MALMÖ UNIVERSITET

Proaktiv Riskhantering:

En kvalitativ studie om dess betydelse för informations- och cybersäkerhetsföretag i sviterna av Covid-19

Proactive Risk Management:

A qualitative study of its importance for information and cyber security companies in the wake of Covid-19

Kandidatuppsats

Ludwig Bauhn

Fanny Ahlén

IT- och Ekonomi
Kandidatnivå
13 HP
VT2023
Handledare: Sven Tengström

Sammanfattning

Digitaliseringen sker i en rasande fart världen över, vilket resulterar i en ofantlig ökning av data som cirkulerar. Detta i sin tur både bringar nya möjligheter men också stora utmaningar för företag då man ständigt måste vara redo på det oväntade vilket inte minst märktes då Covid-19 pandemin slog till. Organisationer tvingas stänga ner sina kontor och istället arbeta hemifrån, vilket innebär ännu större risker gällande hot och säkerhet om man inte var väl förberedd. Syftet i denna studie är att studera företag inom informations- och cybersäkerhetsbranschen och hur deras interna, proaktiva riskhanteringsarbete ser ut. Med grund i Covid-19 vill vi dessutom studera de lärdomar dessa företag tog med sig från pandemin. För att uppnå detta har vi genomfört en kvalitativ studie baserad på 9 intervjuer med individer inom branschen som fått berätta om deras tankar och åsikter kring proaktiv cybersäkerhet och Covid-19. Studien har resulterat i en sammanställning av de strategier och metoder som anses centrala för att bedriva en så framgångsrik riskhantering som möjligt med stort fokus på individen och dess medvetenhet och kunskap vilket anses vara en central del. Exempelvis kan företag arbeta efter Zero trust-principen för att verifiera och kontrollera vilka tillgångar en individ har, samt arbeta efter de fyra vanligaste arbetssätten; personalutbildning, etiska hackare, jaga hot och proaktiv övervakning av nätverk och slutpunkt, för att proaktivt reducera sannolikheten att exponeras för oönskade risker.

Nyckelord: Covid-19, Proaktivt, Cybersäkerhet, Informationssäkerhet, Riskhantering.

Abstract

The digitalization develops at a blistering pace all around the world which results in an immense increase of circeling data. This in turn brings new possibilities but at the same time a lot of challenges for companies. They constantly have to be ready and expect the unexpected which was not least noticed when the Covid-19 pandemic hit. Organizations were forced to shut down their offices and work from home instead, which in turn implies even greater risks when it comes to threat and security if you are not prepared. The purpose of this study is to study companies in the information- and cybersecurity industry and how their internal, proactive risk management looks like. With Covid-19 as the foundation we also aim to study the lessons learned by companies as they emerged from the pandemic. To achieve this we have carried out a qualitative study based on 9 interviews with individuals in the industry which have had the opportunity to tell us their thoughts and opinions about proactive cybersecurity and Covid-19. The study has resulted in a compilation of the strategies and methods that are considered central to conducting as successful risk management as possible with a strong focus on the individual and their awareness and knowledge, which is considered to be a central part. For example, companies can work according to the Zero Trust principle to verify and control the assets an individual has, as well as work according to the four most common approaches: employee training, ethical hackers, threat hunting, and proactive monitoring of networks and endpoints, in order to proactively reduce the likelihood of being exposed to unwanted risks.

Key words: Covid-19, Proactive, Cybersecurity, Information Security, Risk Management.

1.Inledning

1.1 Introduktion

För varje dag som passerar tar digitaliseringen stora kliv framåt. Företag som tidigare hanterat all information, kundkontakt och interaktion fysiskt börjar nu istället sköta detta genom digitala kanaler och medel. Banker och flygbolag använder sig av chattbotar, sjukhus och vårdcentraler sköter bokningar och träffar patienter genom applikationer som Kry.se och NärhälsanOnline och stora globala företag har möten digitalt över Teams och Zoom. Detta har givetvis resulterat i enorma möjligheter för dagens företag då de kunnat utöka sina verksamheter och utvidga sin kundkrets i en omfattning som för bara några år sedan endast gick att drömma om. Det har samtidigt resulterat i ett kraftigt ökat digitalt informationsflöde, med andra ord en markant ökning av *data* som numera finns tillgänglig vilket i sin tur innebär att fler *risker* uppstår. Denna data behöver skyddas, företagen behöver policys och riktlinjer för att hantera och reglera åtkomsten för att förhindra läckage och intrång vilket i sin tur bidragit till att cybersäkerhet blivit en viktig och integrerad del av företagens övergripande strategier. Detta märktes inte minst vid Covid-19 pandemins utbrott där de som redan innan arbetat med kontinuerlig proaktiv riskhantering tacklade världskrisen bättre än de som inte prioriterat detta.

Ytterligare ett konkret exempel på cybersäkerhetshot och risker som uppstår som ett resultat av digitaliseringen kan ses i form av attacken mot Coops leverentör, Kaseya, i juli 2021. I detta fall har hotaktörerna genomfört en Ransomware-attack genom att placera skadlig mjukvara hos en av Coops leverantörer, vilket resulterade i att deras system blev låsta och en lösensumma begärdes ut i utbyte mot att låsa upp dem igen (Toresson, 2021). För att undvika att dessa typer av situationer uppstår behöver företagen antingen sätta upp avdelningar för att internt hantera sin informations- och cybersäkerhet, eller anställa externa företag eller konsulter som hanterar detta åt dem. De som väljer att anställa extern hjälp gör troligtvis detta då de anser att dessa företag eller konsulter besitter större kunskap och expertis inom området.

Området informatik är ett högst relevant och brett område med fokus på hela dagens digitaliserade samhälle. Den del av informatik som denna studie ämnar belysa rör *konsekvenserna av digitalisering* och *utvecklingen av digitala praktiker och artefakter* från ett *organisatoriskt perspektiv*. Ordet digitalisering innebär med andra ord just förändring, en förändring i hur digitala praktiker och artefakter används och ordet bygger på användningen av digital teknik (SISA, 2021). I denna rapport kommer vi med ordet *digitala artefakter* referera till de system och processer som möjliggjorde distansarbete till följd av Covid-19 och det digitaliseringsarbete organisationer runt om i världen tvingades genomföra. De förändringar som digitalisering fört med sig har påverkat olika företag på olika sätt, möjligheter har öppnats upp men nya risker har som tidigare nämnts också uppkommit till följd av den ökade mängden data som cirkulerar. Vidare är det sistnämnda av de två, risker

inom cybersäkerhetsbranschen, vad som kommer undersökas och belysas i denna rapport där vi ämnar undersöka vilka strategier och metoder företag bör arbeta med för att främja proaktiv cybersäkerhet.

Cybersäkerhet är ett område vars relevans och betydelse ökat under de senaste åren. Vad cybersäkerhet innebär i sig är svårt att exakt definiera men i en rapport skriven av Cains m.fl. (2022) försöker författarna sig på ett närmande av en gemensam definition. Genom intervjuer av experter inom området med grund i tidigare definitioner av ämnet har forskarna försökt komma fram till en övergripande förståelse och definition om vad som menas med cybersäkerhet, vilket inte är en speciellt enkel uppgift. Författarna beskriver att det finns en avvikelse mellan olika professioner då man talar om cybersäkerhet, men att det finns ett antal begrepp som uppkommer oftare än andra under intervjuerna. Dessa är *context-driven, resilient system functionality, maintenance of CIA (confidentiality, integrity, availability), threat prediction and prevention* och *protection of resources*. Av detta kan utläsas att majoriteten av respondenterna anser att cybersäkerhet i det stora hela handlar om att skydda digitala system från både interna och externa risker och hot. Det kan därför konstateras att det är ett ytterst relevant område som faller inom ramen för informatik.

