3 Flygplatsverksamhet	0 (0%)
4 Hamnarbete	1 (0%)
5 Järnvägsverksamhet	10 (4%)
6 Ekonomi och administration	57 (25%)
7 Energiförsörjning	9 (4%)
8 Vatten och livsmedel	9 (4%)
9 Finans och försäkring	19 (8%)
10 Läkemedelsförsörjning och/eller djurhälsa	8 (3%)
11 Bevakning och skydd	19 (8%)

Figur 3 Kategorier av deltagare.

4.2 Enkätinstrumentet

Utvecklingen av enkätinstrumentet inspirerades av ett annat frågeformulär för att mäta gemensam verklighet. Det inspirerande frågeformuläret har tidigare validerats för engelska och tyska av Schmalbach m.fl., (2019).[4] Syftet med vår enkät var att mäta tre olika nivåer av förväntningar: kollegers förväntningar på varandra, anställdas förväntningar på chefer, samt chefernas förväntningar på medarbetare.

Innan respondenterna besvarade enkäten fick de läsa ett scenario som beskrev arbetsplatsen *innan* en cyberincident, *under* en cyberincident och *efter* en cyberincident.

Genom att presentera scenariot om en cyberincident innan de svarade på frågorna avsåg vi att väcka respondenternas egna tankar om cyberincidenter. Detta bidrog till att de vid svarstillfället sannolikt hade sitt eget cyberincidentsbegrepp i åtanke när de besvarade frågorna. Eftersom begreppet ”cyber” är ett otydligt begrepp (jfr.kap 2), valde vi denna ansats eftersom scenariot då fungerade som en form av kognitiv förberedelse, vilket

[4] Notera att vår enkät för denna studie endast har validerats för ”face validity”.

gjorde att respondenterna blev mer fokuserade på sitt eget mentala begrepp av ”cyber-incident” (jfr.kap 2). På så vis arbetade vi för att närma oss att deltagarna i viss mån hade någon form av gemensam utgångspunkt och kontext när de svarade på frågorna.

Utöver att läsa tre scenarion fick respondenterna efter läsningen svara på sex frågor per scenario. Dessa frågor rörde (1) uppfattningen om att vara överens om rutiner, (2) uppfattning av medvetenhet om förberedelser, (3) uppfattning av placering av ansvar, (4) uppfattning av beredskap och förberedelser, (5) uppfattningen om myndigheter och (6) uppfattningen om rapporteringsansvar (jfr. Appendix 2b – Enkät 1 till medarbetare– Appendix 2d – Enkät till chefer). Uppfattningar kring rapporteringsansvar inkluderades eftersom rapportering är ett krav enligt MSB och NIS2 och tidigare forskning visat att cyberincidenter inte rapporteras i den utsträckning som lag och förordning kräver jfr.t.ex. Svahn m.fl., (2024).

För att säkerställa att enkäten mätte relevanta aspekter av cybersäkerhet inom samhälls-kritiska verksamheter genomfördes en validering av enkätformuläret. Denna validering skedde genom att sakkunniga inom området granskade och gav återkoppling på frågorna (”face validity”). Återkopplingen implementerades sedan i det slutliga instru-mentet. Sammanlagt har mätinstrumentet en bred grund för att analysera och jämföra skillnader i förväntningar mellan de undersökta grupperna (jfr.kap 5 & 6).

4.3 Variablernas struktur

Enkäten bestod av tre olika enkäter om cybersäkerhet. Enkäterna var uppdelade efter tre olika scenarion: *innan*, *under* och *efter* en hypotetisk cyberincident. Detta resulterade i totalt nio delenkäter bestående av sex frågor vardera. Varje enkäts resultat utmynnade i en variabel vilket gav nio variabler totalt. Varje variabel bestod av medelvärdet av de sex frågorna kring cybersäkerhet för respektive grupp och scenario (Tabell 1) Med andra ord bildar dessa nio variabler nio olika index bestående av sex frågor. Dessa index kan ses som en generell medvetenhet kring cybersäkerheten innan, under och efter en hypotetisk cyberincident.

Personerna utan chefsroll, som i fortsättningen kommer att kallas *medarbetare*, fick fylla i två av enkäterna. I den första enkäten skulle de svara på frågorna om den hypotetiska cyberincidenten utifrån uppfattningen om sina medarbetares (kollegors) perspektiv. I andra enkäten skulle de svara på frågorna utifrån uppfattningen om sina chefers perspektiv. Cheferna svarade på den sista enkäten. Cheferna svarade på frågorna om den hypotetiska cyberincidenten utifrån uppfattningen om personalens perspektiv. Detta mynnade ut i tre olika undersökningsgrupper som vi jämförde i de efterföljande analy-serna. De tre olika grupperna bestod av (a) Medarbetares perspektiv på varandra; (b) Medarbetares perspektiv på chefer; (c) Chefers perspektiv på personalen. Notera att grupp a och b består av samma personer (medarbetarna), medan grupp c består av andra personer (chefer).

Tabell 1 Grupper och scenarion som i analysen bildar index.

	SCENARION		
GRUPPER	**Före**	**Under**	**Efter**
(a) Medarbetares perspektiv på varandra	Medelvärde av 6 frågor	Medelvärde av 6 frågor	Medelvärde av 6 frågor
(b) Medarbetares perspektiv på chefer	Medelvärde av 6 frågor	Medelvärde av 6 frågor	Medelvärde av 6 frågor
(c) Chefers perspektiv på medarbetare	Medelvärde av 6 frågor	Medelvärde av 6 frågor	Medelvärde av 6 frågor

5 Analys och tolkning

Resultatet av enkätundersökningen och analysen presenteras översiktligt här i kapitel 5. En djupare kvantitativ beskrivning finns i Appendix 1 – Beskrivning av statistiska analyser. Först kommer vi presentera deskriptiv statistik för att ge en överblick av datainsamlingen. Därefter kommer vi presentera resultaten från de statistiska jämförelserna mellan medarbetares och chefers uppfattning kring cyberfrågorna i enkäten.

Först redovisas deskriptiv statistik för att bedöma om datainsamlingen fungerat som avsett. I Tabell 2 visas medelvärden (och standardavvikelser) för samtliga enkätfrågor i de tre olika scenarierna (före, under och efter), och för de tre grupperna (medarbetares perspektiv på varandra, medarbetares perspektiv på chefer och chefers perspektiv på medarbetare). Motsvarande siffror presenteras även för index, vilket är en sammanfogning av fråga 1–6. Analysen av medelvärdesskillnader kommer att fokusera främst på dessa index.

Överlag ligger de flesta (40 av 54) frågors medelvärden mellan 4,00 och 5,00 på den sjugradiga skalan. Det lägsta medelvärdet är 4,03 (fråga 6 i scenario: under, för grupp: medarbetares perspektiv på varandra) och det högsta är 5,43 (fråga 2 i scenario: efter, för grupp: medarbetares perspektiv på chefer).

Detta kan tolkas som att ingen av frågorna var formulerade så att de tolkades extremt negativt eller extremt positivt av deltagarna som grupp. Därför kan slutsatsen dras att datainsamlingen fungerade som avsett.

Tabell 2. Medelvärden (och standardavvikelser) för alla enkätfrågor i de tre olika scenariona, över alla grupper. Samt index för alla scenarion och grupper.

