

SYSTEMATISKT INFORMATIONSSÄKERHETSARBETE

— ETT KOMMUNPERSPEKTIV

Kandidatuppsats i Informatik

Muamer Cukur
Selma Jakupovic

2024KANI36



HÖGSKOLAN
I BORÅS

Svensk titel: Systematiskt informationssäkerhetsarbete - ett kommunperspektiv.

Engelsk titel: Systematic information security work - a municipal perspective.

Utgivningsår: 2024

Författare: Muamer Cukur & Selma Jakupovic

Handledare: Patrik Hedberg

Abstract

Information security is a critical aspect for organizations today given the increased digitalization in society. This study investigates the success factors and obstacles among medium and small municipalities with the aim of improving municipal information security work. The study employs a qualitative method in the form of semi-structured interviews with CISOs and a cybersecurity expert with expertise in municipal information security. The interviews were analyzed thematically to identify various patterns in the form of challenges and success factors. The results of the study indicate that the greatest challenges are characterized by a lack of specialized competence, limited financial resources, and a low level of competence among employees. The study concludes that there is a need for increased education and security awareness among those involved in municipalities, along with improved resource allocation. Further research should focus on developing good awareness among employees through educational programs and learning models between municipalities.

Keywords: Information Security, Swedish municipalities, Risk Management, Obstacles, Success factors

Sammanfattning

Informationssäkerhet är en kritisk aspekt inom organisationer idag med hänsyn till den ökade digitaliseringen i samhället. Denna studie undersöker framgångsfaktorer och hinder bland medelstora och små kommuner i syfte att förbättra det kommunala informationssäkerhetsarbetet. Studien använder en kvalitativ metod i form av semi-strukturerade intervjuer med CISO:s och en cybersäkerhetsexpert med kompetens i kommunalt informationssäkerhetsarbete. Intervjuerna som genomfördes analyserades med en tematisk analys där olika mönster identifierades i form av utmaningar och framgångsfaktorer. Resultatet av undersökningen indikerar att de största utmaningarna karaktäriseras i form av brist på specialiserad kompetens, begränsade ekonomiska resurser och en låg kompetensnivå bland de anställda. Studien fastslår att det behövs en ökad utbildningsnivå och säkerhetsmedvetande bland de involverade i kommunerna i samband med förbättrad resursallokering. Vidare forskning bör fokusera på att utveckla en god medvetenhet bland de anställda i form av utbildningsprogram samt inlärningsmodeller mellan kommunerna.

Nyckelord: Informationssäkerhet, Svenska kommuner, Riskhantering, Hinder, Framgångsfaktorer

Förord

Vi vill börja med att rikta ett stort tack till vår handledare Patrik Hedberg. Patrik har försett oss med väldigt goda exempel och framförallt varit ett bra stöd under dessa åtta veckor och även under de seminarier som samtliga, även författare, varit delaktiga i. Alla delar i uppsatsen har skrivits tillsammans, vilket intygas av både Muamer och Selma. Dessa åtta veckor har varit intensiva men framförallt väldigt lärorika.

Innehållsförteckning

1. Inledning	3
1.1 Bakgrund	3
1.2 Tidigare kunskap	5
1.2.1 Myndighetsrapporter	5
1.2.2 Framgångsfaktorer inom informationssäkerhet	6
1.2.3 Hinder inom informationssäkerhet	7
1.3 Problemdiskussion	9
1.4 Syfte och forskningsfråga	10
1.5 Målgruppen	10
2. Metod	11
2.1 Forskningsansats	11
2.2 Datainsamlingsmetod	11
2.2.1 Dokumentanalys	11
2.2.2 Litteratursökning	12
2.2.3 Empiriskt urval	12
2.2.5 Kvalitativa intervjuer	14
2.3 Analys	15
2.4 Etiska överväganden	16
3. Teoretisk referensram	17
3.1 Information och informationssäkerhet	17
3.2 Systematiskt informationssäkerhetsarbete	18
3.2.1 Metodstöd för systematiskt informationssäkerhetsarbete	19
3.3 ISO 27000-serien	20
3.3.1 Ledningssystem och systematiskt arbete samt säkerhetsåtgärder enligt ISO 27000	21
3.4 Infosäkkollen	21
3.5 Informationstillgångar och informationsklassificering	22
3.6 Risk, hot och sårbarheter	22
3.7 Incident och incidenthantering	23
4. Resultat	24
4.1 Cybersäkerhetsexperten	24
4.1.1 Framgångsfaktorer för att arbeta systematiskt	24
4.1.2 Hinder med säkerhetsarbetet	27
4.2 Kommun 1	28
4.2.1 Framgångsfaktorer för att arbeta systematiskt	29
4.2.2 Hinder med säkerhetsarbetet	30
4.3 Kommun 2	31
4.3.1 Framgångsfaktorer för att arbeta systematiskt	31
4.3.2 Hinder med säkerhetsarbetet	33

5. Analys	36
5.2 Framgångsfaktorer för att arbeta systematiskt	36
5.2.1 Riskbedömning	36
5.2.1.1 Genomföra konsekvensbedömning	36
5.2.1.2 Informationssäkerhetskultur	36
5.2.2 Systematisk informationssäkerhetsarbete	37
5.2.2.1 Intern utbildning och regelbundna övningar	37
5.2.2.2 Samverkan och strategi	38
5.2.3 Ramverken för strukturerad informationssäkerhet	38
5.2.4 Erfarenhetsutbyte och riskdiskussion	39
5.3.1 Bristande ledningsstöd och förståelse från ledningen	39
5.3.2 Bristande budgetresurser	40
5.3.2.1 Bristande resursallokering	40
5.3.3 Bristfällig utbildning och kunskapsnivå	40
5.3.4 Brist på systematiskt arbete med riskanalys och kontinuitetshantering	41
5.3.5 Arbetsbelastning	41
6. Diskussion	42
7. Slutsatser	49
7.1 Svar på frågeställningen	49
7.2 Förslag till vidare forskning	50
7.3 Metodreflektion	51
8. Referenser	52
9. Bilagor	
Bilaga 1: Intervjuguide - riktad till kommunerna.	
Bilaga 2: Intervjuguide - cybersäkerhetsexpert	

1. Inledning

1.1 Bakgrund

En jämförelse mellan alla EU-medlemsstater visade att Sverige ligger bland toppen inom digitalisering. En möjliggörare tros vara den digitaliseringsstrategi som antogs av Sveriges riksdag 2017. Syftet med digitaliseringsstrategin är att agera kompass i ledningen mot att nå ett antal beslutade digitaliseringsmål. Strategin syftar även till att, tillsammans med andra strategier, positionera Sverige som världsledande i att utnyttja digitaliseringsmöjligheter. I och med detta finns även en ambition att utforma en offentlig sektor som är digitalt avancerad, rättssäker och tillgänglig (Europeiska kommissionen 2022).

En viktig del av Sveriges funktionalitet är den offentliga sektorn, där digitaliseringen har pågått sedan 1950-talet (Karlsson & Islam 2022). Sveriges offentliga sektor är till stor del skattefinansierad och omfattar statens, regionernas och kommunernas verksamhet. Det är kommunerna som ansvarar för stora delar av den samhällsservice som finns där individerna bor, till exempel äldreomsorg, socialtjänst och grundskola (NE 2024; SKR 2022). I takt med att samhället i stort, både kommuner och andra organisationer, rör sig mot att bli alltmer digitaliserat öppnar detta upp för nya möjligheter samtidigt som det också för med sig fler risker. De ökade riskerna handlar bl.a. om större sårbarhet för att samhället ska bli utsatt för exempelvis hackerattacker av samhällskritisk verksamhet som flera delar av den offentliga sektorn innefattar (Myndigheten för digital förvaltning 2022).

Sverige har sedan länge ett säkerhetsperspektiv med hänsyn till den digitala sfären och har sedan Rysslands invasion av Ukraina vidtagit ytterligare åtgärder för att stärka IT-säkerheten (Europeiska kommissionen 2022). Allt fler svenska kommuner har trots det utsatts för IT-attacker den senaste tiden. En IT-attack mot Kalmar kommun resulterade i att över 7000 lösenord läckte ut i offentligheten. Samtidigt rapporterar andra kommuner som Umeå kommun att det ständigt utförs överbelastningsattacker i syfte att försöka komma in i kommunens system (SVT 2024a, 2024b).

Sveriges kommuner och regioner (SKR) genomförde en enkät i syfte att undersöka hur långt svenska kommuner har kommit i sitt informationssäkerhetsarbete. Utifrån resultaten kan det konstateras att kommunerna har en genomgripande och omfattande insikt i för hur viktigt det systematiska informationssäkerhetsarbete är för att bedriva den fortsatta digitaliseringen. (Sveriges kommuner och regioner 2019).

Leverantörer av samhällsviktiga och digitala tjänster, s.k. NIS-leverantörer, är de organisationer som levererar några av Sveriges viktigaste tjänster för samhällets funktionalitet. Offentliga aktörer räknas som NIS-leverantörer. NIS-regleringen ställer krav på att samtliga NIS-leverantörer bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. Detta ska innefatta arbete med riskanalys och framtagande av åtgärder samt rapportering av eventuella incidenter. Kommunerna utgör därför en central del av samhällets informations- och cybersäkerhet, vilket betonar behovet av att de är säkerhetsmedvetna och agerar för att hantera säkerhetsrisker på ett effektivt sätt (NIT-leverantörers IT-incidenthantering 2022).

Trots tidigare forskning inom området och stora satsningar på offentliga organisationers IT-säkerhetsarbete, visar flera rapporter att svenska kommuner utsätts för olika typer av IT-attacker. (SVT 2024a, 2024b). Undersökningar visar att det sker cirka 400 cyberattacker per vecka mot svenska kommuners digitala system (Europaportalen 2023). Samtidigt beskrivs det säkerhetspolitiska läget i Europa sämre än på länge. Ett systematiskt informationssäkerhetsarbete beskrivs vara avgörande för att skydda sig mot olika typer av IT-hot och attacker. Mot bakgrund av de utmaningar som beskrivs ovan är det därför aktuellt undersöka hur svenska kommuner arbetar med sitt systematiska informationssäkerhetsarbete för att hantera risker, sårbarheter och hot som de står inför.

1.2 Tidigare kunskap

1.2.1 Myndighetsrapporter

I en omfattande studie från SKR (2019) undersöktes informationssäkerhetsarbetet inom svenska kommuner. Syftet var att inte bara stödja kommunerna i deras arbete med uppföljning som är en kritisk del av det systematiska informationssäkerhetsarbetet, utan även att få en bred förståelse för hur arbetet ser ut överlag. Genom att använda en webbenkät gavs kommunerna möjligheten att utvärdera sin egen ståndpunkt när det gäller informationssäkerhet. Resultatet från undersökningen indikerar att de kommuner som deltog har en god förståelse kring hur viktigt det systematiska informationssäkerhetsarbetet är. I samband med detta betonar Sveriges kommuner och regioner (SKR) att målet är att samtliga kommuner som deltog i undersökningen skall arbeta systematiskt med sitt informationssäkerhetsarbete. (ibid.)

Trots att tidigare studier visade på att kommuner skapat en allmänt god förståelse kring hur viktigt det systematiska informationssäkerhetsarbetet är, visade en ny undersökning genomförd av MSB tillsammans med SKR att kommuner är den aktörsgrupp som presterat med svagast resultat i "Infosäkkollen" år 2023. Ett bra resultat i infosäkkollen beskrivs som särskilt viktigt med tanke på att de omfattar noggrant utvalda områden i samband med att infosäkkollen ger en översiktlig bild och betonar hela organisationens systematiska informationssäkerhetsarbete (MSB 2024). I en undersökning som genomfördes med verktyget "Infosäkkollen" år 2021, visar resultatet att kommuner är en av aktörerna som inte når upp till den genomsnittliga nivån vad gäller systematiken i deras informationssäkerhetsarbete. (Digitala Sverige 2023)

I en tidigare undersökning genomförd av SKR (2015) visar att en majoritet av kommunerna arbetar systematiskt med riskanalyser för informationssäkerhet. Trots detta utförs riskanalyser, med jämna intervaller, endast av cirka 2% av kommunerna där lika många har en fastställd metod för att arbeta med riskanalys. I samband med detta lyfts det fram hur kommuner har en utmaning att integrera riskhantering i sina interna processer. (ibid.) I dagsläget saknar ungefär en fjärdedel av svenska kommuner ett verktyg för att arbeta med analys av deras informationssäkerhetsrisker (MSB 2024).

Vidare beskrivs det hur Sveriges kommuner inte har motsvarande informationssäkerhetsföreskrifter i relation till statliga myndigheter, vilket sannolikt har bidragit till större brister inom kommunerna, särskilt avseende informationsklassning och riskanalyser. Denna brist på tydliga riktlinjer och standarder kan vara en utmaning för kommunerna när de strävar efter att förbättra sin informationssäkerhet (MSB 2015).

I dagsläget jobbar typkommunen med att utbilda sin personal inom informationssäkerhet. När utbildning genomförts har inte typkommunen arbetat med att undersöka de anställdas informationssäkerhetsmedvetande, i form av att de vet hur man arbetar på ett informationssäkert sätt (MSB 2024). I samband med detta, har typkommunen de senaste två åren inte följt upp sitt informationssäkerhetsarbete i form av informationsklassning och analyser. Uppföljningen gäller även det systematiska informationssäkerhetsarbetet (ibid.)

MSB (2024) påpekar i sin studie att övning är avgörande för att säkerställa att en kommun vet hur den ska agera i krissituation. Regelbundna övningar inom kommunerna minskar risken för misstag och ineffektivitet under verkliga incident. En kontinuitetsplan som inte regelbundet testas och revideras tenderar att bli föråldrad, eftersom den inte anpassas till förändrade förhållanden, ny teknik eller nya hotbilder. Detta leder till att planen förlorar sin relevans och effektivitet, vilket kan resultera i allvarliga konsekvenser när en kris väl inträffar. (ibid.)

För att öka samverkan och sprida information om aktuella händelser, såsom situationen i Ukraina, har SKR bjudit in IT-ansvariga från kommuner och regioner till ett digitalt samarbetsrum. Där hålls regelbundna träffar för att dela erfarenheter och skapa förutsättningar för ökat samarbete och kunskapsdelning, vilket ytterligare stärker kommunernas förmåga att hantera eventuella kriser och säkerställa informationssäkerheten i en snabbt föränderlig digital miljö (MSB 2024).

1.2.2 Framgångsfaktorer inom informationssäkerhet

Informationssäkerhet definieras som en viktig del med syfte för att skydda en organisation och informationstillgångar samt för att bevara dess värde och rykte. I samband med den ökade användningen av webbaserade teknologier har även antalet säkerhetsshot ökat, vilket ställer krav på att både organisationer och individer använder sig av informationssäkerhet. (AlGhamdi, Tran & Vlahu-Gjorgievska 2020; Safa, Von Solms & Fernell 2016) Informationssäkerhet ligger till grunden för att skydda det primära inom organisationer, vilket är information. En god skyddsnivå inom offentliga organisationer resulterar i att stora ekonomiska kostnader motverkas och att skador på människoliv förebyggs (AlGhamdi, Tran & Vlahu-Gjorgievska 2020).

För att skydda ens informationstillgångar inom organisationen kan det implementeras ett informationssäkerhetssystem, däribland ISO 27000-serien. (Bergquist, Tinet & Gao 2021) Genom att implementera ISO 27000-serien möjliggörs det för organisationer att systematiskt skydda sina informationstillgångar så att de förblir i säkert förvar (Barafort, Mesquida & Mas 2017.). Genom att skydda sina informationstillgångar möjliggörs arbetet med informationsklassificering. Informationsklassificeringen är en integrerad del av informationssäkerhetssystemet (ISMS) där information baseras utifrån ett visst värde med hänsyn till så kallade CIA-triaden. CIA-triaden utgör de centrala aspekterna som ska beaktas inom informationssäkerhet och dessa är konfidentialitet, riktighet och tillgänglighet (Bergquist, Tinet & Gao 2021). Vidare lyfts det fram att informationssäkerhetsklassificeringen utgör en grund för alla aktiviteter inom informationssäkerhet (ibid.)

I samband med höga krav på ett ledningsstöd och utveckling av en säkerhetskultur som de anställda kan förhålla sig till, utvecklas en god informationssäkerhetspolicy. En bra framtagen informationssäkerhetspolicy definieras som en avgörande faktor för att etablera en stark säkerhetskultur inom organisationen. När de anställda har god kunskap om själva informationssäkerhetspolicyen och dess regler kan detta förbättra säkerhetskulturen inom organisationen enligt De Veiga (2016).

För att personalen vidare skall erhålla god kunskap om informationssäkerheten inom organisationen, borde det genomföras en säkerhetsutbildning i syfte att förbättra säkerhetsförmågorna hos de anställda. Säkerhetsutbildningen karaktäriseras i form av ett program som syftar till att utöka personalens kompetens vad gäller exempelvis informationssäkerhetspolicyn inom organisationen. En god och tillräcklig kompetens om informationssäkerheten resulterar i ett mindre antal incidenter. (Pérez-Gonzales, Preciado & Solana-González 2019)

Utöver att observera beteendemönster och attityder hos individerna inom organisationerna, ligger ansvaret på själva ledningen. AlGhamdi, Tran & Vlahu-Gjorgievska (2020) lyfter fram hur engagemang och delaktighet från ledningen är högst avgörande för att successivt kunna utveckla en organisationskultur och säkerhetskultur för informationssäkerhet, vilken medarbetarna kan förhålla sig till. Detta skulle engagera medarbetarna tillräckligt att ständigt arbeta för organisationens skydd. I samband med detta bidrar positiva beteenden hos ledningen och övriga anställda till att förbättra säkerhetsbeteenden inom en organisation, vilket senare resulterar i en god säkerhetskultur. (AlGhamdi, Tran & Vlahu-Gjorgievska 2020; Ali, Dominic, Azhar & Sohail 2021)

Inom en del IT-avdelningar är många aktiviteter relaterade till riskhantering, däribland informationssäkerhet enligt Barafort, Mesquida & Mas (2017). Informationssäkerhetsklassificeringen räknas som den viktigaste tillgången inom riskhanteringen och ses även som en framgångsfaktor i att arbeta med riskanalys inom organisationer. (Bergquist, Tinet & Gao 2021) Riskhanteringen beskrivs som central inom både IT-organisationer och IT-avdelningar (Barafort, Mesquida & Mas 2017). I takt med att man arbetar systematiskt med informationssäkerhet, är riskhanteringen en central aspekt för att möjliggöra detta.