När det kommer till ordet risk beskriver författarna Huang m.fl. (2020) *risk* som en objektiv kvantitet vilken används för att beskriva nivån av skada på ett specifikt system. Vidare beskrivs ordet risk av Nationalencyklopedin (u.å.) som sannolikheten att en specificerad omständighet leder till en specificerad oönskad händelse under en viss tidsperiod. Inom cybersäkerhetsbranschen ligger fokus ofta just på risk, strategier och en medvetenhet måste finnas för att hantera de interna riskerna som finns inom företaget samtidigt som ett kontinuerligt arbete med extern riskhantering behöver finnas för att skydda sig mot attacker och cyberhot. Vid plötsliga händelser, såsom Covid-19, kan risken att något oönskat händer öka om företaget inte redan innan har en proaktivt utarbetad plan för hur man ska agera och hantera det nya tillståndet (Alawida m.fl, 2022). När det kommer till risk finns i huvudsak två komponenter av relevans; *sannolikheten för en oönskad konsekvens* samt *konsekvensens storlek* (Nationalencyklopedin, u.å.). I denna rapport kommer vi inte hantera risk på ett tekniskt plan med numeriska värden, utan snarare fokusera på de kvalitativa effekterna på organisationen i sig när det kommer till risk och riskhantering. Att arbeta med riskhantering är väsentligt för alla företag och organisationer i dagens samhälle, då explicita systemrisksdefinitioner och tillvägagångssätt behöver arbetas fram för att reducera sannolikheten och/eller konsekvenserna av dem (Huang m.fl., 2020).

Den digitalisering organisationer runt om i världen tvingades genomgå på bara några veckors tid till följd av pandemins utbrott öppnade upp för en hel del av dessa risker när det kommer till informations- och cybersäkerhet. De företag som inte tidigare satt upp ramverk och strategier för att mitigera och reducera sannolikheten av att dessa skulle inträffa kunde råka ut för förödande konsekvenser medan de som redan innan arbetat med proaktiv riskhantering hade ett betydligt bättre underlag vid denna digitala transformation. I denna rapport ämnar vi undersöka detta område djupare för att ta reda på hur några av dagens informations- och

cybersäkerhetsföretag internt arbetar med proaktiv riskhantering samt vilka lärdomar de tagit med sig från de gångna åren sedan utbrottet av Covid-19 pandemin.

1.2 Problematisering

Hot inom cybersäkerhetsbranschen är någonting som alltid kommer finnas då digitaliseringen växer, vilket främjar cyberattacker och cyberbrottskampanjer. Ett tydligt exempel på detta är Covid-19 vilket enligt Alawida m.fl. (2022) beskrivs som världens största cybersäkerhetshot. Pandemin öppnade upp företag i cybersäkerhetsbranschen för sårbarhet gällande deras säkerhet, både internt och externt. Just därför kommer denna rapport att använda denna förändring som grund då vi undersöker dessa risker och hot som trätt fram till följd av Covid-19. Detta är något som skapat stora problem för företag vilket syntes väldigt tydligt i USA då landet i snitt spenderar cirka 6 miljarder dollar per år på att motverka och hantera hot och risker inom cybersäkerhet, men trots detta femdubblades antalet cyberattacker efter utbrottet av Covid-19 (Chaturvedi m.fl., 2020).

Enligt artikeln *Cybersecurity Risks in a Pandemic* lyfter Chaturvedi m.fl. (2020) att det finns många olika delar av problematiken gällande de hot som uppstår i samband med en pandemi, särskilt Covid-19, med anknytning i cybersäkerhet. Artikeln lyfter digitala artefakter som ett hjälpmedel för digitaliseringen men som också används av hackare för dataintrång hos företag. Under pandemin blev det mycket enklare för hackare att utföra attacker som ett resultat av bristen på säkerhet inom företag. Detta då arbetet förflyttades från att göras på företagets fysiska plats med säkert Wi-Fi och bra brandväggar till att göras från hemmet där nätverkssäkerheten är betydligt sämre än på företaget (Glassberg, 2020).

Mellan år 2006 och 2011 niodubblades all mängd data i världen, och idag räknas det med att datamängden fördubblas varje år (Grossman & Pedahzur, 2020). Orsaken till detta var Industry 4.0 vilket var en form av revolution i hur företag tillverkar, förbättrar och distribuerar sina varor och tjänster (IBM, u.å.). Många arbetsuppgifter automatiserades, arbetsprocesser effektiviserades och det ställdes helt nya krav på organisering och struktur på arbetsplatser på alla plan. Detta skedde snabbt, men inte över en natt. Företag insåg redan innan vad som var påväg att hända och kunde därmed adaptera sig till förändringen. Med Covid-19 tvingades människor världen över till olika typer av restriktioner, allt ifrån tillfälligt reseförbud till komplett lock-down vilket resulterade i att företag ännu en gång behövde tänka om när det kommer till sina arbetssätt och processer, men betydligt snabbare denna gång. Det gick inte längre att träffas fysiskt utan företagen behövde snabbt komma på nya vägar för att arbeta och överföra information sinsemellan. Resultatet blev distansarbete vilket kan definieras som “arbete som utförs med hjälp av informationsteknik i hemmet eller på annan plats på avstånd från en mer traditionell arbetsplats” (SOU 1998:15, s.13). Detta gjorde att användarantalet på plattformar som Zoom och Teams fick ett explosionsartat uppsving. Mellan November 2019 och Mars 2020 ökade antalet konsumenter av tjänsten Teams från 20 till 44 miljoner, där 12 miljoner av dessa kom under bara en vecka (Roos, 2022). Denna pandemieffekt fortsatte att påverka arbetsstilen och i oktober samma år var siffran på 115 miljoner användare. Organisationer gick alltså över från att använda sig av fysiska

interaktioner till att istället använda sig av digitala artefakter såsom webbkameror och datorer vilket både ställer helt nya krav på företagets ledning men framförallt också på användarna. Lösenordsskydd i form av bland annat tvåfaktorsautentisering blev nästan till ett måste för att hålla den nya digitala informationen som produceras säker. Tvåfaktorsautentisering är en säkerhetsåtgärd gällande lösenord och konton som i helhet handlar om att ha två lager av skydd för att ta sig in på ett konto (Bhanderi m.fl., 2023). Ett av lagren är användarnamn och lösenord och det andra lagret är engångslösenord för att höja säkerheten. Vidare uppkom, eller i alla fall ökade, denna övergång till ett mer digitalt samhälle risken för cyberattacker samt cyberbrottskampanjer (Singh Lallie m.fl., 2021). De som utfört dessa har varit kreativa och använt sig av den oro som genomsyrat samhället, men också utnyttjat den snabba övergång som medfört brister i informationssäkerheten hos företag. Detta har resulterat i en ny nivå av cybersäkerhetsproblem och utmaningar som industrin och medborgarna aldrig tidigare stått inför och gör det därmed till ett otroligt intressant problem att dyka djupare i.

Hackare runt om i världen använder sig av internet för att dela känslig information och kunskap och idag blir informationssystem kontinuerligt utsatta för cyberattacker (Ericsson m.fl., 2021). Ett sätt att minska detta är genom att analysera kommunikationen och beteendet hos hotaktörer för att proaktivt minska sannolikheten att en cyberattack äger rum. Detta kallas för “Proaktiv Cyberhot Intelligens” och med detta menas att användarna av datorsystem ska använda sig av den data som finns om cyberattacker för att kunna förbereda sig om detta äger rum. Detta görs genom att analysera hotaktörernas kapacitet, intresse samt vilka tillgångar de har för att enklare förbereda sig på en kommande cyberattack (Ericsson et. al., 2021). Själva problemet är att det är väldigt svårt för företag att göra detta. Det kostar mycket pengar, det kräver kunskap och det tar tid som kanske inte finns vilket gör att man kanske väljer att hantera cyberattackerna när de uppstår istället för att proaktivt arbeta för att förebygga dem.