	Fråga 1	**Fråga 2**	**Fråga 3**	**Fråga 4**	**Fråga 5**	**Fråga 6**	**Index**
Scenario och grupper							
FÖRE							
Medarbetares perspektiv på varandra	5,18 (1,39)	4,67 (1,53)	4,83 (1,55)	4,38 (1,55)	5,03 (1,29)	4,43 (1,71)	**4,75 (1,06)**
Medarbetares perspektiv på chefer	4,74 (1,47)	4,80 (1,43)	5,16 (1,33)	4,54 (1,47)	5,07 (1,27)	4,97 (1,56)	**4,88 (1,14)**
Chefers perspektiv på medarbetare	4,81 (1,45)	4,45 (1,60)	5,02 (1,69)	4,91 (1,60)	5,28 (1,44)	4,64 (1,65)	**4,85 (1,20)**
UNDER							
Medarbetares perspektiv på varandra	4,33 (1,37)	4,20 (1,42)	4,80 (1,55)	4,18 (1,48)	4,77 (1,48)	4,03 (1,79)	**4,39 (1,12)**
Medarbetares perspektiv på chefer	4,82 (1,46)	4,77 (1,54)	5,03 (1,36)	4,57 (1,60)	4,97 (1,53)	4,95 (1,56)	**4,85 (1,20)**
Chefers perspektiv på medarbetare	4,91 (1,28)	4,81 (1,70)	4,89 (1,46)	4,68 (1,59)	4,79 (1,56)	4,53 (1,97)	**4,77 (1,25)**

EFTER							
Medarbetares perspektiv på varandra	4,66 (1,42)	5,22 (1,34)	5,09 (1,36)	4,66 (1,33)	4,66 (1,64)	4,58 (1,71)	**4,81 (1,06)**
Medarbetares perspektiv på chefer	4,92 (1,28)	5,43 (1,21)	5,24 (1,26)	5,13 (1,38)	5,04 (1,40)	5,15 (1,50)	**5,15 (1,08)**
Chefers perspektiv på medarbetare	4,87 (1,50)	4,77 (1,49)	4,85 (1,44)	4,55 (1,46)	4,70 (1,53)	4,66 (1,80)	**4,73 (1,29)**

5.1 Analys av medelvärdesskillnader

I detta avsnitt kommer vi att presentera resultaten från enkätundersökningen. Notera att medelvärdesskillnader för specifika frågor inte kommenteras vidare i analyserna om de inte är statistiskt signifikanta. Eftersom detta är en explorativ ansats kommer vi att kommentera medelvärdesskillnader om effektstorleken är liten – trots signifikant skillnad. Däremot kommer vi belysa signifikanta medelvärdesskillnader kring specifika frågor som har medelstor eller stor effektstorlek.

Före en cyberincident

I den första analysen av medelvärdesskillnader mellan grupper, där deltagarna blev tillfrågade om cybersäkerhet *före* en potentiell cyberincident, syns inga märkbara skillnader mellan indexen (Tabell 3). Det innebär att medarbetare har ungefär samma generella medvetenhet sinsemellan (*Medarbetares perspektiv på varandra*) som chef har om dem (*Chefers perspektiv på medarbetare*), kring cybersäkerhet inför en hypotetisk cyberincident. Detsamma gäller för jämförelsen mellan *Medarbetares perspektiv på chefer*, och de två andra grupperna (*Medarbetares perspektiv på varandra* och *Chefers perspektiv på medarbetare*). Med andra ord tycks medarbetare anse att chefer har ungefär samma generella medvetenhet som de själva har kring cybersäkerhet inför en hypotetisk cyberincident. Samt att medarbetare anser att chefer (*Medarbetares perspektiv på chefer*) har ungefär samma medvetenhet kring cybersäkerhet inför en hypotetisk cyberincident som chefer själva har på medarbetarna (*Chefers perspektiv på medarbetare*). Med andra ord tycks gemensam verklighet alltså råda.

Tabell 3. Medelvärden och (standardavvikelse) för enkätfrågor i scenario FÖRE, över alla grupper. Samt index för varje grupp.

	Fråga 1	**Fråga 2**	**Fråga 3**	**Fråga 4**	**Fråga 5**	**Fråga 6**	**Index**
Scenario och grupper							
FÖRE							
Medarbetares perspektiv på varandra	5,18 (1,39)	4,67 (1,53)	4,83 (1,55)	4,38 (1,55)	5,03 (1,29)	4,43 (1,71)	**4,75 (1,06)**
Medarbetares perspektiv på chefer	4,74 (1,47)	4,80 (1,43)	5,16 (1,33)	4,54 (1,47)	5,07 (1,27)	4,97 (1,56)	**4,88 (1,14)**

Chefers perspektiv på medarbetare	4,81 (1,45)	4,45 (1,60)	5,02 (1,69)	4,91 (1,60)	5,28 (1,44)	4,64 (1,65)	**4,85 (1,20)**

När det gäller enskilda frågor fanns det dock signifikanta skillnader mellan grupperna *Medarbetares perspektiv på varandra* och *Medarbetares perspektiv på chefer* i fråga 1, 3, och 6, där gruppen *Medarbetares perspektiv på varandra* uppvisar högre medelvärde än *Medarbetares perspektiv på chefer* i fråga 1 (uppfattningen om att vara överens om rutiner) och *Medarbetares perspektiv på chefer* uppvisar högre medelvärde i fråga 3 (placering av ansvar) och 6 (uppfattningen om rapporteringsansvar) än gruppen *Medarbetares perspektiv på varandra*. Skillnaden i fråga 3 var relativt liten i statistisk mening dock var skillnaderna för fråga 1 och 6 medelstora. Fråga 1 handlade om medarbetares uppfattning om vilka rutiner som gäller vid en potentiell cyberincident. Resultaten tycks visa att medarbetare anser att de vet vilka rutiner som gäller före en cyberincident i högre utsträckning än vad de tror att cheferna vet. Fråga 6 däremot handlade om huruvida medarbetare trodde att övriga (respektive chefer) visste att en teknisk analys skulle skrivas vid cyberincident. Detta resultat indikerar att medarbetare tror att chefer känner till att det ska skrivas en initial rapport vid en cyberincident i högre utsträckning än vad medarbetarna tror om sig själva.

I jämförelsen mellan grupperna *Medarbetares perspektiv på varandra* och *Chefers perspektiv på medarbetare* fann vi en medelstor signifikant medelvärdesskillnad för fråga 4 (uppfattning om att kunna arbeta på reducerad nivå). Denna fråga handlar i vilken utsträckning medarbetare och chefer anser att medarbetarna är på samma våglängd gällande förberedda rutiner för att arbeta på en reducerad nivå vid en cyberincident. Resultaten verkar visa att chefer anser att medarbetare är på samma våglängd i högre utsträckning av vad medarbetarna själva anser att de är.

Slutligen visade analyserna inga signifikanta skillnader i jämförelserna mellan grupperna *Medarbetares perspektiv på chefer* och *Chefers perspektiv på medarbetare* i någon av de enskilda frågorna.

Under en cyberincident

I den andra analysen av medelvärden, scenariot *under* en cyberincident, visar resultatet att gruppen *Medarbetares perspektiv på varandra* har signifikant lägre medelvärde på indexet än både gruppen *Medarbetares perspektiv på chefer* och *Chefers perspektiv på medarbetare* (Tabell 4).

Tabell 4. Medelvärden och (standardavvikelse) för enkätfrågor i scenario UNDER, över alla grupper. Samt index för varje grupp.

	Fråga 1	Fråga 2	Fråga 3	Fråga 4	Fråga 5	Fråga 6	Index
Scenario och grupper							
UNDER							
Medarbetares perspektiv på varandra	4,33 (1,37)	4,20 (1,42)	4,80 (1,55)	4,18 (1,48)	4,77 (1,48)	4,03 (1,79)	**4,39 (1,12)**
Medarbetares perspektiv på chefer	4,82 (1,46)	4,77 (1,54)	5,03 (1,36)	4,57 (1,60)	4,97 (1,53)	4,95 (1,56)	**4,85 (1,20)**
Chefers perspektiv på medarbetare	4,91 (1,28)	4,81 (1,70)	4,89 (1,46)	4,68 (1,59)	4,79 (1,56)	4,53 (1,97)	**4,77 (1,25)**

Dessa resultat kan tolkas som att medarbetare (*Medarbetares perspektiv på varandra*) känner sig ha en lägre generell medvetenhet kring cybersäkerhet under en hypotetisk cyberincident, jämfört med vad cheferna anser att medarbetarna har (*Chefers perspektiv på medarbetare*). Med andra ord tycks chefer tro att medarbetare har bättre beredskap inför en cyberincident än vad medarbetare själva tror att de har. Vi kan se att i det mest stressande scenariot, det om vad som skulle hända under en cyberincident, så råder inte längre gemensam verklighet mellan medarbetare och chefer. I ett stressat läge spricker den gemensamma verkligheten.

I de specifika jämförelserna mellan grupperna *Medarbetares perspektiv på varandra* och *Chefers perspektiv på medarbetare* visar analyserna signifikanta skillnader i fråga 1 (uppfattningen om att vara överens om rutiner) och 2 (uppfattning om vilka åtgärder som ska vidtas) där gruppen *Chefers perspektiv på medarbetare* har högre medelvärde på båda frågorna. Skillnaden i fråga 2 var medelstor medan skillnaden i fråga 1 visade sig vara stor. Fråga 2 handlar om respondenternas uppfattning om vilka åtgärder som skall vidtas vid en potentiell cyberincident. Detta resultat kan tolkas som chefer anser att medarbetare har en större insikt i vilka åtgärder som skall tas än vad medarbetare tror att de själva har. Fråga 1 handlade däremot om medarbetares uppfattning om vilka rutiner som gäller vid en potentiell cyberincident. Här verkar det återigen som att chefer har en större tro på att medarbetarna vet vilka rutiner som gäller vid en cyberincident än vad medarbetarna har på varandra.

