LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Att förbereda sig inför det oundvikliga

En kvalitativ studie om kommuners arbete med risk- och kontinuitetshantering ur ett IT-perspektiv

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Victor Johnsson
Filip Vester

Handledare: Odd Steen

Rättande lärare: Miranda Kajtazi
Paul Pierce

Att förbereda sig inför det oundvikliga: En kvalitativ studie om kommuners arbete med risk- och kontinuitetshantering ur ett IT-perspektiv

ENGELSK TITEL: To prepare for the inevitable: A qualitative study on municipalities' work with risk and continuity management from an IT perspective

FÖRFATTARE: Victor Johnsson och Filip Vester

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: maj, 2023

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 65

NYCKELORD: risk, kontinuitet, kommun, IT, planering

SAMMANFATTNING:
I en tid där kommuner mottar tusentals attacker i veckan är det av stor vikt att förbereda sig för verksamhetsavbrott. Tidigare studier visar dock att kommuner har hög riskprofil men låg mognadsgrad gällande risk- och kontinuitetshantering. Syftet med denna studie är att ge en ökad förståelse kring hur kommuners arbete med risk- och kontinuitetshantering bedrivs. Detta genom intervjuer med representanter från IT-verksamheten i fyra kommuner. Resultatet av denna studie visar på en avsaknad av ett verksamhetsöverskridande syfte. Det framkom att lagkrav samt erfarenheter av faktiska incidenter är drivande faktorer. Valideringsarbetet bedrivs reaktivt, vilket dissonerar med den teoretiska referensramens rekommendationer.

Innehåll

Tabeller

1 Introduktion

I ett högt digitaliserat samhälle har risken för cyberattacker ökat drastiskt. Check Point Research Team (2022) rapporterade 2022 att organisationer i genomsnitt mottog 1130 attacker per vecka, en ökning på nästan 30% jämfört med samma period föregående år. Dessa attacker riktar sig mot den privata sektorn, samt mot den offentliga sektorn såsom myndigheter, regioner och kommuner.

Under 2022 blev 44% av Sveriges kommuner utsatta för IT-attacker (Willander & Håkansson, 2023). Till exempel utsattes Norrköping kommun för en större IT-attack där ryska hackare fick tillgång till hela kommunens IT-miljö (SVT, 2022). Det lyckade intrånget tvingade Norrköping kommun att stänga ner hela IT-miljön inklusive kommunikation och radera alla konton med tillhörande lösenord. Efter att kommunen lyckats stänga ute angriparna påbörjades ett omfattande arbete med att bygga upp infrastrukturen från grunden. När infrastrukturen stängdes ner tvingades kommunens samtliga verksamheter aktivera manuella, alternativa rutiner och bedriva arbete utan IT-stöd (Norrköping kommun, 2023).

Ett liknande exempel är Kalix kommun som under 2021 utsattes för en ransomware-attack där angripare gjorde intrång på deras servrar och krypterade data (Kalix kommun, 2023). Intrånget tvingade kommunen att släcka ned samtliga servrar och inleda ett omfattande återställningsarbete. Kommunens IT-miljö låg nere under totalt tre veckors tid och började sedan återställas system efter system. Under tiden tvingades verksamheterna till analogt arbete utan IT-stöd (Andersson, 2022).

Kommunerna har ett lagstadgat ansvar att bedriva grundläggande och viktig samhällsservice för sina invånare, varav de viktigaste är för-, grund- och gymnasieskola, socialtjänst och äldreomsorg (Sveriges Kommuner och Regioner, 2022). De ansvarar för verksamhet som måste fungera även under kriser, vilket gör kommunerna till en vital del av samhällets krisberedskap (Myndigheten för samhällsskydd och beredskap, 2021).

Som en del av det krisförebyggande arbetet har Sveriges kommuner enligt lag ansvar att ”minska sårbarheten i sin verksamhet och ha en god förmåga att hantera krissituationer” (SFS 2006:544, 1 kap. 1 §). De har en skyldighet att ”analysera vilka extraordinära händelser i fredstid som kan inträffa i kommunen … och hur dessa händelser kan påverka den egna verksamheten” (SFS 2006:544, 2 kap. 1 §). En extraordinär händelse definieras i lagen som en ”händelse som avviker från det normala, innebär en allvarlig störning i viktiga samhällsfunktioner och kräver skyndsamma insatser av en kommun” (SFS 2006:544, 1 kap. 4 §). Kommunerna ska värdera och sammanställa resultatet av detta arbete i en risk- och sårbarhetsanalys. Utifrån risk- och sårbarhetsanalysen ska kommunerna sedan ”fastställa en plan för hur de ska hantera extraordinära händelser” (SFS 2006:544, 2 kap. 1 § 2 st.).

En rapport från 2017 visade att kommuner ur ett IT-perspektiv har en låg mognadsgrad för risk- och kontinuitetshantering i kombination med en hög riskprofil (Advenica, et al., 2017). Vidare menar Jafar och Taneja (2017) att brist på kunskap kring risk- och kontinuitetshantering inklusive dess verktyg kan bidra till ineffektiv hantering av verksamhetsstörningar trots en existerande kontinuitetsplan. Än mer belyser Sveriges Kommuner och Regioners (2021)

studie från 2019 att det finns en avsaknad av struktur i kommuner och regioners risk- och kontinuitetsarbete ur ett IT-perspektiv. De menar att det på många håll återstår ”styrning, ledning, avsatta medel och resurser för arbetets planering och genomförande samt en tydlig uppföljning som är integrerad i övrig verksamhetsuppföljning” (Sveriges Kommuner och Regioner, 2021, p. 4).

Bland tidigare forskning behandlas till stor del teoretiska referensramar för hur arbetet med risk- och kontinuitetshantering bör bedrivas (Moh Heng, 2015; Sambo & Bankole, 2016; Setiawan, Wibowo & Hartanto Susilo, 2017). Dock finner vi bristande vetenskaplig kunskap om hur kommuners risk- och kontinuitetsarbete utförs i praktiken. Därmed vill vi med denna studie bidra till ökad kunskap om hur kommuner planerar, genomför och följer upp sitt arbete med risk- och kontinuitetshantering.

1.1 Forskningsfråga

I denna studie kommer följande frågeställning att besvaras:

- Hur arbetar kommuner med risk- och kontinuitetshantering?

1.2 Syfte

Denna studie syftar till att ge en ökad förståelse kring hur kommuners arbete med risk- och kontinuitetshantering bedrivs.

1.3 Avgränsningar

Studien avgränsas till att behandla kommuners arbete med risk- och kontinuitetshantering ur ett IT-perspektiv. Vidare avgränsas studien till att behandla kommuners risk- och kontinuitetsarbete på en strategisk nivå och därmed utelämna en djupare förståelse om deras specifika operativa rutiner och dess utförande. Valet att utelämna behandlingen av operativt arbete motiveras av att sådan information sannolikt är belagd med sekretess enligt Offentlighets- och sekretesslag (2009:400). Enligt Myndigheten för samhällsskydd och beredskap (2020) är huvudregeln att insynen i kommuners risk- och sårbarhetsarbete ska vara offentlig, men begränsad om nödvändigt. De menar att exempelvis detaljerade beskrivningar av kommuners agerande vid händelse av en incident kan behöva beläggas med sekretess. Detta då informationen, om den kommer ut, skulle kunna innebära skada för kommunen eller samhället i stort (Myndigheten för samhällsskydd och beredskap, 2020).

2 Risk- och kontinuitetshantering

Under de senaste decennierna har beroendet av IT ökat vilket utsatt organisationer för en mängd risker såsom cyberattacker, maskinvarufel och programbuggar (Krisinformation, 2023). Följaktligen har det blivit alltmer avgörande att skapa en strategisk kontinuitetsplanering och -hantering för att minimera effekten av dessa risker. En sådan plan representerar ett proaktivt tillvägagångssätt för att identifiera potentiella hot och sårbarheter, bedöma dess möjliga konsekvenser och utveckla strategier för att säkerställa att organisationer kan upprätthålla sina grundläggande affärsverksamheter under och efter en incident.

Herbane (2010) beskriver att kontinuitetsledning och -hantering under lång tid drivits utifrån reglering och standarder vilka grundats i USA, Storbritannien och Singapore. Till en början belyste dessa regleringar betydelsen av mänskliga fel och illvillg avsikt i förhållande till elektroniska lagringssystem. Efter 11:e september-attackerna ökades införandet av dessa riktlinjer och förordningar. Dessa krävde att medlems- eller användarorganisationer hade verifierbara processer för verksamhetskontinuitet. Fokus låg på att införa minimikrav för skydd i starkt sammanlänkade sektorer som handel och teknik (Herbane, 2010).

Vidare menar Herbane (2010) att det från mitten av 2000-talet sattes fokus vid internationalisering av standarder och riktlinjer som överskrider bransch- och nationsgränser. De sökte att etablera erkända kapabiliteter och bästa praxis. Dessa standarder betonade vikten av samarbete mellan organisationer under kriser och tjänade inte bara till att säkerställa organisatorisk efterlevnad, utan fastställde även minimikrav angående framgång för leverantörer av återställningscenter (Herbane, 2010).

Arbetet med risk- och kontinuitetshantering börjar i många fall först efter att en incident uppstått. Både Phillips och Landahl (2020) och Rima och Snedaker (2014) påpekar hur en katastrof, antingen hos den egna organisationen eller hos närliggande organisationer, är ett av de mest effektiva medlen för att öka medvetandet över risk- och kontinuitetshanteringens vikt.

2.1 Syftet med risk- och kontinuitetshantering

Det främsta målet med en kontinuitetsplan är att minimera driftsavbrott och bevara kritiska funktioner för att skydda en organisations tillgångar och anställda (Hayes, et al., 2013). Detta innebär att man skapar långsiktiga, strategiska och evidensbaserade planer som är utformade att säkerställa att organisationer fortsätter fungera effektivt, oavsett de hot eller risker de kan stöta på. Framför allt säkerställer kontinuitetshantering organisationsresiliens genom att förbereda organisationen att effektivt hantera oförutsedda händelser eller kriser, vilket ger organisationen möjlighet att snabbt återuppta sina viktigaste verksamheter. Phillips och Landahl (2020) framhäver resiliens som en av de främsta vinster med kontinuitetshantering, det vill säga abiliteten att stå emot, absorbera, reagera och adaptera sin verskamhet efter avbrott.

En kontinuitetsplan utrustar organisationen för att studsa tillbaka och återuppta verksamheten efter en katastrof eller kris. Rima och Snedaker (2014) understryker hur kontinuitetshantering proaktivt låter organisationer upptäcka och spåra framväxande kontinuitetshot och samtidigt

utforma strategier för att minska effekterna av betydande risker. Det ger organisationer de nödvändiga verktygen för att reagera snabbt och effektivt samt att minska påverkan på anställda, varumärke, kunder och externa intressenter (Phillips & Landahl, 2020).

Dessutom bevarar risk- och kontinuitetsarbete kundförtroende och organisationsrykte. Phillips och Landahl (2020) menar att kunder styr blickarna ifrån verksamheter de tror agerat bristande vid katastrofer eller ifall kundinformation inte förvarats på ett säkert sätt. Genom att organisationer implementerar en robust plan kan de visa sitt engagemang för motståndskraft och beredskap, vilket kan bidra till att behålla deras kundbas och upprätthålla förtroendet hos intressenter. Vidare menar Rima och Snedaker (2014) att en utformad plan även bidrar till att bibehålla de anställda efter en kris genom att snabbare gå tillbaka till normal verksamhet samt att behålla lugnet hos de anställda.

Vissa branscher kräver risk- och kontinuitetsarbete för regulatorisk efterlevnad, eftersom organisationer juridiskt är skyldiga att upprätthålla detta. I dessa branscher är det avgörande att följa reglerna för att undvika böter, straff och andra potentiella konsekvenser till följd av regelbrott. Enligt Hayes, Kotwica och Correia (2013) listar 74% av organisationer statlig reglering som en primär drivkraft för att implementera ett risk- och kontinuitetsarbete.

Slutligen ger risk- och kontinuitethantering konkurrensfördelar där organisationer med en väl genomförd hantering är mer benägna att återhämta sig snabbt från en incident. Det ger därmed fördelar jämfört med organisationer med en mindre effektiv plan eller avsaknad av plan. Rima och Snedaker (2014) jämför kontuinitetshantering med en bilförsäkring, som är något man helst inte vill behöva använda sig av men vilket man inte vill bli påkommen utan.

Syftet med risk- och kontinuitetshantering är därmed mångtaligt. Det finns lagkrav på organisationer samtidigt ger det större förtroende för både intressenter och anställda vid och efter en krissituation. Risk- och kontinuitetshantering förbereder organisationen för att snabbt kunna återgå till normal verksamhet samt minskar effekterna av större verksamhetsavbrott.

2.2 Referensram för risk- och kontinuitetshantering

Arbetet med risk- och kontinuitetshantering består av sju faser. Den exakta benämningen och uppdelningen av dessa varierar i forskningen, men kan sammanställas enligt följande:

1. Initiering av program
2. Riskbedömning
3. Effekt- eller konsekvensanalys
4. Val av riskbehandlingsstrategier
5. Utveckling av återställningsplaner
6. Träning och test av återställningsplaner
7. Underhåll av återställningsplaner

Faserna genomförs i kronologisk ordning där resultatet av en fas är indata till nästkommande, men många av faserna kan övergå i varandra eller genomföras parallellt (Moh Heng, 2015). I följande kapitel presenteras de olika faserna och dess innehåll.

2.2.1 Initiering av program

Den första fasen i risk- och kontinuitetshantering handlar om att initiera ett risk- och kontinuitetsprogram inom organisationen (Devargas, 1999). Under denna fas ska programmets omfattning samt organisationens kontinuitetsmål definieras (Moh Heng, 2015). Swanson, Bowen, Wohl Phillips, Gallup och Lynes (2010) menar att detta är för att programmet ska bli så effektivt som möjligt samt att säkerställa att de anställda helt förstår programmets krav. Iyer och Bandyopadhyay (2000) menar att definitionerna ska vara så precisa som möjligt och att målen ska ligga i linje med organisationens vision, mission och strategier.

Organisationens ledningsgrupp ska ansvara för definitionen av programmets omfattning och kontinuitetsmål (Lindström, Samuelsson & Hägerfors, 2010). De ska, enligt Sambo och Bankole (2016), stötta och vara inkluderade i det genomgående arbetet med risk- och kontinuitetshantering.

Programmet ska innehålla förebyggande kontrollinstrument, varav en eller flera definierade hanteringsplaner för risk och kontinuitet är det mest kritiska instrumentet, enligt Setiawan, Wibowo och Hartanto Susilo (2017). Andra instrument är riskbedömning, effektanalys, strategival, träning och test av risk- och kontinuitetshanteringsplaner samt underhåll av dessa, vilka beskrivs under respektive fas i kommande underkapitel.

Gibb och Buchanan (2006) menar att under initieringen av programmet ska roller för olika ansvarsområden definieras och tillsättas. Vidare ska en tidsplan skapas, samt en budget avsättas (Moh Heng, 2015).

2.2.2 Riskbedömning

Iyer och Bandyopadhyay (2000) definierar risk som potential för förlust på grund av katastrof. Risk- och kontinuitetsarbetet handlar enligt Moh Heng (2015) i denna fas om att bedöma risker och syftet med riskbedömningen är att mildra eller minimera riskerna och hoten mot organisationen. Bedömningen är viktig då risker som inte hanteras på rätt sätt kan störa kontinuiteten i verksamheten, exempelvis genom att utnyttja sårbarheter i system vilka kan komma att påverka verksamhetens processer eller funktioner (Dey, 2011).

Riskbedömningen börjar med att identifiera risker dels för varje affärsområde, dels för de mest kritiska processerna som vid händelse av avbrott snabbt måste åter fungera (Setiawan, et al., 2017). Riskidentifiering bygger på antaganden om möjliga hot mot organisationen (Iyer & Bandyopadhyay, 2000) och kan generellt delas upp i naturligt förekommande risker, såsom brand eller strömavbrott, och artificiella risker vilka är ett resultat av den mänskliga faktorn (Gibb & Buchanan, 2006). De artificiella riskerna kan i sin tur delas in i avsiktligt och oavsiktligt förekommande. En avsiktlig risk kan vara ett dataintrång och en oavsiktlig risk kan vara att en anställd oaktsamt modifierar, flyttar eller raderar data, programvara eller dokumentation (Iyer & Bandyopadhyay, 2000).

Efter riskidentifiering följer riskutvärdering som syftar till att skatta sannolikheten för att en viss identifierad risk uppstår (Gibb & Buchanan, 2006). Kriteriet som används för att skatta sannolikheten definierar Setiawan, Wibowo och Hartanto Susilo (2017) som sannolikheten för i vilken utsträckning en identifierad risk kan orsaka eller utveckla ett hot mot organisationen. Den skattade sannolikheten ska kategoriseras efter sannolikhetsgrad. Gibb och Buchanan

(2006) menar att det också är viktigt att skatta den sannolika frekvensen för en identifierad risk.

Riskbedömning ska genomföras av en oberoende part inom eller utanför organisationen som vanligtvis arbetar med att genomföra bedömningar eller granskningar enligt formella metoder (Setiawan, et al., 2017). Resultaten ska dokumenteras och rapporteras till ledningen (Moh Heng, 2015).

2.2.3 Effekt- eller konsekvensanalys

Risk- och kontinuitetsarbetet handlar i denna fas om att analysera och skatta effekterna, alltså de affärsmässiga konsekvenserna, av de bedömda riskerna från föregående fas. En effekt- eller konsekvensanalys, på engelska kallad Business Impact Analysis, skapar en bättre uppfattning om organisationens kritiska processer, system och funktioner vilket gör återställningen efter avbrott effektivare (Iyer & Bandyopadhyay, 2000). Iyer och Bandyopadhyay (2000) menar att information om det operativa arbetet inklusive hårdvara, nätverk och mjukvara ska samlas in för att kunna analysera och kategorisera vilka processer, system och funktioner som är kritiska, viktiga, användbara samt oväsentliga. Clark (2010) menar att utan en effekt- eller konsekvensanalys har organisationen ingen uppfattning om vilka system och funktioner som faktiskt är betydande för verksamheten och vad som skulle kunna göras utan dessa om det skulle behövas.

Effekt- eller konsekvensanalysen ska även behandla kombinationen av risk samt konsekvenser i flera led, det vill säga de risker och konsekvenser som eventuellt kan uppstå till följd av en specifik risk och konsekvens. Detta ska göras dels för de risker som inte påverkar varandra, dels för de risker som påverkar sannolikheten för att andra risker kan uppstå (Gibb & Buchanan, 2006).

En viktig del av effektanalysen är att kvantifiera avbrott i olika processer, system och funktioner. Dey (2011) menar att en organisation ska kvantifiera hur långt ett avbrott i en process, ett system eller en funktion kan pågå utan att få allvarliga konsekvenser för organisationen, så kallat Maximum Tolerable Downtime. Gibb och Buchanan (2006) menar att det är viktigt att fastställa den tidpunkt där avbrottet pågått under så lång tid att konsekvenserna blivit så stora en återställning blir omöjlig att genomföra. De menar vidare att de mest sårbara systemen och funktionerna är de felkritiska systemdelarna[1] samt de som är beroende av tredje part. Kvantifieringen är också viktig för att kunna ge riktlinjer till val av lämpliga återställningsmetoder (Swanson, et al., 2010).

Vidare ska en organisation kvantifiera återställningstiden för olika processer, system och funktioner vid händelse av avbrott. Återställningstiden, kallad Recovery Time Objective, innebär enligt Sambo och Bankole (2016) den tid det tar att återställa en process, ett system eller en funktion till normal drift efter ett planerat eller oplanerat avbrott eller katastrof. De menar att kvantifieringen är viktig för att välja lämplig återställningsteknik som håller sig inom ramen för Maximum Tolerable Downtime.

Resultaten av effektanalysen ska sammanställas och presenteras för organisationsledningen i form av en skriftlig rapport, ofta kallad Business Impact Analysis Report (Moh Heng, 2015).

[1] En felkritisk systemdel är en ”del av ett it-system som måste fungera för att it-systemet som helhet, eller centrala funktioner i systemet, ska fungera” (IDG, 2020).

De mest intressanta resultaten ska även presenteras muntligt. I samband med detta ska ledningen uppdateras om hur resultaten kommer att påverka val av riskbehandlingsstrategier i den efterföljande fasen i risk- och kontinuitetsarbetet.

2.2.4 Val av riskbehandlingsstrategier

Med resultaten från effektanalysen som utgångspunkt ska organisationen i denna fas utveckla riskbehandlingsstrategier. Setiawan, Wibowo och Hartanto Susilo (2017) menar att syftet med riskbehandlingsstrategier är att reducera de risker som hotar organisationens affärs- och IT-kontinuitet. Utvecklingsarbetet består av att fastställa och välja operativa strategier för att upprätthålla eller fortsätta de kritiska processerna, systemen och funktionerna vid händelse av avbrott (Moh Heng, 2015). Enligt Devargas (1999) ska fastställande och val av strategier baseras på upprätthållningen av verksamheten vid korta, medellånga respektive långa avbrott.

Setiawan, Wibowo och Hartanto Susilo (2017) beskriver fyra riskbehandlingsstrategier att välja att implementera i en organisation:

- *Acceptera risk*: Denna strategi innebär att acceptera risken genom att behålla den utan att vidta någon ytterligare åtgärd. Att behålla risken räknas i sig som en aktiv åtgärd. Kostnaden för att implementera denna strategi är låg, men blir hög när risken uppstår och en återställning behöver genomföras.

- *Ta bort risk*: Denna strategi är motsatsen till att acceptera risk och innebär att organisationen reducerar risken till en nivå som är så låg som möjligt, till exempel genom att stänga av ett kritiskt system. Kostnaden för att implementera denna strategi är mycket hög, medan återställningskostnaden är låg.

- *Begränsa risk*: Denna strategi innebär att vidta åtgärder för att begränsa att risken uppstår, till exempel genom att göra dagliga säkerhetskopior av kritiska data. Riskbegränsning är den vanligaste strategin att tillämpa.

- *Överföra risk*: Denna strategi innebär att överföra eller dela risken med en annan aktör. Detta görs vanligtvis genom ett avtal med en leverantör eller ett försäkringsbolag. Risköverföring är relaterad till kostnadsutgifter och kostnaden för överföringen bör vara mindre än kostnaden för att ha kvar ansvaret för risken.

2.2.5 Utveckling av återställningsplaner

Denna fas handlar om att skapa en implementeringsplan i form av ett dokument med specificerade åtgärder för återställning av process, system eller funktion vid händelse av avbrott, på engelska kallad Disaster Recovery Plan, vilken baseras på effektanalysrapporten och valda riskbehandlingsstrategier (Moh Heng, 2015).

Enligt Cerullo och Cerullo (2004) ska det i planen tydligt framgå vilken anställd som har det primära eller sekundära ansvaret för en specifik åtgärd, samt instruktioner för hur denna åtgärd genomförs. De menar att instruktionerna ska inkludera ett tillvägagångssätt för alternativt operativt arbete vid händelse av avbrott samt hur den drabbade verksamheten ska återställas till normalt läge. Instruktionerna ska även inkludera en lista med kontaktuppgifter till

ledning och relevanta chefer, samt en lista över alternativa mötesrum och lokaler för incidenthantering (Cerullo & Cerullo, 2004).