Informations- och cybersäkerhet är ett relativt nytt forskningsområde som snabbt rör sig framåt, och mycket har hänt på senare år då det är kopplat till digitalisering och digitaliseringsarbete, men vi anser att det finns ett glapp i den tidigare forskningen. Det skrivs otroligt mycket om hur de risker som uppkommer kan, eller ska hanteras på ett reaktivt sätt men betydligt mindre om hur ett proaktivt arbete borde finnas för att förebygga dem från första början. Detta speglas de siffror som presenterats rörande cybersäkerhetsbrott vilka hade varit betydligt lägre om företagen redan hade en utvecklad strategi för att hantera dessa hot och risker på ett optimalt sätt. Vidare anser vi att det saknas studier på hur det interna arbetet inom cybersäkerhetsföretag går till. Det skrivs otroligt mycket om hur banksektorn, hälso- och sjukvården, skolor och kommuner bedriver, och bör bedriva sitt informations- och cybersäkerhetsarbete men det finns en märkbar brist på forskning kring de företag som faktiskt anställs för att hantera cybersäkerhet. Cybersäkerhetsbranschen förändras för varje dag i takt med digitaliseringen och det som följer den. Utan rätt förberedelser i form av välgrundade och välutvecklade strategier och metoder, omfattande förståelse och hög medvetenhet för att hantera cyberattacker innan de uppstår kommer det att medföra otroliga risker för företag. Med detta arbete vill vi därför, genom att fokusera på informationssäkerhets- och cybersäkerhetsföretag, komma med en form av förklaring till hur organisationer kan, och bör arbeta med proaktiv riskhantering på ett internt plan.

1.3 Syfte och Frågeställning

1.3.1 Syfte

Syftet med denna rapport är att, med hjälp av insamlade data i form av tidigare forskning och intervjuer, komma med en förklaring på hur informations- och cybersäkerhetsföretag jobbar, och bör jobba med ett proaktivt cybersäkerhetsarbete. Vidare kommer rapporten att mynna ut i en förklaring på vilka de främsta hot och risker företag inom cybersäkerhetsbranschen står inför samt hur dessa hanterades innan respektive efter pandemins utbrott. Med studien vill vi generera en ökad förståelse när det kommer till proaktiv riskhantering av information och data internt inom cybersäkerhetsbranschen. De slutsatser studien leder fram till kommer sedan kunna generaliseras och eventuellt användas av andra typer av företag för att få lärdomar från de som anses vara experter inom området. Trots att fokusområdet för uppsatsen specifikt är informations- och cybersäkerhetsföretag kommer resultatet med andra ord kunna användas av alla de organisationer som på något vis arbetar med IT-säkerhet, vilket är majoriteten av företagen i dagens digitaliserade samhälle. Med denna studie vill vi vidare bidra till att fylla det litterära hålrum som idag finns och öppna upp för vidare forskning inom området. Detta eftersom det är ett högst relevant informatikproblem då det med fokus i digitaliseringen starkt relaterar till utvecklingen av digitala processer och artefakter på allt från individ- till samhällsnivå.

1.3.2 Frågeställning

I detta arbete kommer en central fråga användas med två tillhörande underfrågor vars funktion är att fungera som en kompass för arbetets gång och riktning. Genom att besvara denna fråga och dess underfrågor kommer arbetets resultat att tydliggöras i kapitel *7. Slutsats*. Frågan är utformad efter informatik samt det ämne som arbetet kommer att specialisera sig i. Följande frågor kommer att besvaras:

- *Vilka strategier och metoder bör informations- och cybersäkerhetsföretag arbeta internt med för att främja proaktiv riskhantering?*
    - Hur bedriver utvalda informations- och cybersäkerhetsföretag sitt proaktiva riskhanteringsarbete idag?
        - Vilka lärdomar tog dem med sig efter situationen med Covid-19?

1.4 Avgränsning

Då fokus i denna rapport ligger på informations- och cybersäkerhetsföretag och deras riskhantering används primärt ett organisationsperspektiv. Informationssökningen kommer ske med ett organisationsfokus där vi analyserar, drar kopplingar och hittar samband mellan intervjurespondenternas svar och tidigare forskning relaterat till andra företag. Då vi genomför intervjuerna vill vi främst ta reda på företagens strategier och arbetsmetoder och hur dessa kommuniceras och implementeras, snarare än individens upplevelse av det. Därav kan man argumentera för att studien främst utgår från ett organisationsperspektiv. Dock går det inte att undvika att det dessutom förekommer inslag av individperspektiv då vår primära datainsamlingsmetod är semistrukturerad intervju, varpå respondenternas åsikter och

upplevelser kommer tas i beaktning. Det organisatoriska perspektivet blir speciellt av intresse då vi ämnar undersöka vilka lärdomar utvalda informations- och cybersäkerhetsföretag tagit med sig från den hastiga övergången till distansarbete efter Covid-19, snarare än individens känslomässiga påverkan av det.

Något som därför hamnar utanför ramen av arbetet är de sociala faktorerna relaterat till arbetet som bedrevs, och delvis fortfarande bedrivs hemifrån. Trots att övergången till distansarbete haft stor påverkan på individnivå kommer arbetet behöva avgränsas till det organisatoriska perspektivet i största möjliga utsträckning. Med sociala faktorer menas i detta sammanhang arbetsmiljöfaktorer, hälsa och välmående samt eventuell brist på arbetsmoral. Om även dessa aspekter inkluderats hade risken funnits att fokus skiftats från det vi ämnar studera, det vill säga företagets interna strategier och metoder. Ytterligare en avgränsning som gjorts är kopplat till val av process inom organisationerna i fråga. Fokus har legat på hur organisationer bedriver *proaktivt* riskarbete, före respektive efter Covid-19 samt på de nya hot som uppkommit till följd av övergången till distansarbete. Vi har alltså inte studerat hur företagen hanterar hot och risker *reaktivt* efter att de redan inträffat, utan snarare hur de arbetar för att förebygga dem från första början. De hot och risker som fanns innan pandemin kommer heller inte inkluderas, mer än som jämförelse och referensram för det "nya" respektive "gamla".

De företag vi valt att rikta in oss mot är företag inom informations- och cybersäkerhetsbranchen, eller alternativt uttryckt, företag som arbetar med informations- och cybersäkerhet. Detta då deras roll påverkats otroligt mycket av de gångna åren och individens placering i hemmet snarare än på företagen. Vi är medvetna om att alla företag som övergått till distansarbete genomgått stora förändringar och att de blivit påverkade på olika sätt, men valet att arbeta mot företag och organisationer som arbetar med informations- och cybersäkerhet kändes självklart då de har haft, och fortfarande har, en central roll i det digitaliseringsarbete som genomförts. De lärdomar och slutsatser som studien förhoppningsvis leder fram till kommer i sin tur kunna generaliseras och appliceras på andra företag för att ge guidning och riktlinjer i framtiden.