I jämförelsen mellan gruppen *Medarbetares perspektiv på varandra* och *Medarbetares perspektiv på chefer* visar resultatet att den senare gruppen hade signifikant högre medelvärde på indexet. Detta kan tolkas som att medarbetare (*Medarbetares perspektiv på varandra*) anser att chefer (*Medarbetares perspektiv på chefer*) har en högre generell medvetenhet kring cybersäkerheten under en hypotetisk cyberincident än vad de själva har. I jämförelsen av specifika frågor mellan dessa två grupper visade resultaten att gruppen *Medarbetares perspektiv på chefer* hade signifikant högre medelvärde i fråga 1 (uppfattningen om att vara överens om rutiner), 2 (uppfattning om vilka åtgärder som ska vidtas), 4 (uppfattning om att kunna arbeta på reducerad nivå), 6 (uppfattning om

att en teknisk analys ska skrivas). Effektstorlekarna var medelstora undantaget för fråga 6, som uppvisade en stor effekt. Fråga 1 handlade däremot om medarbetares uppfattning om vilka rutiner som gäller vid en potentiell cyberincident. Här verkar det som att medarbetare har en större tro på att chefer vet vilka rutiner som gäller vid en cyberincident än vad medarbetarna har på varandra. Fråga 2 handlade om respondenternas uppfattning om vilka åtgärder som skall vidtas vid en potentiell cyberincident.

Denna skillnad i medelvärde kan tolkas som medarbetare anser att chefer har en större insikt i vilka åtgärder som skall tas än vad medarbetare tror att de själva har. Fråga 4 handlade om huruvida medarbetarna uppfattade att det skulle upprättas rutiner för medarbetare att arbeta på reducerad nivå under en cyberincident. Resultatet tycks visa att medarbetare verkar tro att chefer har en högre medvetenhet kring upprättande av rutiner för att arbeta på reducerad nivå än vad de tror att övriga medarbetare har. Och slutligen handlade fråga 6 om huruvida medarbetare trodde att övriga medarbetare (respektive chefer) visste att en teknisk analys skulle skrivas vid en cyberincident. Detta resultat tycks visa att medarbetare tror att chefer känner till åtgärderna som ska vidtas (skriva en initial rapport) vid en cyberincident i högre utsträckning än övriga medarbetare.

Återigen visar analyserna inga signifikanta skillnader i jämförelsen av varken indexen eller de specifika frågorna mellan grupperna *Medarbetares perspektiv på chefer* och *Chefers perspektiv på medarbetare*. Det kan tolkas som att ingen råder skillnad mellan medarbetares syn på chefers generella medvetenhet kring cybersäkerhet under en hypotetisk cyberincident och chefers syn på medarbetares medvetenhet.

Efter en cyberincident

I den sista jämförelsen mellan grupperna, det vill säga frågorna gällande scenariot *efter* en cyberincident, visar analyserna att gruppen *Medarbetares perspektiv på chefer* hade signifikant högre medelvärde i indexet jämfört med både gruppen *Medarbetares perspektiv på varandra* och *Chefers perspektiv på medarbetare* (Tabell 5).

Tabell 5. Medelvärden och (standardavvikelse) för enkätfrågor i scenario EFTER, över alla grupper. Samt index för varje grupp.

	Fråga 1	**Fråga 2**	**Fråga 3**	**Fråga 4**	**Fråga 5**	**Fråga 6**	**Index**
Scenario och grupper							
EFTER							
Medarbetares perspektiv på varandra	4,66 (1,42)	5,22 (1,34)	5,09 (1,36)	4,66 (1,33)	4,66 (1,64)	4,58 (1,71)	**4,81 (1,06)**
Medarbetares perspektiv på chefer	4,92 (1,28)	5,43 (1,21)	5,24 (1,26)	5,13 (1,38)	5,04 (1,40)	5,15 (1,50)	**5,15 (1,08)**
Chefers perspektiv på medarbetare	4,87 (1,50)	4,77 (1,49)	4,85 (1,44)	4,55 (1,46)	4,70 (1,53)	4,66 (1,80)	**4,73 (1,29)**

Detta kan tolkas som att medarbetare anser att chefer (*Medarbetares perspektiv på chefer*) har en högre medvetenhet kring cybersäkerheten efter en hypotetisk cyberincident än vad de själva har (*Medarbetares perspektiv på varandra*). I de specifika jämförelserna mellan grupperna visar analyserna signifikanta skillnader i fråga 1 (uppfattningen om att vara överens om rutiner), 2 (uppfattning om vilka åtgärder som ska vidtas), 4 (uppfattning om att kunna arbeta på reducerad nivå), 5 (uppfattning om andra myndigheters stöd) och 6 (uppfattning om att en teknisk analys ska skrivas), där gruppen *Medarbetares perspektiv på chefer* hade genomgående högre medelvärden. Dessa effekter är dock relativt små förutom fråga 4 och 6 som uppvisar en medelstor respektive stor effekt. Fråga 4 handlade om huruvida medarbetarna uppfattade att det skulle upprättas rutiner för medarbetare att arbeta på reducerad nivå efter en cyberincident. Resultatet tycks indikera att medarbetare verkar tro att chefer har en högre uppfattning kring upprättande av rutiner för att arbeta på reducerad nivå än vad de tror att övriga medarbetare har. Fråga 6 däremot handlade om huruvida medarbetare trodde att övriga medarbetare (respektive chefer) visste att en teknisk analys skulle skrivas efter en cyberincident. Detta resultat kan tolkas som att medarbetare tror att chefer känner till åtgärderna som ska vidtas (skriva en initial rapport) efter en cyberincident i högre utsträckning än övriga medarbetare.

Skillnaden i jämförelsen mellan grupperna *Medarbetares perspektiv på chefer* och *Chefers perspektiv på medarbetare* kan tolkas som medarbetarna anser att chefer (*Medarbetares perspektiv på chefer*) har en högre medvetenhet kring cybersäkerheten efter en hypotetisk cyberincident än vad chefer (*Chefers perspektiv på medarbetare*) anser att medarbetare har. När det gäller specifika frågor i jämförelsen mellan grupperna visar resultatet att gruppen *Medarbetares perspektiv på chefer* hade signifikant högre medelvärde i fråga 4 (uppfattning om att kunna arbeta på reducerad nivå) och 5 (uppfattning om andra myndigheters stöd) jämfört med gruppen *Chefers perspektiv på medarbetare.* Skillnaden i fråga 5 var relativt liten, däremot var skillnaden i fråga 4 medelstor i statistisk mening. Denna fråga handlade om huruvida respondenterna (chefer och medarbetare) uppfattade att det skulle upprättas rutiner för medarbetare att arbeta på reducerad nivå efter en cyberincident. Resultatet kan tolkas som att medarbetare tror att chefer har en högre medvetenhet kring upprättande av rutiner för att arbeta på reducerad nivå än vad chefer tror att medarbetare har.

I jämförelserna mellan *Medarbetares perspektiv på varandra* och *Chefers perspektiv på medarbetare* visade analyserna ingen signifikant skillnad mellan indexen, och inte heller i de specifika frågorna. Det verkar alltså finnas en samstämmighet mellan medarbetare och chefer i deras syn kring medarbetarnas medvetenhet kring cybersäkerheten efter en potentiell cyberincident.

6 Diskussion och slutsatser

Syftet med denna studie var att undersöka uppfattningar om cybersäkerhetsrelaterat arbete bland ett brett urval av anställda på samhällsviktiga arbetsplatser. Det relevanta med de funna resultaten är de potentiella konsekvenserna av bristande cybersäkerhet på just samhällsviktiga arbetsplatser där en cyberincident kan få allvarliga följder för samhällets funktionalitet och säkerhet. Det ställer särskilt höga krav på just dessa arbetsplatser att undvika diskrepanser och missförstånd. Det är inte arbetsplatsens interna struktur eller organisation som är speciell eftersom de förmodligen inte är annorlunda än på andra arbetsplatser.

Resultaten från analysen visade att det i stort sett inte fanns några skillnader i och uppfattningar om cybersäkerhetsrelaterat arbete mellan medarbetare och chefer *före* den hypotetiska cyberincidenten. Även om det fanns några enstaka skillnader i specifika frågor. Det verkar alltså finns en samstämmighet mellan medarbetare och chefer under dessa förhållanden.