Återställningsplanens innehåll inklusive alla åtgärder för återställning ska godkännas av ledningen innan de publiceras. Detta är enligt Moh Heng (2015) viktigt för att ansvarig person ska kunna ta beslut om att aktivera planen vid händelse av avbrott utan att behöva invänta godkännande från högre chef.

Moh Heng (2015) menar att när en plan aktiveras vid händelse av avbrott ska samtliga anställda inom den aktuella avdelningen följa sina tilldelade instruktioner. Det är därför viktigt att säkerställa att varje plan finns tillgänglig för relevant avdelning och eventuella externa aktörer, samt att planen är välstrukturerad med lättlästa steg-för-steg-instruktioner att följa (Moh Heng, 2015).

2.2.6 Träning och test av återställningsplaner

Träning och test är nödvändigt för att säkra en kontinuitetsplan och att denna fungerar. Med hjälp av regelbundna tester säkrar man dess relevans och utförbarhet (Gibb & Buchanan, 2006). Dey (2011) antyder på att träning ökar de anställdas medvetande och kunskap över kontinuitetspolicies och procedurer. Lindström, Samuelsson och Hägerfors (2010) redogör att träning generellt är till för att hjälpa folk att lära sig av erfarenheter och att arbeta mer effektivt. Dessa tester bör utföras på ett regelbundet schema. Gibb och Buchanan (2006) anser att dessa bör göras minst en gång om året efter att man infört en plan.

Vad som bör testas delar Gibb och Buchanan (2006) upp i två huvudkategorier: teknologiorienterade tester och process- och serviceorienterade tester. De teknologiorienterade testerna riktar sig mot att säkerställa att all hårdvara fungerar, som exempel att testa att backupenheter fungerar och att återhämtning av data fungerar från dessa. De process- och serviceorienterade testerna hanterar i stället tillgängligheten av personal, dess responskraft och bekantskap mot specifika test. Resultatet av test och träning ska enligt Devargas (1999) komma från bland annat checkliststest, parallella test och fulla avbrottstest.

2.2.7 Underhåll av återställningsplaner

För att planen ska reflektera organisationen och dess krav behöver den fortsätta uppdateras och underhållas. Målet med underhåll är att inte bli överraskad när en faktisk katastrof eller uppehåll i verksamheten uppkommer (Iyer & Bandyopadhyay, 2000). Enligt Devargas (1999) är det kritiskt att alla förändringshanteringsprocesser ses över mot de etablerade återhämtningsplanerna. Samtidigt understryker Gibb och Buchanan (2006) att det är essentiellt för organisationer att inte bli självbelåtna och därmed misslyckas att uppdatera sina kontinuitetshanteringsplaner.

Det är viktigt att de dokumenterade planerna fortsatt stämmer överens med kontinuitetsstrategin när verksamhetens processer, marknadskrav och beroende teknologi konstant förändras. Organisationen bör enligt Moh Heng (2015) vid underhåll av kontinuitetshanteringsplanerna:

- Säkerställa att planen överensstämmer med den nuvarande verksamheten och den nuvarande operativa konfigurationen.
- Säkerställa tillgängligheten för planen.

- Underhålla planen så att denna uppnår en acceptabel standard och effektivitet.
- Säkerställa att planen ligger i linje med internationella standards.

Genom att underhålla verksamhetens kontinuitetshantering och dess planer kan man säkerställa att dessa förhåller sig till det nuvarande klimatet och de uppdaterade processerna. Med detta kan organisationen uppnå det huvudsakliga målet med kontinuitetshantering om återställningsbarheten av sina processer.

2.3 Standarder för risk- och kontinuitetshantering

I Sverige har Myndigheten för samhällsskydd och beredskap tillsammans med Svenska Institutet för Standarder tagit fram en standard, Vägledning för kontinuitetshantering, vilken syftar till att sammanbinda hela kedjan från vad kontinuitetshantering är till för till hur man ska arbeta med detta (Svenska Institutet för Standarder, 2014). Denna standard grundar sig i ISO 22301 och ger rekommendationer till hur kontinuitetslösningar och verksamheters kontinuitetsförmåga stärks över tid genom att minimera risker för allvarliga avbrott.

Standarden ISO 22301:2019 – Security and resilience – Business Continuity Management Systems – Requirements har som mål att tillhandahålla struktur och krav för upprätthållandet av en kontinuitetshanteringsplan där dessa är rimliga i förhållande till omfattningen av, samt under en störning av, verksamhetskontinuiteten (ISO, 2019).

Kraven och målen i dessa ramverk och standarder är generella och oberoende av organisationsstorlek och -typ för att kunna anpassas utifrån organisationen. Omfattningen av den applicerade planen blir därmed beroende av organisationens komplexitet (Svenska Institutet för Standarder, 2014). Målet är att implementera och hantera system för verksamhetskontinuitet samtidigt som man säkerställer konformitet med en given kontinuitetspolicy. Vidare ska dessa ramverk möjliggöra kontinuerlig leverans av service och produkter under och efter ett avbrott.

3 Metod

3.1 Litteraturstudie

Litteraturstudien är baserad på artiklar som behandlar ämnet risk- och kontinuitetsplanering, på engelska kallat business continuity planning. Genomgången av litteratur utgör enligt Oates, Griffiths och McLean (2022) grunden för studien, med syftet att identifiera teman som kan användas för att vägleda och underlätta insamlingen av relevant empiri. Sökningen efter relevant litteratur gjordes via de kredibla databaserna LUBsearch och Google Scholar. Flertalet söktermer definierades och användes metodiskt i sökningen enligt rekommendationer av Oates, Griffiths och McLean (2022). Dessa sammanfattas i tabell 3.1.

Tabell 3.1: Sammanfattning av söktermer

Sökterm	**I kombination med**
• Business continuity • Business continuity plan • Business continuity planning • Business continuity management • BCP • Risk management	• History • Literature review • Framework • Standard

Sökresultaten sammanställdes till 17 relevanta vetenskapliga artiklar, vilka presenteras i tabell 3.2.

Tabell 3.2: Tema och tillhörande artiklar

Tema	**Källor**
Syftet med risk- och kontinuitetshantering	(Hayes, Kotwica & Correia, 2013), (Phillips & Landahl, 2020), (Rima & Snedaker, 2014), (Herbane, 2010)
Referensram för risk- och kontinuitetshantering	(Cerullo & Cerullo, 2004), (Clark, 2010); (Devargas, 1999), (Dey, 2011), (Gibb & Buchanan, 2006), (Iyer & Bandyopadhyay, 2000), (Lindström, Samuelsson & Hägerfors, 2010), (Moh Heng, 2015); (Sambo & Bankole, 2016), (Setiawan, Wibowo & Hartanto Susilo, 2017), (Swanson et al. 2010)
Standarder för risk- och kontinuitetshantering	(ISO, 2019), (Svenska Institutet för Standarder, 2014)

3.2 Empirisk studie

3.2.1 Val av insamlingsmetod

Efter att en initial forskningsfråga formats och majoriteten av litteraturen sammanställts togs beslutet att den empiriska insamlingen skulle ske med hjälp av intervjuer. Inför detta beslut vägdes olika insamlingsmetoder mot varandra, främst metoderna intervju och enkät, där en kvalitativ intervjustudie ansågs kunna ge det bästa resultatet för studiens syfte. Fördelarna som sågs i att föra intervjuer var möjligheten till mer detaljerade svar på de frågor som skulle ställas samt de övergripande teman studien ämnade att samla information om. Med intervjuer fanns även bättre möjligheter att validera respondenternas trovärdighet inom det valda ämnet. På så sätt kunde det säkras att få in kvalitativa svar över de teman och frågor studien ämnade svara på. Mer detaljerade svar tar Oates, Griffiths och McLean (2022) upp som en av de stora fördelarna med intervjuer samt enklare validering av respondenterna. Informationen som samlas in kommer även vara av stor relevans för den som blir utfrågad (Jacobsen, 2002). Dock är en av de största nackdelarna med intervjuer att de riskerar att bli missledande, där respondenterna säger vad de tycker och tänker i stället för vad som faktiskt är fallet (Oates, Griffiths & McLean, 2022).

Vidare är en nackdel att studien skulle få in färre svar och därmed inte kunna dra generella slutsatser. En enkät skulle med största sannolikhet kunna garantera fler svar på studiens frågor. Dessa svar hade dock inte kunnat valideras till samma nivå då man inte vetat vem som svarat på enkäten. Oates, Griffiths och McLean (2022) menar att formulär används när man vill ha in en större mängd data och där man vill få in relativt korta svar. Denna studie ville dock få in detaljerade och nyanserade svar. Med dessa för- och nackdelar i åtanke valdes det att föra intervjuer som insamlingsmetod då detta ansågs kunna ge det mest kvalitativa och relevanta resultatet.

3.2.2 Intervjuguide

Utifrån den insamlade litteraturen sammanställdes en intervjuguide där frågorna var ämnade att besvara de huvudsakliga teman utifrån kontinuitetsarbetets sju faser vilka ansågs betydelsefulla för driften av ett risk- och kontinuitetsarbete. Frågeformuleringar baserades utifrån det frågebatteri Jangefelt-Nilsson och Skarin (2010) använde under deras studie om kontinuitetsledning vid oförutsedda händelser. Anledningen till att en intervjuguide sammanställdes grundas i Oates, Griffiths och McLean (2022) rekommendationer att en guide är viktig för att få in de övergripande ämnena, dock utan att vara låst till att endast ställa de fördefinierade frågorna.

3.2.3 Urval

Efter val av insamlingsmetod gjordes ett urval över vilka som var tänkt att intervjua. Till en början gick tankarna mot företag som konsulterar inom risk- och kontinuitetshantering, men efter att ha läst flera artiklar angående kommuner som drabbats av intrång eller verksamhetsuppehåll övergick tankarna mot Sveriges kommuner. Efter beslutet att föra intervjuer med kommuner togs beslutet att skicka ut en förfrågan via mejl till de tolv största kommunerna, baserat på statistik från SCB (2022). Dessa var vid tillfället:

- Stockholm
- Göteborg
- Malmö
- Uppsala
- Linköping
- Örebro
- Västerås
- Helsingborg
- Norrköping
- Jönköping
- Umeå
- Lund

Förfrågan sändes till respektive kommuns kontaktcenter. I de fall där kontaktuppgifter till chef för kommunens IT-avdelning eller motsvarande fanns skickades även en direktförfrågan om medverkan.

Av de tolv kommuner som kontaktades inkom svar från sex kommuner. Av dessa svar var det fyra som gick med på att föra en intervju. I och med detta bokades det in fyra intervjuer.

Valet att kontakta Sveriges största kommuner motiveras genom att dessa representerar en stor andel av Sveriges befolkning. Dessa kommuner har samtidigt mer resurser att utföra ett kontinuitetsarbete och därav ansågs dessa som relevanta för denna studie. Det hade även varit intressant att göra en studie över mindre kommuner för att se hur arbetet ser ut där och möjligtvis jämföra större och mindre kommuner med varandra. Detta skulle då blivit för stort gentemot den begränsade tid avsatt för denna studie.

3.2.4 Intervju

Samtliga intervjuer genomfördes via Microsoft Teams. Intervjuerna spelades in med hjälp av Open Broadcaster Software Studio. Båda studieförfattarna deltog vid samtliga intervjuer. En av studieförfattarna ansvarade för att leda intervjun, medan den andre ansvarade för ljudinspelning och tog anteckningar för social kontext och ifall inspelningsstörningar skulle uppstå.

Intervjuerna framfördes på ett semistrukturerat tillvägagångssätt där relevanta sidospår och följdfrågor tilläts ställas. De första intervjuerna var mer åt det strukturerade hållet. I samband med att studieförfattarna fick mer erfarenhet av att bedriva intervjuer ställdes fler följdfrågor och utformningen blev mer semistrukturerad.

Intervjuguiden ansågs vara en vägledande *guide*, men det ansågs viktigt att få med respondenternas synvinkel på intervjufrågorna. Valet att föra semistrukturerade intervjuer baserades till stor del på Oates, Griffiths och McLean (2022) rekommendationer som lyfter möjligheten att få mer detaljerade svar från semistrukturerade intervjuer samtidigt som det låter respondenten säga vad hen verkligen vill.

En sammanfattning av förda intervjuer visas i tabell 3.3.

Tabell 3.3: Sammanfattning av intervjuer med respondenter

Kommun	Antal respondenter	Roll inom organisation	Längd på intervju	Inspelad
Helsingborg	1	Säkerhetsstrateg	40 min	Ja
Norrköping	2	IT-säkerhetsansvarig; IT-säkerhetsarkitekt	50 min	Ja
Umeå	1	Verksamhetschef för IT	35 min	Ja
Uppsala	1	Informationssäkerhetsstrateg	35 min	Ja

3.2.5 Bearbetning av empiri

Förda intervjuer transkriberades med hjälp av verktyget Whisper utvecklat av OpenAI. Det valdes att använda Whisper då det är ett automatiskt taligenkänningsverktyg tränat på 680 000 timmar ljudmaterial med en felfrekvens på 8% för det svenska språket (Radford, et al., 2022). Whisper har ett flertal olika modeller att använda sig utav. I denna studie användes den största modellen för att få lägsta möjliga felfrekvens.

För att använda Whisper skrevs ett Pythonskript vilket läste in ljudfilen av intervjun, transkriberade intervjun och till sist skrev transkriberingen till en textfil. För att validera transkriberingen lästes textfilen igenom och jämfördes med inspelningen. Där transkriberingen inte stämde korrigerades den utefter inspelningen.

Valet att använda Whisper underlättade transkriberingen märkbart då transkriberingen endast behövde korrigeras och formateras på ett fåtal ställen. Därmed uppnåddes hög kvalitet och objektivitet av transkriberingarna.

3.3 Validitet

För att säkerställa studiens validitet och trovärdighet sattes fokus vid informationsinsamlingen och den interna validiteten, där Oates, Griffiths och McLean (2022) menar att man behöver samla in rätt data från rätt källor. Detta gjordes genom att ställa frågor av relevans för studien och att dessa besvarades av respondenter med relevant kunskap och erfarenhet inom forskningsområdet.

Denna studie har däremot svårare att dra generella slutsatser på grund av en begränsad urvalsstorlek på endast fem respondenter från fyra kommuner. Detta bidrog till att studien inte kan säkerställa den externa validiteten, vilket enligt Oates, Griffiths och McLean (2022) säkerställs i de fall resultatet går att generalisera.

3.4 Reliabilitet

Oates, Griffiths och McLean (2022) menar att neutralitet och djup förståelse i forskningsämnet är essentiellt för att verkställa reliabilitet vid kvalitativa studier. För att säkerställa reliabilitet var bägge studieförfattare väl införstådda inom ämnet, i detta fall risk- och kontinuitetshantering, vilket fastställdes genom gedigen litteratursökning och litteraturgenomgång. Detta verkställde att författarna kunde ställa frågor som rörde de kategorier och faser funna i teorin.

3.5 Etik

Inför respektive intervju delades intervjuguiden ut för att ge respondenterna en övergripande blick över ämnet samt de frågor som kunde väntas ställas. Detta gjordes för att respondenterna skulle ha möjlighet för reflektion inför intervjun, vilket Oates, Griffiths och McLean (2022) rekommenderar av samma anledning och även för att ge kredibilitet till studien.

Väl vid intervjutillfället började studieförfattarna med att introducera sig själva och forskningsämnet med syftet att skapa förtroende och medvetande angående studien. Samtidigt beskrevs respondenternas rättighet att dra sig ur medverkan och deras rättighet att inte delta i studien. Genom att informera respondenterna om dessa rättigheter säkerställdes att intervjuerna och studien sköttes på ett etiskt vis. Informering till deltagare om deras rättigheter och att skapa en grundlig förståelse över arbetet och dess syfte är vad Oates, Griffiths och McLean (2022) pekar på som de viktigaste aspekterna för att utföra etisk forskning. Det har därför lagts stor vikt på dessa aspekter under arbetet.

Intervjumaterialet och transkriberingarna lagrades så att tillgång endast fanns till studieförfattarna för att bibehålla konfidentialitet och hindra publik tillgång. När dessa inspelningar var transkriberade avidentifierades respondenterna genom att ta bort namn och starkt identifierande attribut från materialet. Även avidentifiering och konfidentialitet är viktiga aspekter för att kunna utföra etiska forskningsarbeten. Tillvägagångssättet utgick även här ifrån Oates, Griffiths och McLean (2022) som benämner både konfidentialitet och avidentifiering som viktiga delar i det etiska arbetet.

Genom att informera i alla dessa steg togs alla möjligheter att säkra informerat samtycke till deltagandet och det material som delats med studieförfattarna. Detta samtycke är grunden för det etiska arbetet och är enligt Oates, Griffiths och McLean (2022) ett måste för att kunna utföra etisk forskning.

4 Resultat

4.1 Presentation av respondenter

Respondent 1 är verksamhetschef för Umeå kommuns IT-avdelning vilken ligger under teknik- och fastighetsnämnden och teknik- och fastighetsförvaltningen. Kommunen har totalt sett åtta förvaltningar där alla ligger under kommunfullmäktige. Totalt har kommunen runt 11 000 anställda.

Respondent 2 arbetar som informationssäkerhetsstrateg inom IT-staben för Uppsala kommun. Respondentens arbete är placerat under säkerhetsavdelningen och IT ligger inom kommunledningskontoret som har cirka 1800 anställda.

Respondent 3 innehar rollen som säkerhetsstrateg och arbetar inom stadsledningsförvaltningen vid Helsingborg kommun. Denna förvaltning är den övergripande förvaltningen inom kommunen och respondenten har suttit vid sin nuvarande roll i fem år. Kommunen har för närvarande cirka 11 000 anställda.

Respondent 4 arbetar som IT-säkerhetsarkitekt. Respondent 5 är IT-säkerhetsansvarig och gruppansvarig för IT-säkerhet, informationssäkerhet och juridik vid Norrköping kommun. De har jobbat fyra respektive fem år inom kommunen. De båda sitter inom digitaliseringsavdelningen vilken är en del av kommunstyrelsens kontor. De förklarar deras avdelning som ett stöd till kommunens övriga kontor.

4.2 Initiering av program

Respondent 1, Umeå kommun
Respondent 1 berättar att Umeå kommun har en övergripande kontinuitetsplanering. Det övergripande ansvaret ligger inom brand och räddning, med Umeåregionens brandförsvar som förvaltning. All form av skydd är centraliserad och håller ihop kommunens planering. Den bygger nedåt och varje förvaltning har en egen krisledningsdokumentation och styrning som ska matcha med det övergripande arbetet. Det i sin tur bryts ned till varje verksamhetsnivå genom en trappstege som innehåller hela kedjan från kommunledningsperspektiv till enskilda rutiner i verksamheten, exempelvis hur man ska göra vid händelse av bortfall.

Syftet med risk- och kontinuitetshanteringen menar Respondent 1 är att vidmakthålla funktionaliteten som behövs för att ha tillgång till information och systemstöd, för att kunna driva arbetet mot kommunens uppdrag och mål. Hen menar att även om mycket verksamhet kan bedrivas utan teknikstöd så är det mesta i någon mening kopplat mot teknik, vilket gör tillgången till information och systemstöd till en grundförutsättning för att bedriva arbetet i kommunen. Den drivande faktorn är att upprätthålla kommunens förmåga att bedriva verksamhet.

Respondent 1 berättar att Umeå kommun har tillsatta roller och ansvarsområden för kontinuitetsarbete både i den kommunövergripande krisledningsorganisationen och på förvaltningsnivå. Nu pågår ett arbete med att se över och bygga upp en krisledningsfunktion även längre ned i organisationen, utifrån MSB:s uttalade metodik och roller knutna till det. Hen menar att det för Umeå kommun i praktiken innebär att man på förvaltningsnivå och till och med på verksamhetsnivå kan ha en stabssituation med tillsatt stabschef, insatsledare och ansvar för kommunikation.

Vidare berättar Respondent 1 att brand- och räddningsnämndens organisation har en viss budget. De har också en tidsplan att se över alla kris- och kontinuitetsplaner och när det ska vara gjort, för att sedan följa upp att de finns tillgängliga. Hen påpekar att det på verksamhetsnivå inte finns någon dedikerad budget, utan det ingår i den vanliga driften. På verksamhetsnivå finns heller ingen tidsplan annat än att det kontinuerligt ska ses över så att planer och rutiner är uppdaterade och aktuella vid händelse av avbrott.

Respondent 2, Uppsala kommun
Respondent 2 berättar att Uppsala kommun arbetar med en modell som följer MSB:s rekommendationer för hur man ska arbeta med kontinuitet. Arbetet med kontinuitetshantering styrs från säkerhetsavdelningen, där man också arbetar med beredskapsfrågor. Kommunen har även en central modell för arbetet med riskhantering. Med sin befattning inom säkerhetsavdelningen arbetar Respondent 2 med att få in informationssäkerhetsperspektivet i kontinuitetsarbetet.

Kontinuitetsarbetet utgår ifrån perspektivet att upprätthålla samhällsviktig verksamhet, samhällsfunktion, under störningar och höjd beredskap eller krigssituationer, berättar Respondent 2. Detta genom att arbeta med krisberedskap och civilberedskap, vilket aktualiseras i och med Rysslands invasion av Ukraina. Omfattningen av risk- och kontinuitetsarbetet har ett riskbaserat angreppssätt utifrån ett verksamhetsbehov hos respektive verksamhet. Respondent 2 påpekar att i samhällsviktig verksamhet är kraven förstås högre. Hen menar att den drivande faktorn beror på lagar samt i de enskilda verksamheternas intresse att kunna bedriva sitt uppdrag även under kritiska störningar eller avbrott.

Ansvaret för risk- och kontinuitetsarbetet ligger i slutändan på den respektive linjeorganisation som har ett särskilt uppdrag att tillhandahålla samhällsviktiga tjänster, även om kommunledningskontoret verkar stödjande i arbetet. Respondent 2 menar att omfattningen på ansvaret varierar.

Det finns ingen generell tidsplan för arbetet med risk- och kontinuitetshantering, menar Respondent 2, men det finns stöd från den högre ledningen.

Respondent 3, Helsingborg kommun
Respondent 3 berättar att Helsingborg kommun har ett pågående pilotprojekt om kontinuitetshantering med fokus att arbeta likvärdigt i staden med dessa frågor. Kommunen har tagit fram en vägledning för hur kontinuitetsarbete ska bedrivas i staden, samt en mall för hur vägledningen ska följas.

Medvetandet kring kontinuitetsarbetet inom kommunen varierar bland förvaltningarna menar Respondent 3. Till exempel har vård- och omsorgsförvaltningen en ganska god kontinuitetshantering, medan det kan bli bättre på IT-avdelningen. IT-avdelningen arbetar med kontinuitetshantering ”på sitt sätt” (Bilaga E, s.47), men det borde arbetas lite mer strukturerat. Denna struktur är något som ska implementeras i och med det pågående projektet med

kontinuitetshantering. Att det medvetandet varierar menar Respondent 3 beror på att det är många förvaltningar och verksamheter inom kommunen där olika lagar, krav och förordningar som styr.