2. Litteraturgenomgång

2.1. Begreppsdefinition

Social Engineering - Social Engineering, eller uttryckt på svenska; social manipulation är en form av attack där man drar nytta av användarna som använder sig av ett visst system. I boken *Social Engineering: The Science of Human Hacking* definierar författaren begreppet som:

> *"Social engineering is any act that influences a person to take an action that may or may not be in his or her best interest" (Hadnagy, 2018, s.7).*

Utifrån denna breda definition argumenterar Hadnagy (2018) att social engineering inte alltid nödvändigtvis leder till något negativt. I denna studie kommer dock fenomenet studeras

utifrån informations- och cybersäkerhetssynpunkt varpå begreppet kommer användas för att beskriva något oönskat, en form av attack. En mer passande definition för denna studie presenteras av Enisa, European Union Agency For Cybersecurity (u.å.) vilken lyder enligt följande:

> *"Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons" (Enisa, u.å.).*

Malware - Malware är en förkortning på Malicious Software (på svenska skadlig programvara). Begreppet innefattar all typ av invasiv programvara som utvecklats av cyberbrottslingar för att skada eller stjäla programvara, datasystem och datorer (Cisco, u.å.).

Ransomware - Ransomware är en ständigt utvecklande form av *Malware* som är utformad för att kryptera filer på en enhet, vilket i sin tur gör att alla system och filer som är beroende av dem oanvändbara. Skadliga aktörer kräver därefter ut en lösensumma i utbyte mot dekryptering (Cisa, u.å.).

Malicious social media messaging - Denna typ av attack innefattar meddelanden skickade i digital form via sociala medier vilka skickas genom automatiserade informationsbehandlingssystem som kan skada dig eller de system du är ansluten till (Ryan och Kamachi, 2015).

Phishing - Phishing, även känt som *nätfiske*, är en av de vanligaste metoderna hotaktörer (hackare) använder sig av idag. Det är i grunden en form av identitetsstöld där hackaren utger sig för att vara en myndighet, person eller organisation som är känd för mottagaren. Bedragaren skickar då falska meddelanden, exempelvis email, chattmeddelanden eller sms där de uppmanar mottagaren att klicka på länkar (Säkerhetskollen, u.å.). Ett vanligt exempel är att avsändaren lagt till en extra siffra eller bokstav till avsändaradressen vilket mottagaren inte lägger märke till om denne inte är uppmärksam (Polisen, 2020).

Business email compromise (BEC) - denna typ av attack är en av de mest skadliga sett från en finansiell synpunkt. I attackerna drar hotaktörerna nytta av det faktum att många av oss förlitar sig på e-mail för att bedriva såväl professionella som privata affärer. De går till genom att hotaktörer skickar e-mail som kommer från en känd källa med en legitim fråga (FBI, u.å.).

Hacking attacker - Hacking avser de aktiviteter som syftar till att bryta sig in i digitala enheter, såsom smartphones, surfplattor, datorer och till och med hela nätverk (Malwarebytes, u.å.).

Port Shuffling - När NAT öppnar upp en lokal IP-adress blir den offentlig vilket gör den skadlig till cyberattacker. Det port shuffling då gör är att NAT-portarna ändras slumpvis för att det ska bli svårare att ta sig in på IP-adressen. Om portarna ändrar på sig blir det svårare att ta sig in på grund av att de ständigt är i rörelse och svårare att antecipera hur de ser ut.

Detta är ett rörligt målförsvar som gör det svårare för angripare att kontakta systemet på ett tillförlitligt sätt (Berenhaut m.fl., 2014).

2.2. En introduktion till informations- och cybersäkerhet

I och med att denna rapport kommer ta hänsyn till både informations- och cybersäkerhet är det av extrem vikt att vi skildrar dessa två områden och förklarar dem. Informationssäkerhet och cybersäkerhet är två olika områden som dock överlappar med varandra. Informationssäkerhet handlar i största mening om personlig information som är säker, detta innebär alltså att det bara är auktoriserade personer som kan ha tillgång till den informationen (Säkerhetspolisen, 2020). Enligt National Institute of Standards and Technology (NIST) i USA handlar informationssäkerhet om skyddandet av information och de system som tillhör det från att obehöriga individer ska ha åtkomst till det. Anställda på informationssäkerhetsavdelningar i företag analyserar information för att hitta system och andra sätt att skydda data och information och sedan implementera det (Galarita, 2022). Informationssäkerhet jämfört med cybersäkerhet förklaras genom att se på branschen med ett paraply som har all data samlat som sedan flyter ner på mindre nischade delar (Galarita, 2022). På ett sätt är alltså cybersäkerhet en typ av informationssäkerhet men det finns ändå distinkta skillnader mellan de två områdena. Cybersäkerhet innebär att skydda all information och data som är lagrad på nätverk och datasystem. NIST definierar cybersäkerhet som ett arbetssätt av att förebygga skada, återställa samt skydda system och kommunikationstjänster, detta innefattar även den information som finns på dessa system (Galarita, 2022).

De största skillnader mellan informationssäkerhet och cybersäkerhet är att all den information som vill skyddas, lagras och skickas ut finns i cyberrymden. Givet att cybersäkerhet är en del av informationssäkerhet är vissa delar av informationssäkerheten inte inkluderad i cybersäkerhet (Galarita, 2022). Termen informationssäkerhet är övergripande gällande att skapa system och policyer för att skydda fysisk, digital eller intellektuell information samt upprätthålla den informationen. Inom cybersäkerhet ligger fokus på att skydda information och data från attacker som exempelvis ransomware (Galarita, 2022). Givet att det finns skillnader mellan de två områdena finns det även delar som överlappar med varandra då säkerhetsåtgärder liknar varandra väldigt mycket samt att utbildningen i området är väldigt lika. Gällande säkerhetsåtgärderna använder båda sig av integritet, sekretess och tillgänglighet till information för att utveckla samt implementera detta (Säkerhetspolisen, 2020). Integriteten handlar om att det är säkert att informationen inte är manipulerad och att informationen faktiskt stämmer och går att lita på. Sekretessen innefattar att informationen bara är tillgänglig och ändrad av auktoriserade användare. Tillgängligheten av informationen handlar om att den är tillgänglig när den behövs, annars är det poänglöst att ha den (Galarita, 2022). Som ett minsta krav har de som jobbar med informationssäkerhet och cybersäkerhet en utbildning i ett område som relaterar till det och blir därigenom beredd att använda den kunskapen för att kunna förstå sig på komplexa problem inom dessa områden.

2.3. Covid-19 och dess påverkan på organisationer

En central litterär källa i detta arbete är artikeln *A deeper look into cybersecurity issues in the wake of Covid-19: A survey* skriven av Alawida m.fl. (2022). Författarnas artikel bygger på en undersökning gjord från mars 2020 till december 2021 där fokus läggs på vilka och hur många cyberattacker som genomfördes under den tidsperioden. Baserat på svar från företagsledare inom olika organisationer kunde ett samband identifieras mellan pandemins utbrott och ett ökat antal attacker och cyberbrottskampanjer. Studien visade nämligen att från pandemins start ökade antalet cyberattacker nästan exponentiellt allt eftersom tiden gick, där det vissa dagar genomfördes tre-fyra stycken. Vidare nämns att det generellt sett finns ett samband mellan antalet attacker och globala världskriser, och det senaste exemplet förutom Covid-19 var den globala finanskrisen 2008 där hotaktörer även då utnyttjade samhällets sårbarhet. De organisationer som drabbades hårdast av denna kris var dem inom bank och sjukvård där cyberbrottslingar använde sig av phishingattacker via email där dem, genom att dölja skadliga länkar i noggrant designade email, utnyttjade det faktum att människor arbetade hemifrån. Författarna presenterar data för att styrka detta där det framkommer att det i USA vid starten av Covid-19 krisen (under året 2020) genomfördes 1,872 attacker. Året innan pandemin slog till (2019) genomfördes endast 1,108 stycken. Detta innebär en ökning på cirka 760 attacker från ett år till ett annat. Ytterligare information värt att nämna rör attacker relaterat till fysiska brister såsom dokumentläckage och skimming vilka uppges ha drastiskt minskat.