Rapporten identifierar en central diskrepans där chefer tenderar att överskatta medarbetarnas förmåga att hantera en cyberincident, som påverkar verksamheten, medan medarbetarna själva ofta underskattar sin egen förmåga. Detta fenomen kan ha flerdimensionella konsekvenser för samhällsviktiga verksamheter:

Tex. under en cyberincident är det avgörande att beslutsfattande sker snabbt och korrekt. Diskrepansen kan dock skapa osäkerhet och fördröjningar, om medarbetare tvekar på sina egna förmågor eller sitt mandat i tjänsten och därmed drar sig för att agera. Detta medan chefer som kanske inte är fullt medvetna om denna osäkerhet förväntar sig initiativ från personalen. Sådan ovisshet mellan hierarkiska nivåer kan förvärra incidentens konsekvenser, särskilt när tiden är en avgörande faktor och det kan behövas snabba reaktioner. Ett ”djävulens-advokat” perspektiv vore att tänka sig att chefernas optimism kan fungera som en positiv balans i en stressig situation. Medarbetarnas pessimistiska syn på sina egna förmågor kan delvis neutraliseras av chefernas tilltro, vilket kan skapa en slags organisatorisk balans. Optimismen från chefernas sida kan bidra till att bygga förtroende och uppmuntra medarbetarna att agera, även under osäkra förhållanden. Balansen mellan dessa två perspektiv skulle kunna utvecklas i kommande studier.

Det är värt att igen notera att deltagarna i studien var personer med många olika kompetenser och arbetsuppgifter inom samhällsviktiga arbeten, och att studien inte handlade om kompetensen inom cybersäkerhet, utan om vad medarbetare på olika nivåer tror om varandra. Det är möjligt att en studie fokuserad på medarbetare och chefer med utbildning och arbetsuppgifter specifikt inom cybersäkerhet kanske skulle kunna ge ett annat resultat.

I studien har deltagare från samhällsviktiga yrken filtrerats fram i enkäten. Det är svårt att säga om den filtreringen inneburit någon konkret skillnad för resultaten. Vi påstår

inte att blotta det faktum i sig att deltagarna är från samhällsviktiga yrken *per se* är en relevant variabel som påverkar utfallet av studien. Urvalet är studiens tematiska fokus.

Resultaten visar på ett behov av att utveckla och förstärka kommunikationsstrukturer mellan hierarkiska nivåer i samhällsviktiga organisationer för att minska diskrepansen mellan chefers och medarbetares uppfattningar. Genom att implementera regelbunden utbildning, simulering av cyberincidenter och tydliga riktlinjer kan både chefer och medarbetare få en mer realistisk bild av varandras förmågor och roller och en gemensam verklighet utvecklas.

Slutligen visade resultaten att medarbetare ansåg att chefer hade högre medvetenhet kring cybersäkerheten *efter* den hypotetiska cyberincidenten än vad de själva hade. Dessutom verkade medarbetare anse att chefer hade högre medvetenhet kring cybersäkerhet än vad chefer ansåg att medarbetarna hade. Sammantaget kan dessa resultat ses som att respondenterna anser att chefer har en tydligare uppfattning kring cybersäkerheten i efterdyningarna av en cyberincident. Om detta beror på erfarenhet, önsketänk eller ett väl underbyggt resonemang från respondenternas sida går inte utröna av våra data.

6.1 Begränsningar

Denna studie har haft en del begränsningar, här kommenteras en del av dessa. I enkäten betonades att respondenten skulle svara utifrån de datorer och telefoner som användes i arbetet och inte de privata. I många situationer är gränsen mellan arbetsredskap och privat användning inte alltid lika knivskarp.

Filterfrågorna baserades på MSB:s lista och definitioner, den listan erbjuder inte något uttrycklig särskilt svar för anställda i Försvarsmakten.

Studien baseras på en webbpanel. Det användes pga. den effektivitet den metoden erbjuder. Thompson & Utz, (2024) argumenterar för att webbpaneler, kan uppnå hög datakvalitet och representativitet. Det går dock inte att säga något om hur sammansättningen av den aktuella webbpanelen ser ut i relation till det svenska samhället som helhet. Resultaten talar endast för det urval vi hade.

I fig. 3 såg vi att fördelningen av de svarandes yrken dominerades av representanter från hälso- och sjukvård (39 %) samt ekonomi och administration (25 %), medan övriga grupper, som flygplats och hamn, hade liten representation. Denna fördelning speglar sannolikt sammansättningen av yrkesgrupper i samhället, det hade dock varit bra att ha med respondenter från flygplats och hamn. Detta begränsar studiens generaliserbarhet till de sektorer som var mest representerade i studien.

En framtida studie skulle kunna fokusera på en djupstudie av flygplats- och hamnsektorerna för att bättre förstå deras specifika utmaningar och behov inom cybersäkerhet, tex. som fortsättning på Olsén m.fl., (2023), eller på anställda och chefer med utbildning och arbetsuppgifter specifikt inom cybersäkerhet.

7 Tankar för kommande studier

Här följer några idéer och tankar kring möjliga kommande studier för att följa upp vad som framkommit i denna studie. Detta kapitel är inte att betrakta som fastslagna idéer, det är att betrakta som underlag för idéer och tankeprocesser.

7.1 Falsklarm och beslutsfattande under cyberincidenter

Syfte:

Undersöka hur falsklarm i intrångsdetektionssystem påverkar beslutsfattande i samhällsviktiga organisationer. Denna studie har lyft att otydlig ansvarsfördelning kan skapa fördröjningar i kritiska beslut, medan den kompletterande studien tar upp att organisatoriska strukturer kan behöva förbättras för att hantera osäkerhet i intrångsdetektionssystem.

Forskningsfrågor:

Vad orsakar falsklarm, och hur hanteras de av chefer och medarbetare enligt vad denna rapport funnit om hierarkiska perspektiv?

Hur påverkar signal-till-brus-förhållandet beredskapen att agera?

Metod:

Analysera systemloggar och intervjua personal om deras hantering av falsklarm. Bygg vidare på annan forsknings identifiering av hierarkiska motsättningar som hindrar effektivitet.

Potential:

Kan informera förbättringar av incidenthanteringssystem och minska organisatoriska flaskhalsar vid kritiska hot.

7.2 ”Dissonanstriangeln”: IT-avdelningen, chefer och medarbetare

Syfte:

Utforska förväntningar och ansvarsfördelning mellan IT-avdelningen, chefer och medarbetare. Rapportens hierarkiska analys kombineras med teorier om oklara roller och avståndstagande från cybersäkerhet.

Forskningsfrågor:

Hur ser skillnaderna ut mellan dessa grupper vad gäller cybersäkerhetsförväntningar?

Vilka faktorer skapar spänningar inom organisationens ansvarsfördelning?

Metod:

Genomför en djupgående triangulär studie med intervjuer och enkäter. Kompletterande forskningsslutsatser om behovet av klarare roller och samordning används som teoretisk grund tillsammans med denna studies teorier om gemensam verklighet.

Potential:

Kan bidra till riktlinjer för tydligare ansvarsfördelning och förbättrade samarbetsstrukturer.

7.3 Effekter av chefers optimism på medarbetares agerande under cyberincidenter

Syfte:

Utforska hur chefers tilltro påverkar medarbetarnas beteende under pressade situationer. Rapporten belyser chefers överskattning av medarbetares förmågor, denna föreslagna studies granskar detta djupare.

Forskningsfrågor:

Hur påverkar chefers (eventuella) optimism organisationskulturen vid incidenthantering?

När blir (eventuell) optimism en belastning snarare än en tillgång?

Metod:

Kvantitativa online experiment där chefers attityder manipuleras för att studera medarbetares reaktioner under simulerade cyberincidenter.

Potential:

Kan förbättra ledarskapsstrategier och skapa bättre organisatoriska stödstrukturer.

7.4 ”När ska vi trycka på knappen?”: Utveckling av beslutsstöd för incidentrapportering

Syfte:

Granska och utvärdera beslutsstödsverktyg för när och hur medarbetare och

organisationer rapporterar en cyberincident. Kompletterande forskning belyser delvis den ofta förekommande bristande förståelsen för cyberincidenter och lyfter fram vikten av konkreta åtgärder och riktlinjer. Se också Stenerus m.fl., (2020) som ett kompletterande underlag.

Forskningsfrågor:

Vilka indikatorer bör ligga till grund för en snabb och korrekt incidentrapportering?

Hur kan osäkerhet kring rapporteringskrav reduceras?