Lista på framgångsfaktorer inom informationssäkerhet:

- Implementering av informationssäkerhetssystem
- Informationsklassificering
- Riskhantering
- Systematiskt säkerhetsarbete
- Förebyggande av säkerhetshot

1.2.3 Hinder inom informationssäkerhet

Människan definieras som den svagaste länken inom informationssäkerhet, enligt Arbansas, Spremic & Zajdela Hrustek (2021). I samband med detta, framkommer det i en global undersökning att brist på kunskap av informationssäkerhet bland människorna är anledningen till varför organisationer inte uppnår effektivitet med sitt informationssäkerhetsarbete. (Somroo, Shah & Ahmed 2014) De anställdas bristande kunskap kring informationssäkerhet kan bero på många anledningar. Främst handlar det om en bristande användarmedverkan när organisationen utvecklar och tar fram säkerhetspraktiker som används, vilket senare resulterar i att säkerhetspraktikerna inte är anpassade till de faktiska behoven. (Flores, Antonsen & Ekstedt 2013)

Vidare lyfts det fram att en majoritet av de informationssäkerhetsincidenter som sker inom en organisation är på grund av mänskliga brister och svagheter. (Somroo, Shah & Ahmed 2014; Khando, Gao, Islam & Salman 2021) Med hänsyn till att människan utmålas som en omfattande orsak till ineffektivitet i organisationers informationssäkerhetsarbete, betonas det starkt hur människan kan vara inblandad i IT-säkerhetsincidenter där det förekommer stöld av information och regelbrott mot åtkomstpolicyn. Detta resulterar i att människans handlingar utgör ett stort hot mot organisationer som arbetar med informationssäkerhet. (Somroo, Shah & Ahmed 2014)

Trots att människan utmålas som en brist inom organisationer, har forskare inom området talat mycket om att det är viktigt att starkt lyfta fram människan när informationssäkerheten inom organisationen utformas. Det görs bland annat genom att kolla på attityder, övertygelser, beteendemönster och kultur hos individerna i fråga, enligt Flores, Antonsen & Ekstedt (2013). Denna typen av perspektiv kallas för beteendemässig informationssäkerhetsforskning. (ibid.) Vad gäller individerna, betonas även ett ökat säkerhetsmedvetande hos de som en viktig framgångsfaktor i att etablera en god informationssäkerhet. (Safa, Von Solms & Fernell 2016)

Bergquist, Tinet & Gao (2021) lyfter fram i sin studie att det är viktigt att öka medvetenheten och kunskapen bland personalen när det gäller informationssäkerhet. Det betonas att utbildning och en gemensam förståelse för begrepp och principer kring informationssäkerhet är avgörande för att säkerställa en enhetlig tillämpning av modellen och därigenom förbättra organisationens övergripande säkerhetskultur. Studiens praktiska implikationer är mångfacetterade. För det första understryker den behovet av att förstå värdet av information och de potentiella konsekvenserna som kan uppstå vid bristande säkerhetsåtgärder. Vidare betonas vikten av att implementera robusta utbildningsprogram och kommunikationsstrategier för att öka medvetenheten och skapa en kultur där informationssäkerhet prioriteras av alla medarbetare, oavsett deras position eller avdelning inom organisationen. (ibid.)

För att tackla de hinder som förekommer med informationssäkerhet krävs det en god balans mellan de organisatoriska, mänskliga och tekniska faktorerna. Somroo, Shah & Ahmed (2014) betonar att tekniska faktorer som förvärv av ny teknik, mänskliga faktorer som anställning av personal med särskild kompetens och organisatoriska faktorer som utveckling av säkerhetspolicy är ledningens ansvar att genomföra inom organisationen. När högsta ledningen visar sitt engagemang kan detta motivera organisationen att ständigt förbättra sig. (ibid.)

Trots det ständiga arbetet med bland annat tekniska lösningar för att förhindra sin organisation att bli utsatt lyckas hackers ständigt hitta nya sätt att attackera sina mål, beskriver Flores, Antonsen & Ekstedt (2013). Problemen uppstår på grund av flera faktorer, inklusive bristande medvetenhet om informationssäkerhet bland anställda, otillräcklig utbildning samt bristfällig arbetslag och team. Dessa faktorer utgör betydande hot mot organisationers informationssäkerhet och kan leda till olika former av incidenter och risker enligt Arbansas, Spremic & Zajdela Hrustek (2021).

I takt med detta redogörs ett bristande ledningsstöd i samband med begränsade budgetar som två andra huvudsakliga hinder för att uppnå effektivitet med sitt informationssäkerhetsarbete. Dessa utgör allvarliga hot mot organisationers förmåga att skydda sin information och hantera säkerhetsrisker på ett effektivt sätt (Somroo, Shah & Ahmed 2014).

Lista på hinder inom informationssäkerhet:

- Mänskliga fel och svagheter
- Bristande ledningsstöd
- Begränsade budgetar
- Bristfällig utbildning
- Tekniska utmaningar

1.3 Problemdiskussion

Utifrån de tidigare undersökningar som genomförts kring svenska kommuner kan det konstateras att trots den allmänt goda förståelsen kring hur viktigt det systematiska informationssäkerhetsarbetet är, tillkommer det än idag utmaningar där systematiken behöver förbättras (SKR 2019; MSB 2024). I takt med detta ökar även antalet hot och risker, vilket ställer större krav på att svenska kommuner behöver arbeta allt mer systematiskt med deras informationssäkerhet. I samband med detta framgår det att endast en liten del av kommunerna genomför regelbundna riskanalyser, vilket indikerar att de lättare kan bli utsatta för både hot och sårbarheter (SKR 2015).

I samband med detta har informationssäkerhet blivit en central aspekt för organisationer inom den offentliga sektorn, med tanke på de ökade riskerna i samband med att användningen av webbaserade teknologier har ökat avsevärt (Safa, Von Solms & Fernell 2016). Detta mynnar ut i att organisationer blir allt mer desperata av att ta till åtgärder för att systematiskt anpassa sitt informationssäkerhetsarbete, vilket möjliggörs genom att använda sig av en del verktyg och metoder, exempelvis att arbeta med riskhantering. Dessvärre indikerar en undersökning att enbart 25% av svenska kommuner i dagsläget har ett etablerat verktyg för riskanalys (MSB 2024).

Utifrån en studie genomförd av MSB (2024) visar studiens resultat att kommuner är den allra mest sårbara aktörsgruppen, i relation till regioner och offentlig förvaltning. I samband med detta visar den allra första undersökningen som genomförts med användning av metodstödet att kommuner i allmänhet inte når upp till den genomsnittliga nivån vad gäller deras informationssäkerhetsarbete. Trots tidigare forskning kring hur kommuner jobbar med informationssäkerhet, återstår det än idag en problematik med kommuners systematiska informationssäkerhetsarbete (MSB 2024; Digitala Sverige 2022).

I synnerhet består organisationer idag till stor del av människor där även kommuner är involverade. Tidigare forskning lyfter fram hur den mänskliga faktorn är väldigt kritisk med tanke på att mycket av det ineffektiva informationssäkerhetsarbetet är ett resultat av bristande kompetens hos människor (Somroo, Shah & Ahmed 2014; Khando, Gao, Islam & Salman 2021). Genom en undersökning riktad mot kommuner och involverade aktörer inom organisationen avser forskarna att identifiera faktorer som bidrar till bristande kunskap, genom att analysera beteenden och orsaker till kunskapsbristen (Flores, Antonsen & Ekstedt 2013).

Den brist på fokus och resurser som beskrivs återspeglar den aktuella utmaningen kring informationssäkerhetsarbete inom svenska kommuner och betonar behovet av att utöka den befintliga forskningen inom området. För att bättre förstå de underliggande orsakerna till dessa brister är det nödvändigt att genomföra djupgående studier, vilket kan leda till identifiering av potentiella lösningar som stärker skyddet av viktig information inom offentlig

sektor (MSB 2015). En analysrapport från MSB (2016) visar att en betydande del av Sveriges kommuner på grund av budgetbegränsningar inte kan bedriva ett tillfredsställande arbete med informationssäkerhet. Intresset för informationssäkerhet får inte tillräcklig uppmärksamhet, vilket ofta inte märks förrän riskerna för incidenter når en kritisk nivå (SKR 2019).

Problemet som studerats har formulerats som att svenska kommuner i dagsläget fortfarande har problem med att strukturera och arbeta med sitt informationssäkerhetsarbete. Tidigare rapporter understryker att kommuner behöver ökade resurser och stöd för att effektivt hantera hot och sårbarheter på ett systematiskt sätt. Trots detta visar nya undersökningar genomförda av SKR och MSB att det fortfarande finns brister med kommuners systematiska informationssäkerhetsarbete.

Mot bakgrund av detta väcks ett behov för att undersöka hur kommuner arbetar systematiskt med sitt informationssäkerhetsarbete. Genom att identifiera aktuella framgångsfaktorer och hinder hos andra kommuner kan denna undersökning bidra till att stärka kommunernas förmåga att hantera informationssäkerhetsutmaningar på ett mer strukturerat och resurseffektivt sätt.

1.4 Syfte och forskningsfråga

Syftet med studien var att fördjupa förståelsen för vilka faktorer det är som påverkar det systematiska informationssäkerhetsarbetet hos små och medelstora kommuner där vi vill förstå hur enskilda individer uppfattar informationssäkerhetsarbete. I dagsläget finns det redan existerande forskning kring hur kommuner systematiskt hanterar sitt informationssäkerhetsarbete i relation till flera aspekter.

Målet med genomförandet av studien var att utöka den befintliga forskningen genom att komplettera kring vilka framgångsfaktorer och hinder som påverkar hur svenska kommuner systematiskt hanterar sitt informationssäkerhetsarbete. Studiens primära mål grundade sig på frågeställningen vilken definieras som följande:

- *Vilka framgångsfaktorer och hinder påverkar små och medelstora svenska kommuners systematiska informationssäkerhetsarbete?*

1.5 Målgruppen

Undersökningsstudien ämnar sig främst till de kommuner som idag har svårigheter med att systematiskt anpassa sitt informationssäkerhetsarbete. Tanken var även att involvera individer som arbetar inom den offentliga sektorn, oberoende på om det är en kommun eller region, med inriktning på informations-, och cybersäkerhetsnivån. Genom undersökningens genomförande och resultat strävar forskarna efter att öka studenternas intresse för informationssäkerhet som ett relevant område, med en framtida ambition att vidareutveckla den befintliga forskningen inom den offentliga sektorn.

2. Metod

Detta avsnitt syftar till att redogöra för de tillvägagångssätt som användes vid val av metodansats, datainsamlingsmetod, empiriskt urval och intervjuer som används för genomförande, dokumentation och analys av insamlad data.

2.1 Forskningsansats

Denna undersökning genomfördes med en explorativ studie i syfte att undersöka de framgångsfaktorer och hinder som påverkar det systematiska informationssäkerhetsarbetet hos svenska kommuner. Valet av en explorativ studie lämpade sig för denna studie med tanke på att det möjliggjorde en djupare insikt kring forskningsämnet, vilket därmed har producerat ny kunskap i det kommunala informationssäkerhetsarbetet. Med användning av en explorativ studie har forskarna i undersökningen skapat en mer förståelse kring informationssäkerhetsarbete hos kommuner och även bidragit till framtida forskning.

För att möjliggöra detta har undersökarna genomfört intervjuer i form av öppna frågor. Öppna frågor ansågs vara fördelaktiga inom forskningen då de gav informanten möjlighet att utförligt besvara frågorna utan att begränsas av förutbestämda svarsalternativ, till skillnad från enkätundersökningar (David, Parker & Straum, 2012). Vidare uppfattades en bra kvalitativ undersökning som relevant, aktuell, betydelsefull eller tankeväckande (Sarah J. Tracy 2010). Undersökningsämnet i fråga handlar om informationssäkerhet, vilket i dagsläget är väldigt relevant och aktuellt, med tanke på senaste tidens IT-attacker mot svenska kommuner.

Användning av en kvalitativ metodansats ledde till oväntade svar, vilket motiverar användningen av en kvalitativ metodansats att undersöka ämnet mer ingående genom att ställa följdfrågor till de svar som ges. I samband med detta kan en kvalitativ metodansats skapa goda förutsättningar för att ge insikt till att öppna 'den svarta lådan' hos organisatoriska processer vilket möjliggörs genom att intervjua anställda inom organisationen (Azungah 2018). En kvalitativ metodansats var rimlig att genomföra med tanke på att forskarna var intresserade kring hur den enskilde informanten tolkar ett specifikt fenomen (Jacobsen 2017, s. 98 - 99)

2.2 Datainsamlingsmetod

2.2.1 Dokumentanalys

En del av undersökningen tog del i att noggrant analysera de informationssäkerhetspolicier och riktlinjer som respektive kommun tillhandahåller. En analys av informationssäkerhetspolicier och riktlinjer utformade en bra grund kring hur varje kommun arbetar för att därmed se skillnader och likheter i både arbetsätt och riktlinjer. En av kommunerna påpekade dock att deras tillgängliga informationssäkerhetspolicy var utdaterad och att de i dagsläget håller på att utforma en ny policy. Informationssäkerhetspolicyn för respektive kommun fanns tillgängliga på internet med tanke på att de var öppna för

allmänheten. Dokumentanalys fungerade som en grund till att skapa intervjufrågor där undersökarna i förhand ville skapa sig en bild kring hur kommunen arbetar övergripande med sitt informationssäkerhetsarbete genom att analysera kommunernas informationssäkerhetspolicy.

2.2.2 Litteratursökning

För inhämtning av vetenskapliga artiklar och rapporter samt annat material, användes två olika databaser. Sökningar genomfördes för att få fram relevant dataunderlag till tidigare forskning och området som studien bedrivs i. Inhämningen av material utgick främst från Primo, där endast peer-reviewed källor inkluderades. Detta för att säkerställa att forskningen enbart använder sig av granskade och verifierade källor, vilket stärker tilliten till underlaget i den tidigare forskningen. En annan databas som kommit till användning är Diva Portal, där äldre studentuppsatser och undersökningar har framkommit i sökningarna. I form av andra källor har det även använts ResearchGate. Utöver vetenskapliga databaser har undersökarna använt sig av ett antal hemsidor kopplade till informationssäkerhetsarbetet, exempelvis MSB, SKR och Europeiska kommissionen.

Undersökningen har fokuserat på ett antal sökord i databasen Primo och ser ut som följande:

- Information Security
- Information Security management
- Information Security: Challenges (utökad sökning)
- Information Security municipalities
- Informationssäkerhet: Kommun (utökad sökning)
- Information Security: Responsibility (utökad sökning)

Utifrån dessa sökord i databasen Primo resulterade det i ett flertal vetenskapliga artiklar, varav många av dem ansågs som väldigt relevanta att använda för att fylla ut tidigare forskning. I vissa sökord har det använts booleska operatorer, det vill säga utökad sökning med både AND och OR. Många av artiklarna har även använts i andra delar av arbetet. Med användning av sökord kan man få en träffsäker sökningsstrategi med relevanta artiklar inom området (Polit & Beck 2017).

2.2.3 Empiriskt urval

Ett urval av informanter gjordes baserat på deras roll som är kopplad till kommunalt informationssäkerhetsarbete. Informanterna bestod av individer som arbetar i kommuner med olika kommungruppsindelningar samt befolkningsstorlek och en individ som arbetar mot offentlig sektor med att stödja kommuner i deras informationssäkerhetsarbete. Det har genomförts en intervju med vardera informant. Totalt har det genomförts tre intervjuer med tre informanter. En sammanställning av informanterna gjordes i form av arbetstjänst, intervjuformat, datum när intervjuer genomfördes samt kommungruppsindelning för respektive kommun. (Se tabell 1)

Informant	Arbets tjänst	Intervjuformat	Datum
Kommun 1	Informationssäkerhetssamordnare SKR kommungruppsindelning: C	Personlig intervju	2024-04-24
Kommun 2	Informationssäkerhetssamordnare SKR kommungruppsindelning: B	Personlig intervju	2024-04-29
Förening 1	Cybersäkerhetsexpert	Personlig intervju	2024-05-02

Tabell 1: Lista över informanter

Urval av kommuner begränsades till två kommuner och en cybersäkerhetsexpert med hänsyn till omfattning av empiri. Med en begränsning till två kommuner och en cybersäkerhetsexpert kan intervjuer med respektive kommun och cybersäkerhetsexpert genomföras, mängden data från både teori och transkriberade intervjuer analyseras samt redogöras. Från början var tanken att kommuner väljs ut med hänsyn till kommungruppsindelningen enligt SKR och storlekarna i fråga, närmare bestämt A, B och C. I den utsträckningen hade undersökningen skapat en generaliserbarhet kring hur en liten kommun, en medelstor kommun och en stor kommun systematiskt hanterar sitt informationssäkerhetsarbete.

Vi kontaktade 20 större kommuner och fick svar från respektive kommun att de inte kunde ställa upp som informanter i undersökningen med anledning av tidsbrist. De kommuner som ställde upp som informanter, mer specifikt en medelstor kommun från grupp B och en liten kommun från grupp C, har båda en informationssäkerhetssamordnare (CISO) som arbetar med informationssäkerhetsarbetet inom kommunerna. I samband med detta har det genomförts en intervju med en cybersäkerhetsexpert som arbetar med frågor kring det kommunala informationssäkerhetsarbetet med syfte i att skapa en förståelse över hur det systematiska informationssäkerhetsarbetet ser ut hos svenska kommuner överlag.

Anledningen till att det förhöll sig till informationssäkerhetssamordnare i kommuner och en cybersäkerhetsexpert är för att de ses som informanter: de har direkt kännedom om ett fenomen, med andra ord besitter de kunskap om fenomenet som skall undersökas. Studien har även utgått från de olika stegen som finns i urvalsprocessen för att på ett smidigt sätt undersöka fenomenet i fråga. Utifrån urvalskriteriet information valde forskarna ut informanter som ansågs vara relevanta för undersökningen, det vill säga fokusera på personer som besitter bra kunskaper om det som forskarna är intresserade av att undersöka (Jacobsen 2017, s. 119 - 120). Kontakt med kommuner gjordes både via e-mail och telefonnummer.

2.2.5 Kvalitativa intervjuer

Metodvalet har specifikt grundats på semistrukturerade intervjuer. Med användning av semi-strukturerade intervjuer har forskarna utformat en uppsättning frågor för att säkerställa att området täcks med relevanta svar. Intervjuerna spelades in med deltagarnas samtycke i syfte för att senare analysera och transkribera intervjuerna. Intervjufrågorna har utformats med målet att få en omfattande och detaljerad bild av kommunernas arbete med informationssäkerhet. Fokus har legat på att undersöka centrala aspekter av det systematiska informationssäkerhetsarbetet, inklusive riskhantering, upphandling och kontinuitetshantering.

Med användning av semi-strukturerade intervjuer kunde forskarna följa upp med ytterligare frågor baserat på informanternas svar. Detta möjliggör en interaktion och dialog mellan forskare och informanter, för att ge mer utrymme för öppna dialoger och därmed gå på djupet kring fenomenet i fråga (Pietilä, Johnson & Kangasniemi 2016). Semistrukturerade intervjuer har möjliggjort för de intervjuade att dela med sig av sina erfarenheter och kunskaper. I jämförelse med enkäter som har ett förutbestämt urval av svarsalternativ, beskriver Magnusson & Marecek (2015).

Med användning av semi-strukturerade intervjuer kunde frågorna anpassas när det gäller komplexitet och öppenhet för att möta olika människors kunskapsnivå och förutsättningar. (Magnusson & Marecek, 2015). I förhand har det utformats två stycken intervjuguide med relevanta frågor som är kopplade till tidigare forskning inom området (Bilaga 1, Bilaga 2), där tanken var att huvudfrågorna skulle följa en fast ordningsföljd och enbart öppna svar med syfte till att ge informanten chansen att yttra sig fritt (Pietilä, Johnson & Kangasniemi 2016; Jacobsen 2017, s. 99 - 102).

Undersökningsstudien har enbart fokuserat på användning av digitala intervjuer, med hänsyn till att undvika kostnader för resor och att beakta informanternas tidsbrist för fysiska möten. Med användning av digitala intervjuer kunde forskarna därmed få kontakt med informanter som inte befinner sig i dess närhet utan begränsningar på en specifik och geografisk plats (Thunberg & Arnell 2022).

Digitala intervjuer gav även goda förutsättningar genom att undersökarna kan anpassa sig efter informanter i form av flexibilitet vid mån av tid i samband med att genomföra intervjuer i en miljö där de känner sig avslappnade. Detta möjliggjorde för informanterna att känna sig mer bekväma med att berätta om sina upplevelser och sitt perspektiv kring det specifika fenomenet. Vidare kan digitala intervjuer möjliggöra för enkel och bekväm inspelning av intervjuerna, där en inspelning av intervjuerna kan resultera i att forskarna noggrant kan analysera och återanvända informationen som framkommer i inspelningen vid behov. Detta underlättar för både tolkning och referens i själva skrivprocessen. (ibid.)

2.3 Analys

När följande intervjuer har genomförts med informanterna i undersökningen, har forskarna i studien genomfört en analys av det insamlade materialet från intervjuerna. Forskarna har med användning av ett iterativt tillvägagångssätt, där man förbättrar och fördjupar arbetet genom att återkomma till olika delar kontinuerligt, och en tydlig observation kunnat identifiera tematiska mönster som framträder i datan som transkriberats. De tematiska mönster som upptäckts i denna undersökning har kunnat säkerställas med användning av en tematisk analys, vilket har resulterat i att undersökarna därmed kunnat identifiera och analysera tematiska mönster som förekom i intervjuerna som transkriberats (Galetta & E. Cross 2013; Clarke & Braun 2018).