Då artikeln lästes var det dock viktigt att ha i åtanke att författarnas studie genomförts baserat på insamlade data från individer som svarat på en enkät, vilket därför medför en viss brist på trovärdighet. Dock föll valet trots detta på denna artikel på grund av författarnas transparens gällande metod och data vilket dessutom backas upp med en utförlig litteraturstudie av tidigare forskning inom området.

Ytterligare en central artikel i detta arbete som lyfter förhållandet mellan cyberattacker och Covid-19 pandemin är *The Impact of Covid-19 on Cybersecurity* skriven av Ghann m.fl. (2022). Författarna förklarar här påverkan pandemin har haft på samhället i stort och de lyfter dessutom hur den ökade användningen av internet genom distansarbete gjort det om än ännu viktigare med cybersäkerhet och informationsskydd. Detta eftersom arbetsstyrkan förflyttats från det fysiska företaget med välutvecklade brandväggar till att istället jobba hemifrån bakom deras hemmarouter. Detta har resulterat i nya krav på medvetenhet på individnivå medan företagen på organisationsnivå behöver prioritera att utbilda sina anställda för att de ska kunna skydda sig själva. Författarna beskriver följaktligen hur pandemin bringat skräck, förvirring och panik hos befolkningen där världsledare tvingades fatta snabba beslut för att minska spridningen av viruset. Detta öppnade upp för nya möjligheter hos hotaktörerna och det beskrivs i artikeln hur cybersäkerhetshoten förändrades drastiskt till följd där antalet attacker ökade explosionsartat.

Författarna sammanfattar artikeln genom att konstatera att Covid-19 pandemin haft en otroligt stor påverkan på vårt samhälle, framför allt inom cybersäkerhetsbranschen. Det

beskrivs hur det idag saknas den *medvetenhet* som är nödvändig för att handskas med dessa nya hot och att organisationer behöver ta sig an detta genom att utbilda sina medarbetare. Det kan utan tveksamheter konstateras att pandemin förändrat arbetsklimatet där distansarbete kan ses som en del i det "nya normala" vilket medfört ett behov av att förändra tidigare arbetsmetoder och strategier.

En tredje, och minst lika intressant artikel, är *Engaging in cybersecurity proactive behavior: awareness in COVID-19 age* skriven av Alsmadi m.fl. (2022). Författarna i denna artikel tar mer av ett individperspektiv där de ämnar undersöka de anställdas inställning till att engagera sig i, och skapa sig en medvetenhet om, proaktivt cybersäkerhetsarbete. Genom enkäter undersöker författarna varför och hur cyberhotsklimatet förändrats under och efter utbrottet av Covid-19. De beskriver hur hotaktörerna blivit mer sofistikerade och duktiga på att utnyttja brister i de tekniska framstegen företag gör vilket återspeglas i form av virus och skadlig programvara eller till och med nätmobbning och social engineering. Sedan utbrottet av Covid-19 har antalet säkerhetsincidenter blivit allt värre, både till antal och konsekvens och en av dem främsta anledningarna som lyfts i artikeln beror på den mänskliga faktorn. I dagens samhälle räcker det inte att endast fokusera på tekniska medel för att hålla företagets information säker, utan det krävs dessutom en medvetenhet från individerna som använder denna teknik gällande hur man proaktivt förebygger attacker redan innan de inträffat. De sektorerna där ökningen av attacker blev som mest påtaglig är de som är som mest känsliga för intrång, nämligen hälsosektorn, webmail och Software-as-a-Service (SaaS). Dock har även individer påverkats markant, speciellt de som inte tidigare besatt den rätta kunskapen om cyberbrottslighet och de som i allmänhet inte var vana vid att arbeta över internet. Detta resulterade till en ytterligare ångest och oro, utöver den som redan upplevdes inför pandemin i sin helhet, då individen behövde arbeta på sätt som denne inte var van vid sedan innan. Cyberbrottslingar drog nytta av detta där dem genom att utge sig för att representera hälso- och sjukvården, offentliga myndigheter och stödplattformar kunde lansera olika typer av attacker såsom malware, ransomware, malicious social media messaging, business email compromise och mycket mer.

Nivån av medvetenhet hos de anställda beskrivs som en avgörande faktor när det kommer till informationssäkerhet (Alsmadi m.fl., 2022). Ju mer kunskap och färdigheter användaren får om de cybersäkerhetshot som finns, desto högre nivå av medvetenhet och åtgärder vidtas för att förebygga och eliminera dessa potentiella risker. En av åtgärderna som presenteras i artikeln för att åtgärda detta är införandet och implementationen av 'cyber security awareness programs' tillsammans med deras infrastruktur för säkerhet. Dessa program skulle syfta till att öka cybersäkerhetskunskapen genom att först identifiera de faktorer som påverkar användarens medvetenhet om de senaste cyberhoten, speciellt de som uppstod under pandemin. Därefter undersöks användarens attityd gällande sitt eget beteende när det kommer till att skydda sin egen information från potentiella cyberattacker.

Dessa tre artiklar har några saker gemensamt. För det första att antalet cyberattacker och cyberbrottskampanjer fick ett explosionsartat uppsving till följd av övergången till distansarbete där hotaktörer utnyttjade den skräck, oro och förvirring som genomsyrade

individer och samhället i helhet. För det andra pekas den mänskliga faktorn ut som en av de främsta anledningarna till detta där brist på medvetenhet och proaktiv riskhantering på ett individplan antas bidragit till denna ökning.

2.4. Risk och riskhantering

I artikeln av Huang m.fl. (2020) vilken lyftes i introduktionsdelen beskrevs risk som objektiv kvantitet vilken används för att beskriva nivån av skada på ett specifikt system. Denna artikel fungerar som stöd inom diskussionen av vad risk faktiskt innebär, men värt att nämna är att det idag inte finns någon gemensam definition av begreppet. I denna studie kommer vi dock främst utgå från boken *Fundamentals of Risk Management- Understanding, evaluating and implementing effective risk management* skriven av Paul Hopkin (2018) där författaren tar upp grunderna av risk och riskhantering. I denna bok presenteras ytterligare en riskdefinition tagen från The Oxford English Dictionary; *'[…]chance or possibility of danger, loss injury or other adverse consequences'* (Hopkin, 2018, s.15). Denna definition utgår från att risk alltid medför något negativt, men enligt Hopkins (2018) är inte detta helt korrekt. Han förklarar hur risker kan resultera i något dåligt eller oönskat, men det kan också leda till något bra eller oväntat. På dagens globala marknad tar företag ständigt risker, de testar nya arbetssätt för att reducera kostnader och implementerar digitaliseringsåtgärder såsom AI eller maskininlärningsalgoritmer för att öka sin effektivitet. Det genomförs förändringar för att det eventuellt kan medföra något bättre i slutändan, men det kan också få negativa konsekvenser för företaget. Varför företagen ändå väljer att genomföra förändringarna är för att det faller inom ramen för deras *risk appetite* eller *risk capacity.* Dessa två begrepp beskriver nivån av risk ett företag kan tänkas acceptera när det kommer till individuella respektive organisatoriska risker (AngelOne, 2022). För att bli medveten om, och kunna hantera dessa risker behöver företagen alltså en redan utarbetad riskhanteringsstrategi. I boken presenterar Hopkins (2018) en summerad lista på de åtgärder som företag då kan ta till vilka kan bidra till att minska risken för att exponeras för oönskade eller oväntade händelser som faller utanför ramen av företagets acceptans. Då denna lyfts refererar författaren till den globala finanskrisen, men han nämner samtidigt att det ofta saknas ett utarbetat ramverk för riskhantering. Listan presenteras enligt följande;

- För det första bör det finnas gemensamma, processer, terminologi och praxis för att hantera alla sorters risker
- För det andra är det rent avgörande att risktoleransen är fullt förstådd, kommunicerad och övervakad genom hela organisationen
- För det tredje bör riskhanteringspraxis vara invävd i alla de viktigaste arbetsprocesserna och besluten
- Och, för det fjärde, bör ledningen inom företaget ta riskrelaterade beslut med hjälp av riskinformation av hög kvalitet (Hopkin, 2018, s.8).