Potential:

Kan leda till mer konsekvent och effektiv rapportering i linje med krav från regelverk som t.ex. NIS2.

7.5 Återkommande barometer för cybersäkerhet

Syfte:

Etablera en löpande enkätbaserad kvantitativ undersökning för att återkommande mäta förändringar i cybersäkerhetsuppfattningar över tid. Detta för att följa upp vad denna studie påbörjat om förväntning och uppfattningar.

Forskningsfrågor:

Hur utvecklas förväntningar och svårigheter inom cybersäkerhet över tid?

Vilka skillnader uppstår mellan olika sektorer i samhällsviktiga verksamheter?

Metod:

Designa en årlig enkät med inspiration från t.ex. SOM-institutets studier.

Potential:

Kan ge viktiga insikter för strategisk planering och policyutveckling.

7.6 Undersök CERT:ars roll och funktioner

Syfte:

Kartlägga och skapa en modell över CERT-organisationers roller. Både denna studie och annan forskning framhäver behovet av tydligare ansvarsområden och effektiva samarbetsmodeller.

Forskningsfrågor:

Hur definieras CERT-organisationer, och vilka variationer finns globalt och i Europa och mellan statliga och privata?

Hur kan standardisering stärka cybersäkerhetssamarbete?

Metod:

Intervjuer och komparativ analys av olika slag av CERT:ar internationellt och i Sverige. Utgå från etablerad forsknings reflektioner om tydlighet och samordning i cybersäkerhetsarbete, samt från FOI:s övriga arbete kring NIS2 jfr (Lioufas & Melbi, 2025).

Potential:

Kan stärka förståelsen för CERT:ars, särskilt i samhällsviktiga sektorer och kanske öka återrapporteringen av incidenter.

8 Referenser

Ampere, A.-M. (1865). Essai sur la philosophie des sciences ou exposition analytique d'une classification naturelle de toutes les connaissances humaines. http://www.ampere.cnrs.fr/textes/essaiphilosophie/pdf/essaiphilosophiesciences_1.pdf

Aro, E. (2024, december). Lantmäteriet: ”Stängde så fort vi fick det bekräftat”. Sveriges Radio. https://sverigesradio.se/artikel/lantmateriet-stangde-sa-fort-vi-fick-det-bekraftat

Bengtsson, J., Mossberg Sonnek, K., & Hedtjärn Svaling, V. (2023). Digitaliseringens fallgropar i gråzon och krig (R No. FOI-R--5522--SE). FOI. https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5522--SE

Burda, P., Allodi, L., & Zannone, N. (2024). Cognition in Social Engineering Empirical Research: A Systematic Literature Review. ACM Transactions on Computer-Human Interaction, 31(2), 19:1-19:55. https://doi.org/10.1145/3635149

Echterhoff, G., Higgins, E. T., & Levine, J. M. (2009). Shared reality: Experiencing commonality with others' inner states about the world. Perspectives on Psychological Science, 4(5), 496–521. https://doi.org/10.1111/j.1745-6924.2009.01161.x

Edeh, N. C. (2023). Cybersecurity and Human Factors: A Literature Review. I Cybersecurity for Decision Makers (s. 45–56). CRC Press.

Eidenskog, D., Eckersand, U., & Mittermaier, E. (2023). Digitaliseringens risker i hälso- och sjukvård (R no No. FOI-R--5367--SE). FOI.

Europaparlamentets och rådets förordning (EU) 2019/881 (2019). https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX%3A32019R0881

Heiding, F., Katsikeas, S., & Lagerström, R. (2023). Research communities in cyber security vulnerability assessments: A comprehensive literature review. Computer Science Review, 48, 100551. https://doi.org/10.1016/j.cosrev.2023.100551

Higgins, E. T., Rossignac-Milon, M., & Echterhoff, G. (2021). Shared Reality: From Sharing-Is-Believing to Merging Minds. Current Directions in Psychological Science, 30(2), 103–110. https://doi.org/10.1177/0963721421992027

Ingemarsdotter, J., Eidenskog, D., & Swaling, V. H. (2020). Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur (R No. FOI-R--4814--SE). FOI.

Kalix Kommun. (2022). Rapport IT-attacken socialförvaltningen Kalix kommun. (No. 20220815).

Karlén, Å. (2024, maj). IT-attack – så funkar det—Stockholms universitet. https://www.su.se/forskning/nyheter-forskning/it-attack-s%C3%A5-funkar-det-1.710412

Karlzen, H., & Sommestad, T. (2020). När luras personer av nätfiske? En genomgång av publicerade fältexperiment (text No. FOI-R--4951--SE). FOI. https://intranet.foi.se/ovrigt/rapportsammanfattning.html?reportNo=FOI-R--4951--SE

Lioufas, A., & Melbi, A. (2025). NIS2 och incidentrapportering: Farhågor, förhoppningar och förvirring (Memo No. 8815). FOI.

Martin, A. (2024, maj). Sweden's liquor shelves to run empty this week due to ransomware attack. The Record. https://therecord.media/sweden-ransomware-liquor-shortage-skanlog-systembolaget

MSB. (2023). Lista med viktiga samhällsfunktioner—Utgångspunkt för att stärka samhällets beredskap (No. MSB1844). MSB. https://www.msb.se/sv/publikationer/identifiering-av-samhallsviktig-verksamhet--lista-med-viktiga-samhallsfunktioner/

MSB. (2025). Sex av tio organisationer har allvarliga brister i sitt säkerhetsarbete. https://www.msb.se/sv/aktuellt/nyheter/2025/januari/sex-av-tio-organisationer-har-allvarliga-brister-i-sitt-sakerhetsarbete/

Nilsson, P.-E. (2023). Unraveling the Myth of Cyberwar—Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014-2023) (text No. FOI-R--5513--SE). https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5513--SE

Nyheter, S. V. T. (2025, januari 20). Hallandstrafikens hemsida låg nere en vecka – utsatt för överbelastningsattack. SVT Nyheter. https://www.svt.se/nyheter/lokalt/halland/hallandstrafikens-hemsida-nere-utsatt-for-overbelastningsattack

Olsén, M., Valassi, C., & Stenerus, A.-S. (2023). NCS3-Ett skepp kommer lastat—En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar (No. R---5405--SE).

Palmborg, M. (2024, mars 5). Rysk hackergrupp bakom cyberattack mot Sverige. Aftonbladet. https://www.aftonbladet.se/a/onje3W

Perwej, Dr. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, Dr. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 9(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work, 24(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Popova, M. (u.å.). How William Gibson Coined "Cyberspace" – The Marginalian. Hämtad 07 september 2023, från https://www.themarginalian.org/2014/08/26/how-william-gibson-coined-cyberspace/

Sapienza, Z. S., Veenstra, A. S., Kirtiklis, K., & Giannino, S. S. (2016). The Transmission Model of Communication: Toward a Multidisciplinary Explication. ETC: A Review of General Semantics, 73(4), 321–341.

Schmalbach, B., Hennemuth, L., & Echterhoff, G. (2019). A Tool for Assessing the Experience of Shared Reality: Validation of the German SR-T. Frontiers in Psychology, 10. https://doi.org/10.3389/fpsyg.2019.00832

Stasser, G. (1999). The Uncertain Role of Unshared Information in Collective Choice. I Shared Cognition in Organizations. Psychology Press.

Stasser, G., & Titus, W. (1985). Pooling of unshared information in group decision making: Biased information sampling during discussion. Journal of Personality and Social Psychology, 48(6), 1467–1478. https://doi.org/10.1037/0022-3514.48.6.1467

Stenerus, A.-S., Bengtsson, J., & Olsson, M. (2020). IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering (No. FOI-R--4815--SE).

Svahn, M., Jarlsbo, M., Michélsen Forsgren, M., & Lindahl, D. (2024). Delat ansvar är ingens ansvar? En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete (text No.

FOI-R--5546--SE). FOI. https://www.foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5546--SE

Taib, R., Yu, K., Berkovsky, S., Wiggins, M., & Bayl-Smith, P. (2019). Social Engineering and Organisational Dependencies in Phishing Attacks. I D. Lamas, F. Loizides, L. Nacke, H. Petrie, M. Winckler, & P. Zaphiris (Red.), Human-Computer Interaction – INTERACT 2019 (s. 564–584). Springer International Publishing. https://doi.org/10.1007/978-3-030-29381-9_35

Thompson, A. D., & Utz, R. L. (2024). Online surveys: Lessons learned in detecting and protecting against insincerity and bots. Quality & Quantity. https://doi.org/10.1007/s11135-024-01973-z

Tietoevry.com. (2024, januari). Tietoevry: Fortsatt fokus på återställning efter ransomware-attack. https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/tietoevry-fortsatt-fokus-pa-aterstallning-efter-ransomware-attack/

Wickström, A., & Wiman, S. S. (2024, juli 19). Grundproblemet löst efter globala it-störningar. SVT Nyheter. https://www.svt.se/nyheter/utrikes/it-storningar-varlden-over

Wiener, N. (2000). Cybernetics or control and communication in the animal and the machine (2. ed., 10. print). MIT Press.