Respondent 3 berättar att målet med risk- och kontinuitetsarbetet är att upprätthålla kommunens kritiska processer vid händelse av incidenter eller avbrott. Den främsta drivande faktorn är att de analyser som skall göras är lagstadgade. Det innebär att man får en drivkraft och mandat till att bedriva detta arbete, menar hen. En annan drivande faktor är att det finns politiska uppdrag som styr vad verksamheten ska arbeta med.

Det finns en tidsplan för detta pilotprojekt som har löpt under ungefär ett års tid, berättar Respondent 3. Under denna tid har det funnits stöd från högre ledningen. Det var kommunledningen som gav IT-avdelningen i uppdrag att genomföra arbetet i staden, menar hen.

Respondent 4 och 5, Norrköping kommun
Respondent 4 och 5 berättar att Norrköping kommun inte har något uttalat övergripande projektarbete gällande kontinuitet. Däremot finns det en krisledningsplan, som bland annat använts under olika pandemiutbrott. Det finns också ett krisledningsutskott med politiskt inflytande. Efter IT-attacken där ryska hackare kom över huvudnyckeln till kommunens IT-miljö pågår ett arbete med att förbättra kontinuitetshanteringen, men inget konkret projekt har påbörjats. Som ett resultat av IT-attacken har ett antal åtgärder indicerats, som att förstärka robusthet i system och applikationsmiljö, processer, rutiner, roller och ansvar som ligger inom kontinuitetshantering. Detta både på central och verksamhetsnivå. Respondent 4 menar att alla verksamheter bedriver sin kontinuitetsutveckling på olika sätt då olika verksamheter har olika behov och tillgängligheter.

Respondent 5 berättar att kontinuitetsarbetet utgår ifrån kraven på tillgänglighet, konfidentialitet och spårbarhet samt de juridiska kraven. IT-avdelningen har drivit på dessa krav hos kommunledning i styrelse och fullmäktige för att kunna få ett beslut. Hen menar att det dock finns oklarheter i lagstiftningen gällande tillgänglighet och användarbarhet i saker och ting.

Respondent 4 menar att den drivande faktorn kommer ifrån att man har insett att system inte är tillgängliga jämt då man av yttre omständigheter tvingats ta ner system, och därmed insett vikten av att ha tillgänglighetsdefinierade krav i avtal. Man tittar på att formalisera sina relationer mellan de interna verksamheterna för att kunna ställa tydligare krav. Detta för att kraven inom en intern verksamhet sedan innan har varit att göra ”ett bra jobb” (Bilaga F, s.54). Respondent 4 menar att det när en händelse inträffar är viktigt att veta vad som gäller, vad som ska prioriteras och vilka konsekvenser det får, även ekonomiskt. Vidare menar Respondent 4 att det huvudsakligen handlar om kraven på tillgänglighet.

4.3 Riskbedömning

Respondent 1, Umeå kommun
Respondent 1 berättar att riskbedömningar görs internt och att de identifierat risk ur flera perspektiv. I de olika verksamheterna har en klassificering av information som finns i respektive system gjorts. Hen menar att detta sätter ribban för vilken typ av säkerhetsstöd som behövs för att upprätthålla den informationssäkerhet som informationen kräver.

Vidare har Umeå kommun identifierat och bedömt risk för de verksamheter som har de mest kritiska processerna, framför allt de verksamheter där liv och hälsa står på spel. Dessa verksamheter har riskåtgärder och IT-avdelningen är delaktiga ur ett teknikperspektiv för att stötta och säkerställa att åtgärder fungerar så bra som möjligt.

Respondent 1 menar att det är svårt att avgöra om de har identifierat alla kritiska delar, då det alltid kommer att finnas ett scenario i någon process som de inte har tänkt på. Hen förklarar att ett sätt att identifiera så många risker som möjligt är att få in andra perspektiv, både internt och externt. Detta för att kunna dra nytta av varandra och varandras uppfattning om olika scenarion. Hen menar att det trots verksamheternas olikheter kan finnas liknande mönster.

Riskdokumentationen sker med hjälp av Klassa som är ett informationsklassningsverktyg framtaget av Sveriges Kommuner och Regioner, SKR. Kommunen har också dokumentation för respektive område och system, både ur verksamhets- och tekniskt perspektiv.

Respondent 2, Uppsala kommun
Respondent 2 berättar att riskbedömningar drivs internt, men de identifierar även risker med hjälp av externa rapporter och indikationer eller inspel från omvärlden.

Hen menar att varje affärsområde har som uppdrag att göra sina egna riskbedömningar. Detta är kopplat till nämnder, den politiska ledningen och de verksamheter som stödjer den politiska ledningen. Det infaller i respektive affärsområdes uppdrag att genomföra riskbedömningar. Hen kan dock inte svara för hur respektive verksamhet har arbetat med detta.

Respondent 2 förklarar att det finns en uppfattning om vilka verksamheter som är de mest kritiska, eller mer kritiska än andra, men att det är svårt att veta om alla kritiska delar identifierats. Hen menar att det är en intern bedömning och att det krävs ett systematiskt arbete från ledningens perspektiv att arbeta med dessa bedömningar. Respektive verksamhet får göra sin bedömning och rapportera till centralfunktionen, menar hen.

Vidare förklarar Respondent 2 att det ingår i kommunens modell att bedöma sannolikheten för att en specifik risk uppstår samt den sannolika frekvensen, men kan inte gå in på enskilda risker. Riskerna kategoriseras dock utifrån ifall de är strategiska, operativa eller finansiella. Kommunen tittar även på risker ur ett påverkansperspektiv – ifall risker påverkar en verksamhets möjlighet att utföra sitt uppdrag – framför allt där liv och hälsa står på spel.

Ytterligare berättar Respondent 2 att det ingår i deras modell att dokumentera riskerna. Hen menar att det i modellen finns mallar och stöddokumentation med anvisningar om hur risker ska dokumenteras.

Respondent 3, Helsingborg kommun
Respondent 3 berättar att riskbedömningar görs internt och att de har identifierat och kategoriserat risk i exempelvis cyberattacker, fysiska attacker, sabotage eller naturkatastrofer.

Hen berättar att det nu genomförs risk- och sårbarhetsanalyser. Kommunen gör detta vart fjärde år enligt lag. Arbetet drivs från stadsledningsförvaltningen och analyser görs på samtliga förvaltningar och kommunala bolag. Analysen bygger på ett frågebatteri som tagits fram av stadsledningsförvaltningen och består av frågor inom flertalet områden. Varje förvaltning ska svara på dessa och sedan gör stadsledningsförvaltningen en sammanställning av svaren. Sammanställningen ska beslutas i kommunfullmäktige och sedan presenteras.

Respondent 3 berättar att kommunen har bedömt risk för varje affärsområde. Hen vill inte svara på frågan om de har identifierat och bedömt risk för de mest kritiska processerna. Respondent 3 menar dock att kommunen följer sin mall för riskbedömning när de identifierar och skattar risker. Kommunen dokumenterar risker utifrån deras kriteriemodell, konsekvensanalysmodell och beroendeanalysmodell.

Respondent 4 och 5, Norrköping kommun
Respondent 4 och 5 berättar att underlaget för riskbedömning tagits fram tillsammans med externa IT-bolag, men att underlaget för beslut tagits fram internt och presenterats för de olika beslutsfattande instanserna. Vidare berättar de att kommunen har identifierat risk.

Inom området informationssäkerhet har de fokuserat på tillgänglighet och sekretess i förhållande till lagstiftningar, mer specifikt GDPR, Personuppgiftslagen (PUL) samt Offentlighets- och sekretesslagen (OSL). De har till exempel fokuserat på utmaningen med röjning av sekretess för information för oberoende, där kraven är olika höga beroende på om informationen rör exempelvis patientdata eller bygglov. Dessa aspekter har tagits hänsyn till när de bedömer risk och konsekvens.

Respondent 5 lyfter även dessa lagstiftningar som problematiska vid riskanalys men att leverantörer även sett dessa hinder och den osäkerhet lagstiftningen ger organisationer som kommuner och statliga myndigheter. Respondent 4 tillägger att leverantörer utefter dessa hinder har utformat workshops och material för att påvisa möjligheter trots lagstiftningen, där denna ska tolkas och behandlas i respektive verksamhet. Hen menar att Integritetsskyddsmyndigheten (IMY) i slutändan inte enbart kollar ifall man gjort rätt eller fel, utan bedömer de vidtagna åtgärderna för att förhindra informationsspridning samt ifall kommunen granskat och bedömt riskerna för detta.

Informationen klassas i verktyget Klassa från SKR. Respektive verksamhet klassar information genom sin informationssamordnare. Respondent 5 menar att det varierar hur uppdaterade dessa klassningar är beroende på om organisationen har rört på sig eller fått ett annat uppdrag och därmed fått andra processer och annan informationsmängd. Hen menar att om inte så är fallet är det möjligt att de använder äldre klassningar. Men säkerhetsavdelningen granskar och gör revisioner av detta. IT-avdelningen har ingen uppföljning, enligt Respondent 5.

Varje verksamhet, nämnd och myndighet har krav på sig att göra riskanalyser för att förbättra sin verksamhet berättar Respondent 5. Hen menar att vid en omorganisation eller om man får ett nytt uppdrag ska en riskanalys göras. Exempelvis i de fall där man behöver hantera system och information på annat sätt.

Respondent 5 menar att man i Norrköpings kommun inte tar verksamhetsriskerna upp till högre nivå och tittar på riskbilden ur ett helhetsperspektiv. Man tittar inte heller på perspektiv av risk, såsom operativa, informationssäkerhets-, ekonomiska och juridiska risker. Man har inte det arbetssättet, menar hen. Respektive nämnd ansvarar för sina risker, men på kommunnivå vet man inte om risker i helhet. Hen menar att man är lyckligt ovetande över helhetsbilden och vilka risker man har totalt sett. Detta gör att kommunen inte vet vad som är viktigast. Det behövs en strategi, påpekar hen.

Digitaliseringsavdelningen, där Respondent 4 och 5 arbetar, är ett stöd till att göra verksamheterna medvetna om de risker som finns. Respondenterna menar dock att nämnderna är ansvariga för att respektive verksamhet har tagit hänsyn till och bedömt riskerna på rätt sätt samt vidtagit rätt åtgärder.

Vidare menar respondenterna att det är upp till varje verksamhet att identifiera de risker som finns. Verksamheterna kategoriserar risker utefter operativa, ekonomiska eller juridiska risker. De berättar att det finns risker på många nivåer. Riskerna som bedöms på digitaliseringsavdelningen är hur hanteringen av information riskbedöms. Digitaliseringsavdelningen tittar på vilka risker som finns utifall informationen inte är tillgänglig och vad sannolikheten för att det inträffar är.

4.4 Effekt- eller konsekvensanalys

Respondent 1, Umeå kommun
Respondent 1 berättar att Umeå kommun i viss mån har analyserat eller skattat effekterna av förlust. Hen menar sig inte ha sett allt, men påpekar sig inte sett några kvantifieringar. Hen menar dock att det finns beskrivet vad det innebär ifall information försvinner, läcker eller inte är åtkomlig.

Vidare berättar Respondent 1 att IT-avdelningen har ganska god koll på hur lång tid ett enskilt system tar att återställa. Hen menar samtidigt att det knappt går att uppskatta hur lång tid det skulle kunna ta att återställa bortfall av en hel datahall. I ett sådant fall, menar hen, handlar det om att utgå ifrån en dokumenterad prioriteringslista och få i gång det viktigaste först. Hen påpekar att det viktigaste är att få i gång grunden, alltså infrastrukturen, för att kunna få i gång resten. Men det gäller att arbeta ur ett övergripande perspektiv då alla tycker att allting är viktigast, tillägger hen.

Respondent 2, Uppsala kommun
Respondent 2 berättar att det är en del av kommunens modell att göra effekt- eller konsekvensanalyser, men kan inte svara på att det faktiskt gjorts och i vilken omfattning. Hen tror att det kan bli bättre.

Uppsala kommun tittar även på eventuella multipla risker som faller ut samtidigt och orsakar en incident. Ett exempel kan vara att man har sårbarheter i skyddsåtgärderna som inträffar samtidigt, berättar respondent 2. Hen kan dock inte svara på ifall denna analys sker på ett systematiskt sätt eller att det görs specifikt sådana analyser.

Respondent 2 berättar vidare att det ingår i kommunens modell att göra analyser som visar ifall återställning av ett IT-stöd faller in inom tiden för verksamhetens tolerans. Hen menar att det finns en prioritering på vilka IT-stöd som i första hand ska analyseras men det är stor variation på att dessa analyser faktiskt bedrivs.

Respondent 3, Helsingborg kommun
Respondent 3 berättar att respektive verksamhet sköter sina effekt- eller konsekvensanalyser helt och hållet på egen hand men tror inte att det görs några faktiska analyser i någon större utsträckning.

Enligt Respondent 3 dokumenterar Helsingborg kommun sina motsvarande effekt- eller konsekvensanalyser utefter stadsövergripande mallar som tagits fram av stadsledningsförvaltningen i arbetat med risk- och kontinuitetshantering. Respondent 3 menar att de anställda uppskattar att initiativet kommer från stadsledningsförvaltningen gällande hur dessa frågor ska hanteras. Innan har var och en själv hittat egna lösningar som varierat i kvalitet, men i och med detta initiativ har de anställda möjlighet att förstå sambanden hur hela kommunen hänger

ihop, menar hen. Hen tror att det har varit en framgångsfaktor att börja kommunicera med övriga förvaltningar i dessa frågor.

Respondent 4 och 5, Norrköping kommun
Respondent 4 berättar att det finns ett slags verksamhetsutvecklande arbetssätt i de flesta verksamheter inom kommunen. Hen förklarar att de på digitaliseringsavdelningen målar upp fiktiva händelser och incidenter, där de tänker sig att deras ena datahall har gått ner eller att det brunnit i fiber mellan deras hallar, vilket resulterar att de inte kommer åt sina verktyg. Digitaliseringsavdelningen föreställer sig sedan vilka konsekvenser det skulle kunna få. Respondent 4 understryker att när de sitter tillsammans och föreställer sig olika scenarion kommer de på saker att lägga till som de inte tänkte på förra gången. Succesivt blir det bättre och bättre, menar hen.

Respondent 5 berättar att Norrköping kommun inte har kvantifierat specifika tider för återställning av processer, system eller funktioner vid händelse av avbrott. Arbetet fokuserar mer på att koppla verksamhetens krav på tillgänglighet till faktiska investeringar och åtgärder i deras infrastruktur. Det pratas till exempel om kostnadsdifferensen av att ha 98,5% eller 99,5% tillgänglighet och om den extra kostnaden går att motivera.

4.5 Val av riskbehandlingsstrategier

Respondent 1, Umeå kommun
Respondent 1 berättar att Umeå kommun har olika riskbehandlingsstrategier. Kommunen har bland annat redundans på sina miljöer, vilka verifieras minst en gång i månaden att de funkar. Vidare har kommunen ett flertal stödåtgärder, såsom reservkrafter, dieselaggregat och avtal med dieselleverantörer ifall den typen av bortfall skulle inträffa.

Strategier väljs genom att väga vikten av teknikstöd kontra tillgänglighet samt se ifall kommunens förmågor är tillräckliga eller om teknikstöd behöver flyttas ut externt. Respondent 1 menar att det ibland inte är möjligt att flytta ut något på grund av tekniska eller juridiska skäl.

Respondent 1 berättar vidare att Umeå kommuns strategier för återställning definieras i reservrutiner och återgång till normal produktion. Hen menar att det dock kanske inte är infört eller fungerande i olika omfattning beroende vilken verksamhet det handlar om.

Respondent 2, Uppsala kommun
Respondent 2 berättar att Uppsala kommun har fyra olika riskbehandlingsstrategier: acceptera risk, ta bort risk, begränsa risk samt överföra risk. Det vanligaste för kommunen är att arbeta med att begränsa risk, vilket bygger på sannolikhet eller konsekvens. Kommunen arbetar även med att överföra risk genom att låta en privat aktör till en början genomföra ett uppdrag i stället för att kommunen själv gör det, för att vid ett stabilt senare läge ta över uppdraget.

Val av riskbehandlingsstrategi görs exempelvis genom att ställa riskkostnad mot åtgärdskostnad, det vill säga hur dyrt det är att genomföra en riskförebyggande åtgärd i förhållande till riskvärdet. Respondent 2 menar att ifall man talar om legala krav och inte lyckas uppfylla dessa finns det inte mycket annat att göra än att upphöra med den verksamheten.

Respondent 3, Helsingborg kommun
Respondent 3 berättar att Helsingborg kommun arbetar med att begränsa risker genom olika åtgärder, men går inte specifikt in på dessa.

Respondent 4 och 5, Norrköping kommun
Respondent 5 berättar att Norrköping kommun arbetar med att begränsa risk för bortfall av information. Kommunens servicenivåavtal (Service Level Agreement) eller driftavtal (Operating/Operational Agreement) bestämmer ifall ett system ska vara dubblerat, tredubblerat eller replikerat. Respondent 4 menar att det i slutändan handlar om kostnad för redundans kontra kostnad för bortfall – att ha en tillgänglighet på 100 procent eller 99 procent kan skilja rätt många miljoner. De enda pengar som finns i kommunen är skattemedel från kommunmedborgare samt stadsbidrag och Respondent 5 menar att när kommunens skattemedel inte räcker till får de justera sina krav.

4.6 Utveckling av återställningsplaner

Respondent 1, Umeå kommun
Respondent 1 berättar att Umeå kommun har en dokumenterad plan för det enskilda systemet, inom verksamheten benämnd som en rutin. Dokumentet innehåller steg-för-steg-beskrivningar om vad som behöver göras vid händelse av avbrott eller bortfall. De anställda har tillgång till dokumentet. Vid ett bortfall, som i normalfallet är av teknisk karaktär såsom en misslyckad uppdatering, kan systemet återställas utan beslut från högre nivå. Det finns personer med ansvar för att hålla systemen vid liv, samt en beredskapskedja i de situationer ett bortfall inträffar utanför kontorstid. Respondent 1 menar att så länge återställningen sker under kontrollerad form behövs inga särskilda beslutskedjor. Det är först när ett bortfall blir riktigt stort, vilket man i regel märker ganska snabbt, som besluten eskaleras i en definierad hierarkisk ordning. Den hierarkiska ordningen utgår ifrån driftansvarig och sedan vidare till Respondent 1 som vid behov kan eskalera det hela vägen upp till kommunens topp.

Respondent 2, Uppsala kommun
Respondent 2 berättar att det finns en modell för hur respektive verksamhet ska upprätta en ledningsplan för att upprätthålla sin del av verksamheten vid avbrott. Det finns även en dokumentmall för själva ledningsplanen. De anställda har inte tillgång till alla planer utan enbart till de som är relevanta för deras uppdrag. Detta beror på att planerna innehåller uppgifter som inte ska spridas till obehöriga. Tillgången begränsas, men det finns samtidigt en tillgänglighetsaspekt då planerna behöver vara kända. Respondent 2 tror dock inte att de anställda är medvetna om deras tillgång till relevanta planer.

Vid händelse av avbrott behåller kommunen normala beslutsstrukturer så långt det är möjligt. Respondent 2 förklarar att det finns en krisledningsnämnd som kan aktiveras vid extrema situationer när man inte har tid att invänta respektive verksamhets hantering av händelsen.

Respondent 3, Helsingborg kommun
Respondent 3 förklarar att Helsingborg kommun är medveten om att de blir utsatt för intrångsförsök. Försöken sker hela tiden och när angriparna har lyckats göra ett intrång har digitaliseringsavdelningen hanterat händelsen. De flesta händelser hanteras på olika nivåer inom digitaliseringsavdelningen. Digitaliseringsdirektören har det största mandatet och kan vid behov eskalera upp händelsen till stadsdirektören. Kommunen har även en central krisledning som stadsdirektören kan aktivera vid kritiska händelser. Respondent 3 menar dock att många kriser går att lösa utan att den centrala krisledningen behöver aktiveras. Krisen hanteras då av IT-avdelningen vid respektive organisation.

Respondent 4 och 5, Norrköping kommun
Respondent 5 berättar att Norrköping kommun har alternativa åtgärder med vård och omsorgsverksamheten som praktexempel när det kommer till manuella rutiner vid händelse av avbrott. Efter IT-attacken där ryska hackare kom över huvudnyckeln till kommunens IT-miljö fanns det inom vård och omsorg redan rutiner på plats för att arbeta. Omställningen till manuellt arbete var relativt enkel och det gjorde ingenting att IT-miljön var borta i några dagar för de visste hur det manuella arbetet skulle utföras. Respondent 5 betonar vikten av att det måste finnas manuella rutiner för arbete när det handlar om fara för liv.

4.7 Träning och test av återställningsplaner

Respondent 1, Umeå kommun
Respondent 1 berättar att Umeå kommun utför kontinuerliga tester för redundans av datahallar, medan andra rutiner testas enbart i viss mån. Exempelvis genomförs redundanstest där man i praktiken slår av hela eller delar av en datahall för att se hur smidigt övergången går eller om den över huvud taget märks i verksamheten. På systemnivå testas återställning av system för att se att återställningen fungerar och hur lång tid den tar. Då en systemuppsättning kan vara stor är det vanligt att en enbart en delmängd testas. Respondent 1 menar att det har en identifierad förbättringsmöjlighet att i större omfattning och framför allt mot verksamhetssystem göra kontinuerliga tester för att säkerställa att system fungerar som de ska. Respondenten förutsätter att testerna följs upp och att de eventuella fel som ligger utanför normalfallet åtgärdas.

Respondent 2, Uppsala kommun
Respondent 2 berättar att varje verksamhet ansvarar för att öva på och testa sina återställningsplaner. Hen menar att det ingår i kommunens uppdrag att varje verksamhet ska återrapportera att man har en plan som också ska ha testats och förbättrats där det krävs. Respondenten vet dock inte om det finns några rutiner för hur och i vilken frekvens detta ska göras, men gissar att det framför allt utförs skrivbordstester. Hen tror att det är stor variation på hur väl testerna dokumenteras, men har fått rapporterat att tester utförts och att förbättringsåtgärder vidtagits.

Respondent 3, Helsingborg kommun
Respondent 3 menar att det i Helsingborg kommuns arbete med risk- och kontinuitetshantering på ett stadsövergripande plan ska ingå övningar och tester. Syftet med regelbundna övningar och tester är enligt Respondent 3 att de anställda ska bli medvetna om behovet av en plan B samt att de ska förstå konsekvenserna av att inte ha en plan B. Respondent 3 menar att då kommunen har 11 000 anställda kan de inte vara sammanhängande på allt, utan varje förvaltning måste ta eget ansvar i denna fråga för att i slutändan kunna bli självförsörjande.

Respondent 3 berättar att kommunen tidigare haft övningar inom riskhantering. Det har dock inte funnits någon systematik i det utan ofta genomförts vid efterfrågan. I och med det pågående risk- och kontinuitetsprojektet har det nu tagits fram övningsexempel ur ett stadsledningsförvaltningsperspektiv. Det är planerat att genomföras pilotövningar med två förvaltningar. Respondent 3 menar dock att stadsledningsförvaltningen inte kommer att följa upp dessa övningar, utan att ansvaret ligger hos respektive verksamhet.