Givet dessa punkter kan konstateras att det krävs en utarbetad strategi, praxis och ramverk inom företag i dagens dynamiska och tekniska värld för att inte överexponeras för risk(er).

2.5. Proaktivt cybersäkerhetsarbete - vad är det?

Proaktiv cybersäkerhet innebär att agera på ett hot eller en risk, redan innan den uppstått snarare än vänta och reaktivt ta itu med den (Elgan, 2021). Givet att ett företag använder sig av proaktivt cybersäkerhetsarbete innebär det en ansträngning att identifiera, utveckla och förbättra det interna systemet för att minska potentiella hot och svaga punkter innan angripare kan komma åt dem (Rajan, 2022). Rajan (2022) presenterar i sin artikel fyra exempel på proaktiva cybersäkerhetsåtgärder: jaga hot, personalutbildning, etisk hackning samt proaktiv övervakning av nätverk och slutpunkt.

Åtgärden *jaga hot* innebär att företaget försöker förstå sig på hur cyberkriminella tänker och därefter lista ut vilka delar av företagets system som inte är säkra för en cyberattack (Rajan, 2022). Genom att försöka simulera en cyberattack kan företaget analysera de svaga punkterna i systemet och vad som gör dem sårbara och sedan efter att de har identifierats förbättras dessa för att göra det svårare för cyberkriminella att komma åt den informationen. *Personalutbildning* handlar om att utbilda och lära de anställda inom företaget vad de ska och inte ska göra (Rajan, 2022). Författaren förklarar att runt 90% av alla cyberattacker inträffar på grund av att en människa har gjort fel. Därför är det av extrem vikt att alla anställda i ett företag bör få en träning i hur de ska hantera sina personliga uppgifter. *Etisk hacking* innebär att ett företag anställs för att faktiskt utföra en cyberattack för att hjälpa företag (Rajan, 2022). Detta görs för att se hur en cyberattack egentligen går till och vilka delar av ett företags interna system som påverkas av det. Etiska hackare hjälper ett företag att identifiera systemets svaga punkter genom att avslöja dem. Detta beskrivs dessutom i artikeln av Elgan (2021) där han beskriver att etiska hackare använder sig av samma metoder och verktyg som hotaktörerna. *Proaktiv övervakning av nätverk och slutpunkt* innebär att hela tiden övervaka systemet (Rajan, 2022). Genom att implementera ett system som gör just detta och analysera om det är någonting i systemet som inte stämmer och sedan identifierar vilka olika problem som kan komma att bli värre om ingen åtgärd tas.

Att ett företag arbetar proaktivt innebär att de förutser vilka problem, förändringar samt behov som behövs för framtiden. Gällande proaktivt cybersäkerhetsarbete handlar det om exakt samma sak, alltså allt arbete som görs innan ett företag blir utsatt av en cyberattack (Threat Intelligence, 2023). Ett proaktivt arbete till handlar om att agera på ett problem innan det uppstår istället för att agera när problemet har uppstått. Threat intelligence lyfter vidare andra sätt att arbeta med proaktiv cybersäkerhet och dessa är: att omöjliggöra säkerhets- och informationsbrott, att identifiera olika svagheter i nätverket och åtgärda dessa samt utvärdera svagheter och styrkor inom säkerheten överlag (Threat Intelligence, 2023).

Dagens metoder för att motverka cyberattacker besitter vissa brister då många företag i nuläget arbetar reaktivt. I och med detta har cybersäkerhetsbranschen gått mot ett annat perspektiv gällande säkerheten vilket är drivet av intelligens och kallas för “Proaktiv Cyberhot Intelligens” (Ericsson m.fl.., 2021). De reaktiva metoderna som organisationer använder sig av idag för att hantera cyberattacker misslyckas ofta med att fungera effektivt, och anledningen till detta är att huvudfokus ligger på företaget som försvarar cyberattacken.

Genom att negligera hotaktören leder det till att företaget missar att bemöta hälften av hotet (Ericsson m.fl., 2021). Givet detta har cybersäkerhetsbranschen inlett ett bemötande mot ett mer intelligensdrivet säkerhetsarbete, vilket innebär att informera vilka system som oftast påverkas av cyberattacker och hur hotaktörer går tillväga. Genom att anamma detta nya arbetssätt leder det till att företag enklare kan förutse och hindra en cyberattack eller cyberkampanj (Ericsson m.fl., 2021).

I artikeln "*Securing Control and Data Planes From Reconnaissance Attacks Using Distributed Shadow Controllers, Reactive and Proactive Approaches*" skriven av Hyder och Ismail (2021) lyfts många olika sorter av proaktiv cybersäkerhet och det argumenteras med fakta baserad på forskning som tyder på att proaktiv cybersäkerhet är betydligt mer effektiv än reaktiv cybersäkerhet. En metod för proaktiv cybersäkerhet kallas för Port Shuffling och innebär att NAT (Network Address Translation) ändras konstant för att brandväggen inte ska vara lika lätt att bryta sig in i (Hyder och Ismail, 2021). I artikeln beskriver författarna att genom att använda sig av Port Shuffling på ett effektivt sätt minskar risken att en angripare får kontakt med systemet till endast 37%, och om angriparen hade fått kontakt med systemet hade chansen att lyckas med attacken bara ligga på 67%. Detta är betydligt mindre än om ett reaktivt cybersäkerhetsarbete hade anammats. Detta är ett konkret exempel på hur proaktivt cybersäkerhetsarbete är mer fördelaktigt än reaktivt då det gör det svårare för angriparen att faktiskt lyckas med en attack.

2.6 Zero Trust-modellen

Zero Trust-modellen handlar om att de interna och externa hoten alltid är närvarande i nätverket under all tid, och på grund av det måste nätverket alltid vara redo att försvara sig mot hoten (Cheng m.fl., 2023). Det handlar i stort sett om kontroll, hur man ska se till att de som har tillgång till vissa system har den tillgången. I Zero Trust är all trafik som går genom nätverket opålitligt, den måste verifieras vilket modellen i stort sett handlar om. Lita inte på, *verifiera*. De tre delarna av Zero Trust är:

1. Se till att alla resurser är säkra oberoende på plats, anta alltid att all trafik är farlig tills den är verifierad, säkrad och inspekterad (NIST, 2013).
2. Implementera en förmånsstrategi och förstärk kontrollen på vem som har tillgång till systemen. Genom att göra det minskar den mänskliga frestelsen att komma åt resurser och system som de egentligen inte har tillgång till (NIST, 2013).
3. Genom att inspektera och logga all trafik som går genom system och nätverk blir det enklare att analysera om det är hot eller inte. (NIST, 2013).