Wiklund, K. (2024, mars 4). Data från sjukhuset säljs på nätet efter stor hackerattack. https://www.nyteknik.se/tech/data-fran-sophiahemmet-saljs-pa-natet-efter-stor-hackerattack/4240965

Appendix 1 – Beskrivning av statistiska analyser

Reliabilitetstest

För att undersöka om de sex olika frågorna i varje scenario, över de tre olika grupperna, mäter samma konstrukt utförde vi nio *reliabilitetstest*. Detta test undersöker huruvida frågorna i varje scenario (över alla tre grupper) är relaterade till varandra och därmed kan sammanfogas i ett generellt index för varje scenario, över de tre olika grupperna. I statistiska termer undersöker testet om frågorna korrelerar sinsemellan, dvs. om den interna konsistensen per index är hög. Måttet som användas för detta kallas Cronbachs alfa och gränsvärdet för måttet brukar ligga på 0,70. Alla nio test uppvisade Cronbachs alfa-värden mellan 0,79 och 0,91. Detta ska tolkas som att alla nio testen visade tillfredställande intern konsistens. Därmed kan de sex olika frågorna i varje scenario, över de tre olika grupperna, betraktas som enhetliga konstrukt och sammanfogas i nio olika index.

Test av normalitet

Innan vi påbörjade jämförelserna utförde vi ett så kallade *Shapiro-Wilk-test* för att undersöka vilka statistiska analyser som är bäst lämpade för våra data. Detta test undersöker om data är normalfördelade enligt normalfördelningens teoretiska principer: att fördelningen är kyrkklockformad, att den är symmetrisk (dvs. att kurvan ser likadan ut på båda sidorna om mitten) och att fördelningen är asymptotisk (dvs. att fördelningen fortsätter oändligt långt ut på båda sidor utan att någonsin möta x-axeln). Notera att variabler i verkligheten aldrig är perfekt normalfördelade enligt dessa principer. Variabler kan dock vara tillräckligt normalfördelade. Därför brukar man säga att variabeln är *approximativt* normalfördelad. I de fall där data var signifikant icke-normalfördelade (enligt Shapiro-Wilk-testet) använde vi icke-parametriska test för att undersöka medvärdesskillnaderna.

Signifikans

Statistisk signifikans är en term som används i forskning för att beskriva hur sannolikt det är att en skillnad (eller ett samband) som observerats i data är verklig (eller verkligt) och inte bara en slump. När en skillnad eller ett samband är statistiskt signifikant kan man säga att skillnaden eller sambandet inte kan förklaras av slumpen. Därför är det sannolikt att skillnaden eller sambandet är verkligt. För att avgöra om en skillnad eller ett samband är statistiskt signifikant använder man sig av p-värdet. P-värdet är ett mått (en procentsiffra) på hur sannolikt det är att observationen är en slump. P-värdet beräknas genom att jämföra resultatet från studien med vad man skulle förvänta sig att se om alla förutsättningar för studien är sanna. Som regel använder man sig av en gräns på 5 % för att avgöra om ett fynd är statistiskt signifikant. Om p-värdet är lägre än 5 % betyder det att det finns en liten sannolikhet (< 5 %) att observationen är en slump, och

den är därför statistiskt signifikant. Om p-värdet är 5 % eller högre (≥ 5 %) kan observationen vara en slump.

Effektstorlek

I denna undersökning använde vi standardiserade statistiskt mått (*Cohen's d* för parametriska tester och *Rank-Biserial Correlation* för icke-parametriska test) för att bedöma storleken (också kallat effektstorleken) på statistiskt signifikanta resultat – medelvärdesskillnader i vårt fall. Eftersom måttet är standardiserat kan det användas för att jämföra resultat som har uppmätts i olika enheter, eller med ett mått som av mer latent karaktär (t.ex. en Likertskala som användes i denna undersökning). För varje effektstorlek finns konventionellt överenskomna gränsvärden som guidar tolkningen av resultatens storlek. För Cohen's d gäller följande gränsvärden: 0,20 = liten effekt; 0,50 = medelstor effekt; ≥ 0,80 = stor effekt. För Rank-Biserial Correlation gäller följande gränsvärden: 0,10 = liten effekt; 0,30 = medelstor effekt; ≥ 0,50 = stor effekt.

Paired sample t-test

För att jämföra skillnaderna i svaren som medarbetarna gav på frågor om cybersäkerhet från varandras perspektiv (*Medarbetares perspektiv på varandra*) och från chefers perspektiv (*Medarbetares perspektiv på chefer*) utförde vi tre paired sample t-test. Ett jämförande test vardera för *före, under* och *efter* en cyberincident. Paired sample t-test jämför medelvärden från samma individer fast under olika förutsättningar eller tidpunkter. I vårt fall handlar det om samma deltagare som har svarat på två olika enkäter, där deltagarna skulle ha perspektivet av andra medarbete i åtanke i den ena enkäten, och i den andra enkäten ha chefernas perspektiv i åtanke. Dessa två olika perspektiv betraktas i denna undersökning som två olika betingelser. Vid icke-normala fördelningar av variabler utfördes icke-parametriska testet *Wilcoxon signed-rank test*.

One-sample t-test

För att jämföra skillnaderna mellan chefer och medarbetare utförde vi totalt sex olika one-sample t-test över två omgångar. Detta test används när man vill jämföra ett medelvärde mot ett hypotetiskt testvärde eller referensvärde. I första omgången av tester (*Medarbetares perspektiv på varandra* vs. *Chefers perspektiv på medarbetare; före, under* och *efter* en cyberincident) använde vi medelvärdet av medarbetarnas svar om cybersäkerhet från varandras perspektiv som referensvärde. Detta värde jämfördes sedan mot medelvärdet av chefernas svar om cybersäkerhet från medarbetarnas perspektiv. I den andra omgången av tester (*Medarbetares perspektiv på chefer* vs. *Chefers perspektiv på medarbetare; före, under* och *efter* en cyberincident) använde vi medelvärdet av medarbetarnas svar om cybersäkerhet från chefers perspektiv som referensvärde. Detta värde jämfördes sedan mot medelvärdet av chefernas svar om cybersäkerhet från medarbetarnas perspektiv. Även här utfördes icke-parametriska testet *Wilcoxon signed-rank test* vid icke-normala fördelningar av variabler.

Appendix 2a – Introduktion och bakgrundsinformation

Hej och välkommen till denna enkät!

Vi kommer att ställa några frågor om cybersystem och cybersäkerhet. Med det menar vi de olika digitala verktyg och system som du använder i ditt arbete. Det kan handla om IT-system som är viktiga för ditt jobb som du använder på en jobbdator eller appar på din jobbtelefon.

Observera: Vi syftar inte på dina privata datorer eller telefoner som du använder för personligt bruk.

Först vill vi fråga dig vad du arbetar med. Välj det alternativ som bäst beskriver dina huvudsakliga arbetsuppgifter:

Hälso- och sjukvård:

- Någon form av läkare, sjuksköterska, tandvård eller arbete inom primärvården.
- Hemsjukvård, t.ex. sjuksköterskeinsatser, rehabilitering, eller palliativ vård.

Räddningstjänst och säkerhet:

- Polis, brandkår, sjöräddning, fjällräddning eller annan form av räddningstjänst.
- Kommunal hemtjänst, t.ex. personlig omvårdnad, avlösning, ledsagning eller praktisk och personlig hjälp i hemmet.

Flygplatsverksamhet:

- Flygplatsarbete som trafikledning, koordination med flygbolag och markservice, teknisk infrastruktur, säkerhetskontroller, övervakning, eller samarbete med myndigheter som polis och tull.
- Flygplatsarbete som incheckning, bagagehantering, kundservice, lastning och lossning av bagage, banunderhåll, boarding, bränslepåfyllning, eller andra operativa uppgifter på flygplansrampen.