Respondent 4 och 5, Norrköping kommun
Respondent 5 berättar att säkerhetsavdelningen vid Norrköping kommun har ansvar att se till

att verksamheten har ett kontinuitetsarbete, vilket regleras i lagen. De ansvarar även för att övningar och tester utförs. Respondent 5 kan dock inte svara på i vilken frekvens det utförs. Hen påpekar att test av planer sker vid ett faktiskt avbrott, exempelvis vid en incident, men är inget som utförs i det vardagliga arbetet. Respondent 5 menar att testresultaten dokumenteras men kan inte svara på vilken verksamhet som gör vad.

4.8 Underhåll av återställningsplaner

Respondent 1, Umeå kommun
Respondent 1 berättar att det som en del av kommunens kvalitetsarbete ingår att se över och uppdatera planerna. Hen menar att det är på kommunövergripande nivå att ha ett sådant förfogande. Kommunen är ISO-certifierade och har beskrivna processer för hur detta underhållsarbete ska utföras och följas upp. Ibland revideras arbetet där det granskas att kommunen följer det de säger.

Respondent 2, Uppsala kommun
Respondent 2 berättar att den nuvarande mallen för ledningsplan har funnits sedan 2017, men att det inte framgår när och hur ofta den uppdaterats. Hen menar att det är riskexponeringen som avgör hur ofta planen ska uppdateras, men gissar att det sker åtminstone årligen. Det är IT-verksamheten som har ansvar för uppdateringen, men det finns inga särskilda rutiner för underhållsarbetet. Respondenten påpekar att det ser väldigt olika ut i de olika verksamheterna. Inom IT-verksamheten finns ett årshjul att utföra arbetet periodiskt och systematiskt, medan det enligt Respondent 2 är oklart hur arbetet utförs i de övriga verksamheterna.

Respondent 3, Helsingborg kommun
Respondent 3 menar att det är av vikt att driva ett löpande arbete med att hålla planerna uppdaterade. Hen understryker att underhållsarbetet inte är någon engångsgrej utan behöver vara aktuellt. Det finns dock inga rutiner för detta arbete, berättar hen, utan är någonting som ska byggas upp genom pilotprojektet. Detta antingen genom att införa stadsövergripande riktlinjer eller att varje förvaltning själva ansvarar för underhållsarbetet.

Respondent 4 och 5, Norrköping kommun
Respondent 5 menar att en uppdatering av planen görs antingen för att lagstiftaren talar om att det måste finnas vissa saker med i planen eller för att man av erfarenhet inser att det behöver göra uppdateringar av den nuvarande planen. Säkerhetsavdelningen har ansvaret att samordna ett underhållsarbete och att göra förbättringar på strategisk nivå. Förbättringsarbetet sker dock enbart efter att en händelse inträffat. Resultatet av förbättringsarbetet förs sedan nedåt i organisationen för det som är gemensamt, men Respondent 5 menar att det förutom vid krissituationer inte sker något övrigt förbättringsarbete på verksamhetsnivå. Respondent 4 menar å andra sidan att verksamheterna inte väntar på en kris innan de börjar titta på förbättringar. Varje verksamhet har ett naturligt arbetssätt för sina metoder och uppdrag då alla vill arbeta smartare i stället för hårdare. Dock menar hen att det finns olika prioriteringar inom verksamheten beroende på vilket tillstånd man befinner sig i. Finns det mycket tid och kapacitet kan man alltid bedriva mer verksamhetsutveckling, men det är svårt att hitta utrymme för att faktiskt bedriva det då det är brist på kompetens i de många områden som berörs inom IT.

5 Diskussion

5.1 Risk- och kontinuitetsarbetet i praktiken

Samtliga fyra kommuner arbetar med risk- och kontinuitetshantering i någon form, men hur detta arbete utförs skiljer sig däremot kommuner emellan. Umeå respektive Uppsala kommun har en kommunövergripande, men ej verksamhetsöverskridande, kontinuitetsplanering. De båda kommunerna följer MSB:s riktlinjer för kontinuitetshantering. Helsingborg kommun har ett pågående kommunövergripande pilotprojekt för kontinuitetsarbete vilken appliceras på två avdelningar, men har för tillfället inget verksamhetsöverskridande arbete. Norrköping kommun har inget uttalat kommunövergripande kontinuitetsarbete, men har kontinuitetsplaner som använts under pandemiutbrott.

Rima och Snedaker (2014) understryker vikten av ett kontinuitetsarbete för att upptäcka risker och utforma strategier för att reducera riskerna och dess effekter. Samtliga kommuner har identifierat risker och utformat riskbehandlingsstrategier, även om det inte pågår något uttalat kontinuitetsarbete. En välfungerande kontinuitetsplan är enligt Phillips och Landahl (2020) av stor betydelse för att vara förberedd på att kunna återgå till normal verksamhet efter en katastrof eller kris. Samtliga kommuner har dokumenterade planer eller alternativa åtgärder för återställning vid händelse av avbrott vilka baseras på de identifierade riskerna och de valda riskbehandlingstrategierna i enlighet med Moh Hengs (2015) rekommendationer. Respondenterna för Umeå respektive Uppsala kommun uppger att de anställda har tillgång till återställningsplanerna. Respondenten för Uppsala kommun tror dock inte att de anställda är medvetna om tillgången till planerna. Moh Heng (2015) belyser dock vikten av att säkerställa att varje plan finns tillgänglig för relevanta parter att följa vid händelse av avbrott.

5.2 Drivande faktorer

Samtliga respondenter belyser lagkrav som en drivande faktor för att arbeta med risk- och kontinuitetshantering. Lag 2006:544, om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap, ger kommunerna skyldighet att minska sårbarheten i sin verksamhet genom riskanalyser, samt att fastställa en åtgärdsplan (SFS 2006:544, 2006).

Respondent 3 menar att för Helsingborg kommun är lagkrav en positiv drivkraft där det ger mandat att bedriva kontinuitetsarbetet. Respondent 4 och 5 menar å andra sidan att lagkrav kan innebära ett hinder för arbetet med kontinuitetshantering. De tar upp exemplet att outsourca information och infrastruktur till dominerande leverantörer kan riskera röja sekretess och ge oberoende tillgång till information. Respondenterna menar samtidigt att dessa leverantörer är medvetna om de juridiska hindren och därmed hjälper organisationer att föra fram förslag och lösningar på problematiken gällande tillgänglighet i förhållande till sekretess och konfidentialitet. Lagkrav och reglering som drivande faktor lyfts även i tidigare forskning där Hayes, Kotwica och Correia (2013) menar att 73% av organisationer ser det som en

primär faktor till risk- och kontinuitetsarbete, samt av Herbane (2010) som beskriver hur lagar och regleringar drivit arbetet med kontinuitet.

I Norrköping kommun har den benämnda IT-attacken varit en stor drivkraft till att se över risk- och kontinuitetshanteringen. Attacken har slagit upp ögonen för kommunen och ett antal åtgärder har belysts för att förstärka robustheten i system, processer och ansvar inom kontinuitetshantering. Vidare framför både Respondent 2 vid Uppsala kommun och Respondent 4 och 5 vid Norrköping kommun att risk- och kontinuitetsfrågorna i dagsläget drivs utifrån kris- och civilberedskapen. Denna drivkraft har aktualiserats i samband med Rysslands invasion av Ukraina.

Incidenter som drivkraft till risk- och kontinuitetsarbetet beskrivs utav både Rima och Snedaker (2014) och Phillips och Landahl (2020). Umeå och Uppsala kommun blir ytterligare exempel på hur en kris eller incident driver organisationers kontinuitetsarbete. Ytterligare beskriver Herbane (2010) hur större incidenter är drivande krafter för att öka arbetet med kontinuitetshantering. Likt detta nämns både pandemi och krig som kriser vilka driver kontinuitetsarbetet framåt.

5.3 Ansvarsfördelning

Risk- och kontinuitetshanteringen i Umeå, Uppsala respektive Norrköping kommun drivs ifrån en centraliserad avdelning och ansvaret faller ner i hierarkin till nämnder och verksamheter. Endast Respondent 1 beskriver att det finns tillsatta ansvarsroller för risk- och kontinuitetsarbete. Respondenterna vid Norrköping respektive Uppsala kommun nämner inga specifika ansvarsroller men förklarar att denna typ av ansvar i slutändan faller på den enskilda verksamheten eller de enskilda nämnderna. Gibb och Buchanan (2006) och Lindström, Samuelsson och Hägerfors (2010) delar uppfattningen att kontinuitetsarbetet bör ha definierade roller och ansvarsområden. De anser att ledningsgruppen ska ha ansvar över programmets omfattning och mål, samt att ansvarsområden bör definieras och tillsättas.

Ett övergripande tema som identifierats är att kommunernas risk- och kontinuitetshantering saknar ett kommunövergripande perspektiv, utan sker individuellt vid respektive avdelning och verksamhet. Respondent 5 menar att i Norrköping kommun är detta en effekt utav kommunens struktur där man inte har strategier för eller arbetar med risk ur ett helhetsperspektiv. Respondent 3 beskriver hur det inom de olika förvaltningarna vid Helsingborg kommun finns en varierande medvetenhet kring kontinuitetshantering på grund av förvaltningarnas tillämpning av olika lagar, krav och förordningar. Respondent 2 förklarar att Uppsala kommuns kontinuitetsarbete utgår ifrån verksamheternas respektive behov och att varje enskild verksamhet utför sina egna riskbedömningar.

Riskidentifiering bygger enligt Iyer och Bandyopadhyay (2000) på antaganden om möjliga hot mot organisationen. När varje enskild verksamhet arbetar i silo finns en risk att de går miste om andra perspektiv, då utomstående parter kan identifiera möjliga hot som den egna verksamheten inte tänkt på. Ett kommunikativt samarbete mellan verksamheterna stärker därmed möjligheten att lyfta allas perspektiv. Som exempel har Helsingborg kommun med det pågående pilotprojektet påbörjat ett samarbete över verksamhetsgränserna gällande kontinuitetshantering. Respondent 3 ser samarbetet och kommunikationen mellan verksamheterna som en framgångsfaktor då de anställda börjat förstå sambandet mellan verksamheterna. Detta

går i linje med Setiawan, Wibowo och Hartanto Susilos (2017) rekommendationer att en riskbedömning ska genomföras av oberoende part.

5.4 Proaktiv riskanalys

Tre av fyra kommuner skattar effekter och konsekvenser av deras identifierade risker. Dessa effekt- och konsekvensanalyser är enligt Clark (2010) en viktig del utav kontinuitetsarbetet då organisationen utan dessa saknar uppfattning över vilka system och funktioner som faktiskt är betydande för verksamheten. Skattningen i respektive kommun bedrivs däremot på olika sätt:

Uppsala kommun kvantifierar effekt och konsekvens genom analyser av återställningstid av IT-stöd och huruvida de faller inom tiden för verksamhetens tolerans. Umeå kommun skattar effekt och konsekvens genom att beskriva innebörden av informationsförlust och avsaknad av åtkomst, men de kvantifierar inga krav på återställningstid. Norrköping kommun skattar effekt och konsekvens genom att koppla investeringar och åtgärder till verksamhetens krav på tillgänglighet, men de kvantifierar inga krav på återställningstid.

Två av de tre kommunerna ställer därmed inte krav på återställningstid, vilket Sambo och Bankole (2016) och Swanson et. al (2010) menar är viktigt för att kunna välja lämpliga återställningsmetoder och -teknik. Vidare är det enligt Gibb och Buchanan (2006) viktigt för att kunna fastställa när återställning blir omöjlig att genomföra.

Samtliga fyra kommuner har fastställt och valt riskbehandlingsstrategier för att reducera identifierade risker. Moh Heng (2015) menar att detta är nödvändigt för att upprätthålla verksamhetens kritiska processer, system och funktioner vid händelse av avbrott. Samtliga fyra kommuner arbetar med strategin att begränsa risk, vilket Setiawan, Wibowo och Hartanto Susilo (2017) menar är den vanligaste strategin att tillämpa. Med strategin att begränsa risk arbetar både Umeå och Norrköping kommun med redundans för sina IT-miljöer. Två av kommunerna, Umeå och Uppsala, arbetar även med strategin att överföra risk till annan aktör enligt Setiawan, Wibowo och Hartanto Susilos (2017) rekommendationer att ingå avtal med extern leverantör att överföra eller dela risken med.

5.5 Reaktiv validering

Utveckling och implementering av återställningsplaner för verksamheten att aktivera vid händelse av avbrott kan ses som en milstolpe i risk- och kontinuitetsarbetet, men arbetet slutar inte där. Återställningsplanernas relevans behöver valideras genom övningar, tester och underhållsarbete, men detta arbete varierar bland kommunerna.

För samtliga kommuner är det uttalat att övningar och tester ska utföras, men tre av fyra kommuner, Uppsala, Helsingborg och Norrköping, har ingen systematik eller rutiner för detta. Avsaknaden av faktiska tester gör det svårt att validera återställnings- eller kontinuitetsplanerna. Gibb och Buchanan (2006) anser att tester är nödvändiga för att säkra planernas relevans och utförbarhet.

Umeå kommun har genom att göra kontinuerliga tester identifierat förbättringsmöjligheter för funktionaliteten av sina system. Detta går i linje med Lindström, Samuelsson och Hägerfors (2010) som anser att träning hjälper anställda att lära sig av erfarenheter och att arbeta mer

effektivt. Helsingborg kommun ska som en del av pilotprojektet införa övningar och tester för att skapa medvetenhet bland de anställda kring syftet med en fungerande återställningsplan samt konsekvenserna av att inte ha någon. Kommunen har förstått syftet med träning som Dey (2011) menar ökar de anställdas medvetande och kunskap över kontinuitetsarbetet.

Förutom övningar och tester behöver återställningsplanerna valideras genom underhållsarbete. Återställningsplanerna behöver enligt Iyer och Bandyopadhyay (2000) kontinuerligt uppdateras och underhållas för att säkerställa att de är i linje med organisationens krav samt är användbar vid händelse av avbrott. Endast en av de fyra kommunerna, Umeå kommun, har ett systematiskt underhållsarbete med beskrivna processer för hur arbetet ska utföras och följas upp. De övriga tre kommunerna har inga särskilda rutiner för kontinuerligt underhåll eller uppdaterande av återställningsplanerna. Respondent 2 menar att det i Uppsala kommun ser väldigt olika ut i verksamheterna, men att hen inte vet när och hur ofta planerna uppdateras. I Helsingborg kommun har man förstått vikten av att ha ett underhållsarbete och att rutiner ska byggas upp i och med det pågående pilotprojektet. I Norrköping kommun arbetas det med underhåll av planerna enbart efter att en incident inträffat, medan ett försök till kontinuerligt arbete nedprioriteras på grund av tids- och kompetensbrist. Detta ligger i motsats till Moh Heng (2015) som menar att organisationer bör bedriva regelbundet underhåll för att säkerställa planens överrensstämmelse med den nuvarande verksamheten och acceptabel effektivitet.

6 Slutsats

Syftet med studien var att ge en ökad förståelse kring hur kommuners arbete med risk- och kontinuitetshantering bedrivs. Detta genom att besvara följande frågeställning:

- Hur arbetar kommuner med risk- och kontinuitetshantering?

I studien framkom det att tre av de fyra kommunerna har en uttalad kommunövergripande kontinuitetsplanering. Däremot bedrivs inget verksamhetsöverskridande arbete för dessa tre kommuner.

Gemensamt för de fyra kommunerna är avsaknaden av ett verksamhetsöverskridande syfte samt kommunikation, där de inte ser nyttan av att gemensamt arbeta med risk- och kontinuitetshantering ur olika verksamhetsperspektiv.

Arbetet med risk- och kontinuitetshantering drivs främst av två faktorer: lagkrav samt erfarenheter av faktiska incidenter. Lagkrav ger mandat till att bedriva risk- och kontinuitetsarbete, men kan även hämma effektiviteten av arbetet i frågan om tillgänglighet kontra konfidentialitet. Erfarenheter av faktiska incidenter, såsom IT-attacker eller pågående krig, har fastställt behovet av risk- och kontinuitetshantering.

Samtliga av de fyra kommunerna arbetar, i proaktivt syfte, med att identifiera risker och utforma riskbehandlingsstrategier. Vidare har samtliga av de fyra kommunerna dokumenterade planer eller alternativa åtgärder för återställning vid avbrott, vilka baseras på de identifierade riskerna samt de valda strategierna.

Arbetet med validering är däremot reaktivt, då kommunerna testar och underhåller sina återställningsplaner först efter en incident inträffat. Detta är en konsekvens av att kommunerna saknar särskilda rutiner för validering av planernas genomförbarhet. Det verkar finnas en dissonans mellan kommunernas reaktiva valideringsarbete och den teoretiska referensramens rekommendationer för proaktivt och strukturerat valideringsarbete.

6.1 Förslag till vidare forskning

Vidare forskning bör gå djupare in på hur man kan öka medvetandet kring arbetet inklusive syftet med risk- och kontinuitetshantering. Den vidare forskningen bör även beröra hur arbetet kan främjas genom verksamhetsöverskridande samarbeten. Slutligen bör vidare forskning bedrivas gällande hur organisationer kan transformera den reaktiva delen av risk- och kontinuitetshanteringen till ett proaktivt arbete.

Bilaga A: Intervjuförfrågan

Nedan presenteras den intervjuförfrågan som skickades ut till kommunerna.

Ämne: Förfrågan om intervju angående riskhantering och kontinuitetshantering inom IT-sektorn, för kandidatuppsats

Hej,

Vi är två studenter från Lunds universitet som studerar systemvetenskap och för närvarande arbetar på vår kandidatuppsats. Vår forskning fokuserar på riskhantering och kontinuitetshantering inom IT-sektorn, och vi är mycket intresserade av att undersöka hur svenska kommuner hanterar dessa frågor.

Syftet med vårt forskningsprojekt är att förstå och analysera de strategier och metoder som används för att hantera risker och säkerställa kontinuitet inom IT-sektorn på kommunal nivå. Vi tror att detta är en viktig fråga, särskilt med tanke på den ökande digitaliseringen och de potentiella risker det innebär för samhällsfunktioner.

Vi hoppas att ni är intresserade av att delta i vår studie genom att låta oss genomföra en intervju med någon som är ansvarig för risk- och kontinuitetshantering inom er kommun. Intervjun tar cirka en timme och kan genomföras via telefon, videokonferens eller personligt möte, beroende på vad som passar bäst. Vi förstår att er tid är värdefull och uppskattar verkligen ert samarbete.

För att säkerställa att informationen som samlas in används på ett etiskt och korrekt sätt kommer vi att följa de riktlinjer för forskningsetik som fastställts av Lunds universitet. Informationen som samlas in kommer endast att användas för vårt forskningsprojekt.

Om ni är intresserade av att delta eller har några frågor om projektet, vänligen kontakta oss på följande e-postadresser:

Victor Johnsson: vi4248jo-s@student.lu.se

Filip Vester: fi1475ve-s@student.lu.se

Vi ser fram emot att höra från er och hoppas att ni är intresserade av att bidra till vår forskning om risk- och kontinuitetshantering inom IT-sektorn.

Tack på förhand!

Vänliga hälsningar,

Victor Johnsson och Filip Vester

Institutionen för Informatik, Lunds universitet

Bilaga B: Intervjuguide

I denna bilaga presenteras den guide som utgicks från vid intervjuerna med kommunerna.

Bakgrund

- Hur ser organisationen inom kommunen ut?
- Vilken arbetsroll har du i organisationen?
- Hur länge har du arbetat inom organisationen?

Fas 1: Initiering av program

- Har ni ett risk- eller kontinuitetshanteringsprogram?
    - Om nej, varför inte?
    - Om nej, hur arbetar ni med detta?
- Är programmets omfattning (scope) och mål definierade?
    - Om ja, är dessa i linje med kommunens vision, mission och strategier?
    - Om nej, varför inte?
    - Vilka är de drivande faktorerna till varför ni startat programmet?
- Har ni tillsatta roller för olika ansvarsområden inom programmet?
- Har ni en tidsplan och budget för programmet?
- Hur ser stödet från den högre ledningen ut?

Fas 2: Riskbedömning

- Gjordes riskbedömningen internt eller externt?
- Har ni identifierat olika riskfaktorer och -områden?
- Har ni bedömt risk för varje affärsområde?
- Har ni identifierat och bedömt risk för de mest kritiska processerna?
    - Om ja, hur vet ni att alla kritiska delar täckts in?
- Har ni skattat eller bedömt sannolikheten för att en specifik risk uppstår samt den sannolika frekvensen?
    - Om ja, kategoriserar ni sannolikheterna?
        - Om ja, hur?
- Är riskbedömningen dokumenterad?

Fas 3: Effekt- eller konsekvensanalys

- Har ni analyserat eller skattat effekterna av förlust vid olika avbrott i olika processer, system och funktioner?
    - Finansiellt
    - Rykten
    - Legalt

- Har ni analyserat effekten av kombinationer av risk?
    - Beroende risker (interna, externa)
    - Oberoende risker

- Har ni analyserat och definierat återhämtningstiden för olika processer, system och funktioner vid händelse av avbrott?
    - Har ni prioriterat vilka återhämtningar som är viktigast vid händelse av avbrott?
- Hur dokumenteras analysen i denna fas?

Fas 4: Val av riskbehandlingsstrategier

- Vilka typer av riskstrategier har ni?
- Hur valde ni strategier?
- Har ni strategier för återhämtning av processer, system och funktioner?

Fas 5: Utveckling av återställningsplaner

- Har ni en eller flera dokumenterade risk- eller kontinuitetshanteringsplaner?
    - Om en, hur är den strukturerad?
    - Om flera, hur är dessa uppdelade och strukturerade?
    - Om ja, har de anställda tillgång till dokumenten/planen?
        - Om ja, är de medvetna om att dessa finns och var dessa finns?
- Hur ser beslutsvägarna ut vid händelse av avbrott och aktivering av planen?

Fas 6: Träning och test av återställningsplaner

- Kontrollerar ni att planen/planerna är genomförbar(a)?
    - Om ja, finns det några rutiner för detta?
- Utför ni tester?
    - Om ja, vilka typer av tester?
    - Om ja, hur ofta utförs tester?
    - Om ja, hur dokumenteras testresultaten?
        - Hur följs resultaten upp?
        - Revideras resultaten internt eller externt?
- Har ni definierade mål, syfte och strategier för träning och tester av planerna?
    - Om ja, är de anställda medvetna om och insatta i dessa?

Fas 7: Underhåll av återställningsplaner

- Hur länge har ni haft en eller flera planer?
- Har planen/planerna uppdaterats?
    - Om ja, finns det några rutiner för detta?
    - Om ja, hur ofta uppdateras de/dem?

Avslutning

- Är det något ni vill tillägga?
- Får vi återkomma om det är något vi behöver komplettera?

Bilaga C: Transkribering av intervju med Respondent 1

Teamsintervju med Respondent 1, Verksamhetschef för IT, Umeå kommun

Datum och tid: 14 april 2023 kl. 14:00

Hur ser organisationen ut inom er kommun i förhållande till där du sitter?