Intervjuerna har dokumenterats genom att transkribera ljud från en videoinspelning med undersökningsdeltagarna i studien. Transkriberingar har resulterat i en mer fördjupning kring informationernas upplevelser kring fenomenet i fråga, vilket har utökats genom att återigen granska transkriberingarna för att säkerställa en noggrannhet i själva dokumentationen av intervjuerna. När samtliga intervjuer har transkriberats, intervjuerna delades upp i olika teman. Därmed kategoriserades transkriberade datan, där varje segment placerades under relevanta teman. Denna kategorisering baserades både på frågan som ställdes och på svaren som gavs av informanter. Processen av kategoriseringen inleddes genom att använda en av intervjuerna som utgångspunkt. Från frågorna och svaren i denna intervju skapades en preliminär mall som visade vilka teman som behövde skapas. Därefter, upprepades processen med de övriga intervjuerna, med några få tillägg och förändringar baserat på den nya datan. Detta resulterade i en strukturerad dataset där informanter enkelt kunde hittas och analyseras för att utvinna insikter och mönster. Denna granskningen har resulterat i en god tolkning av den insamlade datan och som tidigare nämnt, en uppdelning av en mängd uppenbara teman som är väsentliga för den forskningsfråga som bedrivs i denna studie (Galetta & E. Cross 2013).

När kategoriseringen av datan var klar, påbörjades skrivandet av den samlade datan från intervjuerna i avsnitt 4.0 "*Resultat*". Detta avsnitt bygger helt och hållet på informationen från de olika intervjuerna som är indelad i 3 delar för båda kommunerna och cybersäkerhetsexperten. Denna presentation av informationen framställde endast informationen som den är utan att göra någon form av analys, diskussion eller slutsats. Istället förbehålls analysen av den presenterade datan för avsnitt 5.0 *Analys*. I detta avsnitt gjordes en analys och tolkning av den empiriska datan. I avsnitt 6.0 *Diskussion* genomfördes en diskussion kring den analyserade datan utifrån den teoretiska referensramen och tidigare forskning som presenteras i avsnitt 3.0 "*Teoretisk referensram*" samt 1.2 "*Tidigare forskning*". Detta gjordes för att skapa djupare förståelse och analys av den systematiska informationssäkerhetsarbetet baserat på en teoretisk grund.

2.4 Etiska överväganden

Undersökarna har grundat studiens etik utifrån de forskningsetiska principerna, vilka syftar till att etablera ett förhållande mellan forskarna och undersökningsdeltagarna. Forskningsprinciperna har även använts som en grund och vägledning för att genomföra forskningsstudien. De forskningsetiska principerna karaktäriserades även som fyra huvudkrav, vilka benämns som *informationskravet*, *samtyckeskravet*, *konfidentialitetskravet* och *nyttjandekravet* (Vetenskapsrådet 2002, s. 6).

Forskarna har utifrån *informationskravet* informerat undersökningsdeltagarna inledningsvis kring studien i början av intervjuerna och dess syfte. Det har även förtydligats att deltagandet är helt valfritt och att undersökningsdeltagarna kan avbryta sin medverkan när de vill. (Vetenskapsrådet 2002, s. 7) I enlighet med *samtyckeskravet* har undersökningsdeltagarna en möjlighet att själva bestämma om de vill delta i studien, där de skall kunna avbryta sitt deltagande, exempelvis mitt under intervjun, med omedelbar verkan. (Vetenskapsrådet 2002, s. 7)

Vad gäller *konfidentialitetskravet*, var undersökarna i studien väldigt måna om att skydda undersökningsdeltagarnas personuppgifter på ett sådant sätt där ingen kan ta del av dem. Konfidentialitetskravet kräver därmed anonymiserade uppgifter (Vetenskapsrådet 2002, s. 12) I samband med detta har en muntlig överenskommelse träffats gällande undersökningsdeltagarnas känsliga uppgifter, vilket resulterat i anonymisering av respektive kommun och cybersäkerhetsexpert. Med tillämpning av *nyttjandekravet* har undersökarna enbart använts undersökningsdeltagarnas uppgifter för forskningsändamål (Vetenskapsrådet 2002, s. 14).

3. Teoretisk referensram

Detta avsnitt beskriver de olika delarna av studiens ramverk för att erbjuda en omfattande och strukturerad förståelse av informationssäkerhets olika aspekter. Dessa teorier tillsammans täcker både grundläggande och avancerade koncept inom systematiskt informationssäkerhetsarbete, vilket ger en solid teoretisk bas för att analysera och förstå de komplexa utmaningar och framgångsfaktorer som kommuner möter i dagens digitala miljö.

3.1 Information och informationssäkerhet

Information är något som förekommer i nästan alla organisationer och kan anta olika former. Det kan vara något konkret och fysiskt, såsom löneinformation för varje anställd, eller mer abstrakt, som kunskapen om en viss process inom organisation. Denna information kan vara strukturerad och formaliserad i exempelvis tydliga kolumner i en databas, eller icke formaliserad såsom lösa anteckningar eller innehåll på whiteboards. Oavsett formen för informationen är det av yttersta vikt att säkerställa dess integritet, konfidentialitet och tillgänglighet för att skydda den mot hot, skador och obehörig åtkomst (Oscarson, 2019). Detta är det övergripande syftet med informationssäkerhet, vilket strävar efter att etablera och upprätthålla ett tillförlitligt ramverk för hantering och skydd av informationstillgångar inom organisationen (Svenska institutet för standarder, u.å).

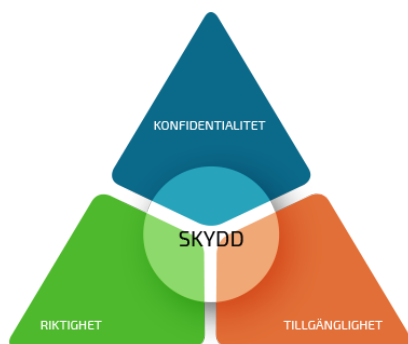
Information betraktas som den viktigaste tillgången i organisationer idag, där själva skyddet av tillgångarna beskrivs som informationssäkerhet (Bergquist, Tinetti, Gao 2021). I dagens samhälle klassas informationssäkerhet som en kritisk aspekt för organisationer med syfte för att skydda deras känsliga information mot obehörigt avslöjande sedan digitaliseringen fått sin fortskridning i samhället. (Safa & Von Solms 2016) Informationssäkerhet som aspekt beskrivs idag som ett väldigt högaktuellt område, med tanke på den omfattande expansionen som olika nätverk har fått i takt med den snabba digitaliseringen. Expansionen har bland annat bidragit med att organisationer lättare utsätts för ökade hot, sårbarheter, risker och säkerhetsattacker (Arbansas, Spremic & Zajdela Hrustek 2021).

Informationssäkerhet handlar om att skydda information från att läckas, förvanskas eller förstöras. Det handlar också om att information är tillgänglig för behöriga personer vid rätt tillfälle. I dagens digitala värld är information lika viktig som andra resurser för organisationer. Vi använder information för att kommunicera, lagra data, bearbeta och styra olika processer. Vissa typer av information är särskilt värdefulla och kan vara avgörande för organisationernas funktion och till och med för människors liv. Det kan vara allt från medicinska journaler till viktiga dokument för företag eller offentliga institutioner (MSB 2024).

Informationssäkerhet syftar till att säkerställa att viktig information är tillgänglig när den behövs, att den är korrekt och opåverkad av manipulation, samt att endast behöriga personer har åtkomst till den. Genom att anpassa skyddet efter behoven kan vi säkerställa att det är tillräckligt effektivt utan att vara för komplicerat eller kostsamt. Brister i hanteringen av information kan leda till minskat förtroende för tjänster och organisationer, och allvarliga eller upprepade incidenter kan orsaka förtroendekriser som sprider sig till andra aktörer och sektorer. I grund och botten handlar informationssäkerhet om att bevara förtroendet för våra

system och tjänster genom att säkerställa att informationen hanteras på ett tillförlitligt och säkert sätt. (ibid.)

Informationssäkerhet handlar om att säkerställa att informationen är konfidentiell, korrekt och tillgänglig, vilket ofta förkortas som CIA-triaden (se figur 1.1). Konfidentialitet innebär att information som inte ska vara tillgänglig för obehöriga inte avslöjas. Riktighet betyder att informationen inte ändras av någon som inte har rättigheter att göra det. Tillgänglighet innebär att informationen är tillgänglig när den behövs för ett system eller en användare. Dessa tre aspekter utgör kärnan i CIA-triaden genom att säkerställa att informationen hanteras på ett säkert och tillförlitligt sätt (Hunstad, Valassi & Lindahl 2018).



Figur 1.1: Belysande exempel av CIA-triaden. (Safestate u.å)

3.2 Systematiskt informationssäkerhetsarbete

Vid arbetet med att hantera sin informationssäkerhet systematiskt innebär det att implementera och upprätthålla administrativa regler som policys och riktlinjer, tekniska skydd såsom brandväggar och kryptering, samt fysiska skyddsåtgärder som skal- och brandskydd. Syftet med att arbeta systematiskt med sin informationssäkerhet är att skapa en övergripande strategi för att säkerställa att organisationens information skyddas på ett effektivt sätt på lång sikt. Organisationer som arbetar systematiskt och baserat på risker inom informationssäkerhet drar nytta av sin information på ett mer effektivt sätt och kan undvika onödiga kostnader för överdrivet skydd. Dessutom minskar risken för oönskade händelser som kan leda till negativa konsekvenser för informationshanteringen (MSB 2024).

Att bedriva systematiskt arbete inom informationssäkerhet innebär att följa en förutbestämd ordning för att identifiera vilken information som är kritisk och sedan implementera lämpliga säkerhetsåtgärder för att skydda den. Det är en metodisk process som säkerställer att organisationen tar de nödvändiga stegen för att hantera och skydda sin information på ett effektivt sätt (MSB). Det första steget innefattar en nulägesanalys som fungerar som bas för utformningen av ett informationssäkerhetssystem. Därefter implementeras och används detta system. Periodiska utvärderingar genomförs regelbundet för att identifiera förbättringsområden och genomföra nödvändiga uppdateringar. I systematiskt informationssäkerhetssystem uppföljningar och uppdateringar utgör en kontinuerlig och återkommande aktivitet (ibid.).

3.2.1 Metodstöd för systematiskt informationssäkerhetsarbete

MSB:s metod riktar sig till organisationer som jobbar med systematiskt informationssäkerhetsarbete, oavsett storlek eller verksamhetsområde. Syftet med själva metodstödet är att stödja organisationer i att komma igång med sitt systematiska informationssäkerhetsarbete. Metodstödet vänder sig både till organisationer som befinner sig i startfasen av sitt systematiska informationssäkerhetsarbete, samt också de organisationer som redan kommit en bit in i sitt informationssäkerhetsarbete (Informationssäkerhet 2018).

Själva metodstödet bygger på ISO 27001-standarden, som är ett ledningssystem för informationssäkerhet (LIS). Metodstödet beskriver hur tillhörande komponenter i ledningssystemet för informationssäkerhet kan utformas där det betonas att informationssäkerhet är en avgörande del i att upprätthålla och ge rätt skydd åt information och omfattar konfidentialitet, riktighet och tillgänglighet (Metodstöd för systematiskt informationssäkerhetsarbete 2021, s. 4-5).



Figur 1.2: Belysande exempel av metodstödet. (Informationssäkerhet.se, 2017)

Metodstödet är uppdelat i fyra metodsteg, se figur 1.2:

Identifiera och analysera. Genom att arbeta med identifiering och analys kan organisationen i fråga anpassa sitt tillvägagångssätt för informationssäkerhet. Detta kan göras genom att genomföra specifika analyser av både den externa miljön samt också den interna verksamheten i syfte att förstå nuvarande situation och även de faktorer som påverkar organisationen. De analyser som genomförs är verksamhetsanalys, omvärldsanalys, riskanalys och gapanalys. Resultaten av dessa analyser kommer att utgöra grunden för utformningen av organisationens tillvägagångssätt med arbetet för informationssäkerhet inklusive de olika styrdokument som ingår, däribland policies, riktlinjer och andra instruktioner (Metodstöd för systematiskt informationssäkerhetsarbete 2021, s. 8).

Utforma. I detta steg utformas de mest centrala komponenterna för organisationens systematiska informationssäkerhetsarbete. Det är även viktigt att genomföra analyser av organisationen, informationssäkerhetsmål, styrdokument, klassningsmodell och handlingsplan. (Metodstöd för systematiskt informationssäkerhetsarbete 2021, s. 13)

Använda. I steget “använda” implementerar organisationen den utformade styrningen av det systematiska informationssäkerhetsarbetet, där man utformar en klassningsmodell, i samband med genomförande och säkerställande av efterlevnad samt utbildar och kommunicerar. Vad gäller klassningsmodell handlar det om hur man klassar information inom organisationen. Genomförande och efterlevnad handlar om att hitta en balans mellan planerade aktiviteter och frågor i samband med att man har en CISO som säkerställer en efterlevnad av att styra och koordinera informationssäkerhetsarbetet. Utbildning och kommunikation handlar om att säkerställa kompetens om informationssäkerhetsarbetet bland anställda genom att tillämpa kontinuerlig utbildning och kommunikation (Metodstöd för systematiskt informationssäkerhetsarbete 2021, s. 18-20).

Följa upp och förbättra. I det sista steget i metodstödet handlar det om att ständigt följa upp och förbättra informationssäkerhetsarbetet samt dess styrning i organisationen. Genom att följa upp och förbättra arbetar man främst med att utvärdera i form av att mäta det systematiska informationssäkerhetsarbetet, riskhanteringsarbetet samt för att säkerställa om alla beslutade säkerhetsåtgärder är utformade ändamålsenligt och fungerar. Detta kan stödja organisationen i att bland annat tidigt upptäcka brister som behöver förbättras och även få en översiktlig bild över hur informationssäkerhetsläget ser ut just nu. I takt med detta har man även en genomgång av ledningen för att säkerställa att det systematiska informationssäkerhetsarbetet är lämpligt, tillräckligt och har en avsedd effekt (Metodstöd för systematiskt informationssäkerhetsarbete 2021, s. 22-23).

3.3 ISO 27000-serien

I dagens samhälle omfattas och består alltmer organisationer av information där syftet är att utbyta information. Vi som samhälle och individer behöver därför ha ett förtroende till att information som lagras även hanteras på ett korrekt sätt för att undvika manipulation och förstörelse av den data som finns lagrad. Med användning av ISO 27000-serien, som erbjuder en ram, kan man säkerställa att informationen behandlas på ett korrekt och säkert sätt, både inom organisationer och samhället i stort. ISO 27000-serien lägger sitt huvudsakliga fokus på att skydda information där cybersäkerhet och dataskydd även ingår, vilka är utvecklade av experter inom ISO och SIS (SIS u.å.).

Serien omfattar även olika typer av ledningssystemstandarder för att främja ett systematiskt arbetssätt och vägledningsstandarder för att implementera olika typer av säkerhetsåtgärder. Genom att tillämpa ISO 27000-serien kan organisationer systematiskt hantera sina processer och säkerställa att lämpliga säkerhetsåtgärder implementeras. När en organisation certifieras enligt ISO 27001 innebär det att organisationen i fråga har ett ledningssystem som uppfyller ISO-standardens krav på att systemet är en integrerad del av organisationens dagliga verksamhet. Vidare behöver systemet kontinuerlig förbättring och granskning av systemet samt ett uttalande som specificerar de säkerhetsåtgärder som inkluderas i certifieringen. Sammanfattningsvis kan ISO-standarderna implementeras av organisationer för att säkerställa en effektiv hantering av information och skydd mot olika risker som finns, däribland sårbarheter, hot och liknande (SIS u.å.).

3.3.1 Ledningssystem och systematiskt arbete samt säkerhetsåtgärder enligt ISO 27000

Systematiskt arbete enligt ISO 27000-serien innebär att en organisation strukturerat anpassar sitt säkerhetsarbete till sin unika situation och följer upp det som en del av sin övergripande verksamhetsstyrning, med ledningens engagemang. Implementeringen av ett ledningssystem för informationssäkerhet är individuell och influeras av faktorer som organisationens storlek, verksamhetsområde, lagar, kontraktskrav och säkerhetsnivå. Det inkluderar att identifiera krav och förväntningar, etablera en riskhanteringsprocess, implementera lämpliga säkerhetsåtgärder baserade på identifierade risker för att skydda information och processer från skada, samt ha kontroll över incidenter och avvikelser genom internrevisioner och mätningar. Ledningen deltar aktivt i att fatta beslut om förbättringar med regelbunden uppföljning. SIS erbjuder fördjupningsutbildningar för att stödja organisationer i införandet och arbetet enligt ISO 27000, med fokus på att realisera nyttan när systematiken är på plats. Genom det systematiska tillvägagångssättet enligt ISO/IEC 27001 kan organisationer applicera säkerhetsåtgärder baserat på risker och kontinuerligt följa upp och förbättra dem. Säkerhetsåtgärderna utgör själva grundbulten för att skydda organisationens tillgångar (SIS u.å.).

3.4 Infosäkkollen

För att skydda digitala system har MSB, myndigheten för samhällsskydd och beredskap, tagit fram en uppföljningsmodell kallad infosäkkollen. Infosäkkollen är en modell som används för att mäta en organisations systematiska informationssäkerhets- och cybersäkerhetsarbete. Infosäkkollen ger en översiktlig bild över hur verkligheten ser ut hos en viss organisation på en *ungefärlig* (approx.) nivå (MSB 2024). Infosäkkollen används som ett metodstöd av organisationer, däribland kommuner, i syfte för att mäta informations- och cybersäkerhetsarbetet inom deras organisation. (ibid.)

Infosäkkollen är konstruerad med bas i MSB:s (Myndigheten för samhällsskydd och beredskap) riktlinjer och stöd, vilka i sin tur utgår från ISO/IEC 27000-serien. Denna verktygslåda syftar till att underlätta strategisk uppföljning och efter genomförande av analysen med Infosäkkollen presenteras resultatet för att utvärdera organisationens grad av systematiskt informationssäkerhetsarbete. Genom användning av Infosäkkollen erhåller organisationen återkoppling angående dess nuvarande nivå samt identifierar områden för framtida utveckling och fokus (MSB 2024).

3.5 Informationstillgångar och informationsklassificering

Informationstillgångar definieras av både information samt de resurser som hanterar informationen. Resurserna består av olika slag i form av datorer, IT-system och databaser (Informationssäkerhet u.å.). Begreppet informationsklassificering handlar om att identifiera viktiga informationstillgångar och därmed värdera dessa utifrån en viss säkerhetsnivå för att sedan implementera säkerhetsåtgärder (Bergström, Åhlfeldt & Anteryd 2016).

Krisberedskapen i kommuner varierar och en viktig del av detta är att säkerställa informationssäkerhet, särskilt inom socialtjänsten. För att stödja kommuner i detta erbjuder SKR verktyget KLASSA, där kommuner kan göra informationsklassningar. Dessa klassningar resulterar i tydliga krav som bör integreras både i upphandling och förvaltning av digitala lösningar inom välfärdsteknik, för att säkerställa att systemen uppfyller säkerhetskraven. Under 2022 lanseras en ny modul inom KLASSA som fokuserar på riskhantering, vilket ytterligare stärker kommunernas förmåga att hantera och minimera risker relaterade till informationssäkerhet. Dessutom finns det ett antal vägledningar inom KLASSA samt satsningar på molntjänster och KLASSA för Internet of Things (IoT), vilket ger kommunerna ytterligare verktyg för att säkerställa säkerheten i sina digitala lösningar (SKR 2022).

3.6 Risk, hot och sårbarheter

Begreppet risk betyder i allmän uppfattning att något oönskat kommer eller skall inträffa (Aven, 2011). Risk karaktäriseras väldigt olika. Det finns individuella risker, risker för samhället av social eller ekonomisk natur eller miljörisker (Beck, 1992). Risk kan även definieras som sannolikheten att en riskkälla leder till en oönskad händelse eller effekt, där begreppet risk kan delas in i två huvudkategorier: sannolikheten för en oönskad konsekvens av en händelse och storleken på konsekvensen (Kaplan & Garrick, 1981).