Hamnarbete:

- Leda den dagliga verksamheten i hamnen, inklusive lastning, lossning, logistik, samordning av fartyg, säkerhet, övervakning och samarbete med tull och kustbevakning. Ansvar för underhåll och drift av hamnens infrastruktur och tekniska system, såsom kranar, maskiner och kajer, samt samordning av logistikflöden.
- Hamnarbete som lastning och lossning av gods från fartyg, kranoperatör, övervakning av hamnområdet, eller underhåll och reparationer av maskiner och infrastruktur.

Järnvägsverksamhet:

- Leda den dagliga driften av järnvägssystemet, inklusive tågtrafik, stationsdrift och samordning med operatörer. Ansvar för säkerhetsföreskrifter och regler inom järnvägsnätet, inklusive spår, stationer och tåg, samt underhåll och utveckling av infrastrukturen. Planering av tågtrafik, tidtabeller, rutter och kapacitet.
- Järnvägsarbete som lokförare, tågvärd, spårtekniker eller signaltillsyningsman.

Ekonomi och administration:

- Ekonomisk administration gentemot offentlig sektor, t.ex. fastställande och inbetalning av arbetsgivaravgifter, inkomstskatt, skatt på kapital, mervärdesskatt och punktskatter.
- Utbetalning eller handläggning av socialförsäkringar, socialtjänst, arbetslöshetsförsäkring, pensioner och pensionsrelaterade förmåner.

Energiförsörjning:

- Produktion, distribution, lagring, infrastruktur och handel med bränslen, flytande drivmedel eller gas.
- Underhåll och funktion av eldistribution
- Produktion, distribution och underhåll av system för fjärrvärme och/eller fjärrkyla

Vatten och livsmedel:

- Underhåll och funktion av avloppssystem,
- Underhåll och funktion av dricksvattenförsörjning eller livsmedelsproduktion och distribution.

Finans och försäkring:

- Betalningsförmedling, finansiell stabilitet, försäkring, sparande, finansiering och finansiell riskhantering inom ett finansinstitut.

Läkemedelsförsörjning och/eller djurhälsa:

- Läkemedelsförsörjning eller smittskydd, t.ex. arbete inom apotek eller distribution av läkemedel (för människor).
- Hälsa och sjukvård för djur, inklusive veterinärläkemedel.

Bevakning och skydd:

- Bevakning och fysiskt skydd av samhällsviktig verksamhet.

Annat (Här går respondenten inte vidare i enkäten).

Min position är:

- Jag är en chef (dvs. jag har personal- och verksamhetsansvar bland mina arbetsuppgifter)
- Jag är inte en chef (dvs. jag har INTE personal- och verksamhetsansvar bland mina arbetsuppgifter)

Appendix 2b – Enkät 1 till medarbetare

Här kommer du få presenterat för dig ett scenario som handlar om de dagliga rutinerna kring cybersäkerhet på jobbet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att du är på jobbet en vanlig dag, och alla digitala system fungerar som de ska. För att motverka cyberincidenter behövs rutiner och förberedelser i det vardagliga arbetet som minskar risken för att kritiska system påverkas eller slås ut. Du tror att det finns rutiner för att säkerhetskopiera data, regelbundet uppdatera programvara och allmän övervakning av kritiska system. Du tänker att förberedelserna är noggrant planerade och genomförda.

Det vi vill veta är: vad tror du om dina kollegor? Notera att vi är framför allt intresserade av hur du *tror* att det ligger till. Inte vad du hoppas.

1. *Jag tror att* vi på jobbet är överens om vilka rutiner som gäller för hur vi hanterar och dokumenterar våra arbetsuppgifter i de digitala systemen.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* vi på jobbet vet vilka cybersäkerhetsrisker som finns för vår arbetsplats.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* vi på jobbet vet vem som har ansvaret för att hantera situationen när en cyberincident händer.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* vi på jobbet är i stort sett på samma våglängd i fråga om att förbereda rutiner och utrustning så att vi klarar oss om en cyberincident händer. T ex skriva ut viktiga dokument, telefonlistor, ha reservdatorer och ha system för lokal drift så att arbetsuppgiften kan utföras, om än på en reducerad nivå.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. *Jag tror att* vi på jobbet förväntar oss att det finns lagar och regleringar som, när de följs, kan förhindra cyberincidenter från att ske på mitt jobb.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Skulle en cyberincident inträffa *tror jag att* vi på jobbet vet att en initial rapport ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Här kommer du få presenterat för dig ett scenario som handlar om rutiner under en cyberincident på jobbet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att du är på jobbet, och plötsligt slutar alla dina digitala system att fungera. Datorn fryser, telefonens appar vägrar öppna sig, systemet går ner, skärmar blinkar och larm piper. Det råder osäkerhet – är det bara ett litet mjukvarufel, eller är det något allvarligare? Du undrar, är detta en sådan där cyberincident som du hört talas om?

Det vi vill veta är: vad tror du om dina kollegor i det här läget? Notera att vi är framför allt intresserade av vad du *tror* skulle hända i en sådan situation. Inte vad du hoppas.

1. I det här läget *tror jag att* vi på jobbet har tidigare definierade rutiner på plats som vi nu kan följa. T.ex. rutiner som inkluderar steg för att säkerställa kvalitet och följa upp på arbetsprocesser även i detta akuta läge.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* vi på jobbet vet vilka cybersäkerhetsåtgärder som ska vidtas i en sådan situation.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* vi på jobbet vet vem som ansvarar för att hantera cyberincidenter i det här läget.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* vi på jobbet klarar oss med de förberedda rutinerna och den förberedda utrustningen så att arbetsuppgiften fortfarande kan utföras om än på en reducerad nivå. T ex genom tidigare utskrivna viktiga dokument, telefonlistor, reservdatorer och andra system förlokal drift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. *Jag tror att* vi på jobbet förväntar oss att myndigheterna nu träder in och stödjer oss under cyberincidenten.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. *Jag tror att* vi på jobbet vet att en teknisk analys nu ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Här kommer du få presenterat för dig ett scenario som handlar om rutiner efter en cyberincident på jobbet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att jobbets digitala system sakta börjar återhämta sig efter cyberincidenten. Du och dina kollegor arbetar metodiskt tillsammans med experter. Ett efter ett återställs program och data medan ni noggrant kontrollerar varje funktion. Varje steg kräver precision och tålamod. Ni skriver rapporter, testar säkerhetskopior, och dubbelkollar integriteten.

Vad tror du att dina kollegor gör nu? Notera att vi är framför allt intresserade av hur du tror att efterdyningarna kommer se ut efter en incident. Inte vad du hoppas.

1. *Jag tror att* vi på jobbet är överens om hur vi ska återgå till våra rutiner för att hantera och dokumentera våra arbetsuppgifter i de digitala systemen.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* vi på jobbet nu har lärt oss om vad cybersäkerhetsrisker kan orsaka på vår arbetsplats
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* vi på jobbet vet vem som ansvarar för att återställa våra digitala arbetsverktyg efter cyberincidenten.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* vi på jobbet vet hur vi förbereder rutiner och utrustning så att arbetsuppgifterna fortfarande skulle kunna utföras om än på en reducerad nivå. T.ex. skriver ut viktiga dokument, telefonlistor, skaffar reservdatorer och andra system för lokal drift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. *Jag tror att* vi på jobbet förväntar oss att myndigheterna träder in och stödjer oss i återställandet av vår arbetsplats.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Jag tror att vi på jobbet vet att en slutrapport ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Appendix 2c – Enkät 2 till medarbetare

Här kommer du få presenterat för dig ett scenario som handlar om de dagliga rutinerna kring cybersäkerhet på jobbet. Notera att nu kommer scenariot handla om chefens/chefernas arbete med cybersäkerhet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att du är på jobbet en vanlig dag, och alla digitala system fungerar som de ska. För att motverka cyberincidenter behövs rutiner och förberedelser i det vardagliga arbetet som minskar risken för att kritiska system påverkas eller slås ut. Du tror att det finns rutiner för att säkerhetskopiera data, regelbundet uppdatera programvara och för allmän övervakning av kritiska system. Du antar att förberedelserna är noggrant planerade och genomförda.

Det vi vill veta är: vad tror du om dina *chefer* i detta läge? Notera att vi är framför allt intresserade av hur du tror att det ligger till. Inte vad du hoppas.