Umeå kommun är ju ganska, ja, den är ju i förhållande till vi stor i Umeå, eller i Sverige. Vår uppbyggnad är att vi har ett antal nämnder, alltså politiska nämnder. Där det är i valet så tillsätts det ju personer som kliver in i de här nämnderna. Och sen så kopplas det någonting som kallas då förvaltning till nämnd. Sen kan det vara flera nämnder mot en och samma förvaltning. Och det kan vara också en nämnd har flera förvaltningar så att det är lite komplicerat. Men i grund och botten så är det alltid politisk styrning och sen så omsätts det i praktiken inom en förvaltning. Och vi har åtta stycken förvaltningar. Och lika många ungefär nämnder. Alla lägger ju under kommunfullmäktige. IT är där jag befinner mig idag, vi ligger under någonting som kallas teknik- och fastighetsnämnden och teknik- och fastighetsförvaltningen. Där vi har förutom IT så ingår fastighet. Det är serviceorganisationen med städ också. Det är måltidsservice och sen är det gator och parker. Så allt det är samlat under samma plym. Och totalt är det ungefär 11 000 personer som är anställda i kommunen. Inom IT så är det ungefär 100. Sen så finns det i dagsläget också en digitaliseringsenhet som ligger under en annan nämnd. Den är just i närtid föreslagen att vi ska gå ihop så att vi får en gemensam digitaliserings- och IT-funktion. Som med all sannolikhet hamnar under min ledning.

Okej. Du nämnde att du sitter i IT. Berätta lite kort om din arbetsroll i IT.

Jag är ju verksamhetschef för IT för hela kommunen. Det är jag som ansvarar för det samlade IT och snart digitaliseringsleveranserna utifrån vad verksamheten behöver. Och ska med tekniken säkerställa att nyttan kommer verksamheten till gagn utifrån behov och prioriteringar som görs. Sen så ligger verksamhetssystemen idag ansvarsmässigt och även budgetmässigt faktiskt ut i respektive förvaltning. Vilket är nytt för mig. I mina tidigare roller har jag haft helheten hos mig på teknik- eller digitaliseringssidan. Men så ser det ut här. Sen har vi också ansvar för IT och cybersäkerheten hos oss. Medan informationssäkerheten och den fysiska säkerheten ligger i en annan nämnd och förvaltning. Så det är inte samlat så. Sen jobbar vi jättenära varandra såklart. Men vi är inte i samma organisation idag. Så lite så ser det ut.

Intressant. Och så undrar jag också hur länge du har varit på din post?

Ganska exakt ett år. Och före det så har jag varit i Region Västerbotten. Och så har jag varit i en annan offentlig storverksamhet, Umeå universitet i många år. Sen har jag varit lite i det privata också och jobbat med säkerhetsprodukter faktiskt. Apropå säkerhet. Men då med kvalitetsansvarsperspektiv.

Spännande. Okej tack. Vi tänkte rikta in oss lite mot risk- och kontinuitetshantering. Och där undrar vi då först och främst, har ni ett risk- eller kontinuitetshanteringsprogram?

Det beror på vad du lägger i begreppet program. Men om du menar att om vi jobbar med risk- och kontinuitetshantering i ett organisationsperspektiv så är svaret ja. Och övergripande ansvaret ligger inom nämnden brand och räddning. Som då har Umeåregionens brandförsvar som förvaltning där det praktiskt ska ske. Det kan man ju tycka att det var en intressant mix. För där är ju naturligtvis brandkåren och behöver den typen av funktion. Den stora verksamheten. Men det ligger också all form av skydd där centraliserat. Så de håller ihop ur kommunhattenperspektiven. Och där finns det ju en övergripande kommunkrisledningsoch kontinuitetsplanering. Sen så bygger den ju egentligen neråt så att varje förvaltning har ju en egen krisledningsdokumentation och styrning som ska mappa in i det övergripande. Och sen så bryts det ner till verksamhetsnivå. Så det är ju en trappstege. Och då får vi med hela kedjan från kommunkrisledningsperspektiv ner till enskilda rutiner på verksamheten. Hur man ska göra i händelse av bortfall eller motsvarande.

Okej. Och då undrar jag det här arbetet som ni jobbar med kontinuitetshantering. Följer det eller är det i linje med kommunens vision och mission?

Det var ju en spännande fråga. Jag skulle inte vinkla det på det sättet tror jag. Det är ju som förutsättningar för att kunna driva mot vårat uppdrag och våra mål. Så betyder det att vi behöver ju ha tillgång till information och systemstöd. För mycket av verksamheten, inte allt, det är mycket som kan bedrivas utan teknikstöd. Men det mesta är ju ändå i någon mening kopplat mot teknik. Så det är ju en grundförutsättning. Men jag skulle inte säga att det är det som vi har som ledord. Utan det är ju kontinuitetsplaneringen och krisledningen. Det syftar till är ju egentligen att vidmakthålla funktionaliteten som behövs.

Okej. Så du skulle säga att det är också de drivande faktorerna till att ni arbetar med just detta?

Ja, att upprätthålla vår förmåga att bedriva verksamhet. Ja, absolut.

Har ni tillsatta roller för olika ansvarsområden inom det här arbetet?

Ja, det har vi. Och de tydligaste rollerna är ju knutna både i den kommunövergripande krisledningsorganisationen. Men också naturligtvis på förvaltningsnivå. Vilka personer och resurser som man knyter an med vilka typer av... Man kan väl kalla det roller eller ansvarsområden. Men det är mycket kopplat till linjen och vad man ansvarar för. Det som är under översyn och uppbyggnad i detta nu, det är ju vad jag är van med från andra verksamheter. Att bygga krisledningsfunktion även längre ner i organisationen, om man säger så. Med MSBs uttalade metodik och roller knutna till det. Vilket i praktiken skulle kunna betyda att vi på förvaltningsnivå eller till och med verksamhetsnivå skulle kunna ha en stabssituation med någon som agerar i rollen stabschef, kommunikation, som är insatsledare och så vidare. Och sen så mappar vi in i övriga strukturen när det behövs. Det är i alla fall det som har diskuterats.

Och du nämnde förut om budget. Men jag tänker berätta lite mer konkret. Har ni en budget och en tidsplan för det här arbetet?

För kontinuitetshanteringen? Inte på något samlat sätt om vi ser annat än det övergripande. Om vi tittar på kommunen, som jag sa, brand och räddningsnämnden och den organisationen har naturligtvis både en viss budget och en tidplan för att genomlysa. För det har gjorts alldeles i närtid. Se över alla kris- och kontinuitetsplaner, när det ska vara gjort och följa upp också att det finns tillgängligt. Sådan tidsplan ansvarar de för och de har viss budget. Men sen är det utifrån respektive organisation så gör man egna krisledningsplaner. Och när det kommer till

verksamhetssystemen så är det mycket upp till verksamheten att kunna beskriva dels i form av vad man har för behov. Hur länge kan man vara borta med teknikstödet innan det blir en allvarlig påverkan? Vad har man för reservrutiner? Vad har man för åtgärdsrutiner för att återställa förmågan? Där skulle jag inte säga att det finns en dedikerad budget för det arbetet utan det ingår i den vanliga driften. Och det finns ju heller ingen tidsplan annat än att det ska ses över med en kontinuitet. Att planer och rutiner är uppdaterade och förenliga med vad vi faktiskt behöver när det eventuellt smäller.

Då tänkte vi ställa några frågor om riskbedömning. Vår första fråga är om riskbedömningen gjordes internt eller om ni tog in extern hjälp, så som konsult till exempel.

Vad jag vet så är det internt.

Då undrar jag om ni har identifierat olika riskfaktorer eller riskområden?

Ja, och den är ju egentligen ur flera perspektiv. Om man tittar på det som ligger närmast verksamheterna så gör man en klassificering av informationen som finns i ett system till att börja med. Det sätter också ribban vilken typ av säkerhetsstöd som vi behöver för att upprätthålla den informationssäkerhet som informationen kräver. Men utöver det så håller vi en plan för själva systemstöden och infrastrukturen med olika scenarier och åtgärder som vi vidtar för att minska risken. Det är ju allt ifrån intrång till belastningsattacker eller liknande. Det är ju en salig blandning. Så ja, det finns.

Intressant. Vi undrar också om ni har identifierat och bedömt risk för era mest kritiska processer?

Ja, det är verksamheterna som har de mest kritiska processerna. Det är framförallt kopplat till där liv och hälsa står på spel eller motsvarande. Det är planer de har och vi delaktiga ur ett teknikperspektiv för att stötta och säkerställa att det blir så bra som möjligt. Sen har de också ett tungt åtagande hos sina leverantörer. För mycket är ändå i drift av externa leverantörer av verksamhetssystem.

Hur validerar ni detta? Hur vet ni att alla kritiska processer och delar täcks in?

Vet man någonsin det? Det tror jag inte att det är många som kan säga med säkerhet. Det kommer alltid att kunna finnas ett scenario som du inte har tänkt på i någon process. Men det är ju efter förmåga att försöka vända och vrida. Ett sätt att försöka komma runt eventuellt att man kör fast är att få in andra ögon. Det kan man göra både utifrån naturligtvis men också andra perspektiv inifrån den ganska stora och omfattande verksamheten i kommunen. Så att man kan dra nytta av varandra och se att vi har tänkt på det här sättet. Det är ett scenario som skulle kunna träffa våra processer också. För vi har liknande men vi är fortfarande olika. Det är väl det närmaste jag kan säga. Men att sätta och säga att vi har koll och täckt precis allt, det skulle jag inte göra.

Har ni dokumenterat den här riskbedömningen och i vilken utsträckning?

Ja det är dokumenterat på flera olika sätt. Vi använder bland annat Klassa. Det gör de flesta offentliga verksamheter ur ett informationsklassningsperspektiv. Men sen har vi också dokumentation för respektive område och system både ur ett verksamhetsperspektiv och ett tekniskt perspektiv. Så ja, det finns omfattning. Det är svårt att säga. Den omfattning som vi just nu anser att vi behöver för att kunna återställa och hålla kontinuiteten öppen.

Sen undrar jag också, nu har vi pratat om risker och bedömning av risker. Men om vi går vidare till nästa steg som är effekten av en risk. Det vill säga förlust av data exempelvis. Har ni analyserat och skattat de här effekterna eller konsekvenserna av riskerna?

Alla riskbedömningar har ju både sannolikhet och konsekvens med sig i sina bedömningar. Så att ja i viss mån. Nu har jag inte sett allt ska jag också vilja säga. Men jag har inte sett att det är kvantifierat i någon mening. Det vill säga att om vi tappar det här så betyder det ett bortfall i någon monetär eller varumärkes uppskattad nivå. Det har jag inte sett. Men däremot en konsekvens som beskriver vad det innebär om vi tappar information eller att det läcker eller att den är inte åtkomlig. Det finns.

Okej. Har ni också definierat, dokumenterat och räknat ut någon form av återhämtningstid? Det vill säga vad är den kritiska tiden? Hur länge kan ett system ligga nere exempelvis?

I princip alla verksamhetssystem som är av stor dignitet har ju en bedömd tidsrymd för när det blir en allvarlig påverkan. Så det finns. Sen hur lång tid det tar att återställa, det är ju svårt att uppskatta beroende på vad det är. Det är framförallt också en stor skillnad. Är det ett enskilt system, då kanske vi kan ha ganska god koll på ungefär hur lång tid det tar att återställa. Ofta är det ju att återställa datan som tar stor kraft. Det är ju dock de situationer jag har varit med om där det har varit problem på riktigt. Det kan vara enskilda system, men det kan ju också vara kluster eller egentligen kanske bortfall av en hel datahall. Jag har varit med om att alla datahallar i en stor organisation försvann [gick ner/förlorade kontakt], inte på grund av intrång, utan på grund av ett tekniskt fel som inträffade i samband med ett elarbete som sköt ner både dieselaggregat, alla batterier och rubbet i två hallar som var redundanta. Det går ju knappt att uppskatta. Det blir ju bara att veta utifrån den lista man har, vad som är det viktigaste som vi måste få upp. Vi måste först få upp infrastrukturen för att det är grunden, annars funkar det ändå ingenting. Sen har man ju en verksamhetsprioriterad lista med vad som är viktigast. Alla tycker att allting är viktigast, så det får man ju ändå trixa med ur ett övergripande perspektiv. Men inte med tydlighet att om vi skulle tappa allt, då tar det så här lång tid. Men ett enskilt system kan man nog säga är ganska hyggligt hur lång tid det tar.

Det du nämnde med att tappa allt, det är ju om du har upplevt det någon form av värsta scenario. Då finns det ju olika strategier för att på något sätt minska eller flytta den här risken. Vilka sorts riskstrategier använder ni er av?

Nu ska jag svara luddigt. Olika. Vi har både redundans på de miljöer som vi har, som verifieras minst en gång i månaden att de funkar. Vi har en massa stödåtgärder, reformer som jag sa. Det är naturligt när man har en datahall. Så det är klart att vi har reservkrafter, dieselaggregat och avtal med dieselleverantörer och annat om det skulle bli den typen av bortfall. I viss mån jobbar vi med externa möjligheter också. Att kunna lyfta över till annat med vissa saker.

Hur kom ni fram till dessa val av strategier?

Genom att väga vikten av att det finns tillgång till den här typen av teknikstöd. Så gör man en bedömning hur viktigt det är att det är åtkomligt. Då får man se om det är tillräcklig nivå med de förmågor som vi har hos oss. Eller behöver vi ta hjälp av något utifrån. I så fall, hur gör man det rent krasst? Det är inte helt givet att allt går att flytta ut. Eller allt går inte att flytta ut, antingen av juridiska eller tekniska skäl.

Själva planerna för om en katastrof inträffar. Har ni en eller flera planer för en specifik process eller system?

Jag skulle säga att för ett system så har vi en plan. Men det är ju inte en plan. När vi börjar prata system så är det inte en plan. Det är mer en rutin. En plan är ju på ett mer övergripande nivå.

Ja. Den här rutinen som ni har, hur är den strukturerad? Är det en slags handbok? Så här går vi till väga. Hur ser den ut?

Det är information som beskriver steg för steg vad som krävs.

Ja. Okej. Och har alla relevanta anställda tillgång till denna plan? Och är de medvetna om vad den finns och att den finns?

Ja.

Ja. Och hur ser beslutsvägarna ut ifall det är så att ni måste aktivera den här rutinen?

Normalfallet om vi får ett bortfall så är det ju i regel någon form av teknisk grej som har inträffat. Det kan vara att det är någon uppdatering som har gått fel eller något nät som har fått någon hicka eller motsvarande. Och där är det ganska enkelt för att vårt åtagande som vi har för de system som vi driftar internt i kommunen så har vi ju en beredskapskedja om det händer utanför arbetstid. Men alltid har vi personer som ändå har ett ansvar för att hålla sakerna vid liv. Så det kräver egentligen inga särskilda beslut om att få upp grejerna så länge det är i den typen av kontrollerad form. Det är ju egentligen först om man märker att det här är stort på riktigt och det märker man i regel ganska snabbt. Då eskaleras det i en definierad hierarkisk ordning. Så att först går det till den som är driftansvarig och sen så går det vidare till mig. Och beroende på vad det är så kan jag också eskalera det högre hela vägen upp till kommunens topp om det skulle behövas.

Har ni behövt aktivera eller tillämpa de här rutinerna någon gång?

Rutinerna för att upprätthålla eller återställa funktion? Absolut. Det inträffar ju lite då och då. Sen i stor skala har jag inte varit med här på kommunen och har faktiskt inte hört att det har varit någon sådan typ av situation i närtid. Däremot har jag erfarenhet av det från andra organisationer där det har varit mycket mer kritiskt att återställa också.

Jag tänker så här, förutom då när rutinerna eller när det händer ett skarpt avbrott om man säger och ni tillämpar rutinen. Kontrollerar ni i övrigt att rutinerna är genomförbara? Utför ni några tester på dem eller är det endast vid skarpa situationer som detta faktiskt testas?

Det testas i viss mån. Som jag sa det är en redundans av hallar som testas kontinuerligt. I viss mån testas andra rutiner också. Men det har en identifierad förbättringsmöjlighet att faktiskt i större omfattning och framförallt mot verksamhetssystemen göra kontinuerliga tester för att säkerställa att vi faktiskt håller hela vägen även där.

Okej. Vad är det för typer av tester då?

Ja, nu ska jag fundera på hur mycket jag ska berätta. Men i princip, för hallredundans slå av en hall mer eller mindre i praktiken. Hur smidigt går övergången eller märks övergången

överhuvudtaget är ju en form av stortest. Sen på systemnivå så kan man ju sätta upp testmiljöer och liknande och återställa och se hur lång tid det tar och att det funkar. Oftast gör man ju inte det med precis allt utan det gör man med en delmängd för att en systemuppsättning kan vara rätt stor.

Och hur dokumenteras testresultaten?

Det kan jag inte svara på. För protokollen och liknande har jag inte sett själv.

Okej. Du som har en högre post, är du insatt mer om hur de här resultaten följs upp? Något till er som ni tar hänsyn till eller hur ser det ut?

Inte av den verksamhet som bedrivs kontrollerat om man säger så utan om det händer någonting som är mer skarpt i normalfallet. Och i ärlighet så kan jag också tillägga att jag är ju egentligen inte i behov av att få en löpande uppföljning på den nivån. Utan jag förutsätter att den som är ansvarig för processen har koll på att det görs tester och följer upp att det funkar och uppdateras i en process om det behövs. Men jag är ju inte processägare på den nivån för det här.

Okej. Du sa att du utgår från att processägarna följer upp resultaten och därmed så antar jag att de har ansvar för att rutinerna uppdateras utefter vad testresultaten visar?

Absolut. Och det ligger ju med kvalitetsarbetet. Vi är ju också isocertifierade så vi har ju processer som är beskrivna och som följs upp och ibland får revision där det granskas att vi följer det vi säger. Så det finns ju ett arbete där bakom och det är ju också på kommunövergripande nivå att vi har ett sådant förfarande.

Är det någonting du har som du undrar till oss?

Nej, det fick jag ut efter att jag var efterfrågad. Är det någonting ni känner att ni vill komplettera så är det naturligtvis bara att höra av sig så kan jag se om jag kan svara på det antingen i mail eller i ett samtal eller en annan form om det skulle behövas.

Bilaga D: Transkribering av intervju med Respondent 2

Teamsintervju med Respondent 2, Informationsstrateg, Uppsala kommun

Datum och tid: 18 april 2023 kl. 14:00

Vi börjar bara lite med bakgrund. Vad har du för roll i eran organisation?

Det kallas för informationssäkerhetsstrateg. Min befattning är placerad idag inom IT-staben på kommunledningskontoret. Befattningen är placerad inom säkerhetsavdelningen. Det där kan variera lite grann från tid till annan hur det ser ut. Just nu är det på IT-staben.

Hur länge har du jobbat inom kommunen?

Inom kommunen har jag jobbat fyra och ett halvt år nästan. Innan dess på [statlig myndighet] och jobbat i branschen sedan 1995 ungefär.

Hur ser organisationsstrukturen ut inom kommunen?

Kommunal verksamhet är ganska hysterisk vad gäller organisation och uppdrag. Det är ju allt mellan himmel och jord. Vi har ett antal kommunala bolag som ingår i kommunkoncernern. Vi har ett tiotal nämnder och förvaltningar som stöder de olika nämnderna. Under kommunstyrelsen finns kommunledningskontoret med ungefär 1800 anställda som har som utdrag att serva resten av förvaltningarna och bolag med centrala stöd och tjänster. Inom kommunledningskontoret finns personal, kvalitetsredning, verksamhetsplanering och upphöjning. Ekonomistyrningen, IT-styrningen. Det är ganska mycket som är centraliserat under kommunledningskontoret.

Då börjar vi med lite mer specifika frågor. Har ni i kommunen ett risk- eller kontinuitetshanteringsprogram eller projekt som ni arbetar med?

Kontinuitetshanteringen styrs från säkerhetsavdelningen som jag tidigare nämnde. Det heter avdelningen för trygghet, beredskap och säkerhetsmarknadsvis. Jag kommer inte exakt ihåg vad den heter. Där har man också beredskapsfrågor. Mycket av kontinuitetsfrågorna drivs från civilberedskap och krisberedskap. Det finns modell som följer MSBs rekommendationer för hur man ska jobba med kontinuitet. Tittar vi på riskhantering så har kommunen en central modell och metod för det också. Den ägs av det som jag nämnde som kvalitet och planering tidigare. För min del som jobbar med informationssäkerhet så handlar det om att få in det perspektivet i de modellerna. Det arbetet som drivs av andra delar av kommunledningskontoret.

Okej. För det här, är omfattningen, scopet och dess mål är de definierade?

Det är hela tiden utifrån ett verksamhetsbehov på respektive verksamhet, respektive uppdrag. Att bestämma sig för vilken omfattning jag behöver arbeta med kontinuitet. Vi har samhällsviktig verksamhet, där är förstås kraven högre. Det är ett riskbaserat angreppssätt på vilken omfattning jag ska jobba med kontinuitetshantering.

Okej. Så dessa målen, hur ligger de i linje med kommunens vision och strategier?

Det beror på hur man tänker där. Vi har en samhällsviktig verksamhet, vi har en samhällsfunktion. Det gäller att upprätthålla den även under störningar och höjd beredskap och även krigssituationer. Det är det perspektivet som kontinuitetsarbetet utgår ifrån. Väldigt mycket handlar just nu om att, det aktualiseras mycket mer i och med Rysslands invasion av Ukraina. Att jobba med de här frågorna. Då blir väldigt mycket utifrån krisberedskapsperspektiv och civilberedskap.

Är det det som är de drivande faktorerna för det här programmet? Den här krisberedskapen? Eller finns det några andra drivande faktorer?

Det finns väl i så fall särlagstiftning inom områden som fokuserar mer eller mindre på det här området. Sen ligger det i enskilda verksamheternas intresse att kunna bedriva sitt uppdrag även under starka, kraftiga störningar eller avbrott.

Har ni tillsatta roller för olika ansvarsområden?

Kommunledningskontoret verkar stödjande i det här arbetet. Men ansvaret ligger alltid i den egna organisationen. Inom den linjeorganisation som har ett särskilt uppdrag för att tillhandahålla samhällsviktiga tjänster. Sen kan det se ut lite olika ut beroende på vilken omfattning det är på det ansvaret. Om man har tillsatt särskilda roller för att driva just det här arbetet eller om det ingår i någon annan typ av roll. Så kommunledningskontoret ansvarar i första hand för att stödja resten av verksamheten.

Finns det någon tidsplan eller budget för detta?

Som vanligt ska det väl ingå i normala arbetet att även arbeta med den här typen av frågor. Tidsplanen avgörs från respektive hur långt man har kommit i arbetet. Det finns ingen generell tidsplan vad jag vet.

Finns det stöd från den högre ledningen?

Ja, det är uttalat att det ska jobbas igenom. Det finns både som uppdrag i verksamhetsplanerna att förbereda för analogt arbete vid bortfall av IT-stöd. Det ligger också i internkontrollplaner att kontrollera att det jobbet görs. Det handlar om ständiga förbättringar. Att komma upp på en första nivå, att kunna säga att man har gjort någonting och sedan förbättra det.

Riskbedömning, har det gjorts internt eller externt?

Riskbedömningar görs, eller drivs, internt. Men man tar förstås in externa rapporter eller indikationer eller inspel från omvärlden också i det arbetet. För att identifiera risker finns det många källor.

Har ni identifierat olika riskfaktorer och områden?

Det får nästan varje respektive verksamhet svara på hur man har sett på det. Men riskerna kan vara från väldigt många olika källor förstås. Ja.