När det kommer till hot den kan delas in i tre övergripande kategorier, nämligen de som härstammar från mänskliga faktorer, tekniska hot och naturhot. Samtliga hot medför incidenter som lämnar konsekvenser för informations- och cybersäkerhet, med möjlig påverkan på både enskilda och flera organisationer (MSB, 2020). Dessa hot kan antingen vara externa eller interna och de kan vara bekanta eller okända för organisationer. När det gäller hot från människor kan de ytterligare kategoriseras baserat på deras ursprung, inklusive anställda, kunder, återförsäljare eller hackare. För att underlätta riskbedömning och riskhantering kan hot grupperas efter kriterier såsom åtkomstnivå, expertis och motivationsnivå. Utöver de mänskliga hoten kan miljöfaktorer som brand, översvämningar eller stormar även utgöra potentiella hot (Clark & Hakim, 2017).

Riskhantering är en process som används för att identifiera, bedöma och prioritera risker för att sedan planera och implementera åtgärder för att minska eller hantera dessa risker (Hubbard, 2009). Riskidentifiering och riskurval är viktiga steg i denna process (ISO 31000, 2018). Inom ramen för riskhantering är det möjligt för en organisation att anta flera strategier, beroende på den specifika typen av risk som identifierats. En organisation kan välja att acceptera risken, vilket innebär att man bedömer att det inte finns något praktiskt eller kostnadseffektivt sätt att minimera sannolikheten eller konsekvenserna av en potentiell händelse. Organisationen kan även försöka undvika risken genom att genomföra

beteendeförändringar inom organisationen för att eliminera möjligheten till att risken realiserar (Clark & Hakim, 2017).

När man pratar om sårbarheter, avser det egenskaper hos ett IT-system som ökar dess mottaglighet för attacker. Dessa sårbarheter kan vara tekniska brister, förbiseenden eller mänskliga svagheter, eller en kombination därav. Vanligtvis refererar termen till brister inom system för identifiering, inloggning och rättigheter i datornätverk. Dessutom kan kontrollen av in- och utgående datatrafik samt granskningen av ansluten utrustning och programvara vara föremål för sårbarheter (IT-ord, 2017).

3.7 Incident och incidenthantering

Begreppet incident beskrivs som en oväntad, störande och tillfällig händelse. I IT-sammanhang beskrivs incident som IT-incident och definieras som en oplanerad störning eller en försämring av kvalitén i en tjänst som kan skapa konsekvenser för verksamheten som använder tjänsten. En IT-incident kan uppstå antingen avsiktligt eller av oavsiktligt agerande (Högskolan i Borås 2021).

Begreppet incidenthantering redogör för tillvägagångssättet som används för att hantera alla typer av incidenter. Själva processen för incidenthantering handlar om att i förhand identifiera potentiella hot och risker inom organisationen man arbetar för. För att uppnå detta använder sig av de metoder som organisationen har planerat att använda för att hantera hot och risker (SRS u.å.) Huvudsyftet med incidenthantering är att snabbt återställa den drabbade tjänsten och samtidigt minimera incidentens påverkan på verksamheten. Detta syftar till att säkerställa att tjänsten upprätthåller sin högsta möjliga kvalitet och tillgänglighet (Minina, 2013)

3.8 Kontinuitetshantering

Kontinuitetshantering är en strategisk process som syftar till att säkerställa att en organisation kan fortsätta sin verksamhet på en acceptabel nivå även under extrema omständigheter eller störningar. Det handlar om att förutse potentiella risker och utveckla planer och åtgärder för att hantera dem effektivt, oavsett om det är en störning i arbetskraftens tillgänglighet, otillgängliga arbetslokaler, avbrott i leveranser av viktiga resurser eller en strömavbrott (MSB 2024). En störning kan vara en oväntad händelse eller en förväntad incident som avviker från det normala arbetsflödet. Vad som skiljer en incident från att utvecklas till en kris är organisationens förmåga att effektivt hantera den genom befintliga planer och procedurer. Kontinuitetshantering är nyckeln till att förbereda och reagera på sådana händelser genom att uppmärksamma potentiella hot och faror i förväg (Tómasson, 2022).

Kontinuitetshantering har som huvudsyfte att identifiera och säkra de kritiska delarna av organisationen, såsom avgörande processer, produkter och tjänster. Genom att noggrant kartlägga och analysera dessa nyckelaspekter av organisationen kan man skapa en strategi för att stärka deras robusthet och motståndskraft mot störningar och avbrott. Att öka robustheten innebär att förbättra organisationens förmåga att både förebygga och hantera störningar och avbrott i organisationen. Kontinuitetshantering spelar en avgörande roll i att uppnå detta mål genom att bygga upp en beredskap och en förmåga till kontinuitet inom organisationen. Målet är att säkerställa att organisationen har den kunskap och de resurser som krävs för att effektivt förebygga och hantera avbrott i organisationen (FSPOS, 2021).

4. Resultat

I följande avsnitt redovisas den data som samlades in från intervjuerna, vilka genomfördes med kommunerna och cybersäkerhetsexperten som har fördjupade kunskaper kring det systematiska informationssäkerhetsarbetet.

Kommunerna har benämnts utifrån kommun 1 och kommun 2, med tanke på anonymitet. Resultatet uppdelades i ett antal olika teman, utifrån en genomförd tematisk analys. De uppdelade teman för kommunerna är följande: *det systematiska arbetet med riskbedömning, framgångsfaktorer för att arbeta systematiskt och utmaningar med säkerhetsarbetet.*

4.1 Cybersäkerhetsexperten

Cybersäkerhetsexperten som deltagit i denna undersökning besitter stor kompetens kring både informations-, och cybersäkerhetsarbete som bedrivs i Sverige. Som cybersäkerhetsexpert arbetar respondenten i fråga med rådgivning kring cybersäkerhetsfrågor för olika typer av aktörer att fatta fördelaktiga beslut. Syftet med att intervjua denna respondent kommer ge forskarna en mängd information som kan utgå ifrån och analysera hur kommunerna svarar kring sitt systematiska informationssäkerhetsarbetet.

4.1.1 Framgångsfaktorer för att arbeta systematiskt

Informanten lyfter fram att en möjlig lösning kan vara att skapa samarbeten eller centralisera resurser för att tillhandahålla säkerhetskompetens till mindre kommuner. Dessutom behövs det en förbättrad förståelse från ledningens sida om de potentiella riskerna med cybersäkerhetsattacker och behovet av effektiva skyddsåtgärder. Detta kräver inte nödvändigtvis en anklagelse av bristande kompetens hos ledningen, utan snarare en förbättring av informationsutbytet för att tydligt förklara konsekvenserna av potentiella hot. Informanten betonar även hur viktigt utbildning är för att allokera de anställda inom organisationen om vad de får göra och inte skall göra för att därmed öka säkerhetsmedvetandet.

Informanten beskriver även hur kommuner kan arbeta med övning för att bättre förbereda sig inför kommande IT-attacker. I samband med att bra kompetens nyttjas ute hos kommunerna anser informanten att det i framtiden kan arbetas mer effektivt med kommunernas informationssäkerhet.

“Kan vi nyttja de kompetenta individerna ute hos kommunerna i samband med att vi effektivt nyttjar statens resurser, kan jag se att informationssäkerhetsarbetet hos kommuner i framtiden kan gå bra. Kanske inte så fort som man önskar sig, men i alla fall åt rätt håll.”

En annan framgångsfaktor som informanten tar fram är samarbetet mellan kommuner som nått positiva effekter vilket har visat sig genom ett stort engagemang och intresse mellan kommuner om att jobba ihop vad gäller informationssäkerhet.

“Vi ser en vilja att tillämpliga sig, ett engagemang. Vi har faciliterat kommunerna att gå ihop genom att samarbeta, då de har hittat den digitala agendan om vad de vill driva tillsammans. Vi ser en stor vilja och ett stort engagemang och det tror jag är positivt.”

Informanten betonar att det finns många sätt att svara på frågan om hur en kommun kan förbereda sig inför kommande IT-attacker, beroende på vilket perspektiv som används. Sett ur kommundirektörens synvinkel handlar det om att öva mycket för att kunna hantera olika typer av attacker. Vidare förklarar informanten att övningar stödjer kommuner i att förstå sina beroenden och hur olika verksamheter påverkas vid en attack, men även att förstå vilka typer av förmågor som behövs för att hantera IT-attacker.

“Om vi ser det från kommundirektörens perspektiv, så är det väldigt mycket fokus på träning och övning för att kunna hantera eventuella attacker. Vi behöver utveckla olika förmågor för att kunna möta dessa utmaningar. Men när det kommer till att konkretisera och identifiera exakt vilka förmågor som behövs, kan det vara svårt att göra på ett meningsfullt sätt. Därför anser jag att övning är ett bra första steg för att börja förstå hur våra verksamheter påverkas. Genom att öva får vi en känsla för vad som verkligen är avgörande för vår verksamhet och vad vi är beroende av.”

En annan viktig framgångsfaktor är engagemang och stöd från högsta ledningen i kommunen. Informanten betonar att informationssäkerhetsfrågorna måste lyftas upp till kommunledningen eller kommunstyrelsen för att säkerställa att rätt beslut fattas och att informationssäkerhet får den uppmärksamhet och de resurser som krävs. Ledningens engagemang är avgörande för att skapa en kultur där informationssäkerhet prioriteras och integreras i kommunens övergripande strategier och mål.

Genom att utbilda alla anställda och involverade parter kan kommuner säkerställa att medarbetarna har den nödvändiga kunskapen och förståelsen för informationssäkerhet, men framförallt menar informanten att det är viktigt att alla anställda kommer i kontakt med informationen och lär sig hantera den på ett korrekt sätt.

“Jag tror att utbildningen är viktig, definitivt. Framförallt så tror jag att det stora utbildningsbehovet nu ligger nog kopplat till att försöka få ledningsgrupperna att förstå de risker som cyberangrepp utsätter deras verksamhet för.”

Informanten betonar att kommuner ofta är mycket drivna organisationer, där framgångar ofta kan spåras till enskilda individer som är starkt motiverade och engagerade. Det är dessa individer som ofta gör stor skillnad inom kommunernas informationssäkerhetsarbete. Informanten beskriver detta genom att exemplifiera hur en annan kommun som har sina politiker involverade i deras informationssäkerhetsarbete, vilket därmed har resulterat i att hela organisationen påverkas positivt av detta. Detta i form av att politikerna är väldigt engagerade, ställer frågor och engagerar sig i informationssäkerhetsarbete vilket i sin tur resulterar i att det ställer krav på både kommundirektör och andra kommunledare att också prioritera dessa frågor. Detta leder till att engagemanget och drivet kring dessa frågor blir alltmer viktigare.

“Kommunerna är mycket drivna organisationer, ofta tack vare enskilda individer som har gjort stor skillnad. För närvarande kan man ofta peka ut dessa motiverade personer som har haft betydande påverkan. I kommun x finns det politiker som är väldigt engagerade, vilket har

en smittoeffekt. När en kommundirektör behöver svara på alla frågor, måste denne vända sig till underordnade. Detta skapar ett flöde av information nedåt i organisationen.”

Vidare uttrycker informanten hopp om att framtiden ska innebära mindre beroende av enskilda individer och mer fokus på systematiska arbetssätt för informationssäkerhet. Detta skulle innebära att framgången inte längre är lika starkt kopplad till enskilda drivna personer, utan snarare till etablerade processer och strukturer som säkerställer kontinuerligt och hållbart informationssäkerhetsarbete.

“I detta sammanhang fungerar det delvis, eftersom det faktiskt leder till krav. Dessutom finns det ytterligare en aspekt: det finns mycket drivna IT-chefer, digitaliseringschefer och informationssäkerhetssamordnare. Jag tror att dessa individer är en av de nuvarande framgångsfaktorerna. Däremot förväntar vi oss att vi i framtiden inte kommer att vara lika beroende av enskilda individer, utan snarare kommer att införa ett mer systematiskt arbetssätt.”

Istället understryker informanten att det viktigaste är att föra en öppen och djupgående diskussion kring de specifika riskerna som organisationen står inför. Det kanske är vettigt att genomföra en diskussion med ens kollegor. Genom att inleda diskussionen med att utvärdera organisationens befintliga förmågor från ett säkerhetsperspektiv kan man skapa en klarhet kring vilka områden som behöver förstärkas eller förbättras. Vidare betonar informanten vikten av att lära av andra kommuners erfarenheter och tidigare incidenter för att ytterligare stärka organisationens förmåga att hantera risker och utveckla en mer proaktiv strategi för informationssäkerhet.

“Men det viktiga är att man börjar diskutera de risker man står inför och kanske gör en bedömning av vilka förmågor vi behöver ha. Man kanske kan titta på sina kollegor. Så är ju Härjedalen och Vellinge här drabbade senast, och Kalmar, se vad vi kan lära oss av dem. Vad funkar bra, vad funkar inte. Så man behöver börja prata om risker.”

Informanten underströk vikten av att alla kommuner i Sverige bör anta en helhetsinriktning på sitt informationssäkerhetsarbete genom att tillämpa ett allriskperspektiv. Detta innebär att kommunerna bör aktivt värdera de olika riskerna som deras organisationer kan ställas inför. Genom att arbeta systematiskt och metodiskt kan kommunerna genomföra omfattande riskanalyser inom organisationen. Dessa riskanalyser fungerar som en vägledning för att identifiera och prioritera de åtgärder som behöver vidtas för att säkerställa en robust informationssäkerhetsstruktur.

När det kommer till verktygen som används vid dessa riskanalyser, nämner informanten några av de mest förekommande i branschen, såsom KLASSA, infosäkkollen och ISO 27000. Dessa verktyg fungerar som stöd för kommunerna när de arbetar med sin riskbedömning och utformning av säkerhetsåtgärder. Trots att dessa verktyg rekommenderas för att främja ett systematiskt informationssäkerhetsarbete, framhäver informanten en viktig poäng: verktygen i sig innebär inte en direkt koppling till de konkreta åtgärderna som behöver implementeras. De tillhandahåller snarare en ram eller en vägledning för det generella säkerhetsarbetet och ställer krav på det systematiska informationssäkerhetsarbetet i sig, såsom att utse ansvariga som skall driva informationssäkerhetsarbetet och genomföra regelbundna riskanalyser.

“De ställer egentligen krav på informationsarbetet arbete i sig. Det ska finnas någon som är ansvarig, man ska göra riskanalyser, man ska ha någon som äger systemen och så vidare och

så vidare. Men standarden inklusive infosäkkollen eller klassa säger ju inte vilka skyddsåtgärder man ska vidta.”

Informanten framhåller vikten av att förstå att det systematiska arbetssättet som kommuner använder sig av inte nödvändigtvis ger omedelbara resultat vid enstaka åtgärder. Istället är det en kontinuerlig process som kräver ihärdighet och engagemang. Exempelvis är genomförandet av riskanalyser en återkommande och oupplöslig del av detta arbete. Det är genom denna regelbundna analys och uppdatering av risker som kommunerna kan förbli proaktiva och anpassa sina skyddsåtgärder efter aktuella hot och sårbarheter.

4.1.2 Hinder med säkerhetsarbetet

Informanten beskriver att inom kommuner, trots att det inte finns tydliga statistiska bevis för ökad sårbarhet, utgör bristen på specialiserad expertis inom informationssäkerhet en utmaning. Denna situation förväntas förbli oförändrad och kräver en alternativ strategi för att hantera kompetens- och resursbrist. Framförallt finns det kompetensbrist inom mindre kommuner där respondenten betonar att kompetensbristen är svår att fylla ut med tanke på kostnaderna för de mindre kommunerna. Detta fenomen är särskilt påtagligt i mindre kommuner, där det framhävs att kompetensbristen är svår att lösa på grund av de höga kostnaderna. Vidare beskriver informanten att det är en särskild utmaning att skapa den expertis som är nödvändig för att bedriva informationssäkerhetsarbetet inom mindre kommuner.

“Att i en så liten organisation, däribland mediankommunen på 15 000 invånare, att hitta expertis inom informationssäkerhet är väldigt svårt. I samband med att det är väldigt dyrt blir experterna också eftertraktade. Det resulterar i att det behövs mycket experter i en så liten organisation”

Informanten lyfter även fram den bristande kompetens och förståelse som ledningen har för vilka risker som finns kring de angrepp och liknande som utsätter deras verksamhet. Informanten menar att detta har uppkommit på grund av att de involverade i säkerhetsarbetet, däribland aktörer, varit dåliga på att informera ledningen apropå informationssäkerhet och olika angrepp, vilket därmed resulterat i att det finns brist på kunskap hos ledningen i kommunerna.

“Jag skulle säga att ledningens förståelse för de risker som cybersäkerhetsangrepp och liknande hot utgör för deras verksamhet är en brist som behöver ses över. Det handlar inte om att de är okunniga på något sätt, utan snarare om att vi har varit lite för dåliga på att förklara vad som kan hända.”

Informanten betonar att det finns en bristande målgruppsanpassning från MSB när det gäller deras stöd för informationssäkerhet. MSB riktar sitt stöd till CISO, men många kommuner har i dagsläget inte en dedikerad CISO utan en person som bara arbetar deltid med säkerhetsfrågor, exempelvis ofta mindre än 20% av sin tid. Informanten förklarar att detta skapar betydande utmaningar, eftersom dessa personer inte kan bli experter på informationssäkerhetsområdet när de enbart ägnar en liten del av sin arbetstid till detta.

“Detta är signifikant för att det ser ut som det gör. Det vill säga att det sitter någon annan person som har någon annan uppgift och sen jobbar 20% med informationssäkerhet, en dag i veckan. Det är svårt. Det gör ju att man inte blir expert. Det finns säkert någon annan arbetsuppgift som man lägger mer tid på, typ 40%. Det här skapar ju utmaningar.”

Informanten påpekar att SKR inte har en åsikt om hur mycket tid kommunerna behöver avsätta för informationssäkerhet, men de ser att det kommer att bli svårt att uppfylla de krav som NIS 2-förordningen ställer om det bara finns deltidsanställda inom säkerhet. Den ekonomiska verkligheten för kommunerna gör det svårt att anställa fulltidspersonal för informationssäkerhet, eftersom det skulle innebära att resurser tas från andra viktiga områden som skola, hemtjänst och infrastrukturarbete.

“Däremot så tror jag det kommer vara svårt att uppfylla de direktiv som kommer in i NIS2-förordningen i samband med att man har en som jobbar mindre än en heltidsanställd. Tyvärr är det ju så att det här är bökigt, den ekonomiska verkligheten för kommunerna. De är inte så “feta”, det här är dyr kompetens och innebär flera lärare som jobbar inom. Kommunerna är ju världshandel för samhällsviktig verksamhet och det innebär att när man tar resurser från ett ställe och lägger det på ett annat, då är det något annat samhällsviktigt som inte får pengarna.”

Informanten lyfter fram att det är en utmaning att balansera beslutsfattandet kring skyddsåtgärder mellan kommunledningen och de operativa nivåerna. I stora kommuner som Stockholm med tiotusentals anställda, blir det omöjligt för en enskild kommundirektör att besluta om detaljerade tekniska åtgärder, som exempelvis val av krypteringsalgoritmer. Därför behöver man hitta ett arbetssätt där riskägarskapet delegeras på olika nivåer inom organisationen, så att beslut kan fattas nära verksamheten.

Sammanfattningsvis, informanten lyfter fram flera utmaningar: bristande anpassning av MSB:s stöd, deltidsanställd personal som inte kan bli experter, ekonomiska begränsningar som påverkar resursallokeringen, och behovet av att sprida säkerhetsmedvetenhet och ansvar på alla nivåer inom kommunen. Dessa faktorer försvårar kommunernas förmåga att effektivt förbereda sig inför och hantera IT-attacker.