Man litar inte på människorna som vill ha tillgång till systemet utan man litar på verifieringen som görs genom lösenord, koder eller andra sätt att verifiera sig på. I Zero Trust ger någon sin identitet och sen får den personen tillgång till det den vill ha om den har tillgång till det, baserat på analysen och inspektionen. Vidare har de anställda i företag begränsad tillgång till just de resurserna som de behöver för att uträtta sitt jobb. Istället för att lita på att människorna ska göra rätt sak verifieras detta istället (NIST, 2013).

Figur 1. Zero Trust- modellen (Bhingarkar, 2021)

3. Metod

Då val av metod skulle göras föll valet relativt snabbt på en kvalitativ studie. Detta eftersom vi med problemformuleringen bland annat ville ta reda på vilka lärdomar företag inom cybersäkerhetsbranschen fått med sig efter det snabba digitaliseringsarbete som följde av Covid-19. Målet med studien var att få en bättre inblick i de konkreta interna- och externa hot som finns inom cybersäkerhet samt hur företag på ett proaktivt sätt kan och borde hantera dessa hot. Genom att använda sig av semistrukturerade intervjuer ansåg vi att man på bästa sätt kan få svar på dessa frågor. Om valet istället skulle fallit på insamling av kvantitativa data såsom numeriska värden och siffror hade studien fått ett annat utfall än det vi ämnade att uppnå. Som guide i arbetet användes *Handbok i kvalitativa metoder* skriven av Ahrne och Svensson (2015).

Att valet föll på en kvalitativ datainsamlingsmetod förklaras ytterligare av påståendet av Rienecker och Jörgensen (2018) där författarna beskriver att problemformuleringen styr val av metod. Vår frågeställning som bygger på verkliga händelser och upplevelser var alltså det som avgjorde hur vi skulle samla in vår data. Då vi dock var medvetna om att intervjuer kan präglas av en viss bias och subjektivitet tog vi dessutom beslutet att göra grundlig litteraturgenomgång för att ge en bakgrund och validitet i studien. Givet detta kan studien utifrån Oates (2006) beskrivas som en interpretivistisk ansats med positivistiska inslag. Detta givet att val av metod föll på intervjustudie vilken kan ses som ett subjektivt tillvägagångssätt där respondenternas åsikter och upplevelser står till grund för analysen, vilket går hand i hand med denna ansats. Dock genomfördes dessa intervjuer utifrån vad Oates (2006) beskriver som en semistrukturerad struktur vilken främjar objektivitet då respondenterna hade full möjlighet att berätta saker som inte uttryckligen frågats efter. Att samla in kvalitativa data

gjorde det möjligt att dra mer komplexa tolkningar vilket gav mer djup i analysen och vidare främjade det det resultat och den slutsats vi med studien ämnade uppnå.

Dessutom var det av största vikt att ge *validitet* till arbetet. Genom att vara transparenta med hur data samlats in och att tydliggöra forskningsprocessen samt kritiskt analysera och diskutera samtliga steg uppnådde vi detta. En ökad tillförlitlighet genererades eftersom flera olika källor ställdes mot varandra vilket minskade risken för att felaktiga slutsatser dras. Givet att vi använde metodkombination som forskningsstrategi var det fördelaktigt då denna strategi testade olika källor mot varandra för att öka trovärdighet och validitet i studien (Denscombe, 2018).

3.1 Litteraturgenomgång

För att samla in data och information om ämnet gjordes i början av studien en genomgående avsökning av relevant litteratur. Detta gjordes för att få en bakgrund inom området och den problematik som vi valt att lägga fokus på. Syftet var att få en inblick i vad tidigare forskare studerat inom ämnet och för att kunna identifiera de eventuella kunskapsluckor som denna studie skulle kunna fylla. Vidare ansågs det av yttersta vikt att få en djupgående förståelse för ämnet innan tankar blev till skrift. Redan innan studiens start hade vi som forskare en någorlunda förståelse för cybersäkerhet, riskhantering och digitaliseringsarbetet kopplat till Covid-19 men vi ansåg att denna kunskap behöver stärkas med hjälp av tidigare forskning. Genom att genomföra en omfattande litteraturgenomgång av ämnet skapades en överblick över tidigare forskning och luckor identifierades inom det valda området. Eftersom den huvudsakliga forskningsmetoden i arbetet var *intervjuer* vilket är en kvalitativ och subjektiv datainsamlingsmetod ansågs det vara viktigt att kunna jämföra det som sägs i intervjuerna med tidigare forskning för att stärka validitet och trovärdighet.

Denna litteraturgenomgång fungerar vidare som en form av teoretisk bakgrund där relevanta och centrala begrepp belyses för att ge läsaren en ingående förståelse för vad rapportens fokus är. Dessa begrepp, vilka som sagt är tagna från tidigare forskning, jämfördes sedan med intervjuerna i analysen för att finna likheter och skillnader. Detta arbetssätt är med andra ord likadant som om en konkret teori skulle använts, varpå vi valde att endast fokusera på tidigare forskning snarare än konkreta teorier.

När litteraturgenomgången genomfördes var de primära databaserna *Google Scholar* samt Malmö Universitets databas *Libsearch.* Båda dessa ansågs erbjuda ett brett urval artiklar och rapporter av hög kvalitet. För att säkerställa källornas relevans valde vi endast att fokusera på artiklar skrivna mellan 2018 och nutid. Att valet föll på dessa årtal beror på studiens fokus och problematisering vilken bygger på utbrottet av Covid-19 pandemin vilken inträffade vinter/vår 2019/2020. 2018 togs med på grund av jämförbarheten, det vill säga hur riskhanteringen hanterades inom företagen innan respektive efter pandemin. Under urvalet fokuserade vi främst på abstract och nyckelord, detta då både Libsearch och Google Scholar erbjöd ett brett utbud. Genom att leta efter nyckelord som framkommer tillsammans i artiklarna såsom *cybersecurity, informationsecurity, proactive risk management, risk*

management och *Covid-19* lyckades vi hitta relevanta källor som kommit att bli centrala i studien.

3.2 Datainsamling

3.2.1 Datainsamlingsmetod

I rapporten använde vi *semistrukturerade intervjuer* vilket innebär att frågorna som ställdes till respondenterna inte nödvändigtvis var i samma ordning för att underlätta en röd tråd i intervjun (Oates, 2006). Dessa skedde digitalt över Teams eller Zoom. Semistrukturerad intervju innebär att det finns ett antal frågor som kommer att ställas till respondenterna, men det kunde även uppstå fler frågor om ämnet tar en annan sväng. Detta skapade en mer omfattande intervju och ett djup i svaren då respondenterna fick möjligheten att lyfta egna aspekter som kan hjälpa forskaren att få andra tankar om ämnet (Oates, 2006).

I och med att syftet med arbetet är att ta reda på hur företag bör arbeta med proaktivt cybersäkerhetsarbete var det av extrem vikt att ta reda på hur företag faktiskt jobbar med cybersäkerhet. Detta då alla företag gör detta på olika sätt och därför kunde respondenternas svar variera. På grund av detta fanns det vissa aspekter som lyfts i vissa intervjuer som inte lyfts i andra. Om valet istället fallit på den strukturerade intervjun hade dessa tankar förbisetts och därmed blivit till ett hinder i arbetet. Strukturerad intervju innebär att exakt samma frågor ställs till varje respondent och det kan inte uppkomma fler frågor under intervjun vilket då leder till att flexibiliteten som kan behövas inte blir möjlig (Oates, 2006). Semistrukturerad och icke-strukturerad intervju tillåter respondenten att tala fritt om deras tankar och fokus ligger på att ta reda på information och inte att kolla att fakta stämmer (Oates, 2006). Dock innebär icke-strukturerade intervjuer att ett ämne läggs fram till respondenterna utan frågor och de får svara med sina tankar om ämnet (Oates, 2006).