Så när ni bedömer risk, vet du om ni gör det för varje affärsområde?

Det ligger i varje affärsområdes uppdrag att göra sina riskbedömningar. Allt det är kopplat till nämnder, den politiska ledningen och de verksamheter som stödjer den politiska ledningen. Och där ska de kommunala uppdragen utföras. Och det är utgångspunkten för riskanalyserna.

Så de mest kritiska processerna, är de identifierade och har man bedömt riskerna för dem?

Det finns samhällsviktiga verksamheter som pekas ut av vissa direktiv och så. De är skyldiga att jobba med riskhantering och kontinuitetshantering utifrån de direktiven. Sen är det en intern bedömning. Och det finns en uppfattning om vilka verksamheter som är mest kritiska, eller mer kritiska än andra.

Hur vet man då att alla kritiska delar täcks in?

Ja det är jättesvårt. Det krävs ett systematiskt arbete från ledningens perspektiv att jobba med de bedömningarna. Så respektive verksamhet får göra sin bedömning och sen rapportera tillbaka till centralfunktionen och var man ligger någonstans.

Har ni skattat eller bedömt sannolikheten för att en specifik risk uppstår samt den sannolika frekvensen?

Det ingår i modellen att göra det. Det kan jag inte gå in på enskilda risker.

Och kategoriserar ni då sannolikheterna?

I modellen ingår det att göra det utifrån olika påverkansperspektiv. Så vi har även riskkategorier utifrån om det är strategiska risker, operativa risker eller finansiella risker. Men påverkan finns också då på om det påverkar liv och hälsa eller om det påverkar ekonomi eller påverkar vår möjlighet att genomföra uppdragen. Det är en demokrati.

Så den riskbedömningen är dokumenterad?

Det ingår i modellen att dokumentera och följa upp riskerna och det finns anvisat hur man kan göra det där. Det finns mallar och den typen av stöddokumentation som kan göra det.

Har ni analyserat och skattat effekterna av förlust vid olika avbrott i olika processer, system och funktioner?

Återigen det är en del av modellen att göra det. Att det har gjorts och i vilken omfattning det blir en annan fråga.

Är det något du kan svara på?

Det kan bli bättre.

Har ni gjort en vidare analys för att om en viss risk uppstår så följer den risken av en effekt som i sin tur kan leda till att andra risker uppstår?

Det kan jag inte riktigt svara på. Då får man gå in och titta på om man har gjort sådana bedömningar i enskilda fall. Man brukar använda tanken i katastrofplanering. Schweizerostprincipen [modellen], att man har flera olika risker som sammanfaller eller faller ut samtidigt. Och att det då blir en kris eller katastrof. Man har sårbarheter i skyddsåtgärderna som

samtidigt inträffar. Men det kan jag inte svara på att det sker på något systematiskt sätt. Eller att det görs specifikt sådana analyser.

Analyserar ni och definierar ni återhämtningstiden på olika processer, system och funktioner?

Det är stor variation. Det ingår också i modellen att göra just den typen av analyser så att man vet om en återställning av ett it-stöd faller in inom tiden för verksamhetens tolerans.

Prioriteras då vilka återhämtningar som är viktigast?

Det finns en prioritering på vilka it-stöd som i första hand ska bedömas och det ska göras en sådan analys på.

Hur dokumenteras analysen på den här fasen? Det här med effekterna av hur man skrattar effekterna och det. Dokumenteras det och hur i så fall?

Det finns med alla för hur vi jobbar med riskbedömningar, riskanalys och även systematiskt arbete av exempelvis it-leveranser.

Vilka typer av riskstrategier jobbar ni med?

Riskbehandlingsstrategier? Vi följer skolboken där man har både mitigerande risker och överföring av risk. Vi har eliminering av risk eller acceptans av risk. Det brukar vara de där fyra olika riskbehandlingsstrategierna. Men det vanligaste och det man bygger för idag är att minimera riskerna. Sannolikhet eller konsekvens. Det händer väl också att vi jobbar med överföring av risk. Det har hänt också. Man låter en privat aktör genomföra ett uppdrag istället för att man själv gör det. Och sen när det är ett stabilt läge så går kommunen själv in och utför uppdraget. Sådana saker kan det finnas också.

Kan du ge oss något konkret exempel på hur ni jobbar med att minimera risk?

Att minimera risk handlar om att genomföra skyddsåtgärder eller detekterande åtgärder.

Hur väljer ni vad för strategi som ni vill använda er av?

Det kan vara riskkostnad gentemot åtgärdskostnad. Det beror på hur dyrt det är att genomföra en åtgärd i förhållande till riskvärdet. Det kan vara en grund för det. Ibland så kanske... Det är klart att om man kommer in på legala krav så har man inte så mycket annat än att upphöra med den verksamheten om man inte lyckats uppfylla de legala kraven. Det får man bedöma från fall till fall.

Har ni strategier för återhämtning av processer och system och funktioner?

Det ligger ju i reserverutiner och återgång till normal produktion. Så det finns ju ett sätt att jobba med det också. Sen är det kanske infört och fungerar i olika omfattning beroende på vilken verksamhet man tittar på.

Ni dokumenterar ju detta. Finns det en eller flera risk- eller kontinuitetshanteringsplaner?

Alla verksamheter är ju ålagad sin del i det här. Sen finns det en central krisledning om du skulle komma på den nivån. Men det finns ju en tanke och en modell för hur respektive verksamhet ska upprätta en ledningsplan för att upprätthålla sin del av verksamheten.

Vet du hur dessa är strukturerade?

Ledningsplanerna finns det mallar för. Det kan jag ju skicka över om ni vill se ett exempel på en sån mall så finns det ju ett exempel på ledningsplan så det tror jag att ni skulle kunna få ett sånt.

Det hade varit jätteintressant att få det. Absolut. Och har de anställda i kommunen tillgång till dessa dokument och dessa planer?

De som behöver, skulle jag säga. Det kan ju vara så att planerna innehåller uppgifter som inte ska spridas. Då begränsas det förstås samtidigt som det finns en tillgänglighetsaspekt på de där också. De behöver vara kända.

Och de anställda är medvetna om att dessa finns och var dessa finns?

Vet inte. Troligtvis inte skulle jag säga.

Och beslutsvägarna vid händelser av avbrott eller aktiveringar av planen, hur ser de ut?

Låt bibehålla normala beslutsstrukturer så långt det bara möjligt. Sen finns det också en krisledningsnämnd som kan aktiveras och tanken med det är att kunna ta koncernbeslut i extrema situationer då man inte har tid att invänta respektive verksamhets egen hantering utav det.

Så kontrollerar ni att dessa planer är genomförbara på något sätt?

Jag tror inte det finns något central kontroll utan det är att varje verksamhet ansvarar för sin ledningsplan och att öva och testa dem.

Och vet du om det finns några rutiner för detta?

Inte specifikt vad jag vet. Jag vet inte. Det ingår i uppdraget som jag nämnde och i internkontrollen att återrapportera att man har en plan och att man har testat den och att man har förbättrat den. Det är olika.

Vet du vad för typ av tester som utförs då?

Jag gissar att det framför allt är skrivbordstester.

Har du någon indikation på hur ofta de görs?

Nej, inget generellt.

Men du kanske vet om testresultaten dokumenteras på något sätt?

Det är en variation på det också kan jag tänka mig. Jag har inte tagit testprotokoll så.

Har du någon koll på hur resultaten följs upp av dessa tester?

Jag kan se indikationer på det. Man har rapporterat att man har genomfört tester och man har också sagt att man har tagit till sig förbättringsåtgärder.

Har ni några definierade mål, syften och strategier för träning och tester av planerna?

Det vet inte jag. Jag kan inte svara på det.

Hur länge har ni jobbat med kontinuertshanteringsplaner?

När man tittar på mallerna för ledningsplan så använder jag den gamla loggen. De har funnits ett tag. De här stöddokumentationerna har funnits ett tag, men oklart hur länge. De har i alla fall funnits med.

Uppdateras dessa planer?

2017 såg det på den här mallen i alla fall. Det finns lite historik där bakom.

Finns det någon rutin för att uppdatera dessa planer?

Ingen särskild vad jag vet. Det är lite beroende på var man tittar. Det finns ett sånt där årshjul, systematik inom IT-verksamheten att göra det här arbetet periodiskt och systematiskt. Det är lite oklart hur det ser ut för verksamheterna i övrigt. En del har årshjul och gör det här med någon viss periodicitet och repeterbarhet. Det ser väldigt olika ut.

Har du någon indikation på hur ofta de uppdateras?

Nej. IT-verksamheten ska göra det. Det beror på riskexponeringen hur ofta man ska göra det. Åtminstone årligen.

Det var väl de frågor vi hade i övrigt.

Vi kan lägga den här mallen som vi pratade om i chatten så får vi se hur den ser ut.

Annars har du våra mailadresser. Kan du mejla den?

Ja. Är det något annat?

Är det okej att vi återkommer om vi känner att vi behöver komplettera med något?

Ja. Den här typen av undersökningar blir det väldigt mycket generella svar av naturliga skäl. I och med att det är en stor verksamhet så är det svårt att säga vad specifika verksamheter faktiskt har gjort och utfallet av den här typen av jobb. Det blir de generella strukturerna som går att redovisa. Går man in på respektive jobb så kommer man kanske in på sårbarheter som man inte vill redovisa för öppet. Det får en bild i alla fall.

Tack så mycket.

Lycka till!

Bilaga E: Transkribering av intervju med Respondent 3

Teamsintervju med Respondent 3, Säkerhetsstrateg, Helsingborg kommun

Datum och tid: 25 april 2023 kl. 10:30

Då börjar vi lite enkelt. Vad har du för roll i Helsingborgs kommun?

Jag jobbar som säkerhetsstrateg och främst med inriktning på informationssäkerhet. Jag jobbar då på stadsledningsförvaltningen som är den övergripande förvaltningen i Helsingborg stad. Som ska styra, leda och fördela arbetet.

Okej, och hur länge har du jobbat där?

Ja, jag har jobbat i Helsingborg stad i 23 år. Jobbat inom IT tidigare, både som förändringshantering och driftchef. Och nu jobbar jag med informationssäkerhet. Och informationssäkerhet har vi jobbat med här ungefär fem år nu.

Okej, och hur sitter er avdelning i förhållande till kommunen och organisationen?

Vi tillhör avdelningen som heter strategisk samhällsplanering. Och där är, vi får se hur många avdelningar. Vi organiseras av stadsledningsförvaltning och sen finns det åtta förvaltningar till. Men vi är ju den övergripande så att säga. Och under vår förvaltning så finns det avdelningar som drivs av varsin direktör. Och sen har de avdelningarna enheter under sig. Och då tillhör jag enheten som heter trygghet och säkerhet.

Ja, ja men gott. Så då börjar vi ställa några frågor om kontinuitetshantering och så. Har ni i kommunen ett risk- och kontinuitetshanteringsprogram eller projekt?

Alltså just nu så genomförs ju risk- och sårbarhetsanalyser. Som genomförs vart fjärde år som är lagstadgat. Och det driver vi från den här enheten. Jag är inte den som är drivande utan en kollega. Men det görs ju på samtliga förvaltningar och bolag i staden.

Okej, ja. Och omfattningen av dessa, hur stor är de? Vad är omfattningen där?

Hur menar du med omfattningen? Alltså den bygger ju på att vi har gjort ett frågebatteri. Som man ska svara på inom väldigt många olika områden. Och sen är det varje förvaltning och bolag som ska svara på de här frågorna. Och sen så gör vi en sammanställning av den. Sen ska den då beslutas i KF [kommunfullmäktige]. Och sen presenteras den. Och den innehåller då ju RSA-sekretess [risk- och sårbarhetsanalys]. Så det finns ju en publik del så att säga. Så den är ändå ganska omfattande.

Okej, ja. Finns det, i den, mål definierade, vad ni vill komma fram med i denna analysen?

Nej, det tror jag inte det är. Utan det är ju bara typ frågor till förvaltningarna. Hur de hanterar olika situationer.

Okej. Jag har en fråga där också. De här analyserna som ni gör, är det en del av något större kontinuitetsarbete? Eller ligger fokus på de här frågorna?

Just den här RSA, den är ju som sagt ett krav som alla Sveriges kommuner ska göra vid varje mandatperiod, vart fjärde år då ju. Sen så bedriver väl förvaltning… jag kan inte försvara för alla förvaltningar. Sen kan de ju bedriva egen RSA ute på sina… Och det gör de säkert också. Men just den är den som vi håller samman. Och sen har vi ett projekt också med kontinuitetshantering som pågår nu. Vi har en konsult som ska hjälpa oss. Och vi ska jobba likvärdigt i staden med kontinuitetshantering.

Okej. Hur insatt är du i detta arbete? Kan du ge oss lite mer om just detta arbete?

Ja, det ska vi väl kunna göra. Jag ska se om jag kan ta upp. Så jag inte ljuger för er. Jag kan ju dela så kan ni få se hur det ser ut. Då har vi först och främst tagit fram en vägledning hur vi ska bedriva arbetet i staden. Den ser ut så här. Och då har jag framtagit en kriteriemodell också.

Just det. Finns det möjlighet för oss att få ta del av detta dokument lite djupare?

Ja, det tror jag. För detta är bara en vägledning så detta är ingen bedömning.

Nej, precis. Det ser mer ut som en mall utan att innehålla känsliga uppgifter.

Ja, nej. Så det kan ni inte säkert få. Sen har vi tagit fram en mall. Och hur man ska jobba att fylla i den.

Ja. Om möjligheten finns så tar vi jättegärna del av den här vägledningsmallen.

Och sen den här mallen också som vi har tagit fram. Och sen har vi tagit fram lite övningsexempel också. Så vi ska ha övningar med två pilotförvaltningar.

Okej. Vad menar du med övningar? Vad är det för typ av övning?

Ja, vänta så ska jag visa den också. Det är lättare om ni får se det.

Ja. Just det. Men jag tycker vi kom in på övning här lite. Hur ofta utför ni sådana här övningar?

Inom just kontinuitetshantering? Ja. Jag tror inte det finns någon systematik i det, men övningar genomförs i riskhantering. Och det är väl oftast om verksamheten efterfrågar det. Jag tänkte det här som vi tar fram här nu i kontinuitetshantering, det är inom ramen för projektet. Så detta har väl inte övats så från ett stadsledningsförvaltningsperspektiv tidigare. Sen kan det mycket väl ha övats ute i förvaltningarna.

Men är då tanken att det ska bli mer rutin på att göra de här övningarna?

Ja, det är det ju. Alltså detta är ju tanken att detta ska bli ett stadsövergripande sätt att kontinuitetshantera på. Och då ingår det i övning också. Så i detta projekt så är det ju också att vi ska ”train the trainer” ungefär. Så att de ska kunna bli självförsörjande där ute. Vi är ju ganska många anställda i staden, vi är ju 11 000 anställda. Så vi kan ju inte vara sammanhållande på allt, därför måste de ju själv ta sitt ansvar i varje förvaltning.

Ja, ja, det är kul. Och vad för resultat är det ni vill få ut av ett sådant här test?

Alltså dels är det ju att de ska vara medvetna om att de behöver ha en plan B. Och att de själv kan förstå konsekvenserna om de inte har det.

Ja, och hur skulle ett resultat här följas upp?

Ja, alltså vi kommer ju inte… från stadsledningsförvaltningens perspektiv så kommer vi ju inte följa upp, utan vi ger dem ett verktyg och sedan ligger det i deras verksamhetsansvar att de ska genomföra detta.

Jag tänkte att du nämnde där om syftet att öka förståelsen och medvetandet kring kontinuitetsarbetet. Upplever du att det medvetandet inte finns i samma utsträckning idag bland medarbetarna?

Det kan vara väldigt skiftande. De som jobbar till exempel inom vår och omsorgsförvaltningen, de har ju ganska god kontinuitetshantering. Det är något som måste finnas. Sedan finns ju de förvaltningarna där det är mindre god förmåga. I och med att det är så många olika verksamheter och det är olika lagar, krav och förordningar som styr oss. Så vi som vården måste ju till exempel ha planer. Det är väldigt svårt att säga generellt för en hel stad. Vi har ju både vården, skolan, räddningstjänsten, miljöförvaltningen, socialförvaltningen, arbetsmarknadsförvaltningen, stadsbyggnadsförvaltningen. Det är väldigt spritt av verksamheter.

Hur tycker du det ser ut inom IT där du sitter?

Ja, jag kan väl säga att de kan bli bättre. Om jag kan uttrycka mig så. Det är väl oftast så att de har kontinuitetshantering på sitt sätt. Men de borde göra det lite mer strukturerat. Men de ingår ju också i detta arbete. Så ja, hoppas att det blir bättre. Eller blir bra.

Men med detta projekt som ni är igång med, finns det en tidsplan och en budget för detta?

Ja, det gör det. Vi har väl projektavslut nu under, jag kan inte exakt datumen på det, men det är nu under våren. Och det har väl löpt under ungefär ett års tid tror jag.

Ja, och liksom stöd, tycker du det är stöd från den högre ledningen? Hur ser det ut?

Jo, men detta är där stöd för. För detta var ett av ett uppdrag som vi fick. Att detta skulle genomföras i staden från kommunledningen. Så det kan man väl säga att det är stöd i.

Och då, vi går vidare till lite riskbedömning. Har det gjorts internt eller externt?

Det tror jag väl har varit internt skulle jag nog tro.

Och har ni då inte identifierat lite olika riskfaktorer och olika områden?

Ja, det har vi. Nu har vi haft, vi har kollegor som har jobbat med detta. Så jag har inte varit så involverad i det. Absolut.

Har du någon, lite övergripande, lite olika områden eller faktorer som ni har identifierat?

Ja, men det kan väl man, om man tittar på de här så är det ju cyberattacker, fysiska attacker, naturkatastrofer, sabotage. Jag kan plocka fram det för jag kan ju hitta det i vår dokumentation.

Ja, jag är nyfiken. Har ni då även bedömt risk för var affärsområde?

Ja, alltså. Ja, men det är det väl ju. För det är ju massor av el och vatten och de bitarna. Renhållning och avfall. Absolut.

Och har ni identifierat och bedömt risk för de mest kritiska processerna?

Ja, men det tror jag vi gjort. Då kan vi se. Ja, jag får nog backa på den.

Det är inga problem. Men så när ni bedömer en risk, skattar ni risken på något sätt och bedömer sannolikheten för dem?

Ja, men det gör vi. Det är klart att det är identifierat risker och de skattas. Jo, men det görs det.

Vet du hur ni kategoriserar risken och kategoriserar sannolikheten för dem?

Vi har ju den här, om den skulle vara till hjälp. Den här mallen vi har tagit fram för riskbedömning.

Där finns lite. Lite så man kan se hur lång tid det skulle ta att återställa den och vem som är ansvarig.

Precis. Och här har vi kriterie-modellen. Ja, den som var i det dokumentet. Och så här är konsekvensanalysen. Precis. Och beroendeanalysen.

Jag tänker, skattar ni effekterna av en förlust vid avbrott? Eller förlusterna? Hur mycket hade det kostat till exempel? Blir det legala avbrott? Skattar ni det?

Nej, men det tror jag inte att det görs faktiskt. Inte i någon större utsträckning. Det kanske kan ske på de bolag som har el och vatten och så vidare. Men de är hos oss egna bolag. De sköter de här bitarna helt och hållet själv.

Om det nu sker, eller snarare när det sker, ett avbrott. Har ni definierat olika återställningstider för de olika systemen ni använder? Eller sköts allt detta externt av de andra bolagen?

För staden är det det vi vill uppnå med det här kontinuitetsprojektet. Och bolagen kan nästan med största sannolikhet säga att de har redan det.

Har ni prioriterat vilka system och vilka delar som är viktigast att återhämta ifall det sker ett stort avbrott?

Ja och nej. Jag tror inte det finns helt klart nedtecknat, men det finns en stor medvetenhet om det.

Jag har en fråga med, du har visat mallarna så vi ser bevis på att ni har förberett för dokumentation. Men har ni faktiskt dokumenterat era resultat från riskbedömning och så vidare?

Ja men det har vi ju, för där sker ju fler riskbedömningar. Men det finns dokumenterat. Sen inte inom områden naturligtvis, för det är därför vi håller på med det här kontinuitetsplaneringsprojektet, för att vi vill bli bättre på det.

Ja precis, bara så att jag förtydlar min fråga, även fast dessa mallar är framtagna så undrar jag mer om mallarna faktiskt används och fylls i?

Ja, det gör de på dem. Nu har vi bara två piloter i detta ju, men de har ju fyllt i dem. Och de är ju väldigt på och engagerade. Sen är ju tanken att det ska ut till övriga efter det ju. Så ja det tycker jag att de gör. De uppskattar ändå att de har fått en stadsövergripande mall och det är lättare att följa upp också om någon, stadsdirektören eller så, vidare skulle vilja veta hur det ser ut.

Ja, på vilket sätt uppskattar de det? Är det att det blir tydligare och att det finns ett syfte med varför de gör det eller hur vill du beskriva det?

Jag tror de uppskattar det för att det kommer faktiskt från stadsledningsförvaltningen hur de ska hantera de här frågorna. Innan har liksom var och en själv hittat på egna lösningar och det kan vara jättebra och kanske lite sämre. Men just att de, jag tror även det här att de har haft lite workshopar och sånt och då har de kunnat prata med varandra och de kan förstå sambanden att hela staden hänger ihop. Jag tror faktiskt det har varit en framgångsfaktor att man börjar prata mer om det med övriga förvaltningar.

Mm. Vet du, om vi går till riskstrategier och den delen, så vet du om ni jobbar med någon specifik riskstrategi eller är det flera riskstrategier där?

Jag vet faktiskt inte, skulle jag vilja säga. Men jag tror ju att någon från vår sida på min enhet jobbar med det. Alltså vi har ju också de här lagstadgade säkerhetsskyddsanalyserna och där ingår det ju det också. Mm.

Skulle du säga, är det liksom lagarna och det som är den drivande faktorn till varför ni utför det här, alltså arbetet eller finns det andra faktorer, drivande faktorer och drivkrafter, varför ni utför kontinuitetsarbetet?

Ja, alltså RSA och säkerhetsskyddsanalyserna är lagstadgade så det är klart att de driver mycket. Det gör ju att man får en helt annan drivkraft och har mandat att komma ut till det. Men sen har du ju ändå bedrivit arbete här utan att det är lagstadgat så det är klart att vi gör det också ju.

Ja men så liksom det som är, om vi säger det som driver, som inte har varit lagstadgat, vad har det varit liksom? Är det bara personligt intresse eller har det varit?

Nej, men det finns ju politiska uppdrag vad vi ska jobba med. Ja, så att, ja men det är ju krisberedskap, ja. Vi jobbar ju mycket med civilförsvar, krisberedskap, ja det är väl egentligen det vi jobbar med och så informationssäkerhet inom den enheten jag tillhör.

Inom då informationssäkerhet, när ni har identifierat och analyserat en risk och sådär, har ni några strategier då för att exempelvis minimera de här riskerna? Eller flytta risker kanske till externa bolag eller skaffa en försäkring, alltså de typerna frågor, har ni några riktlinjer där?