4.2 Kommun 1

Kommun 1 är den största kommunen, sett till invånarantal, av de två som presenterats i denna undersökning och beskrivs enligt SKR:s definition som en *pendlingskommun nära en storstad*. Informanten i fråga är anställd som informationssäkerhetssamordnare (CISO) på kommunen och har arbetat där i x antal år. Under intervjun nämner informanten att de sammanfattningsvis arbetar systematiskt med sitt informationssäkerhetsarbete genom att följa ISO 27000-serien som en standard, där det ingår att arbeta operativt genom att utbilda personal samt genomföra både riskanalyser och informationsklassningar. Informanten beskriver det systematiska tillvägagångssättet som en metod för att stärka kommunens skydd mot externa hot.

4.2.1 Framgångsfaktorer för att arbeta systematiskt

Vid frågan kring framgångsrika exempel inom kommunen lyfter informanten fram det systematiska arbetssättet som en avgörande framgångsfaktor. Med stöd av det systematiska arbetssättet säger informanten att de kan få fram olika beslutsunderlag, vilka används som ett stöd i att fatta viktiga beslut för organisationen. Vidare likställer informanten det systematiska arbetssättet med hur man i skolan infört robotar vilka fungerat som ett hjälpmedel för att i förväg identifiera risker och reducera dem.

“Man har ju följt de här olika delarna och har lyckats jobba med att identifiera väldigt mycket risker innan man tagit något i drift. Detta har resulterat i att man med ett gott samvete kan implementera denna lösning. Med verktyget har man lyckats reducera väldigt många risker, vilket fungerar på samma sätt med det systematiska arbetssättet.”

Informanten beskriver hur en bra samverkan mellan juridik, informationssäkerhet och IT inom deras organisation har varit centralt för att skapa en gemensam agenda kring det hela. Enligt informanten har en samstämmighet kring olika strategier och planer inom organisationen varit en avgörande framgångsfaktor.

“Vi har gjort tvärtom och skapat en bra samverkan mellan oss. Genom att samarbeta har vi kunnat skapa en gemensam agenda och ett gemensamt mål. Detta förenklar verksamheten. När vi är samstämmiga i strategier, planer och framgång, blir det enklare att uppnå våra mål.”

Informanten som representerar kommunen beskriver hur ISO 27000-serien är det standardramverk som används inom organisationen för att kunna arbeta systematiskt med sitt informationssäkerhetsarbete. Med användning av ISO 27000-serien arbetar informanten operativt i form av att utbilda personal inom organisationen samt genomföra både riskanalyser och informationsklassningar av deras informationstillgångar.

Utöver utbildning av personal inom organisation, beskriver informanten att en viktig del av det systematiska arbetssättet är att hålla i olika typer av metoder och processer som ingår genom att kartlägga information, genomföra informationsklassningar, uppföljning och leverantörskontakt.

“I uppstartsfasen för några år sedan så var det ganska operativt. I form av att utbilda personal, hålla i olika typer av metoder och processer i det systematiska arbetssättet, kartlägga information, riskanalys, informationsklassning, uppföljning, leverantörskontakt och så vidare.”

Informanten beskrev arbetet med riskbedömning och riskanalysen som ett obligatoriskt moment i deras del med att arbeta systematiskt. Kommunen lyfter fram hur arbetet med det systematiska informationssäkerhetsarbetet fortgår i takt med att genomföra riskanalyser minst

en gång per år där man utgår från en mall som har utformats för riskanalys. Syftet med att genomföra en riskanalys för deras del är att det kan handla om att man vill genomföra en förändring inom verksamheten eller implementera en större anskaffning av något annat.

“Vi har liksom en mall för att genomföra riskanalyser. Riskanalys är ett obligatoriskt moment i det systematiska arbetet. Inom vår verksamhet gör man det minst en gång per år. Man gör innan man genomför förändringen, innan man anskaffar en ny lösning att bli med om en del av. I samband med att implementera ett nytt system till exempel.”

Vidare beskriver informanten verktyget riskanalys som en naturlig del av arbetet med hänsyn till upphandlingsförfarande eller förändring. Huvudtanken med riskanalysen är att man skall ha förstått sannolikheten eller konsekvenserna av något som kan tänkas hända innan man bestämmer sig för att införa något nytt inom verksamheten.

“Det naturliga arbetet är upphandling, förfarande eller förändring. Om man ska gå över, till exempel från egen drift till en måldrift eller med driften av något, eller gå över till mål, att man har ett riskbaserat perspektiv. Och det gör man genom riskanalys i metod. Man har tänkt igenom konsekvenserna och sannolikheten innan man gör.”

4.2.2 Hinder med säkerhetsarbetet

Informanten lyfter fram att den allra största utmaningen med att arbeta systematiskt är att framförallt utbilda människorna i relation till teknisk utbildning inom organisationen. Informanten beskriver att en av de huvudsakliga arbetsuppgifterna för honom inom kommunen är att utbilda människorna inom exempelvis deras informationssäkerhetspolicy. För respondenten handlar utbildningen om att informera den enskilde individen om vad den ska göra med informationen i den digitala miljön.

“Den kunskapen beskriver jag som ganska låg. Den har blivit högre, men den är fortsatt för låg. Individen kan ha god kunskap om det fysiska, till exempel larm och låslarm, men i den digitala miljön är det få som vet hur det fungerar.”

En annan utmaning som informationssäkerhetssamordnaren betonar är att det enbart krävs att en enskild individ gör ett misstag inom organisationen, genom att klicka på ett phishing-mail, för att det skall initiera en attack. I deras fall skulle en försenad hantering, där man inte identifierar attacken i förväg, kunna riskera att slå ut hela organisationen. En okunskap kring detta menar informationssäkerhetssamordnaren beror på bristande utbildningsnivå.

“Den typen av kunskap är en utmaning även i vår organisation. Eftersom vi delar nätverk, krävs det bara att en enskild individ är sårbar för att en attack ska kunna ske. Om vi inte identifierar och hanterar hotet i tid, riskerar vi att hela organisationen slås ut. Detta kan hända på bara några timmar.”

4.3 Kommun 2

Kommun 2 är den minsta kommunen, sett till invånarantal, av de två som presenterats i denna undersökning och beskrivs enligt SKR:s definition som en *landsbygdskommun*. Informanten i kommunen är anställd som en informationssäkerhetssamordnare (CISO) på heltid och besitter mångårig erfarenhet av att arbeta med informationssäkerhet inom kommuner. Kommunen i fråga följer huvudsakligen ISO-27000 serien som standardramverk och uttrycker även hur olika styrdokument inom organisationen stödjer dem i att arbeta systematiskt med sin informationssäkerhet. Sammanfattningsvis betonas det hur det systematiska informationssäkerhetsarbetet hjälper kommunen att förbereda sig inför kommande IT-attacker.

4.3.1 Framgångsfaktorer för att arbeta systematiskt

Informanten lyfter fram hur ett systematiskt arbetssätt är det som avgör att man är på rätt väg med sitt informationssäkerhetsarbete, med betoning i att det är svårt att missa något viktigt när man arbetar systematiskt. Informanten beskriver att de utifrån ett systematiskt tillvägagångssätt kollar på flera olika steg som handlar om hur de hanterar data inom organisationen.

“Om man levererar utifrån ett systematiskt arbetssätt är det väldigt svårt att missa något. Det är de som är en viktig framgångsfaktor. Första steget vi kollar på är, vilken typ av data hanterar vi, nästa steget är: hur skyddar vi den datan? Nästa steget är, om någon får tag i den datan - hur gör vi då? Om datan inte finns, hur agerar vi? Det är då man börjar implementera kontinuitet för att kunna arbeta med återställningsmöjligheter av datan. Det är viktigt att se att man lyckats komma långt med en systematiskt tankesätt.”

Informanten förklarar att de huvudsakligen följer ISO 27000-standarden och NIST som en del i att arbeta systematiskt med deras informationssäkerhetsarbete. Informanten förtydligar att ISO 27000-standarden mer beskriver vad man ska göra för att utföra sitt informationssäkerhetsarbete, men inte hur. NIST-ramverket däremot används som ett stöd i att förstå hur och när något ska göras. Informanten beskriver att de olika ramverken används som en sorts vägledning i att arbeta med sitt informationssäkerhetsarbete i form av ett verktyg.

“Om man skulle tolka olika regelverk som finns blir det jättesvårt om man inte har kunskap i det området. Men, med användning av olika verktyg kan man arbeta med granskning och så kan man titta på de olika ramverken. Exempelvis kan man använda ISO 27000-standarden när man tar fram olika stöddokument.”

Informanten betonar att det inte är optimalt att anlita konsulter för informationssäkerhetsarbete, utan förespråkar att bevara kunskap inom organisationen genom intern utbildning och regelbundna övningar. Informanten förklarar att genom att utbilda personalen internt, finns det möjlighet att bygga upp en stark kunskapsbas som kan användas långsiktigt. Detta skapar en kontinuitet och en stabilitet som är svår att uppnå med konsulter, som ofta bara genomför snabba insatser och lämnar efter att ha presenterat sina förslag.

“Jag är inte så förtjust i anlita konsulter. Jag tror mer på att bevara kunskap. Då måste man utbilda internt. Och öva. Så jag tror att det är bättre. Då har du möjlighet att vända tillbaka. Till personer som hjälper. Och sätter upp den. Men du kan inte vända tillbaka till konsulter. För det är ingenting som konsulter gör. Som upplever det i kommunen. Ofta bara en snabb insats. Lämnar fram förslag. Då försvinner de.”

Vidare belyser informanten vikten av att öva på olika scenarier för att stärka organisationens beredskap. Genom kontinuerlig planering och hantering av möjliga incidenter kan organisationen analysera och lära sig från dessa övningar. Informanten framhåller att detta systematiska arbete, trots att det ännu inte är djupt rotat, är på gång och visar potential för att bli en positiv kraft inom kommunens informationssäkerhetsarbete. Det handlar om att skapa en stark förvaltning och beredskap för olika roller och situationer, vilket är avgörande för att hantera informationssäkerhet effektivt.

“Ja, övning gör vi. Det är upphandling. Det blir inte på det sättet. Men det är mer kopplat till kontinuitet. Planering och hantering. Så det övar vi. Det har vi kanske inte gjort tidigare. Men det har vi påbörjat i alla fall. Att lägga fram olika typer av scenario. Och kunna analysera den. Och titta på vad vi har lärt oss från det här scenariot. För att försöka spela olika roller. För att alla som är med. Men det är på gång. Det är på pipeline. Jag tror att det kan vara svårt att se det nu. Men som det ser ut. Det kommer att bli något positivt.”

Informanten förklarar att även om det är svårt att mäta effekterna av dessa insatser just nu, finns det en förväntan om att de kommer att leda till positiva resultat på sikt. Att bygga upp en intern kompetens och kontinuerligt arbeta med utbildning och övningar skapar en grundläggande förståelse och ett praktiskt tillvägagångssätt som är mer hållbart än att förlita sig på externa konsulter.

“Jag tror att det kan vara svårt att se det nu. Men jag tror att eftersom det inte är något som har varit utbrett. Man börjar visa en stark förvaltning.”

Sammanfattningsvis framhåller informanten att de största utmaningarna inom kommunernas informationssäkerhetsarbete är bristande kunskap och resurser, samt behovet av en systematisk och långsiktig strategi för utbildning och övning. Genom att fokusera på internutbildning och kontinuerliga övningar kan kommunerna skapa en starkare och mer resilient informationssäkerhetsstruktur, vilket i sin tur minskar beroendet av externa konsulter och främjar en djupare förståelse och beredskap inom organisationen.

Informanten beskriver att de inom kommunen inte har arbetat aktivt med riskhantering när det gäller att ha en konsekvensbild. Detta trots att det nu finns en lag som betonar hur viktigt det är att arbeta med risker. Vidare beskriver informanten att han i varje upphandlingsprocess, i samband med att utforma stöddokument, introducerar riskhantering och uppmantrar de involverade att ständigt jobba med riskbedömningar. Kommunen rör sig alltmer mot att vara en del av en säkerhetskultur och att det i dagsläget inte finns någon förhållning på ett kontinuerligt sätt.

Vidare förklarar informanten att deras organisation arbetar med två typer av riskbedömningar. En av dem är konsekvensbedömningar, där fokus ligger enbart på GDPR. Mer specifikt undersöker de personuppgifter och tolkar vad som är tillåtet att göra med dessa.

“Ofta tittar man på personuppgifter och behandlingar, där vi kollar på om vi är rädda för att behandla denna typ av personuppgifter. Om svaret är nej, då tittar vi på regelverk som kan luta mot vad vi skulle kunna göra.”

Informanten förklarar vidare att arbetet med konsekvensbedömningar är obligatoriska och baseras på en lag som ställer krav på att kommunen måste genomföra dessa bedömningar med tanke på att det handlar om personuppgifter och att GDPR ingår i lagen om dataskyddsförordningen.

“Medan för GDPR är det lag på att göra konsekvensbedömningar när man ska behandla personuppgifter.”

Den andra typen av riskbedömningar som kommunen arbetar med är riskanalys. Informanten menar att det är bra för organisationen att ha riskanalysen som en rutin för att därmed skapa en kontinuitetsplanering utifrån de risker som har upptäckts. Vidare understryks det för hur de inom kommunen har en mall för riskanalys men att inte alla systemen som kommunen använder har det, utan enbart de nyare systemen.

“Men när man tittar på riskbedömning, eller riskanalys för informationssäkerhet, är det något jag ofta påpekar för verksamheter idag. För att genomföra detta utifrån riskanalysen är det bra att ha välfungerande rutiner och samtidigt bygga en kontinuitetsplanering baserad på de upptäckta riskerna. Vi har en mall för riskanalys idag, men den har inte implementerats i alla system inom kommunen. Dock finns den i många av de nya systemen. De system som kallas samhällsviktiga och verksamhetskritiska har vi börjat genomföra riskanalyser för ur ett informationssäkerhetsperspektiv.”

4.3.2 Hinder med säkerhetsarbetet

Informanten i fråga beskriver hur de i dagsläget inte arbetar aktivt med riskanalys, vilket beskrivs som en stor utmaning inom deras organisation. Trots att de arbetat med frågan kring riskanalys väldigt länge, har det än idag inte blivit någon rutin för det inom organisationen. Informanten betonar även att riskhanteringen kopplat till deras kontinuitetsplan, vilket handlar om deras återställningsmöjligheter kring datan som de hanterar.

“När det handlar om kontinuitet för vår del, handlar det om när det smäller, så kan vi bara gå tillbaka till papper och penna, för att därifrån dela ut ansvar i samband med att återställa vår digitala miljö”

Vidare betonar informanten att de enbart befinner sig i början vad gäller deras kontinuitetshantering och att de behöver arbeta mer aktivt med den för att säkerställa kontinuitet. Informanten berättar att deras kontinuitetshantering är en del av deras systematiska arbete och att det beskrivs som en viktig del för att arbeta systematiskt, vilket

därför är lite problematiskt att de precis börjat arbeta med sin kontinuitetshandling. Vid en följdfråga kring varför de inte börjat tidigare lyfter informanten fram att brist på kunskapsnivå är den omfattande orsaken till det. Trots att detta är något som lyfts fram till kommunledning särskilt ofta är det inget som tas på allvar, vilket gör att det skjuts fram hela tiden.

“Jag tror det är också kunskapsnivå. Ja, kunskapsnivå. Tyvärr. Det är också kunskapsnivå. Man ser inte sammanhang. Och man kan inte riktigt sälja den till ledningen. Det är absolut det viktigaste.”

Informanten betonar att en stor utmaning i kommunernas informationssäkerhetsarbete är att personalen ofta måste balansera både operativa och strategiska uppgifter, vilket leder till tidsbrist och ineffektivitet. Informanten förklarar att även om utbildning är en nyckelaspekt, finns det en genomgående låg kunskapsnivå bland de anställda inom kommunerna, vilket gör det svårt att förstå och implementera effektiva informationssäkerhetsåtgärder.

“Ja, det kan man göra. Jag tror att ett annat problem som kan vara problematiskt är att man jobbar både som operativt och som strateg. Det gör att inte alla har tid. Samtidigt är det en annan aspekt, kunskapsnivå. Men det är inte ofta man får de resurserna från kommunerna.”

Informanten förklarar att det finns en tydlig kontrast mellan den privata sektorn och den offentliga sektorn, där kommunerna befinner sig. I den privata sektorn handlar det mer om pengar, där man köper tjänster och ställer krav på tjänsteleverantörer i syfte att upprätthålla höga säkerhetsstandarder. Informanten betonar att om inte tjänsteleverantörerna lever upp till förväntningarna, är det lätt att byta ut dem. Inom kommuner har informationssäkerhet en helt annan innebörd och betraktas som en samhällstjänst, där god kunskap kring informationssäkerhet inte finns på grund av bristande resurser.

“I privata sektorn så är det pengar som stiger. Så man köper tjänster och lägger ställer krav. Så om du inte kan leverera så kan vi lika väl hitta något som kan göra det. Medan i kommunen så är det mer samhällstjänst. Så kunskap finns inte. Man känner inte till allvaret i det här. Så staten själva förvaltar. Man ska kanske leverera ett kvalitetsarbete. Men samtidigt räcker inte resurserna från kommunerna till.”

Vid frågan kring hur kommunen samverkar med andra kommuner, betonar informationssäkerhetssamordnaren att det i dagsläget inte finns mycket kunskap kring informationssäkerhet kommunerna emellan, med betoning i att det inte befinner sig på den nivå som önskat. Informationssäkerhetssamordnaren menar att det finns en låg kunskapsnivå i informationssäkerhet på grund av bristande resurser och att de är i behov av fler resurser samt rätt kompetens tillsätts.

“Jag tror att en lösning är att man hittar rätt kompetens plus rätt resurs. För du kan skjuta hur mycket pengar som helst i kommunen. Men det hamnar bara på en hög med papper. Då anlitar vi en jurist att få en informationssäkerhetssamordnare. Och juristen får mer betalt, mer i lön. Men du får ingen effekt av resultatet. Så det ska matcha både kunskapsnivå och resurser. Annars är det mer resurser utan kunskapsnivå.”

Enligt informanten är en av de huvudsakliga utmaningarna i rollen som informationssäkerhetssamordnare den generellt låga kunskapsnivån hos organisationens medlemmar. Det framgår att det är vanligt att informations säkerhetsbegrepp kan verka främmande och svårbegripliga för många, vilket gör det svårt att kommunicera på ett effektivt sätt. Informanten uttrycker att det kan kännas som att man pratar på ett främmande språk när man försöker förklara och diskutera ämnet med andra.

“Jag tror att utmaningen generellt är att kunskapsnivå är ganska liten. Så ofta att det låter som man pratar grekiska. Så det är inte så många som förstår när man börjar gå så djupare. Det är en utmaning. Hur kan man få det enkla arbetet på ett tydligt, enkelt sätt utan att tappa meningen i ord.”

Vid frågan kring om kommunen har en metod för upphandling, betonar informationssäkerhetssamordnaren att det finns en metod för upphandling med betoning i att den inte alltid är uppföljd. Anledningen till detta handlar om den allmänt låga kunskapsnivån bland de anställda. Vid upphandling handlar det om att man ska införa något inom verksamheten och att det är något man kollar särskilt mycket på.

“Jag tror att det är låg kunskapsnivå. Jag skulle säga. För det är upphandling. Det är inte alltid mindre resurser. Och det är någonting man ska införa. Det krävs mycket arbete. Så om man har tid att titta på. Och man ser inte nytta av den. Och man förstår inte att den är det absolut viktigaste.”

5. Analys

Följande avsnitt bygger på den empiri som redogjorts under resultatavsnittet. Avsnittet syftar till att analysera de kategorier som identifierats i avsnittet "4. Resultat".

5.2 Framgångsfaktorer för att arbeta systematiskt

5.2.1 Riskbedömning

Resultatet från de transkriberade intervjuerna visade att båda informationssäkerhetssamordnarna i respektive kommun arbetar med riskbedömning i form av riskanalyser och riskhantering som en del av deras vardagliga arbetsuppgifter. I rollen som CISO är riskbedömningen en central del i det systematiska informationssäkerhetsarbetet, där man genomför riskanalyser i syfte att identifiera risker i förhand för att på så sätt avvärja eventuella IT-attacker. Cybersäkerhetsexperten betonar vikten av en holistisk ansats i form av ett allriskperspektiv där alla svenska kommuner kontinuerligt bedömer och värderar de risker som de ställs inför.