1. *Jag tror att* mina chefer har tänkt på beredskapen för en cyberincident och fastställt vilka rutiner som gäller för hur vi hanterar våra arbetsuppgifter skulle det hända.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* våra chefer vet vilka cybersäkerhetsrisker som vår arbetsplats är utsatt för.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* våra chefer vet vem eller vilka som ska ha ansvaret för att hantera situationen den dag en cyberincident inträffar.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* våra chefer är i stort sett på samma våglängdmed varandra i fråga om att förbereda rutiner och utrustning så att arbetsuppgifterna kan utföras, om än på en reducerad nivå. T.ex. skriva ut viktiga dokument, telefonlistor, ha reservdatorer och ha system för lokal drift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. *Jag tror att* våra chefer förväntar sig att det finns lagar och regleringar som, när de följs, kan förhindra cyberincidenter från att inträffa på vårt jobb.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Skulle det trots allt inträffa en cyberincident av något slag *tror jag att* våra chefer vet att en initial rapport ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Här kommer du få presenterat för dig ett scenario som handlar om rutiner under en cyberincident på jobbet. Återigen handlar scenariot om chefens/chefernas arbete i en sådan situation. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att du är på jobbet, och plötsligt slutar alla dina digitala system att fungera. Datorn fryser, telefonens appar vägrar öppna sig, systemet går ner, skärmar blinkar och larm piper. Det råder osäkerhet – är det bara en litet mjukvarufel, eller är det något allvarligare? Du undrar, är detta en sådan där cyberincident som du hört talas om?

Vad tror du att dina *chefer* gör nu? Notera att vi är framför allt intresserade av vad du tror skulle hända under en sådan incident. Inte vad du hoppas.

1. I det här läget *tror jag att* våra chefer har tidigare definierade rutiner på plats som vi nu kan följa. T.ex. rutiner som inkluderar steg för att säkerställa kvalitet och följa upp på arbetsprocesser även i detta akuta läge.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. Jag *tror att* våra chefer vet vilka cybersäkerhetsrisker som vår arbetsplats är utsatt för.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. Jag *tror att* våra chefer vet vem som ansvarar för olika aspekter av vårt arbete i det här läget.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. Jag *tror att* våra chefer har beredskap så att arbetsuppgifterna fortfarande kan utföras, om än på en reducerad nivå. T.ex. genom att tidigare tagit fram utskrivna viktiga dokument, telefonlistor, reservdatorer och system förlokal drift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. *Jag tror att* våra chefer förväntar sig att myndigheterna nu träder in för att stödja oss under cyberincidenten.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Jag tror att chefer vet att en teknisk analys ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Här kommer du få presenterat för dig ett scenario som handlar om rutiner efter en cyberincident på jobbet. Återigen handlar scenariot om chefens/chefernas arbete i en sådan situation. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att jobbets digitala system sakta börjar återhämta sig efterincidenten. Du och dina kollegor arbetar metodiskt tillsammans med experter. Ett efter ett återställs program och data medan ni noggrant kontrollerar varje funktion. Varje steg kräver precision och tålamod. Ni skriver rapporter, testar säkerhetskopior, och dubbelkollar att allt funkar.

Vad tror du att dina chefer gör nu? Notera att vi är framför allt intresserade av hur du tror att efterdyningarna kommer se ut efter en incident. Inte vad du hoppas.

1. Jag tror att våra chefer är överens med varandra vilken typ av beredskap som behövs för att motverka framtidacyberincidenter.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* våra chefer nu har lärt sig mer om vad cybersäkerhetsrisker kan orsaka på vår arbetsplats.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* våra chefer vet vem som ansvarar för att återställa olika aspekter av vårt arbete efter cyberincidenten.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* våra chefer nu kommer att förbereda rutiner och utrustning så att arbetsuppgifterna fortfarande skulle kunna utföras om än på en reducerad nivå. T.ex. genom att skriva ut viktiga dokument, telefonlistor, skaffa reservdatorer och andra system för lokal drift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. Våra chefer i samarbete med myndigheterna *får nu se till att* det inte händer cyberincidenter på vår arbetsplats igen.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Jag tror att våra chefer vet att en slutrapport ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Appendix 2d – Enkät till chefer

Här kommer du få presenterat för dig ett scenario som handlar om de dagliga rutinerna kring cybersäkerhet på jobbet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att du är på jobbet en vanlig dag, och alla digitala system fungerar som de ska. För att motverka cyberincidenter behövs rutiner och förberedelser i det vardagliga arbetet som minskar risken för att kritiska system påverkas eller slås ut. Du tror att det finns rutiner för att säkerhetskopiera data, regelbundet uppdatera programvara och allmän övervakning av kritiska system. Du tänker att förberedelserna är noggrant planerade och genomförda.

Det vi vill veta är: vad tror du om din personal? Notera att vi är framför alltintresserade av hur du tror att det ligger till. Inte vad du hoppas.

1. *Jag tror att* personalen har fastställt vilka rutiner som gäller för hur de hanterar sina arbetsuppgifter om en cyberincident inträffar.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* personalen vet vilka cybersäkerhetsrisker som finns för vår arbetsplats.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* personalen vet vem som har ansvaret för att hantera situationen när en cyberincident inträffar.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* personalen är på samma våglängd med varandra gällande att förbereda rutiner och utrustning så att arbetsuppgifterna kan utföras, om än på en reducerad nivå. T.ex. genom att skriva ut viktiga dokument, telefonlistor, ha reservdatorer och ha system för lokal drift förberedda.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. *Jag tror att* personalen förväntar sig att det finns lagar och regleringar som, när de följs, kan förhindra cyberincidenter från att inträffa på arbetsplatsen.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Skulle en cyberincident inträffa *tror jag att* personalen vet att en initial rapport ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Här kommer du få presenterat för dig ett scenario som handlar om rutiner under en cyberincident på jobbet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att du är på jobbet, och plötsligt slutar alla dina digitala verktyg att fungera. Datorn fryser, telefonens appar vägrar öppna sig, systemet går ner. Kollegor runt dig ser förvirrade ut, skärmar blinkar och larm piper. Det råder osäkerhet – är det bara en teknisk glitch, eller något allvarligare? Du undrar, är detta en sådan där cyber-incident som du hört talas om?

Vad tror du att personalen gör nu? Notera att vi är framför allt intresserade av vad du tror skulle hända under en sådan incident. Inte vad du hoppas.

1. I det här läget *förväntar jag mig att* personalen har tidigare definierade rutiner på plats som de nu kan följa. T.ex. rutiner som inkluderar steg för att säkerställa kvalitet och följa upp arbetsprocesser även i detta akuta läge.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. Jag *tror att* personalen vet om de cybersäkerhetsrisker som vår arbetsplats är utsatt för och nu vet vad de gör.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. Jag *tror att* personalen vet vem som ansvarar för olika aspekter av deras arbete i det här läget.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. Jag *tror att* personalen har beredskap och t.ex. tidigare harskrivit ut viktiga dokument, telefonlistor, ordnat reservdatorer och system för lokal drift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. Det är nu upp till personalen att samverka med myndigheter för att stödja oss i denna cyberincident på jobbet.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. Jag tror att personalen vet att en teknisk analys ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

Här kommer du få presenterat för dig ett scenario som handlar om rutiner efter en cyberincident på jobbet. Efter detta ska du svara på 6 frågor kopplade till scenariot.

Scenario: Tänk dig att cybersystemen på din arbetsplats sakta börjar återhämta sig efter en cyberincident. Du och dina kollegor arbetar metodiskt, en efter en återställs program och data, medan ni noggrant kontrollerar varje funktion. Varje steg kräver precision och tålamod. Vad tror du att personalen gör nu? Notera att vi är framför allt intresserade av hur du tror att efterdyningarna kommer se ut efter en incident. Inte vad du hoppas.

Vad tror du att personalen gör nu? Notera att vi är framför allt intresserade av hur du tror att efterdyningarna kommer att se ut efter en incident. Inte vad du hoppas.

1. *Jag tror att* personalen är överens kring beredskapen inför nya cyberincidenter.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

2. *Jag tror att* personalen vet vilka cybersäkerhetsrisker som finns för vår arbetsplats.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

3. *Jag tror att* personalen vet vem som ansvarar för olika aspekter av deras arbete efter cyberincidenten.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

4. *Jag tror att* personalen har beredskap så att arbetsuppgifterna kan utföras, om än på en reducerad nivå. T.ex. genom att tidigare ha skrivit ut viktiga dokument, telefonlistor, ordnat med reservdatorer och system för lokaldrift.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

5. Personalen är nu ansvarig för att arbeta tillsammans med myndigheterna för att se till att det inte händer cyberincidenter på vår arbetsplats igen.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

6. *Jag tror att* personalen vet att en teknisk analys nu ska skrivas.
   Inte alls 1 2 3 4 5 6 7 Helt och hållet

FOI

ISSN 1650-1942

www.foi.se