Alltså det finns inga direkta riktlinjer för det faktiskt. Det jobbas med det också kan jag ju säga. Men just nu så är det ju numera att de som har verksamhetsansvar liksom har tagit den rollen. Men inom informationssäkerhet så håller vi på och klassar våra informationsinventarier, informationstillgångar och sen säkerhetsklassa de, sätter olika skyddsvärden på dem. Och då måste man göra en riskbedömning på dem och minimera riskerna med olika åtgärder.

Så då har ni identifierat och tagit fram olika åtgärder för att minimera de här riskerna?

Ja, vi använder oss av MSB:s riktlinjer, det syftar ju på ISO 2700 standarden. Så det är de 93 säkerhetsåtgärderna som är rekommenderade till statliga myndigheter som vi använder oss av.

Ja, okej. Säg att det sker ett avbrott, hur ser beslutsvägarna ut då?

Ja, är det någonting inom IT så är det ju digitaliseringsdirektören som har det största mandatet där, eller så får han gå till statsdirektören. Det beror på vilken art det är av avbrott så att säga. Men det mesta hanteras nu inom digitaliserings [-avdelningen] i olika nivåer där.

Okej, och hur aktiveras detta?

Ja, just inom Digi det vet jag inte riktigt, men om du syftar på att vi har en central krisledning så finns ju det också. Då kan ju statsdirektören aktivera den centrala krisledningen.

Okej, ja. Hur eskalerat behöver en situation eller ett avbrott bli för att krisledningen ska behöva aktiveras, eller är det någonting ni kan lösa innan dess så att säga?

Det är många kriser som går att lösa utan att den aktiveras. Det ska ju vara samhällskritiska kriser, just som när det var corona till exempel, då aktiverade CKL [centrala krisledningen] den ju. Men annars hanteras det ofta IT på förvaltningarna med olika verksamhetsansvar.

Okej, har du något exempel till oss på en lite mindre då risksituation som har uppstått?

Ja, men det har ju säkert massor, men jag kommer inte på någon nu.

Nej, till exempel om det är något system som har gått ner eller om det är en hel datahall kanske som har tappat anslutning?

Ja, alltså vi som alla andra är ju utsatta för intrångsförsök hela tiden, det är vi ju fullt medvetna om ju. Och ibland händer det att de lyckas också ju. Men när det händer så har det ju varit digitaliseringsavdelningen som har hanterat dessa. Och där har ju inte aktiverats någon central krisledning utan det har de gjort innanför sin organisation ju. Så då har de väl tillkallat sin stab där och hanterat krisen där. Och det är väl ofta så det går till.

Men så nu när ni då håller på att införa den här planen, hur tänker ni sedan fortsätta arbetet? Kommer ni fortsätta uppdatera dessa planer?

Ja, absolut. Det måste ju vara ett löpande arbete. Det är liksom ingen engångsgrej utan de ska ju vara aktuella ju. Och sen måste vi antagligen bygga lite rutiner för hur det ska gå till ju.

Men de rutinerna, de är inte bestämda ännu?

Nej, för det är ju det som jag sa innan. Det är ju lite svårt om vi ska liksom lägga ansvaret på varje förvaltning att de ska göra det själva eller om man ska ta över några statsövergripande riktlinjer eller någonting.

Jag känner att vi har fått svar på allt vi hade faktiskt. Men jag tror att vi har fått rätt mycket svar.

Ja, det var bra. Annars är det bara att mejla.

Ja, jag tänkte kolla, är det något du vill tillägga?

Nej, alltså. Ska ni intervjua flera kommuner? Är det bara inom Kommunsverige eller är det privata företag också?

Det är bara Kommunsverige. Du är tredje personen vi intervjuar och vi har en till nu i eftermiddag. Så det blir fyra kommuner här i Sverige. Ta gärna en bedömning och se vad vi kan få ta del av dessa mallar. Vi är jätteintresserade av att läsa igenom de här lite mer i detalj om det finns möjlighet till det.

Ja, ni behöver inte sprida dem i så fall.

Men är det okej att vi, vad ska man säga, refererar till dem eller kommenterar dem?

Ja, men det är det. Ja, absolut. Jag ska bara kolla så att det inte är någon form av… att någon tycker att det är för känsligt.

Tack så mycket.

Ja, tack själv. Och lycka till med uppsatsen.

Ja, tack. Och vi skickar nog den sen när vi är färdiga med dem.

Ja, gör det. Det var intressant. Jättebra.

Tack så jättemycket.

Tack själv.

Bilaga F: Transkribering av intervju med Respondent 4 och 5

Teamsintervju med Respondent 4, IT-säkerhetsansvarig, och Respondent 5, IT-säkerhetsstrateg, Norrköping kommun

Datum och tid: 25 april 2023 kl. 13:00

Ja, vi börjar lite enkelt. Vad har ni två för roll där i kommunen?

Respondent 5: Jag jobbar som IT-säkerhetsansvarig, gruppansvarig för IT-säkerhet och informationssäkerhet och juridik.

Respondent 4: Jag jobbar som IT-säkerhetsarkitekt. Vi har varit några år på kommunen båda två. Jag kom in 2019 och Respondent 5 året innan.

Respondent 5: Fem år tror jag det blir nu. Vi kommer båda från statliga myndigheter, innan dess har vi båda varit i privatsektor. Så vi har väl sett lite olika sidor av den här verksamheten.

Perfekt, då fick jag också svar på min andra fråga. Hur länge ni hade varit inom kommunen? Hur är er avdelning i förhållande till resten av kommunen?

Respondent 5: Jag kan väl säga, om jag vill inleda. Vi sitter inom en organisation som heter digitaliseringsavdelningen. Det är en avdelning som sitter under, eller som är en del av kommunstyrelsens kontor. Här finns det en digitaliseringsdirektör. Alla avdelningar på en kommun har direktörer, det känner ni säkert till. De andra verksamheterna i kommunen har vård- och omsorgsdirektörer, socialdirektörer och så vidare. Vi är jämställda kan man säga. Vi är ett stöd åt verksamheterna, de andra kontoren som man brukar kalla det här.

Respondent 4: Kommunen består av ett antal nämnder som också utgör myndigheter. Kommunstyrelsen är sin egen nämnd. Sen har man de här kärnverksamheterna som skola, vård och omsorg som är sina egna nämnder. Vi jobbar mycket inom de här verksamheterna. Sen har kommunen också bolag som inte omfattas av IT-säkerhetsfunktionen centralt. Bolagen har sitt eget ansvar. Sen samverkar vi med bolagen, men inte på samma premisser.

Respondent 5: Bolagen har sina egna ägardirektiv. De är helägda av kommunen, men de har ett eget ansvar. Det innebär att vi inte kan styra dem på det sättet eftersom de är aktiebolag. Genom ägardirektiven, det vill säga, i det här fallet Rådhus AB som är det övergripande bolaget som äger kommunens… de andra sju bolagen. Vi har som ni säkert vet en hamn, en flygplats, fastighetsbolag och rätt många olika typer av bolag.

Ja, men gott. Vi börjar med lite mer frågor om kontinuitetshantering. Har ni inom kommunen ett risk- eller kontinuitetshanteringsprogram eller projekt åt det hållet?

Respondent 5: Det beror lite på hur man menar. Det finns en krisledningsplan, en kontinuitetsplan. Den har man använt på olika sätt i pandemiutbrottet till exempel. Man har övat det på olika sätt. Det finns en krisledning, ett krisledningsutskott till exempel där representanter från politiken sitter med i tjänstemannasidan. Finns det ett program, projekt just nu? Svaret är

väl nej skulle jag vilja säga. Vi har haft en större cybersäkerhetsincident där vi jobbar med att förbättra vår kontinuitetshantering. Men det finns inget startat än efter det.

Respondent 4: Jag kan lägga till att informationen är grunden för kraven på tillgänglighet. Ni känner till hela CIA-triangeln och spårbarheten i sig. Det är den som är utgångspunkten för hur högtillgänglig en lösning måste vara. Verksamheterna i sin tur har krav på att ha manuella rutiner som tar vid om någonting inte längre fungerar digitalt. Vården är väldigt duktig på det. Skolan har det lite tuffare idag för de har gått så långt i sin digitalisering. Man är lite mitt emellan med socialtjänst och fritidsnämnd. Det är väldigt olika för att kraven på tillgänglighet är olika. Man är inte alltid beredd att betala för högtillgänglighet om man inte har en omedelbar kravbild från lagstiftning eller brukare. Allting har inte högsta tillgänglighet. Det är inte så att vi kan leverera det. Det är en oerhörd kostnadsdrivande fråga om allting skulle vara högsta möjliga säkerhet, högsta möjliga tillgänglighet, högsta möjliga prestanda. Då betalar man oerhört mycket utan att ha krav på det och kunna finansiera det. Kommuner i regel får göra en tydlig avvägning. Man börjar med informationskartläggning och informationsklassning och sen bedömer man därifrån vilka åtgärder man måste vidta.

Du sa lite snabbt att ni hade haft något cybersäkerhetsincident rätt nyligen. Kan du berätta något om den?

Respondent 4: Den är relativt väl beskriven. Det finns en film på vår hemsida där vår digitaliseringsdirektör, dåvarande informationssäkerhetsstrateg, redogjorde för incidenten i sig. Det var en händelse under sent november där vi bara fick intrång genom tekniska sårbarheter. Som sen kavlades upp och blev en ganska långvarig process att mota ut de agitatorer som hade angripit oss. Det pågick i större delen av december också. Vi arbetade med en av de större IT-säkerhetsorganisationerna i Sverige. De har en ganska antattande CIRT [Cyber Incident Response Team] och en duktig SOC [Security Operations Center] som heter Truesec som ni säkert känner till. Det var inte tänkt att det skulle vara så kommunicerat, tyckte jag, vad vi jobbade med. De var väldigt hemlighetsfulla från början. Deras VD var sen ute och pratade i morgonssoffan på TV4 och berättade om oss. Då var väl hela hemligheten inte så väl bevarad längre. Sen har vi fortsatt med Truesec som SOC. Det är en grej som vi nu håller på att upphandla för att förlänga. Kanske inte nödvändigtvis med Truesec, men vi är inne i en upphandlingsfas som offentliga verksamheter måste bedriva genom LOU [Lag (2016:1145) om offentlig upphandling]. Då håller vi på att upphandla en mer långsiktig SOC-lösning som ska ha plats efter sommaren.

Respondent 5: Det var där jag sa att vi har inget program för att jobba med kontinuitet. Men som ett resultat av incidenten har man indicerat ett antal åtgärder. Det kan innebära att man behöver förstärka på olika sätt i verksamheten. Men även robustheten i system och applikationsmiljö. Och även processer, rutiner, roller och ansvar som ligger i kontinuitetshantering. Både centralt och i verksamheten.

Respondent 4: Ni kan kika på filmen om ni vill. Det är inga hemligheter, även om vi inte berättar mycket detaljer. Det är ungefär som att gå till tandläkaren och upptäcka att man har hål. Det är en bra erfarenhet, men man är gärna utan den. Det är samma sak med en cybersäkerhetsincident. Det är bra för att bygga erfarenhet, men man är gärna utan den. Det är en helt annan dialog när man har haft en incident. Det är mycket lättare att resonera kring att sannolikheten inte är obefintlig. Den är ganska hög. Man ska inte uppmuntra folk att bli hackade, men det ger en helt annan dialog.

Är det en drivande faktor för att jobba med kontinuitetshantering?

Respondent 4: När man har insett att saker och ting inte är tillgängliga jämt utifrån att man har varit tvungen att ta ner system eller tvingats av yttre omständigheter att systemet inte fungerar inser man också vikten av att ha tillgänglighetsdefinierade krav i avtal. Det är jättelätt att gå till en leverantör på utsidan och säga att man vill att de kommer hit på tio minuter om det här händer. Men i en intern verksamhet är det mer så att man är nöjd om man gör ett bra jobb. Man är inte så formell. Man tittar mer på att formalisera sina relationer mellan de interna verksamheterna så att man blir mer kundleverantör och kan ställa tydligare krav men också acceptera att det finns en kostnad i de åtgärder som vidtas. Det här med informellt kan vara jättebra men när skiten träffar fläkten då är det viktigt vem som är först. Vem betalar för att vi ska vara snabbast hos dem och vem betalar minst för att vi ska komma fort till dem. Så att de sedan förstår konsekvenserna av sina beslut och sina konsekvenser av att man faktiskt har valt att inte vara högst på listan. Det är väl ett arbete. Sen har vi ständigt en dialog. Bara det här kontra on-prem och moln är en sån grej som också pågår. En av konsekvenserna hos oss är att vi har fattat beslut om att molnifiera oss. Innan det här var det mer en diskussion om, kan vi, vad säger juridiken om de prövningar som har gjorts, de diskussioner som har varit lite mer hänsynstagande till andra aspekter så har det blivit viktigare med tillgängligheten. Man har kanske tagit bort andra aspekter ur resonemanget på gott och ont.

Om jag förstår rätt så har det gjorts en riskbedömning och även en kontinuitetsbedömning över var ni ska ha era tjänster?

Respondent 5: Man har tagit alla aspekter från tillgänglighet, konfidentialitet och spårbarhet och alla de juridiska kraven. De har man i princip manglat hos kommunledning och kommunpolitiken i kommunstyrelsen och kommunfullmäktige. Man har gått så långt som man har kunnat för att få ett beslut. Då är det balanserat mellan den juridiska oklarheten och tillgängligheten och användbarheten i saker och ting. Eftersom att lagstiftningen är som den är och det finns en del oklarheter när det gäller olika typer av lagstiftning och regelverk som FISA [Foreign Intelligence Surveillance Act] och Cloud Act. Allt vad man nu kallar det för någonting.

Den här bedömningen, är det som ni har gjort internt? Eller har ni även här tagit in konsulttjänst? Ni hade jobbat med TrueSec och där. Är det i samband med dem eller är det internt?

Respondent 5: När det gäller framtagandet underlaget i sig själv? Underlagen har samarbetats med leverantörer. Men själva underlaget för beslut och så vidare när det gäller risk- och konsekvensbedömningar är framtagen internt och presenterad för de olika instanserna som måste fatta beslut.

Respondent 4: Man kan väl nämna det att många av de här leverantörerna som erbjuder molntjänster har ju sett hindren som finns i lagstiftningen. Osäkerheten som det ger i organisationer som kommuner och regioner och även statliga myndigheter. Så de har ju arbetat med workshops för att påvisa möjligheterna som ändå finns trots att lagstiftningen egentligen är ett hinder. Den ska tolkas och den ska på något sätt behandlas i varje verksamhet. Och då gör många av de här organisationerna som vi samarbetar med inom de större it-bolagen den typen av uppgifter att hjälpa kommuner och offentliga aktörer att komma fram till beslut som ändå håller rimligt bra. För många gånger när man pratar om det här med att man får en revision från IMY, Integritetsskyddsmyndigheten, då tittar ju inte de bara på att man har gjort rätt eller fel utan också vilka vidtagna åtgärder man har gjort för att förhindra att information ska spridas felaktigt eller om man har gjort sina granskningar och analyser och bedömt risk. Så det finns mycket man kan göra för att ändå komma fram till ett beslut som inte är riktigt solklart enligt

lagstiftningen. Men där det finns andra faktorer som har vägts in och gjort att man ändå kunnat komma fram till målbeslut.

Men så har ni då, när ni identifierar risk, gör ni det för olika områden, olika riskfaktorer?

Respondent 5: Ja det är klart, men egentligen är det om, vad ska jag säga, om man nu pratar om just den här målfrågan som handlar oftast om tillgänglighet och sekretess, konfidentialitet då egentligen, så är det ju två lagstiftningar som är mest problematiska. Det är ju GDPR, personuppgiftslagstiftningen och offentlighet- och sekretesslagstiftningen. Där man har manglat mycket saker har det inte varit personuppgifter som har varit det som har varit problemet utan det som har varit utmaningen är ju sekretesslagstiftningen med att röja sekretess för information för oberoende. Det är ju det som Cloud Act egentligen handlar om, man röjer det för obehöriga och de obehöriga är ju de amerikanska nationella myndigheterna som man inte har kunnat garantera då, särskilt för lagstiftning när det gäller kanske patientdata-uppgifter till exempel eller uppgifter som rör socialtjänstlagen till exempel. Massa sådana saker som är utmaningar i det här och det har man ju fått vägt, om man säger så, utifrån risk och konsekvens som man ska säga på det sättet. Plus förslagit ett antal åtgärder som man kommer att implementera och det är ju olika åtgärder beroende på vilken sekretess vi pratar om. Sekretess för patientdata är ju på ett sätt och sekretess för socialtjänstuppgifter är ju en annan då, eftersom att det är olika lagrum. Och det gäller ju även tillgängligheten skulle jag säga också.

Respondent 4: Nej men det är ju så, varje enskilt fall prövas utifrån de förutsättningar som gäller den informationsmängden och den nämnden och den juridiska domänen som de befinner sig inom och de är olika. Sen är ju kommunlagen eller kommunallagen är ju gemensam för de flesta verksamheterna. OSL [Offentlighets- och sekretesslag (2009:400)] är ju gemensam och säkerhetsskyddslagen i den fallen tillämpas ju också kommungemensamt. Så att flera lagområden täcker ju hela organisationen och måste finnas med i aspekterna. Sen är det mer domänspecifikt eller verksamhetsspecifika lagstiftningar som patientdata eller skoldata.

Respondent 5: Det är väl det som gör det komplext i sig självt. Det är inte en lagstiftning som bara täcker allt utan det är ju flera lagstiftningar som täcker delar av verksamheten. Det är ju det som en kommun gör det rätt komplext att hantera juridiskt. Särskilt när man ska gå upp i moln. Samma sak som Respondent 4 sa här också, att diskutera kontinuitet egentligen när det gäller återläsning till exempel och återstart till exempel. Det är ju helt beroende på vilken tillgänglighet du behöver ha på den informationen som du har klassat. Patientdatauppgifter kanske har en helt annat krav på tillgänglighet än vad den har på information om bygglov som är inom plan- och bygglovslagstiftningen. Det finns många saker att ta hänsyn till på det sättet.

Som jag förstår är att ni försöker ändå identifiera och skatta vilka är de mest kritiska processerna och prioritera era processer och system och delar av organisationen?

Respondent 4: Det här gör ju verksamheterna. Informations- och itsäkerhet är ju definitivt som vi sa inledningsvis ett stöd i det här. Att informationen klassas och göra de medvetna om de riskerna som finns. Men i slutändan så ligger ansvaret och ägandeskapet av informationen på nämnderna. De här myndigheterna vi nämnde tidigare. De är också ansvariga för att de verksamheter de bedriver har tagit hänsyn till riskerna på rätt sätt och bedömt dem och bidragit rätt åtgärder. Och sedan också ställt krav på tillgänglighet och informationsintegritet.

Respondent 5: Precis vad man kan säga egentligen. Man behöver ju ställa kanske två frågor. Vilka informationsmängder använder organisationen? Har ni dokumenterat det? Vet ni var de finns någonstans? Och den andra frågan är hur länge får den informationen vara borta? Icke tillgänglig? Är det en minut, en timme, ett dygn? Det kommer ju ställa krav på hur kontinuiteten måste vara då. Och vad är alternativen då om informationen inte är tillgänglig då? Ska det finnas en kopia i kassaskåpet eller ska ni jobba manuellt, ni skrivit ut den på papper? Det finns ju många grader i helvetet om man säger så. Allting är ju inte bara it-system utan det handlar om hur arbetar man i stället. Den är väl jätterelevant i dessa tider när vi pratar om vad är kommunens huvuduppdrag och vad är uppdraget i civilförsvaret till exempel. Då kan man inte förvänta sig i princip någonting. Och vad som är kärnverksamheten i en sådan situation är ju inte vad det är i en normal situation som vi har nu.

Då förstår jag att ni gör analys på återhämtningstider och vad är kravet på när detta systemet måste igång igen?

Respondent 5: SLA [Service Level Agreement] eller OLA [Operating/Operational Agreement] ställer ju krav på återläsning. Det i sin tur har att göra med hur länge det får vara borta. Minimumtid för återläsning. Det bestämmer ju ska systemet vara dubblerat, tripplerat, ska det vara replikerat. Alla de kommer ner i tekniska åtgärder i slutändan. Det finns ju modeller för att räkna på saker och ting när det gäller RTO [Recovery Time Objective] till exempel. Alla de här olika begreppen finns i modeller som man kan använda. Förutsättningarna att man har koll på den informationen som ska vara tillgänglig. Så det är grunden i informationscentret.

Respondent 4: Det är också en realitet eller ett uppvaknande för många verksamheter. Om man börjar prata om att det kostar att få 98,5% eller 99,5%. Man är inte alls insiktfull om vilka effekter det får i den underliggande infrastrukturen. För även om vi lägger allting i molnet så tänker man att nu är allting färdigt. Men i själva verket så är det ju bara någon annans datahall. Så det är inte så att det blir 100% tillgänglighet bara för att vi hittar en outsourcingpartner. Oavsett om det är Microsoft eller Kalles datafirma på hörnet. Man brukar börja väldigt ambitiöst och tycka att allting ska vara 100% och inga problem. Man tillåter sig att gå med på någon form av resonemang. Men man kan inte tänka i tiotal eller delar av procent utan att tycka att det blir för mycket. Ända fram tills prislappen presenterats då blir det ett helt annat debattklimat. Det är väl därför också att det blir den här kopplingen mellan informationsägandeskapet och klassningen och kraven kopplas ju direkt tillbaka till verksamheten när den ska omvandlas i åtgärder. Och då blir det väldigt lätt att resonera med verksamheterna kring det. Till syvende och sist är det de enda pengar som finns i kommunen det är ju skattemedel. Det är kommunmedborgare och det är statsbidrag. Och när de inte räcker till då får man justera sina krav.

Jag tänkte begrepp som RTO exempelvis. Har ni kvantifierat dessa? Finns det dokumenterat?

Respondent 5: Svaret är nej skulle jag säga på det sättet. De finns ju informationsklassningar. Och det är ju SKR:s Klassa som används för att få ut informationsklassningskraven från konfidentialitet, riktighet, tillgänglighet, spårbarhet. Där finns de då. Så det är ju respektive verksamhet som gör det här genom deras informationssamordnare. Och det är ju varierande om hur nya eller hur gamla de här är. Det beror lite på då. Dels om organisationen har rört på sig och fått annat uppdrag så kanske de har andra processer och annan informationsmängd. Har de inte det så har de kanske äldre informationsklassningar som de lutar sig på. Så det finns ju. Man tittar på det här och gör revision av de här sakerna. Men det görs av säkerhetsavdelningen. Men vi har ingen uppföljning på IT-säkerhet utan vi vill ju koppla kraven till faktiska

investeringar eller faktiska åtgärder i vår infrastruktur för att möta de här kraven. Och då blir det ju en prislapp. Och då blir det precis som Respondent 4 har sagt, det blir en diskussion mellan vad är önskemålen och vad är verkligheten. Och där jobbar man fram och tillbaka i det här. För det är ju äskningar som man måste göra i budget i slutändan. Varje år eller att man till exempel måste gå upp ända till kommunfullmäktige och tala om att här behöver vi göra åtgärder av olika skäl.