Riskanalysen är en etablerad och central aspekt hos kommun 1 där riskanalyser genomförs minst en gång per år eller vid större förändringar hos verksamheten i form av ett nytt system eller olika upphandlingar. Denna systematik hos kommun 1 säkerställer att risker bedöms konsekvent och att sannolikheten samt konsekvenser av potentiella händelser i form av IT-attacker noggrant övervägas innan en ny lösning implementeras inom verksamheten. Detta kontinuerliga arbete med riskanalyser kan ge en viss garanti för ett mer robust informationssäkerhetsarbete inom kommun 1.

5.2.1.1 Genomföra konsekvensbedömning

Informanten i kommun 2 förklarar att de i dagsläget jobbar med två olika typer av riskbedömningar, vilka är konsekvensbedömningar och riskanalys. Vad gäller konsekvensbedömningar är de lagstadgade och är obligatoriska att genomföra. Konsekvensbedömningarna är riktade mot GDPR och handlar om personuppgifter, medan riskanalyserna är mer riktade mot att identifiera risker i förhand och i samband med detta skapa en bra kontinuitetsplan.

5.2.1.2 Informationssäkerhetskultur

Vad gäller riskhanteringsarbetet hos kommun 2, förklarar CISO som leder och samordnar informationssäkerhetsarbetet att de inte har arbetat aktivt med riskhantering i samband med att ha en konsekvensbild. Trots ett inaktivt riskbedömningsarbete, arbetar informationssäkerhetssamordnaren inom kommun 2 ständigt med att introducera riskhanteringen i upphandlingsprocesser och i samband med detta uppmuntra de involverade att kontinuerligt arbeta med riskbedömningar för att på så sätt bygga en starkare informationssäkerhetskultur.

5.2.2 Systematisk informationssäkerhetsarbete

Informationssäkerhetsarbetet i respektive kommun är väsentlig för att skydda känslig data och informationstillgångar. CISO i kommun 2 betonar vikten av det systematiska informationssäkerhetsarbetet, vilket säkerställer att inget viktigt förbises. Det systematiska arbetssättet hos dem omfattar flera steg, bland annat identifiering av vilken typ av data som hanteras, skyddsåtgärder för denna typ av data, beredskap för potentiella dataintrång och återställningsplaner vid dataförlust. Genom att arbeta systematiskt kan organisationen minimera risken för allvarliga säkerhetsincidenter och samtidigt skapa en kontinuerlig förbättringsprocess.

Ett systematiskt arbetssätt möjliggör, i form av riskanalyser, ett framtagande av goda beslutsunderlag. I kontrast till kommun 2 framstår kommun 1 som mer etablerad i sitt systematiska informationssäkerhetsarbete. Genom att följa ett systematiskt arbetssätt menar CISO i kommun 1 att de i förväg kan identifiera och reducera risker innan man tar beslut på att nya lösningar implementeras i verksamheten. Detta belyses som en viktig framgångsfaktor i att arbeta systematiskt, med tanke på att de gynnar både ekonomin och framförallt kommunen som arbetar med detta. CISO i kommun 1 likställer riskbedömningsarbetet med skolans riskbedömning, där man i förhand implementerat robotar för att på sikt identifiera och reducera risker.

5.2.2.1 Intern utbildning och regelbundna övningar

CISO i kommun 2 framhåller att intern utbildning och regelbundna övningar vad gäller kontinuitetshantering är väsentliga att genomföra för att bibehålla och förbättra kunskapsnivån inom kommunen. Detta resulterar i ett minskat beroende från externa konsulter och främjar ett systematiskt informationssäkerhetsarbete, med tanke på att kunskapsnivån med all sannolikhet blir högre. Övningarna karaktäriseras i form av olika scenarier där man övar i syfte att stärka kommunens beredskap inför kommande IT-attacker. Genom att öva på scenarier kan kommunen därmed bli bättre på att hantera faktiska händelser som sker, i detta fall, en storskalig IT-attack. Vidare beskrivs övningar som en central del att genomföra i samband med att kommunerna skall förstå de beroenden som finns och även utveckla de förmågor som krävs för att hantera en IT-attack.

CISO i kommun 2 förklarar hur övningar som görs visar det en potential på en positiv kraft genom att stärka kommunens informationssäkerhetsarbete, trots att övningarna inte är djupt rotade i deras systematiska informationssäkerhetsarbete. CISO är förväntansfull att övningarna kommer ge resultat på sikt och därmed främja deras kontinuitetshantering. I samband med detta lyfts en stark förvaltning och beredskap för olika roller som en framgångsfaktor för effektiv hantering av kommunens informationssäkerhetsarbete. Utbildning är viktig för att säkerställa ett starkt informationssäkerhetsmedvetande, men också för att utbildningen är kritisk i samband med att de anställda vet vad de ska göra med informationen ute i den digitala miljön. Därmed kan en starkare informationskultur integreras inom organisationen. Sammanfattningsvis betonar CISO i kommun 2 att genom ett kontinuerligt arbete med övningar i samband med att bygga upp en intern kompetens inom kommunen, kan kommunen bygga en robust och säker informationssäkerhetsstruktur.

5.2.2.2 Samverkan och strategi

En annan framgångsfaktor som betonas är den goda samverkan mellan juridik, IT och informationssäkerhet inom kommun 1. En gemensam agenda och samstämmighet kring strategier och planer förenklar arbetet i själva verksamheten och resulterar även i att målen uppnås. Kommunen utgår huvudsakligen från ISO 27000-serien som används för att CISO skall kunna arbeta operativt, i form av att utbilda personal, genomföra riskanalyser och även informationsklassningar. Genom att utbilda personal kan kommunen säkerställa att kunskapsnivån bland de anställda är på en god nivå, samtidigt som de har ett högt informationssäkerhetsmedvetande. I takt med detta är informationsklassningar en viktigt del av det systematiska informationssäkerhetsarbetet, med tanke på att man klassar organisationens tillgångar utifrån ett visst värde.

5.2.3 Ramverken för strukturerad informationssäkerhet

Ett allriskperspektiv, där olika risker aktivt värderas och prioriteras, är avgörande för att säkerställa en robust säkerhetsstruktur. Verktyg som KLASSA, infosäkkollen och ISO 27000 rekommenderas för att stödja detta arbete. Dessa verktyg tillhandahåller en ram och vägledning för säkerhetsarbetet, men de dikterar inte specifika åtgärder. Istället betonar de systematik, ansvarsfördelning och regelbundna riskanalyser. Detta innebär att medan verktygen kan stödja en systematisk ansats, ligger ansvaret för att implementera konkreta skyddsåtgärder hos organisationerna själva.

Kommun 1 använder ISO 27000-standarden och kommun 2 använder huvudsakligen ISO 27000-standarden och NIST-ramverket för att strukturera sitt informationssäkerhetsarbete. CISO beskriver fördelarna med att använda ISO 27000 i form av att den beskriver vad som skall göras medan NIST-ramverket ger mer vägledning om hur och när skyddsåtgärderna skall genomföras. Denna kombination av ramverk fungerar som en effektiv metod för kommunen att utgå ifrån när det gäller att skapa stöddokument, exempelvis informationssäkerhetspolicy, och att implementera säkerhetsåtgärder. En användning av olika ramverk kan därmed säkerställa att man är på rätt väg med sitt informationssäkerhetsarbete.

Vidare betonas en centralisering av resurser i samband med att skapa samarbeten är centralt för de mindre kommunerna i Sverige. Samtidigt beskrivs även ledningens förståelse kring informationssäkerhetsarbetet och de risker samt behovet av skyddsåtgärder som särskilt avgörande för att etablera ett ledningsstöd. Utöver ett starkt ledningsstöd, är behovet av utbildning bland de anställda särskilt viktigt att poängtera.

5.2.4 Erfarenhetsutbyte och riskdiskussion

Cybersäkerhetsexperten betonar att det framförallt är viktigt att föra en diskussion kring vilka risker man står inför i samband med att man betonar vikten av att lära sig från andra kommuners erfarenheter och IT-incidenter. Att lära av andras misstag och framgångar gör det möjligt att undvika fallgropar och att stärka de områden som kräver extra uppmärksamhet. Detta genom att diskutera kring vad som fungerat bra och mindre bra hos de tidigare utsatta kommunerna, för att därmed skapa en helhetsbild vilket kan resultera i en mer effektiv och anpassad strategi för sin egen informationssäkerhet. Genom att identifiera och utvärdera de förmågor som finns, kan man skapa en bättre förståelse var förbättringspotentialen ligger och vilka områden som behöver förbättras hos de involverade.

5.3 Hinder med informationssäkerhetsarbetet

Utifrån resultatet från de transkriberade intervjuerna kan det konstateras att de involverade kommunerna i undersökningen och cybersäkerhetsexperten lyfter fram ett antal utmaningar med informationssäkerhetsarbetet.

5.3.1 Bristande ledningsstöd och förståelse från ledningen

En av de mest framträdande utmaningarna med kommunernas informationssäkerhetsarbete i allmänhet är bristen på specialiserad expertis, vilket är särskilt förekommande hos de mindre kommunerna. Cybersäkerhetsexperten beskriver att anledningen till detta är framförallt den ekonomiska verkligheten för de mindre kommunerna i form av mindre resurser, vilket gör det tämligen svårt att rekrytera och behålla kompetent personal. Detta resulterar i att det blir en hög efterfrågan på experter i samband med höga kostnader, vilket gör det svårt för mindre kommuner att ha någon dedikerad som arbetar med informationssäkerhetsfrågor. Detta resulterar i att de mindre kommunerna tvingas ha en deltidsanställd som sannolikt aldrig kommer utveckla någon expertis för informationssäkerhetsarbetet, med tanke på den arbetsomfattning som individen arbetar med.

Framförallt tillkommer kritik mot MSB:s metodstöd som enbart vänder sig till heltidsanställda CISO:s, men cybersäkerhetsexperten betonar som, tidigare nämnt, att många mindre kommuner i dagsläget har en deltidsanställd vilket försvårar det. Cybersäkerhetsexperten betonar att det är en bristande målgruppsanpassning och att det inte når kommuner som faktiskt behöver hjälp, vilket resulterar i att mindre kommuner blir särskilt utsatta av detta och därmed blir de svårare för dem att implementera säkerhetsåtgärder.

En annan central utmaning som lyfts fram är ledningens bristande förståelse för de säkerhetsangrepp som deras organisation kan utsättas för. Cybersäkerhetsexperten menar att detta främst beror på att de som arbetar med säkerhetsfrågor har varit dåliga på att kommunicera dessa risker till ledningen. Denna bristande förståelse och medvetenhet på ledningsnivå har resulterat i att informationssäkerhetsfrågor inte prioriteras tillräckligt högt, vilket därmed försvårar informationssäkerhetsarbetet med att skydda kommunernas IT-infrastruktur.

5.3.2 Bristande budgetresurser

Den ekonomiska verkligheten för kommunerna innebär att det är svårt att avsätta tillräckliga resurser för informationssäkerhet. Både cybersäkerhetsexperten och CISO i kommun 2 betonar att det är svårt att anställa en heltidsanställd CISO, med tanke på att kommunen är en samhällsviktig tjänst. Detta resulterar i att man tar resurser från något som är samhällsviktigt och därmed lägger det på kommunerna, vilket innebär att man tar viktiga resurser från exempelvis skola och hemtjänst. Detta är problematiskt med tanke på att det därmed blir svårare för kommunerna att uppfylla det NIS2-direktiv som kommer framöver, vilket ställer krav på att kommunerna skall ha någon som arbetar heltid med att leda och samordna informationssäkerhetsarbetet.

5.3.2.1 Bristande resursallokering

En annan utmaning som CISO i kommun 2 lyfter fram är den bristande resursallokeringen från kommunerna. Det saknas ofta tillräckliga medel för att anställa eller utbilda kompetent personal inom informationssäkerhet. Detta problem förvärras av att det inte finns tillräckligt med samarbete och kunskapsutbyte mellan kommunerna. Informanten betonar att det finns ett behov av fler resurser och rätt kompetens, och att detta måste matchas med en hög kunskapsnivå för att ge effektiva resultat.

5.3.3 Bristfällig utbildning och kunskapsnivå

Hos kommuner i allmänhet, men i synnerhet hos de involverade kommunerna i denna undersökning, lyfts det fram hur utbildning av personalen är särskilt utmanande. Det finns en generellt låg kunskapsnivå hos de anställda när det gäller informationssäkerhet, med betoning i att de anställda inte vet vad de ska göra med informationen som de arbetar med. Trots att det finns en viss medveten kring fysiska åtgärder som vanliga låslarm, förekommer det en bristande kunskapsnivå kring hur man hanterar informationen i den digitala miljön. Denna brist på kunskap och medvetenhet riskerar att anställda råkar utföra ett misstag, som att klicka på ett phishing-mail, vilket kan resultera i att allvarliga säkerhetsintrång inträffar och därmed slår ut hela organisationen.

En av de mest grundläggande utmaningarna, enligt CISO i kommun 2, är den låga kunskapsnivån hos organisationens anställda. Informationssäkerhetsbegrepp kan verka främmande och svårbegripliga för många, vilket gör det svårt att kommunicera på ett effektivt sätt. Detta leder till att diskussioner kring informationssäkerhet ofta uppfattas som tekniskt komplicerade och svårtillgängliga, vilket ytterligare försvårar arbetet med att implementera och upprätthålla säkerhetsåtgärder.

5.3.4 Brist på systematiskt arbete med riskanalys och kontinuitetsshantering

CISO i kommun 2 beskriver att de inte arbetar aktivt med riskanalys, vilket är en stor utmaning. Trots att riskanalys har diskuterats under en lång tid, har det ännu inte blivit en rutin inom organisationen. Vidare är deras kontinuitetsshantering fortfarande i ett tidigt skede, vilket innebär att de inte är tillräckligt förberedda för att hantera och återställa sin digitala miljö efter en incident. Denna brist på systematiskt arbete med riskanalys och kontinuitetsshantering gör att kommunerna är sårbara för IT-attacker.

5.3.5 Arbetsbelastning

CISO i kommun 2 påpekar att personalen ofta måste balansera både operativa och strategiska uppgifter, vilket leder till tidsbrist och ineffektivitet. Den höga arbetsbelastningen gör det svårt för de anställda att tillägna tillräcklig tid och uppmärksamhet åt informationssäkerhetsfrågor, som ofta kräver noggrannhet och eftertanke. Resultatet blir att säkerhetsåtgärder kan bli fördröjda eller otillräckligt genomförda, vilket försvagar kommunens förmåga att skydda sin IT-infrastruktur och känslig information mot potentiella hot. Vidare riskerar denna situation att skapa en negativ spiral där bristen på fokus och tid för informationssäkerhet leder till ökade säkerhetsrisker, vilket i sin tur kan generera ytterligare operativa problem som ytterligare försvårar det strategiska arbetet.

6. Diskussion

Följande avsnitt diskuterar studiens huvudsakliga delar, där man utgår från frågeställningen "Vilka framgångsfaktorer och hinder påverkar medelstora och små kommuners systematiska informationssäkerhetsarbete" Inledningsvis består diskussionsdelen av de kategorier som analyserats i avsnitt "5. Analys" och diskuteras kring tidigare forskning och teoretisk referensram.

Resultatet av denna undersökning identifierade ett flertal framgångsfaktorer och hinder i de båda kommunernas systematiska informationssäkerhetsarbete och även hur cybersäkerhetsexperten tolkar det kommunala informationssäkerhetsarbetet. Empirin i denna undersökningen omfattar därmed ett antal framgångsfaktorer vad gäller det systematiska informationssäkerhetsarbetet hos informanterna, vilka definieras som följande:

- Riskbedömning

Det framgår att riskhanteringen ses som en central del av det systematiska informationssäkerhetsarbetet där det ingår att genomföra riskbedömningar i form av riskanalyser. Riskhanteringen ses som en viktig del av det systematiska informationssäkerhetsarbetet, vilket även (Barafort, Mesquida & Mas 2017) betonar i att riskhanteringen utgör en viktig del i organisationer.

Cybersäkerhetsexperten förklarar att alla kommuner i Sverige bör arbeta utifrån ett allriskperspektiv genom att värdera de risker som de ställs inför, i form av att kontinuerligt arbeta med att genomföra riskanalyser. Genom att arbeta med riskanalys säkerställer man att det systematiska arbetssättet följs. Riskanalysen är även en del av steget "Identifiera och analysera" enligt metodstödet för systematiskt informationssäkerhetsarbete (2021, s. 8). I samband med detta är det väsentligt att kommuner i Sverige etablerat ett verktyg för riskanalys för att på så sätt i förhand kunna identifiera och reducera riskerna innan de sker.

Vad gäller i båda fallen hos kommunerna är syftet att förstå och hantera risker genom att säkerställa kontinuitet och säkerhet i kommunerna. Det som urskiljer de båda kommunerna i arbetet med riskhanteringen är att kommun 1 bedöms vara mer avancerad i sin tillämpning av riskhanteringen i form av årliga riskanalyser och en etablerad process, medan kommun 2 är på väg att införliva detta i sin verksamhet för att därmed främja en säkerhetskultur. I samband med detta lyfter cybersäkerhetsexperten fram att det är viktigt att föra öppna och djupgående diskussioner vilka specifika risker som finns inom kommunerna. Detta understryker betydelsen av att involvera alla relevanta parter för att identifiera och hantera risker på ett effektivt sätt. Enligt MSB (2024), bedöms integrering av riskhantering vara avgörande för att identifiera de mest kritiska processerna, inklusive deras stödprocesser, genom att säkerställa att riskhanteringen är effektiv och målinriktad.

- Genomförande av konsekvensbedömningar

Informanten, som är CISO i kommun 2, förklarar att deras organisation arbetar med två typer av riskbedömningar. En av dessa är konsekvensbedömningar, där fokus ligger enbart på GDPR. Mer specifikt undersöker organisationen personuppgifter och tolkar vad som är tillåtet att göra med dessa. Vidare förklarar informanten att arbetet med konsekvensbedömningar är obligatoriskt och baseras på lagkrav, eftersom kommunen måste genomföra dessa bedömningar på grund av att det handlar om personuppgifter och att GDPR ingår i lagen om dataskyddsförordningen.

- Uppmuntrande av informationssäkerhetskultur

Det framgår i analysen att informanten hos kommun 2, närmare sagt CISO hos den mindre kommunen, att han ständigt försöker introducera riskhanteringen i deras upphandlingsprocesser genom att uppmuntra de involverade i informationssäkerhetsarbetet att kontinuerligt arbeta med deras riskbedömningar. Vad gäller informationssäkerhetsarbetet hos kommuner överlag kan ett uppmuntrande av riskbedömningsarbete resultera i att man i tid upptäcker risker och hot som påverkar organisationen på ett dåligt sätt.

- Intern utbildning och regelbundna övningar

I det systematiska informationssäkerhetsarbetet arbetar informationssäkerhetssamordnarna operativt med att genomföra utbildningar inom organisationen, vilket är en del av det systematiska informationssäkerhetsarbetet. Detta är något som även metodstödet indikerar i steget "Använda" där det ingår utbildning av personal enligt Metodstöd för systematiskt informationssäkerhetsarbete (2021, s. 18-20). Syftet med att genomföra utbildningar är för att säkerställa att människorna inom organisationen upprätthåller sin kunskap kring informationssäkerhet och även håller sig uppdaterade kring olika skyddsåtgärder som ska vidtas. Detta lyfter även Pérez-Gonzales, Preciado & Solana-Gonzalez (2019) i tidigare forskning fram att utbildning bör genomföras i syfte för att upprätthålla samt förbättra säkerhetsmedvetandet hos de anställda.

Informationssäkerhetssamordnaren inom den kommun 2 föreslår dock att det är viktigare att istället lägga fler resurser på att utbilda dem anställda inom kommunen, för att på så sätt bevara rätt kunskap och även förhöja nivån på säkerhetsmedvetandet bland individerna. Detta är något som Bergquist, Tinet & Gao (2021) betonar i hur viktigt det är att genomföra säkerhetsutbildning inom organisationen i syfte att skapa en gemensam förståelse kring informationssäkerhetsbegrepp för de anställda inom organisationen. I dagsläget anlitar de ofta en konsult som skall hjälpa med olika delar i informationssäkerhetsarbetet men betonar att detta inte är hållbart i längden, då det är svårt att följa upp med konsulter.