Respondent 4: Det finns ju alternativa åtgärder. En alternativ åtgärd som är ganska vanlig i kommunal verksamhet är att man har manuella rutiner. För att ha en hundraprocentig lösning, det har nästan inget verksamhetsråd med när man tittar till alla tänkbara scenarier när saker och ting inte längre fungerar. Och då hittar man olika sätt att lösa det. Och att ha en tillgänglighet på hundra procent eller en tillgänglighet på 99 procent kan skilja rätt många miljoner. Det är ganska många medarbetare som kan vara manuellt arbetande under en tid för att det här ska lösas i alla fall. Det finns många sätt att omhänderta ett faktiskt skallkrav. Det är inte bara digitala lösningar som är åtgärderna. Att hitta arbetssätt och rutiner när saker och ting verkligen går åt sidan. Det går att hitta det också.

Respondent 5: Praktexempel kan man säga att vård och omsorg har ju jobbat med det här och är van att arbeta manuellt. För deras verksamhet där är ju kritiskt. Där finns ju rutiner redan på plats. Och det kunde vi ju se under den här cybersäkerhetsincidenten. Att deras omställning då var relativt enkel att göra. De kunde vara borta i ett par dagar. Det gjorde ingenting. För att de visste vad de skulle göra i stället. För de vet att fara för liv. Det måste finnas manuella rutiner för hur man gör saker.

Har ni något exempel på en sån här manuell rutin? Och hur har dessa manuella rutiner tagits fram? Är det efter erfarenhet från skarpa situationer? Eller finns det något förebyggande arbete för det?

Respondent 5: Det är lite svårt att säga hur verksamheten har gjort. De jobbar lite olika med det. Vi ser ju bara grunderna i informationsklassningen och de sakerna. Jag skulle säga att det är lite svårt. Men jag skulle säga att det är säkert en kombination. Närmast när jag har pratat med våra informationssamordnare i vård och omsorg. Så är det väldigt mycket utifrån erfarenhet man tar. Man vet vilka guldägg man har och det man måste ha för att kunna bedriva verksamheten framåt oavsett om man har ett IT-stöd eller inte. Man har jobbat fram till exempel listor för saker och ting när det gäller journaler för hemtjänsten. Alla de här sakerna finns, det vet jag. Sen finns det säkert mer saker som jag inte känner till. Men jag tror att man har byggt på erfarenhet. Och man har reviderat det. Och det beror på att man har övat. Vi har haft pandemier och vi har haft massa sådana här saker. Där skulle jag säga att den verksamheten har blivit rätt duktig på att anpassa sig.

Respondent 4: Ja man kan lägga till att IT är ett ganska nytt verktyg inom de här kärnverksamheterna. Man har blivit skola och vårdomsorg långt innan vi hade IT-stöd. Det ska nog inte underskattas heller kravet som finns i lagstiftningen på att man ska tillhandahålla tjänst till medborgarna. Och då måste man omsätta det ansvaret i någon form av förmåga. Även om datorerna stannar. Så jag tror att man har erfarenhet. För man har sett det här i flera olika tillfällen. Man har ju perspektiven att det här kommer att någon gång hända. Men som sagt man känner också till det ansvar man har långsiktigt. Det finns nog flera faktorer. Så arbetet sker nog ständigt. Man har något verksamhetsutvecklande arbetssätt i de flesta verksamheter. Och vi sitter ju naturligtvis med vår incidentförmåga när saker händer. Och vi faktiskt inte kommer åt sig våra normala verktyg. Då måste vi ha våra reservrutiner. Och det är väl just att man bygger upp det här utifrån scenarier. Vad är det som ska hända? Vad gör vi då? Ni pratade

säkerligen om de här skrivbordsövningarna. Nu låtsas vi att vårt ena datacenter har gått ner. Okej, vad får det för konsekvenser? Det har brunnit i fiber mellan våra hallar. Vad får det för konsekvenser? Så ritar man upp det och så bygger man ju sina rutiner från det som... När man kollektivt sitter och tänker på ett scenario så kan man ju utveckla någon form av... Det här hade vi inte tänkt på förra gången. Det här måste vi lägga till. Och så blir det bättre och bättre successivt. Jag tror att det är ganska vanligt inom verksamheten att de har den typen av förbättringsarbete. Och höja sin förmåga oavsett om det är normala tider eller lite mer avvikelser.

Respondent 5: Jag kan väl nämna att ni känner till att Aurora 23 körs ju nu. Där är ju kommunen inblandad också på olika sätt. Särskilt vård- och omsorg och räddningstjänsten som är kommunförbund. Det vill säga det är kommunerna som äger det här. Så de samverkar ju det här under andra typer av scenarier som de övar. Så utifrån det där kommer det säkert komma en massa åtgärder. Det är ju extremt i krigssituationer i och för sig. Men det är väl det ultimata skulle jag säga.

Det jag tänkte var... Ni sa ju det här om sjukvården och omsorgen. De var väldigt bra på att anpassa sig. Är det något som de andra verksamheterna tar tillvara på? Att de kan dela informationen mellan dem?

Respondent 5: Jag ska låta det vara osagt. Samverkande mellan verksamheter som inte har någon beröring tror jag kommuner har generellt svårt med. Men det är min personliga åsikt att det är så. Där man har samverkan till exempel skolhälsovård och vård och omsorg. Till exempel när det gäller skola. Där finns naturliga kopplingar. Socialtjänst till exempel med vård och omsorg finns i vissa kopplingar. De övriga verksamheterna, där tror jag man har en utmaning i kommunerna. Man jobbar mycket stuprör. Eftersom, som Respondent 4 sa, verksamheterna är egna myndigheter via sina nämnder. Tvärfunktionellt är svårare att arbeta eftersom de har egna nämnder, egna myndigheter och egna budgetar. Så det ligger lite i kommunallagen och sättet en kommun är organiserad. En medger inte samverkan riktigt organisatoriskt på det sättet. Men det är min personliga åsikt. Det kan mycket väl vara så att det finns. Men det är något som inte jag känner till. Jag har varit här i fem år men jag har inte hört att man gör det på det sättet. Men det är en bra punkt. Det borde finnas, så ska jag väl säga.

Respondent 4: Sen bedriver ju alla verksamheter sin verksamhetsutveckling på olika sätt. Det är inte så att vård och omsorg har insett behovet av att finnas även när elektroniken har stannat. Det gäller ju även socialtjänsten, kultur och fritid. De har olika behov och tillgängligheter. Om allting går riktigt illa och det blir någon form av kris i samhället så kommer kanske inte så många att behöva gå till Stadsmuseet i Norrköping. Det är ganska många som kommer att behöva sin vård och omsorg och äldreboende och ambulerande hemtjänst. Det är livsuppehållande. Så man kanske också ställer kraven utifrån när det går riktigt illa. Vad är det som vi kommer att förväntas göra? Då kanske inte vi och museum är det riktiga stället.

Respondent 5: Vad som händer egentligen, det vet ni säkert, är att myndigheter eller kommuner går upp i stabsläge. Ett stabsläge är ju den situationen en kommun samlas och prioriterar vad som är kärnverksamhet och viktigt. Det är inte förrän då egentligen man samarbetar över alla verksamhetsgränser. Jag skulle säga att krisledningens erfarenhet när man drar av de situationer som har uppstått, det är ju där egentligen man gör förbättringar i saker och ting. Det sker liksom inte på verksamhetsnivå i en vanlig situation skulle jag säga. Jag ser inte det i alla fall.

Som jag förstår rätt, då låter det som att ni samlas och jobbar tillsammans först när en händelse har inträffat. Det är först då som ni börjar titta på eventuella förbättringar.

Respondent 5: Ja, det är ju tyvärr så. Man kan väl säga att det görs på två sätt. Antingen så är det lagstiftaren som talar om att det måste finnas saker. Den andra delen är att man gör det på grund av att man vet av erfarenhet att man måste göra vissa saker. Därav kommer samarbetet. Själva krisledningen och den som leder kris i en kommun det är ju säkerhetsavdelningen som har huvudansvaret att göra det. Det är de som samordnar det här, egentligen inom en kommun, inom Norrköpings kommun i alla fall. Så de har ju det ansvaret att just göra den här samordningen och förbättringen. Sen så trycks det ner i organisationen för det som är gemensamt då.

Respondent 4: Jag skulle även säga att varje verksamhet har ju ett naturligt arbetssätt och har sina arbetsmetoder och uppdrag. Så det är inte så att vi väntar på en kris innan vi börjar titta på något annorlunda. Det skiljer ständigt inom alla verksamheter. Det är inte någon skillnad på ett privatföretag eller en offentlig organisation. Alla vill jobba smartare istället för hårdare. Men sen kanske det har olika prioriteringar runt vilket tillstånd man befinner sig i. Har man mycket tid och mycket kapacitet så kan man alltid bedriva mer verksamhetsutveckling. Ni vet ju att det pratas mycket om att vård- och omsorgsapparaten är ganska underbemannad. Man har svårt att få tag på rätt kompetens. Precis som inom IT. Det är rätt många områden som berörs. Då är det svårt att hitta utrymme för att faktiskt göra det här. Även om det långsiktigt gynnar oss att göra bättre saker framåt så är det svårt att hitta tid nu att göra sakerna mer effektiva om några månader.

Respondent 5: Jag tror att när det kommer till kritan och det har man lärt sig under många år och har en erfarenhet av att lösa kommunens kärnuppdrag. Precis som du säger så finns det en massa uppdrag som kommunen har som inte är kärnverksamhetsuppdrag. Då kommer det till de här klassiska frågorna: Mat för dagen, tak över huvudet, se till att det finns rent vatten. Sådana här väldigt basala saker. Man pratar nu till exempel lite mer om att när det är riktig kris att man fortfarande ska kunna bedriva skolverksamhet till exempel under längre kriser. Men det är ju ingenting som är uttalat. Men normalt sett är de här väldigt basala sakerna. Och det kanske inte medborgare riktigt förstår. Att det man har som kommunservice i en normal situation och det man kommer att få under en riktig kris är något helt annat. Det är väl någonting man måste kommunicera ut till medborgare och kommunicera ut vad det innebär. Det handlar om att bygga upp civilförsvaret till slutändan. Skulle jag säga.

Ni säger ju att det testas när det sker en kris. Det testas nu med Aurora 23. Men sker det testsimuleringar också?

Respondent 5: Det kan inte jag svara rakt av så här på. Det är ju säkerhetsavdelningen som håller ihop det. Jag misstänker att det görs men jag har ingen frekvens på det. Att de har ansvaret att se till att verksamheten har kontinuitetsplanering – svar ja. Det har de. Det har de enligt lag. Så det är inga svårigheter med det. Men i vilken frekvens man gör det här. I så fall får jag återkomma för jag kan inte svara rakt ut.

Du har inte koll på om det dokumenteras testresultat och sånt?

Respondent 5: Jag vet att det görs men jag vet inte i vilken frekvens och vilken verksamhet som gör vad. Svaret är ja, det görs. Det kan jag säga.

Vi kan beröra det här med riskbehandlingstrategier. Kan ni berätta någonting om det? Hur väljer ni och tillämpar de riskbehandlingstrategierna?

Respondent 4: Det klassiska är väl att man utgår från sannolikhet och konsekvens. Det finns ett metodstöd för den här klassningen som vi tittade på tidigare. Men det är upp till verksamheten att identifiera risker som finns. Nu utgår vi från informationen. Sen finns det andra typer av risker. Man kan prata om operativa risker, ekonomiska risker, juridiska risker. Det finns risker på många nivåer. Riskerna som vi nu funderar på är hur hanteringen av information riskbedöms. Om den inte är tillgänglig, vilka risker finns med det? Hur ser sannolikheten ut för att det händer? Vad är konsekvenserna av att informationen inte är tillgänglig? Vad händer om informationen förvanskas? Konsekvenserna av det, sannolikheten för det? Så vidtar man de åtgärderna. Det är en ganska klassisk metod när man utgår från informationen i sig. Sen får det sättas i något sammanhang.

Respondent 5: Sen är det så att verksamheterna, de olika verksamheterna, nämnderna, myndigheterna. De har krav på sig att göra riskanalyser för verksamhetsförändringar. Organiserar man om saker och ting så gör man riskanalyser för det. För det hänger ihop lite med, får man ett nytt uppdrag till exempel. Så får man ju också kanske hantera system, information på ett annat sätt. Vad innebär det då utifrån konfidentialitet, riktighet, spårbarhet, tillgänglighet? Plus att man tittar på hur organisationen förändras i sina processer. Det görs på verksamhetsnivå. Det som är anmärkningsvärt i Norrköpings kommun, det kan jag nämna, det är ingen hemlighet. Det är att man inte tar verksamhetsriskerna och aggregerar upp dem och tittar på hela riskbilden. Det kanske är lite konstigt tycker jag. För det pratar vi mycket om. Hur kan vi säkerställa att kommunens ledning och kommunens politiker förstår den hela riskbilden? Det är alla perspektiv av risk. Utifrån operativa risker, informationssäkerhetsrisker, där innefattas tillgänglighet och konfidentialitet. Ekonomiska risker, juridiska risker. Det perspektivet, man har inte det arbetssättet på det sättet skulle jag säga. Jag tror inte det är unikt för den här kommunen, utan det är hur kommunerna är uppbyggda.

Respondent 4: Respektive nämnd får ansvara för sina risker, men på kommunnivå vet man egentligen inte.

Respondent 5: Inte i helhet tror jag. Man är lyckligt ovetande. Varenda direktör vet ju. Och säkert varenda nämndordförande vet ju. Men om man tittar på vem som håller kontroll över hela bilden och värderar det här. Om vi ska fungera som en kommun med alla de verksamheter som har, vilka risker har vi totalt? Så vi vet vad som är viktigast att springa på i så fall. Den stora planen om man säger så. Det är en jätteutmaning för en kommun skulle jag säga. Det behövs en strategi. Absolut.

Är det någonting ni vill tillägga?

Respondent 5: Är det någonting man kan ta del av sen?

Vi skickar ut det när vi är färdiga. Tack så jättemycket för att ni tog er tid och att vi kunde få till den här intervjun.

Respondent 4: Kommer ni på något ni vill höra av er eller boka något mer. Dela gärna med er när ni har författat era uppsatser och fått ner det så läser vi gärna.

Det ska vi göra.

Referenser

Advenica, Dataföreningen, SIG Security, Magnusson, C., Radar & Swedish Association for Civil Security. (2017). Svenskt IT-Säkerhetsindex, Available Online: https://f.hubspotusercontent30.net/hubfs/8791031/content/Svenskt_IT_Sakerhetsindex_2017%20(2).pdf

Andersson, A.-L. (2022). Rapport IT-attacken socialfvaltningen Kalix kommun. En summering av arbetet fe, under och efter it attacken som drabbade kommunen den 16 december 2021, Available Online: https://www.kalix.se/globalassets/omsorg/hemtjansten/it-attacken-socialforvaltningen-220815.pdf [Accessed 10 May 2023]

Cerullo, V. & Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach, *Information systems management*, vol. 21, no. 3, pp.70–78

Checkpoint Research Team. (2022). Check Point Research: Third Quarter of 2022 Reveals Increase in Cyberattacks and Unexpected Developments in Global Trends, *Check Point Blog*, Available Online: https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/ [Accessed 15 May 2023]

Clark, P. (2010). Contingency Planning and Strategies, in *2010 Information Security Curriculum Development Conference*, 2010, pp.131–140

Devargas, M. (1999). Survival Is Not Compulsory: An Introduction to Business Continuity Planning, *Computers & Security*, vol. 18, no. 1, pp.35–46

Dey, M. (2011). Business Continuity Planning (BCP) Methodology—Essential for Every Business, in *2011 IEEE GCC Conference and Exhibition (GCC)*, 2011, IEEE, pp.229–232

Försvarsdepartementet. (2006). Lag (2006:544) Om Kommuners Och Regioners Åtgärder Inför Och Vid Extraordinära Händelser i Fredstid Och Höjd Beredskap, 2006:544, Pub. L. No. 2006:544, Available Online: https://rkrattsbaser.gov.se/sfst?bet=2006:544 [Accessed 15 May 2023]

Gibb, F. & Buchanan, S. (2006). A Framework for Business Continuity Management, *International journal of information management*, vol. 26, no. 2, pp.128–141

Hayes, B. E., Kotwica, K. & Correia, D. (2013). Business Continuity. Playbook., *ScienceDirect EBooks - Freedom Collection Books Backlist; ScienceDirect EBooks - All Access*, [e-book] Elsevier, Available Through: ePublications https://ludwig.lub.lu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat02271a&AN=atoz.ebs1883166e&site=eds-live&scope=site

Herbane, B. (2010). The Evolution of Business Continuity Management: A Historical Review of Practices and Drivers, *Business history*, vol. 52, no. 6, pp.978–1002

IDG. (2020). Systemkritisk felpunkt | IDG:s ordlista, *IT-ord*, Available Online: https://it-ord.idg.se/ord/systemkritisk-felpunkt/ [Accessed 14 April 2023]

ISO. (2019). Security and Resilience -- Business Continuity Management Systems -- Requirements, 22301:2019, Available Online: https://www.sis.se/produkter/foretagsorganisation/foretagsorganisation-och-foretagsledning-ledningssystem/foretagsorganisation/iso-223012019/ [Accessed 15 May 2023]

Iyer, R. K. & Bandyopadhyay, K. (2000). Managing Technology Risks in the Healthcare Sector: Disaster Recovery and Business Continuity Planning, *Disaster Prevention and Management: An International Journal*, vol. 9, no. 4, pp.257–270

Jacobsen, D. I. (2002). Vad, Hur Och Varför : Om Metodval i Företagsekonomi Och Andra Samhällsvetenskapliga Ämnen., [e-book] Studentlitteratur, Available Through: Library catalogue (LUBcat) https://ludwig.lub.lu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat07147a&AN=lub.1444498&site=eds-live&scope=site

Jafar, E. & Taneja, U. (2017). Business Continuity Planning—a Survey of Hospitals in Delhi, *Journal of Public Health*, vol. 25, pp.699–709

Jangefelt Nilsson, Jenny and Skarin, Helena. (2010). Nyttan av Business Continuity Management vid oförutsedda händelser- en studie av verkliga fall, Available Online: http://lup.lub.lu.se/student-papers/record/1719808

Kalix Kommun. (2023). Kalix kommuns hantering av driftfel till följd av IT-attacken, *Kalix Kommuns hemsida*, Available Online: //www.kalix.se/Samhalle/kalix-kommuns-hantering-av-driftfelen-till-foljd-av-it-attacken/ [Accessed 15 May 2023]

Krisinformation. (2023). It-Störningar Och Informationssäkerhet - Krisinformation.Se, Available Online: https://www.krisinformation.se/detta-kan-handa/internetsakerhet [Accessed 15 May 2023]

Lindström, J., Samuelsson, S. & Hägerfors, A. (2010). Business Continuity Planning Methodology, *Disaster Prevention and Management: An International Journal*

Moh Heng, G. (2015). Business Continuity Management Planning Methodology, *International journal of disaster recovery and business continuity*, vol. 6, no. 1, pp.9–16

Myndigheten för samhällsskydd och beredskap. (2020). Sekretess i risk- och sårbarhetsanalys, Available Online: https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/risk--och-sarbarhetsanalyser/sekretess-i-risk--och-sarbarhetsanalys/ [Accessed 14 May 2023]

Myndigheten för samhällsskydd och beredskap. (2021). Kommunens krisberedskap, Available Online: https://www.msb.se/sv/amnesomraden/skolmaterial/samhallets-krisberedskap/kommunens-krisberedskap/ [Accessed 13 April 2023]

Norrköpings kommun. (2023). Informationsfilm om cybersäkerhetsincidenten [text], *Norrköpings kommun*, Available Online: https://norrkoping.se/nyhetsarkiv/nyheter/2023-03-03-informationsfilm-om-cybersakerhetsincidenten [Accessed 15 May 2023]

Oates, B. J., Griffiths, M., McLean, R. & Oates, B. J. (2022). Researching Information Systems and Computing., Second edition., [e-book] SAGE, Available Through: Library catalogue (LUBcat)

https://ludwig.lub.lu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat07147a&AN=lub.7057354&site=eds-live&scope=site

Phillips, B. D. & Landahl, M. (2020). Business Continuity Planning - Increasing Workplace Resilience to Disasters, edited by B. D. Phillips & M. Landahl, [e-book] Butterworth-Heinemann, Available Online: https://www.sciencedirect.com/science/article/pii/B9780128138441000099

Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C. & Sutskever, I. (2022). Robust Speech Recognition via Large-Scale Weak Supervision, *arXiv preprint arXiv:2212.04356*, [e-journal], Available Online: https://cdn.openai.com/papers/whisper.pdf [Accessed 20 April 2023]

Rittinghouse, J. W. (1) & Ransome, J. F. (2006). Business Continuity and Disaster Recovery for InfoSec Managers, *Business Continuity and Disaster Recovery for InfoSec Managers*, [e-book] Elsevier Inc., Available Through: Scopus® https://ludwig.lub.lu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edselc&AN=edselc.2-52.0-85013954336&site=eds-live&scope=site

Sambo, F. & Bankole, F. O. (2016). A Normative Process Model for ICT Business Continuity Plan for Disaster Management in Small, Medium and Large Enterprises., *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 6, no. 5

SCB. (2022). Befolkningen koncentreras till allt färre kommuner, *Statistiska Centralbyrån*, Available Online: https://www.scb.se/hitta-statistik/artiklar/2022/befolkningen-koncentreras-till-allt-farre-kommuner/ [Accessed 15 April 2023]

Setiawan, A., Wibowo, A. & Susilo, A. H. (2017). Risk Analysis on the Development of a Business Continuity Plan, in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 2017, pp.1–4

SIS. (2014). Samhällssäkerhet — Ledningssystem För Kontinuitet — Vägledning till SS-EN ISO 22301, Available Online: https://www.sis.se/produkter/ledningssystem-e07b0fe8/samhallssakerhet/ss223042014/

Snedaker, S. & Rima, C. (2014). Business Continuity and Disaster Recovery Planning for IT Professionals, Second Edition., [e-book] Boston: Syngress, Available Online: https://www.sciencedirect.com/science/article/pii/B9780124105263000015

Sveriges Kommuner och Regioner. (2021). Kommunernas Informationssäkerhetsarbete, Available Online: https://skr.se/download/18.4d3d64e3177db55b16630f51/1615461671520/Kommunernas%20informationss%C3%A4kerhetsarbete%20rapport.pdf [Accessed 13 May 2023]

Sveriges Kommuner och Regioner. (2022). Kommuner och regioner [text], Available Online: https://skr.se/skr/tjanster/kommunerochregioner.431.html [Accessed 15 May 2023]

SVT. (2023). Ryska hackare låg bakom cyberattacken mot Norrköpings kommun, *SVT Nyheter*, 27 February, Available Online: https://www.svt.se/nyheter/lokalt/ost/ryska-hackare-lag-bakom-it-attacken-mot-norrkopings-kommun [Accessed 3 May 2023]

Swanson, M. M., Bowen, P., Phillips, A. W., Gallup, D. & Lynes, D. (2010). Contingency Planning Guide for Federal Information Systems, Available Online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Willander, F. & Håkansson, J. (2023). Hackarna slog ut barnens skolskjuts – ”Fick ta fram papper och penna”, *TV4*, Available Online: https://www.tv4.se/artikel/7rAHkljlvZguTU3r4YCHOS/hackarna-slog-ut-barnens-skolskjuts-fick-ta-fram-papper-ochpenna [Accessed 15 May 2023]