Övningar är avgörande för att förbereda kommuner för IT-attacker. Genom att simulera olika scenarier kan kommunerna analysera och lära sig från dessa övningar, vilket stärker deras beredskap och förmåga att hantera incidenter. Övningar hjälper kommunerna att förstå sina beroenden och hur olika verksamheter påverkas vid en attack. Detta systematiska arbete, även om det inte är fullt etablerat, visar potential för att bli positiv kraft inom kommunernas

informationssäkerhetsarbete. MSB (2024) påpekar att övningar är essentiella för att säkerställa att personalen vet hur de ska agera under en krissituation. Kontinuitetsplaner som inte utsätts för regelbundna övningar tenderar att inte bli reviderade, vilket leder till att dessa planer med tiden blir föråldrade och förlorar sin effektivitet.

- Systematiskt informationssäkerhetsarbete

Systematiskt informationssäkerhetsarbete i kommun 1 och i kommun 2 visar på vikten av att skydda känslig information och för att skapa en kontinuerlig förbättringsprocess. I kommun 2 betonas vikten av att följa en strukturerad process för att säkerställa att alla viktiga aspekter, såsom dataskydd och återställningsplaner vid incidenter, tas i beaktande. I kommun 1 har detta arbetssätt nått en högre mognadsnivå, där riskanalyser genomförs för att i förväg identifiera och hantera risker innan nya tekniska lösningar implementeras. Detta proaktiva sätt att arbeta återspeglar en nyckelfaktor för framgångsrikt informationssäkerhetsarbete, vilket också stöds av MSB riktlinjer (2024), som lyfter fram betydelsen av att ha en strukturerad och metodisk process på plats.

- Samverkan och strategi

Samverkan mellan juridik, IT och informationssäkerhet spelar en central roll inom kommun 1. När dessa avdelningar arbetar med en gemensam agenda och samstämmiga strategier, skapas en enhetlig riktning för organisationens säkerhetsarbete. Detta samarbete säkerställer att olika perspektiv och kompetenser integreras i beslutsfattandet, vilket förbättrar möjligheterna att identifiera och hantera potentiella risker.

Enligt CISO beskrivs en strategisk samverkan inom ramen för ISO 27000-serien som möjliggörs genom en effektiv informationsklassificering, där tillgångar bedöms och skyddas baserat på deras värde och känslighet. Detta innebär att organisationen kan prioritera sina säkerhetsinsatser där de behövs mest, och på så sätt optimera användningen av resurser. Genom att kombinera strategisk planering med operativt samarbete mellan olika avdelningar kan en organisation inte bara uppnå sina säkerhetsmål, utan även skapa en dynamisk och anpassningsbar säkerhetskultur som står emot både nuvarande och framtida hot.

- Ramverken för strukturerad informationssäkerhet

Vid arbetet med riskanalyser nämner både kommun 1 och cybersäkerhetsexperten olika verktyg, exempelvis KLASSA, infosäkkollen samt ISO 27000-standarden, vilka används för att stödja riskanalyser och informationsklassningar. Dessa verktyg ses som viktiga för att främja ett systematiskt informationssäkerhetsarbete samt att det också betonas av cybersäkerhetsexperten att verktygen i sig inte garanterar konkreta åtgärder utan snarare ger en ram för säkerhetsarbetet. I samband med detta lyfter MSB (2024) fram att verktyget infosäkkollen ger organisationer en möjlighet att erhålla en mer nyanserad och relevant bild av deras informationssäkerhetsarbete. ISO 27000-standarden möjliggör för organisationer genom att säkerställa att deras information hanteras på ett korrekt sätt (SIS u.å.).

- Erfarenhetsutbyte och riskdiskussion

En möjlig lösning som framhävs av informanten är att skapa samarbeten eller centralisera resurser för att tillhandahålla säkerhetskompetens till mindre kommuner. Detta skulle inte bara öka tillgången till nödvändig expertis, utan också främja en mer enhetlig och effektiv hantering av informationssäkerhet. Det är också tydligt att det finns ett behov av att förbättra förståelsen från ledningens sida om de potentiella riskerna med cybersäkerhetsattacker och vikten av effektiva skyddsåtgärder. Istället för att se detta som en anklagelse mot ledningens kompetens, bör det ses som en möjlighet till förbättrat informationsutbyte och utbildning. Genom att tydligt förklara konsekvenserna av potentiella hot kan ledningen bättre förstå och prioritera informationssäkerhetsarbetet. Detta understryker vikten av en öppen och transparent kommunikation inom organisationen.

Empirin i denna undersökningen omfattar ett antal hinder vad gäller det systematiska informationssäkerhetsarbetet hos informanterna, vilka definieras som följande:

- Bristande ledningsstöd och förståelse av ledningen

Cybersäkerhetsexperten beskriver också problematiken med att ha någon som enbart arbetar deltid med att samordna informationssäkerhetsarbete, med betoning i att det är svårare att bli expert i området. Detta är också något som CISO i kommun 2 lyfter fram vad gäller utmaningar och beskriver att det ofta finns något som jobbar både operativt och strategiskt, vilket resulterar i att informationssäkerhetsarbetet inte bedrivs bra. Precis som (Somroo, Shah & Ahmed 2014) poängterar beskrivs ett bristande ledningsstöd som ett huvudsakligt hinder till att organisationer misslyckas med att uppnå effektivitet med sitt informationssäkerhetsarbete.

- Bristande budgetresurser för mindre kommuner

Vidare betonar de båda kommunerna och även cybersäkerhetsexperten att bristen på resurser också är anledningen till att kommuner inte helt kan uppnå effektivitet med sitt informationssäkerhetsarbete. Resursbristen omfattas i form av både ekonomiska finansieringar och resursbrist i form av rätt kompetens för det arbete som skall utföras. Särskilt beskriver cybersäkerhetsexperten att det förekommer en brist på förståelse från kommunledningen hos kommunerna i allmänhet, vilket har resulterat i en viss okunskap och bristande ledningsstöd kring informationssäkerhetsarbetet. Detta är något som (Somroo, Shah & Ahmed 2014) beskriver resursbegränsningar som en omfattande orsak till ineffektivitet inom organisationer. Cybersäkerhetsexperten förklarar att en lösning till detta är att de aktörer som är stöd till kommuner vid informationssäkerhetsarbetet, behöver bli bättre på att vidarebefordra viktig information.

- Bristande resursallokering

Informanten beskriver att inom kommuner, trots att det inte finns tydliga statistiska bevis för ökad sårbarhet, utgör bristen på specialiserad expertis inom informationssäkerhet en utmaning. Denna situation förväntas förbli oförändrad och kräver en alternativ strategi för att hantera kompetens- och resursbrist. Framförallt finns det kompetensbrist inom mindre kommuner där informanten betonar att kompetensbristen är svår att fylla ut med tanke på kostnaderna för de mindre kommunerna. Detta fenomen är särskilt påtagligt i mindre kommuner, där det framhävs att kompetensbristen är svår att lösa på grund av de höga kostnaderna. Vidare beskriver informanten att det är en särskild utmaning att skapa den expertis som är nödvändig för att bedriva informationssäkerhetsarbetet inom mindre kommuner.

- Bristfällig utbildning och kunskapsnivå

Trots rekommendationer från både metodstöd och andra verktyg som används i det systematiska informationssäkerhetsarbetet, betonar de båda informationssäkerhetssamordnarna i respektive kommun att de idag har väldigt mycket utmaningar med att utbilda människan. Utmaningarna kommer i form av att trots att man aktivt arbetat med att genomföra utbildningar inom organisationen, finns det än idag en låg kunskapsnivå bland individerna inom kommunerna. Detta betonas även av Bergquist, Tinet & Gao (2021) att de anställda har ett bristande informationssäkerhetsmedvetande i samband med att de ses som orsaken till säkerhetsintrång. Särskilt beskriver kommun 1 hur det krävs att enbart en individ behöver göra ett misstag, vilket kan resultera i att organisationen kan bli utsatt för en IT-attack. Detta lyfter även Arbansas, Spremic & Zajdela Hrustek (2021) fram att människan beskrivs som den svagaste länken inom informationssäkerhet.

Informanten hos kommun 2 förklarar att även om utbildning är en nyckelaspekt, finns det en genomgående låg kunskapsnivå bland de anställda inom kommunerna, vilket gör det svårt att förstå och implementera effektiva informationssäkerhetsåtgärder. En orsak till att det blir svårt att implementera effektiva informationssäkerhetsåtgärder kan bero på en låg grad av användarmedverkan från de anställda enligt Flores, Antonsen & Ekstedt (2013). En lösning till detta för kommunen är att i fortsättningen involvera de anställda i samband med att de tar fram olika säkerhetsåtgärder baserade på deras riskanalyser.

Enligt informanten hos kommun 2 är en av de huvudsakliga utmaningarna i rollen som informationssäkerhetssamordnare den generellt låga kunskapsnivån hos organisationens medlemmar. Det framgår att det är vanligt att informationsäkerhetsbegrepp kan verka främmande och svårbegripliga för många, vilket gör det svårt att kommunicera på ett effektivt sätt. Informanten uttrycker att det kan kännas som att man pratar på ett främmande språk när man försöker förklara och diskutera ämnet med andra. Utifrån tidigare forskning i en undersökning genomförd av MSB (2024) beskrivs det att kompetensutvecklingen, vad gäller informationssäkerhet inom kommunerna, inte sker på ett strukturerat sätt och är i en mycket begränsad omfattning.

- Brist på systematiskt arbete med riskanalys och kontinuitetshantering

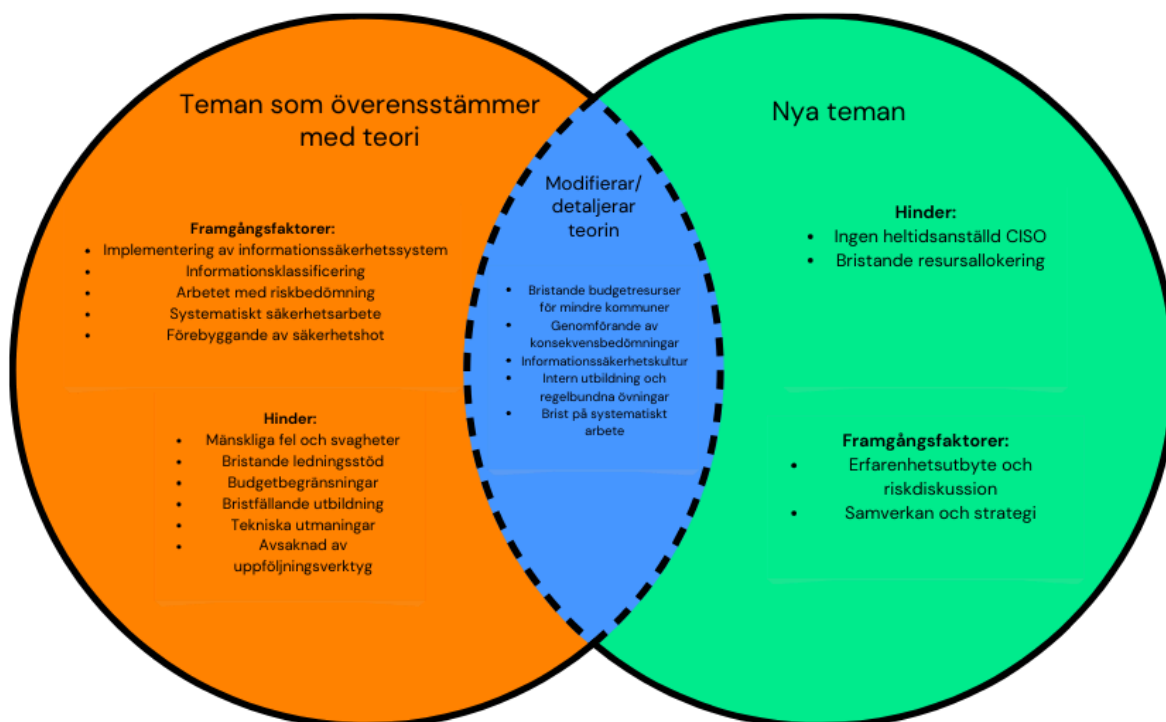
En annan utmaning som enbart lyfts fram av kommun 2 är deras arbete med kontinuitetshantering. Informanten i fråga betonar att de enbart befinner sig i början av deras kontinuitetshantering och att de behöver arbeta mer aktivt med den. Med tanke på att kontinuitetshantering beskrivs som en viktig del av deras systematiska informationssäkerhetsarbete, anser informanten att det är problematiskt. Anledningen till detta är den låga kompetensnivån i samband med att ledningen inte alls uppmärksammar detta, trots att det har lyfts fram flera gånger. Ett ouppmärksammat beteende från ledningen resulterar i ineffektivitet i organisationen på grund av det bristande ledningsstödet enligt Somroo, Shah & Ahmed (2014). Vidare är den låga kompetensnivån hos människor särskilt förekommande i organisationer som arbetar med informationssäkerhet, enligt Khando, Gao, Islam & Salman (2021).

- Arbetsbelastning

Cybersäkerhetsexperten betonar att en stor utmaning i kommunernas informationssäkerhetsarbete är att personalen ofta måste balansera både operativa och strategiska uppgifter, vilket leder till tidsbrist och ineffektivitet. Detta är ett resultat av att kommunerna inte har en CISO anställd på heltid, vilket försvårar för kommunen att enbart arbeta med operativa arbetsuppgifter som rör informationssäkerhetsarbetet. Detta beskrivs som ett nytt tema som förekommer i undersökningens resultat och är något som främst finns hos mindre kommuner. Anledningen till att mindre kommuner inte har en heltidsanställd CISO är för att de har begränsade resurser med tanke på att kommuner är en samhällsviktig tjänst. Det betyder att om man ger mindre kommuner fler resurser, resulterar detta i att man tar resurser från andra samhällsviktiga tjänster såsom skola och omsorg.

- Avsaknad uppföljningsverktyg

En annan utmaning som förekommer hos kommun 2 är avsaknaden av ett uppföljningsverktyg. I en tidigare undersökning genomförd av MSB (2024) framkommer det att typkommunen under senaste tvåårsperioden arbetat att utbilda 0-25% av de anställda inom organisationen. Efter genomförd utbildning har inte typkommunen undersökt personalens kunskaper. Med användning av ett uppföljningsverktyg kan man följa upp viktiga säkerhetsåtgärder som implementerats och även uppföljning av personalens säkerhetsmedvetande. Steget "*Följa upp och förbättra*" i MSB:s metodstöd innehåller steget uppföljning och används av CISO:s för att följa upp, som tidigare nämnt, implementerade säkerhetsåtgärder enligt Metodstöd för systematiskt informationssäkerhetsarbete (2021, s. 22-23). Rekommendationer till kommuner som saknar ett uppföljningsverktyg, är det viktigt för dem att etablera ett uppföljningsverktyg i takt med att använda MSB:s metodstöd.



Figur 2. Illustration av författarnas Venn-diagram om framgångsfaktorer och hinder inom informationssäkerhet.

7. Slutsatser

7.1 Svar på frågeställningen

Undersökningen har fokuserat på svenska kommuners hinder och framgångsfaktorer i samband med hur en cybersäkerhetsexpert tolkar det systematiska informationssäkerhet hos kommunerna. Syftet med att genomföra undersökningen har varit att fördjupa förståelsen kring vilka framgångsfaktorer och hinder som påverkar det kommunala informationssäkerhetsarbetet hos medelstora och små kommuner.

Studien har lagt sitt fokus på att besvara en frågeställning bestående av två forskningsfrågor. Nedan kommer en formulering att ges till forskningsfrågan för att definiera hur den är besvarad.

- *Vilka framgångsfaktorer och hinder påverkar små och medelstora svenska kommuners systematiska informationssäkerhetsarbete?*

Syftet med denna undersökning har varit att identifiera eventuella hinder och framgångsfaktorer som påverkar det systematiska informationssäkerhetsarbetet hos en medelstor och en liten kommun, i samband hos kommuner generellt.

Från resultatet av studien framkommer det att kommunerna i dagsläget har svårigheter med de anställda kring deras säkerhetsmedvetande, vilket medför utmaningar inom kommunerna. Utmaningarna förekommer i samband med ledningens bristande engagemang i informationssäkerhetsarbetet. Ledningen behöver vara mer involverad i det kommunala informationssäkerhetsarbetet för att därmed höja medvetenheten hos anställda. Framförallt handlar utmaningarna hos de anställda om osäkerhet och låg kompetensnivå kring begreppet informationssäkerhet, där ett misstag från en individ kan resultera i att hela organisationen utsätts för en IT-attack.

I detta fallet visar resultatet av studien hur utbildning och kunskapsnivå inom informationssäkerhet beskrivs som både en framgångsfaktor och ett hinder. Studien betonar det viktiga kring hur ett systematiskt och välplanerat utbildningsprogram utgör en central del av informationssäkerhetsstrategin som bedrivs inom kommunerna. Trots detta framkommer det att utbildning och kunskap även är ett hinder inom det kommunala informationssäkerhetsarbete med hänsyn till de utmaningar som förknippas med att säkerställa en tillräcklig och effektiv spridning av säkerhetsmedvetande inom organisationen.

Den kompetensbrist och låga kunskapsnivå som befinner sig inom kommuner idag, understryker behovet av en mer strukturerad och omfattande strategi för att säkerställa att utbildningarna verkligen når fram och ger den önskade effekten. För att övervinna dessa hinder krävs det att utbildningarna är regelbundna och innehållsmässigt relevanta, och även anpassade till målgruppens förutsättningar och att det finns ett starkt engagemang från hela organisationen.

I takt med detta, behöver det även tilldelas resurser till kommunerna, för att kunna anställa en CISO på heltid. Detta kan resultera i att kommuner uppnår mer systematik i deras informationssäkerhetsarbete. Det är framförallt viktigt för kommunerna att införliva en kontinuerlig övning för att i framtiden vara bättre förberedda på kommande IT-attacker, genom att införliva scenarier. I samband med en heltidsanställd kommer det bli allt lättare för kommuner att uppfylla de direktiv som förekommer i den kommande NIS 2-förordningen. Försättningsvis är det avgörande för kommuner att aktivt arbeta med det systematiska informationssäkerhetsarbete i form av att genomföra kontinuerliga riskbedömningar.

Sammanfattningsvis har författarna identifierat ett antal nya teman som förekommer tillsammans med undersökningens resultat (se Figur 2). Ett nytt tema som förekommit vad gäller hinder i informationssäkerhetsarbetet är att kommuner i dagsläget har väldigt svårt att balansera sitt informationssäkerhetsarbete och därmed resulterar detta i att det inte läggs tillräcklig tid och resurser på informationssäkerhetsarbetet. Temat berör arbetsbelastning och är särskilt förekommande i mindre kommuner som har begränsade resurser. Vad gäller framgångsfaktorer, har författarna förekommit att samverkan mellan juridik, IT och informationssäkerhet är väldigt viktigt för att skapa en enhetlig riktning för kommunernas säkerhetsarbete. Förutom det, understryks vikten av att diskutera de risker som är förknippade med informationssäkerhet genom att dra lärdom av andra kommuners erfarenheter och IT-incidenter.

7.2 Förslag till vidare forskning

Denna studie har undersökt hur informationssäkerhetsarbetet ser ut i en liten och medelstor kommun. Studien har fokuserat på hur de informanter som deltar i undersökningen arbetar utifrån att leda och samordna informationssäkerhetsarbetet i kommuner. En intressant studie att bedriva hade varit att genomföra en liknande undersökning mot offentlig sektor, specifikt regioner, i hur de leder och samordnar sitt informationssäkerhetsarbete. Tidigare undersökningar genomförda av både MSB och SKR visar att regioner också är en särskilt utsatt enhet på grund av IT-attacker och en undersökning riktad mot detta område hade i fortsättningen kunnat vara som stöd till regioner. I samband med detta är NIS2-direktivet en kommande lag som ställs på både kommuner och regioner. En intressant frågeställning hade kunnat utformas som följande:

- *Vilka framgångsfaktorer och hinder påverkar svenska regioner när de anpassar sig till NIS2-direktivet?*

7.3 Metodreflektion

Studien har fokuserat på att enbart använda sig av den kvalitativa metodansatsen, vilket har resulterat i en omfattande rad för- och nackdelar. Undersökarna i själva studien har reflekterat kring den kvalitativa metodansatsen genom att analysera hur de har bidragit till studien, både positivt och negativt.

Denna studie har fokuserat på att undersöka det systematiska informationssäkerhetsarbetet hos en liten och en medelstor kommun i relation till hur en cybersäkerhetsexpert tolkar det systematiska informationssäkerhetsarbetet hos svenska kommuner. Med användning av en kvalitativ metodansats i form av öppna, individuella intervjuer har detta möjliggjort en djupare insikt genom att förstå hur respektive informant tolkar och meningsbestämmer ett visst fenomen (Jacobsen 2017, s. 99). I denna undersökning har en kvalitativ metodansats varit passande med tanke på att relativt få enheter har undersökts (ibid.). Endast tre informanter har blivit intervjuade, vilket motsvarar det relativt begränsade antalet enheter som nämns i referensen.

En kvalitativ metodansats med semi-strukturerade intervjuer har varit passande för denna typ av undersökning, främst på grund av dess flexibilitet. Genom att använda semi-strukturerade intervjuer kan forskaren systematiskt sammanställa en intervjuguide med relevanta frågor. Denna metodik möjliggör också en dynamik där informanter ger utrymme att ställa följdfrågor baserat på deras svar. Denna flexibilitet är avsevärt fördelaktig, eftersom det tillåter forskarna att utforska nya aspekter av det fenomen de studerar. Qu & Dumay (2011)

Med användning av en kvalitativ datainsamlingsmetod för denna typ av undersökning har detta resulterat i djupgående insikter i det systematiska informationssäkerhetsarbetet och skapat en förståelse kring hur deltagarna i studien tolkar det specifika fenomenet ur sitt egna perspektiv (Jacobsen 2017, s. 99; Azungah 2018). Detta gav informanten möjligheter att dela med sig av sina egna erfarenheter genom att svara fritt, vilket inte hade varit möjligt med en kvantitativ studie där svarsalternativen är begränsade.

Undersökarna har i denna typ av undersökning enbart fokuserat på att genomföra digitala intervjuer, antingen via Zoom eller Microsoft Teams. Ett huvudsakligt fokus på enbart digitala intervjuer lämpar sig i dagsläget med tanke på att digitala intervjuer kan indikera ett bra flyt i samtalet och dessutom lägre kostnader med tanke på att man inte behöver planera några resor. Samtidigt får man även tillgång till personer som är geografiskt isolerade (Jacobsen 2017, s. 100).

Trots de omfattande fördelarna med att använda digitala intervjuer, kan användning av digitala intervjuerna resultera i en svagare etablering av tillit och öppenhet. (Jacobsen 2017, s. 100) Tidigare forskning har även beskrivit telefon- och videokommunikationsteknologier som väldigt tveksamma metodiker att använda med tanke på att de ses som underlägsna gentemot de fysiska intervjuerna. Man betonar hur ansikte-mot-ansikte intervjuer istället för digitala intervjuer möjliggör mer observation till informanten och därmed skapar mer rik information (Villers, Farooq & Molinari 2021).

8. Referenser

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, 99, 102030-
<https://doi.org/10.1016/j.cose.2020.102030> [2024-04-10]

Arbansas, K. Spremic, M. Zajdela Hrustek, N. (2021): *Holistic framework for evaluating and improving information security culture*. Hämtad från:
<https://doi-org.lib.costello.pub.hb.se/10.1108/AJIM-02-2021-0037> [2024-04-09]

Aven, Terje. (2011). *On some recent definitions and analysis frameworks for risk and vulnerability*. *Risk Analysis*, 31(4), 515-522. [Bok]

Barafort, B. Mesquida, A-L. Mas, A. (2017): *Integrating risk management in IT settings from ISO standards and management systems perspectives*. Hämtad från:
<https://doi.org/10.1016/j.csi.2016.11.010> [2024-04-12]

Beck, Ulrich. (1992). *Risk society: towards a new modernity*. London: Sage. [Bok]

Bergström, E., Åhlfeldt, R-M., Anteryd, F. (2016). Informationsklassificering och säkerhetsåtgärder. Hämtad från: <urn:nbn:se:hj:diva-47021> [2024-04-30]

Bergquist, J., Tinet, S., & Gao, S. (2021). An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality. *Information and Computer Security*, 30(2), 153-172. Hämtad från: <https://doi.org/10.1108/ICS-03-2021-0032>

Böðvar Tómasson (2022). Using business continuity methodology for improving national disaster risk management. *Journal of Contingencies and Crisis Management*, 31(1), ss.134-148. Hämtad från: <https://doi.org/10.1111/1468-5973.12425>

Clark, Robert M.; Hakim, Simon. (2017). *Cyber-Physical Security*. Schweiz: Springer International Publishing. [2024-05-12] - [Bok]

Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*, 12(3), 297–298. Hämtad från:
<https://doi-org.lib.costello.pub.hb.se/10.1080/17439760.2016.1262613> [2024-05-10]

De Villiers, C., Bilal Farooq, M., Molinari, M. (2022): *Qualitative Research Interviews Using Online Video Technology - Challenges and Opportunities*. Hämtad från:
DOI:10.1108/MEDAR-03-2021-1252 [2024-05-01]

Da Veiga, A. (2016). *Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study*. *Information and Computer Security*, 24(2), 139–151. Hämtad från:
<https://doi.org/10.1108/ICS-12-2015-0048> [2024-05-01]

David, G. B., Parker, C. A. & Straub, D. W. (2012). *Writing the doctoral dissertation: a systematic approach*. 3rd ed. Hauppauge, N.Y.: Barron's [2024-04-29]

Digitala Sverige (2022) *En samlad analys av samhällets digitalisering*. Hämtad från: [Digitala Sverige 2022 \(digg.se\)](#) [2024-04-14]

Europaportalen (2023): *Ingen cybersäkerhet i EU utan kommunerna*. Hämtad från: [Ingen cybersäkerhet i EU utan kommunerna \(europaportalen.se\)](#) [2024-04-14]

Flores, R. Antonsen, E. Ekstedt, M. (2013): *Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture*. Hämtad från: <https://doi.org/10.1016/j.cose.2014.03.004>

FSPOS Arbetsgrupp Kunskapsspridning (2021). *Vägledning för Kontinuitetshantering*. Hämtad från: <https://www.msb.se/contentassets/af96031de7124f69a19fb936b78a478b/fspos-vagledning-for-kontinuitetshantering-version5.0.pdf>

Gao, S., Khando, K., Islam, S., & Salman, A. (2021): *Enhancing employees information security awareness in private and public organisations: A systematic literature review*. Hämtad från: <https://doi.org/10.1016/j.cose.2021.102267> [2024-05-14]

Galletta, A. & Jr, Cross,. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication*. 1-245. [Bok]

Hsieh, H. & Shannon, E (2005). *Three Approaches to Qualitative Content Analysis: Qualitative Health research*, 2005-11, Vol.15 (9), p.1277-1288. Hämtad från: <https://doi.org/10.1177/1049732305276687> [2024-05-04]

Hubbard, Douglas. (2009). *Failure of Risk Management : Why It's Broken and How to Fix It*. hämtad från: 10.1002/9781119521914.

Högskolan i Borås (2021): *Riktlinjer för hantering av IT- och informationssäkerhetsincidenter*. Hämtad från: <https://www.hb.se/contentassets/9d5840f01cca4f9f8223632b8696a42c/incidenthantering-f-or-informationsakerhet-2022.pdf>

Islam, Sirajul, M & Karlsson, F. (2023): *The Public Sector Cloud Service Procurement in Sweden: An Exploratory Study of Use and Information Security Challenges*. Hämtad från: [viewtitle.aspx \(igi-global.com\)](#) [2024-04-29]

IT-ord (2017) Hämtad från: [https://it-ord.idg.se/ord/sarbarhet/#:~:text=\(vulnerability\)%20%E2%80%93%20n%C3%A5got%20som%20g%C3%B6r,f%C3%B6r%20identifiering%2C%20inloggning%20och%20r%C3%A4ttigheter.](https://it-ord.idg.se/ord/sarbarhet/#:~:text=(vulnerability)%20%E2%80%93%20n%C3%A5got%20som%20g%C3%B6r,f%C3%B6r%20identifiering%2C%20inloggning%20och%20r%C3%A4ttigheter.)

Index för digital ekonomi och digitalt samhälle (DESI) 2022. Hämtad från:
<https://digital-strategy.ec.europa.eu/sv/library/digital-economy-and-society-index-desi-2022> [2024-05-01]

Jacobsen, D. (2017): Hur genomför man undersökningar? - *Introduktion till samhällsvetenskapliga metoder* [Bok]

Kaplan, Stanley, & Garrick, B. John. (1981). *On the quantitative definition of risk. Risk Analysis*, 1(1), 11-27. [Bok]

Kallio H., Pietilä A.-M., Johnson M. & Kangasniemi M. (2016) Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing* 72(12), 2954–2965. Hämtad från: doi: 10.1111/jan.13031 [2024-05-06]

Magnusson, Eva & Marecek, Jeanne. (2015). *Doing Interview-based Qualitative Research: A Learner's Guide*. Hämtad från: DOI:[10.1017/CBO9781107449893](https://doi.org/10.1017/CBO9781107449893). [2024-05-12]

Myndigheten för samhällsskydd och beredskap (2021) *Metodstöd för systematiskt informationssäkerhetsarbete - en översikt*. Hämtad från: [Metodstöd för systematiskt informationssäkerhetsarbete – En översikt \(informationssakerhet.se\)](https://www.msb.se/publikationer/metodstod-for-systematiskt-informationssakerhetsarbete-en-oversikt) [2024-04-27]

Myndigheten för samhällsskydd och beredskap (2024) *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen : Resultatredovisning av Infosäkkollen och It-säk kollen*. Hämtad från:
[https://www.msb.se/sv/publikationer/det-systematiska-informations--och-cybersakerhets-arbetet-i-den-offentliga-forvaltningen--resultatredovisning-av-infosakkollen-och-it-sakkollen-/](https://www.msb.se/sv/publikationer/det-systematiska-informations--och-cybersakerhets-arbetet-i-den-offentliga-forvaltningen--resultatredovisning-av-infosakkollen-och-it-sakkollen/) [2024-04-20]

Myndigheten för samhällsskydd och beredskap (2024) *Om informationssäkerhet*. Hämtad från: [Om informationssäkerhet \(msb.se\)](https://www.msb.se/publikationer/om-informationssakerhet) [2024-04-14]

Myndigheten för samhällsskydd och beredskap (2018): *Virtualisering inom industriella informations- och styrsystem*. Hämtad från: [Defense Technology as Security Policy Jenny Clevström and Mike Winnerstig \(msb.se\)](https://www.msb.se/publikationer/defense-technology-as-security-policy) [2024-04-14]

Myndigheten för samhällsskydd och beredskap (2019): *Informationssäkerheten i Sveriges kommuner : Analys och rekommendationer utifrån MSB:s kommunenkät 2015*: Hämtad från: [Informationssäkerheten i Sveriges kommuner : Analys och rekommendationer utifrån MSB:s kommunenkät 2015](https://www.msb.se/publikationer/informationssakerheten-i-sveriges-kommuner) [2024-04-16]

Myndigheten för samhällsskydd och beredskap (2022) *It-incidenter som påverkar samhällsviktiga och digitala tjänster: NIS-leverantörers it-incidentrapportering 2021 årsrapport*. Hämtad från: [It-incidenter som påverkar samhällsviktiga och digitala tjänster : NIS-leverantörers it-incidentrapportering 2021 årsrapport \(msb.se\)](https://www.msb.se/publikationer/it-incidenter-som-paverkar-samhallsviktiga-och-digitala-tjanster-nis-leverantorerars-it-incidentrapportering-2021-arssrapport) [2024-04-14]

Natalia Minina (2013) *Development of Knowledge Management Process to Enable Incident Management*. Hämtad från:

https://www.theseus.fi/bitstream/handle/10024/63175/Natalia_Minina_Masters_Thesis.pdf?sequence=1&isAllowed=y [2024-05-10]

Oscarson P. (2019): Informationssäkerhet. Upplaga 1. [Bok]

Polit, D. F., & Beck, C. T. (2017). Essentials of nursing research: appraising evidence for nursing practice. (8. ed.). Lippincott Williams & Wilkins.

Pérez-González, D., Preciado, S., Solana-Gonzalez, P., (2019): Organizational practices as antecedents of the information security management performance : *An empirical investigation*
Hämtad från: <https://doi.org/10.1108/ITP-06-2018-0261>

Redaktionen (2017). *Informationssäkerhet.se*. Hämtad från:
<https://www.informationssakerhet.se/metodstodet/> [2024-04-19]

Sohrabi, N. R. Furnell, S. Von Solms, R. (2016): *Information security policy compliance model in organizations*. Hämtad från:
<https://doi.org/10.1016/j.cose.2015.10.006> [2024-04-14]

Sohrabi, N. Von Solms, R. (2016): *An information security knowledge sharing model in organizations*: Hämtad från:
<https://doi.org/10.1016/j.chb.2015.12.037> [2024-04-17]

Somroo, A. Shah, Hussain. Ahmed, J. (2014): *Information security management needs more holistic approach: A literature review*: Hämtad från:
<https://doi.org/10.1016/j.ijinfomgt.2015.11.009> [2024-04-13]

Sveriges kommuner och regioner (2019) *Kommunernas informationssäkerhetsarbete*. Hämtad från: [Kommunernas informationssäkerhetsarbete \(skr.se\)](#) [2024-04-14]

Sveriges kommuner och regioner (2022) *Kommuner och regioner*. Hämtad från: [Kommuner och regioner | SKR](#) [2024-04-27]

Sveriges kommuner och regioner (2022) *Informationssäkerhet kräver långsiktigt arbete*. Hämtad från: [Informationssäkerhet kräver långsiktigt arbete | SKR](#) [2024-04-22]

Sveriges television (2024a) *7 000 lösenord till anställda läckte efter it-attacken mot Kalmar kommun*. Hämtad från: [7 000 lösenord till anställda läckte efter it-attacken mot Kalmar kommun | SVT Nyheter](#) [2024-04-10]

Sveriges television (2024b) *Tusentals IT-attacker varje dygn mot Umeå kommun*. Hämtad från: [Tusentals it-attacker varje dygn mot Umeå kommun | SVT Nyheter](#) [2024-04-10]

Svenska institutet för standarder (u.å.) *Detta är ISO 27001*. Hämtad från: [Detta är ISO 27001 för cyber- och informationssäkerhet - Svenska institutet för standarder, SIS](#) [2024-04-17]

Svenska institutet för standarder (u.å.) *Riskhantering - Vägledning (ISO 31000:2018, IDT)*. Hämtad från:

<https://www.sis.se/produkter/foretagsorganisation/foretagsorganisation-och-foretagsledning-ledningssystem/foretagsorganisation/ss-iso-310002018/>

Tómasson, B. (2022). Using business continuity methodology for improving national disaster risk management. *Journal of Contingencies and Crisis Management*, 31(1), ss.134-148 [Bok]

Thunberg, S., & Arnell, L. (2022). Pioneering the use of technologies in qualitative research - A research review of the use of digital interviews. *International Journal of Social Research Methodology*, 25(6), 757–768. Hämtad från:
<https://doi.org/10.1080/13645579.2021.1935565> [2024-05-16]

Tracy, S. J. (2010). Qualitative Quality: Eight “Big-Tent” Criteria for Excellent Qualitative Research. *Qualitative Inquiry*, 16(10), 837–851. Hämtad från:
<https://doi.org/10.1177/1077800410383121> [2024-05-09]

Vetenskapsrådet (2002) *Forskningsetiska principer - inom humanistisk-samhällsvetenskaplig forskning*. Hämtad från:
<https://vr.se/analys/rapporter/vara-rapporter/2002-01-08-forskningsetiska-principer-inom-humanistisk-samhällsvetenskaplig-forskning.html> [2024-05-18]

Qu, S.Q. and Dumay, J. (2011), "The qualitative research interview", *Qualitative Research in Accounting & Management*, Vol. 8 No. 3, pp. 238-264.
<https://doi.org/10.1108/11766091111162070> [2024-05-17]

9. Bilagor

Bilaga 1: Intervjuguide - riktad till kommunerna.

Introduktion

- Presentation av oss författare/skribenter som genomför undersökningen i fråga.
- Fråga respondenten om det är OK att spela in - berätta varför - de inspelade intervjuerna skall användas för att transkriberas och är en del av undersökningen. Förtydliga att inspelningen endast kommer att ses enbart av författarna!
- Gå igenom upplägget av intervjun.

Frågor som riktas till respondenten:

- Berätta gärna lite kort om dig själv.
- Hur länge har du arbetat som informationssäkerhetssamordnare i kommunen?
- Har du sedan tidigare jobbat med informationssäkerhet inom offentlig sektor?

Frågor som rör undersökningen:

- Hur ser ni på rollen som CISO i att driva och övervaka informationssäkerhetsarbete?
- Hur arbetar ni med riskbedömning/riskanalys som en del av erat systematiska informationssäkerhetsarbete?
- Hur arbetar ni med incidenthantering som en del av erat systematiska informationssäkerhetsarbete?
- Har ni något samarbete med andra kommuner eller aktörer?
- Har ni ett etablerat arbetssätt för upphandling och hur jobbar ni med att kvalitetssäkra det?
- Har ni ett etablerat arbetssätt för kontinuitetshantering? Om inte, vad beror de på?
- Jobbar ni med uppföljning som en del av ert systematiska informationssäkerhetsarbete?
- Har ni använt er av infosäkkollen?
- Vilka åtgärder som genomförts inom kommunen har påverkat informationssäkerhetsarbetet på ett positivt sätt?

Bilaga 2: Intervjuguide - cybersäkerhetsexpert

Introduktion

- Presentation av oss författare/skribenter som genomför undersökningen i fråga.
- Fråga respondenten om det är OK att spela in - berätta varför - de inspelade intervjuerna skall användas för att transkriberas och är en del av undersökningen. Förtydliga att inspelningen endast kommer att ses enbart av författarna!
- Gå igenom upplägget av intervjun.

Frågor som riktas till respondenten:

- Berätta gärna lite kort om dig själv och din roll som cybersäkerhetsexpert i föreningen.
- Hur länge har du arbetat som cybersäkerhetsexpert?

Frågor som riktas till undersökningen:

- Din roll som cybersäkerhetsexpert, vad är dina arbetsuppgifter mer specifikt?
- Hur bör kommuner arbeta med informationssäkerhet?
- Hur bedrivs ett systematiskt informationssäkerhetsarbete hos kommuner?
- Hur viktig är rollen som CISO i en kommun?
- Hur kan kommuner förbereda sig inför kommande IT-attacker?
- Hur kan man involvera och utbilda anställda inom kommunen för att höja medvetenheten om informationssäkerhet och minska risken för incidenter?
- Trots att alltför många kommuner jobbar systematiskt blir de fortfarande kraftigt utsatta enligt senaste rapporter - hur kan man motverka detta?
- Efter era rekommendationer om att kommuner skall samarbeta med varandra - har detta visat på positiva effekter?
- Vilka framgångsfaktorer, utöver samarbete dessemellan, har ni som myndighet identifierat hos kommuner som klarat sig bäst med sitt systematiska säkerhetsarbete?
- Vad gäller brister eller hinder hos kommuner som olyckligtvis blivit mål för IT-attacker - vilka har ni identifierat? Eller vad är brister eller hinder som gör att kommuner blir lättare utsatta?
- Sammanfattningsvis - hur ser du på framtiden och hur kan kommuner arbeta mer systematiskt?.



HÖGSKOLAN
I BORÅS