3.2.2 Urval

Enligt Ahrne & Svensson (2015) är urval en vital del gällande en kvalitativ forskning då det handlar om att välja ut relevanta personer som ska beaktas för att kunna få svar på frågeställningen som en rapport har. Det är av extrem vikt att rätt typ av urvalsmetod används för att få den information som behövs av intervjuerna. Vidare måste forskaren vara kritisk till det urval som har gjorts och kunna argumentera för det för att skapa en transparens i rapporten, detta för att ge möjlighet till att kunna använda rapporten på ett generaliserat plan (Ahrne & Svensson, 2015). Med detta finns det olika metoder för att komma fram till urvalet och det som denna rapport använde sig av var en typ av *kritiskt urval*. Kritiskt urval handlar om att forskaren kritiskt analyserar vilka personer som kan användas som respondenter baserat på deras kunskap och egenskaper för att komma fram till om en potentiell respondent besitter den kunskap som är relevant för rapporten (Ahrne & Svensson, 2015). Denna metod valdes då den anses vara den mest fördelaktiga för rapporten gällande att hitta personer som kan ge mer djupa tankar och åsikter om riskhantering och cybersäkerhet. För att få en mångsidig bild av branschen tog vi kontakt med en bredd av anställda, från VD:s till vanliga medarbetare. Dock är majoriteten av respondenterna chefer av olika slag, detta på grund av

att vi vid starten av arbetet trodde att dessa individer skulle ha en bättre förståelse för den övergripande riskhanteringen på företaget och därav kunde ge mer utförliga svar.

Att intervjua flera personer innebar att vi fick olika perspektiv i varje intervju vilket i sin tur mynnade ut i en större förståelse för hur företag arbetar med cybersäkerhet, och det belyser vidare hur de bör arbeta med proaktiv cybersäkerhet. Nedan finns en tabell med respondenterna, deras företagsroll/ansvarsområde och typ av företag de arbetar på samt om de var aktiva på det nuvarande företaget under Covid-19. Valet att lägga fokus på just dessa faktorer berodde på studiens fokusområde. Roll och ansvarsområde ansågs relevanta att ha med för att belysa respondenternas betydelse och relevans i rapporten, och likaså om de arbetade på företaget under pandemin eftersom en del av arbetet handlar om att studera lärdomarna av Covid-19. De respondenter som inte jobbade på det nuvarande företagen vid pandemins utbrott började på företaget relativt nära efter, vilket gör att de ändå har påverkats av pandemins effekter. Därav kunde de bidra med relevant information för att uppfylla denna rapports syfte. Att personliga faktorer såsom ålder och kön förbises beror på rapportens fokusområde, vilket som tidigare nämnts ligger på den organisatoriska aspekten snarare än den individuella, vilket gör att dessa faktorer faller utanför ramen av arbetet.

Tabell 1. Sammanställning av respondenter

Respondent	Roll	Ansvarsområde	Arbetade på företaget under Covid-19
1	Executive Vice President	Ansvarig för företagets säkerhetserbjudanden	JA
2	Sales Manager Cybersecurity	Säljchef och Regionansvarig	JA
3	Director of Operations	Hjälper företag som utsatts för cyberattacker	JA
4	Identity and Access Manager Advisor	Rådgivare på Informationssäkerhet med huvudvikt på identity and access management	NEJ
5	Business Solution Director	Ansvarar för affärstjänster (moln och Saas)	JA
6	Consultant Manager	Fokus på informationssäkerhet	NEJ
7	Risk Manager	Att holistiskt jobba med bolagsrisker på företaget	NEJ
8	VD & grundare	Ansvar för hela företaget	JA
9	CISO	Informationssäkerhetskonsult	NEJ

3.2.3 Etiskt förhållningssätt

Etik är en viktig del i forskningen och att ha ett etiskt förhållningssätt och ett tydligt etiskt ramverk är väsentligt för att skydda såväl deltagare som forskare. I boken *Research Information Systems and Computing* skriven av Briony J Oates (2006) erbjuds ett sådant ramverk vilket ligger som grund för studien. Författaren beskriver där att ett tydligt etiskt ramverk säkerställer forskningens kvalitet och tillförlitlighet vilket är av största vikt i denna studie. Genom att följa etiska riktlinjer säkerställde vi som forskare att data och det resultat som genereras är tillförlitligt och av hög kvalitet samt att forskningen genomförs på ett

objektivt och rättvist sätt. Eftersom vår studie främst bygger på insamlad data från intervjuer behöver respondenternas rättigheter och integritet beaktas. Oates (2006) beskriver att etiska riktlinjer syftar till att skydda de forskningsobjekt som deltar i forskningen från obehag och skada och detta görs bland annat genom att säkerställa att respondenterna gett samtycke till att delta. Dessutom har vi som forskare varit öppna och transparenta med vad för typ av studie som genomförs samt hur den data som samlas in ska användas.

Detta går dessutom att koppla till Robert K. Mertons fyra principer *Communism, Universalism, Disinterestedness* och *Organized Scepticism* vilka går under namnet CUDOS-kraven. Dessa utgör enligt Merton ett "moral consensus" för vetenskapen (Orre, 2023). *Communism* står för en form av öppenhet där forskningsresultaten ska göras tillgängliga för allmänheten, vilket är fallet med studien. Vi som forskare var medvetna om detta och tydliggjorde detta för våra intervjuobjekt. Nästa bokstav, U, står för *Universalism* vilket innebär att studien inte ska bedömas utifrån andra kriterier än rent vetenskapliga. Detta faller utanför ramen av studien då det inte var vi själva som utförde bedömningen, men det kan däremot på sätt och vis appliceras på intervjuerna där vi som forskare var noggranna med att inte diskriminera eller döma respondenterna. D står för *Disinterestedness* vilket innebär att forskaren inte ska ha andra motiv än rent vetenskapliga. Målet med studien är att undersöka och analysera riskhanteringen inom cybersäkerhetsbranschen och inget annat vilket medför att även detta krav uppfylls. Det sista kravet, *Organized Scepticism,* innebär att forskaren ständigt ska granska och ifrågasätta den data som genereras och att vänta med att ge en bedömning, i detta fall ett resultat, innan det finns tillräcklig grund att stå på. Vi som forskare var källkritiska genom studien och använde oss endast av välkända källor. I de fall där andra källor än vetenskapliga rapporter, tidskrifter och böcker användes verifierade vi källans trovärdighet genom att ställa källan mot andra. Dessutom var vi, då intervjuerna genomfördes, skeptiska och källkritiska till både det som sägs, men också till våra egna bearbetningar av materialet. För att på bästa sätt reducera den bias som kan komma att prägla våra tolkningar kodade vi intervjuerna separat innan de sammanställs i empirin.

Oates (2006) presenterar vidare fem rättigheter som bör följas vid genomförandet av intervjuer vilka är; *Rätten att inte delta, Rätten att dra sig ur, Rätten att ge informerat samtycke, Rätten till anonymitet* samt *Rätten till sekretess*. Vi var noggranna med att följa alla dessa rättigheter. För det första var vi tydliga med varför studien görs och hur data används. Den information respondenterna lämnar ut användes endast av oss forskare, de presenteras alltså inte i rapporten i sig utan låg endast som grund till analysen vilket garanterade att sekretess uppfylls. För det andra bad vi respondenterna, redan vid början av intervjun, att uttryckligen ge oss samtycke till dess medverkan. Dessutom tydliggjorde vi att de kan välja att dra sig ur, antingen redan innan intervjun eller om de vill göra det vid ett senare tillfälle. Respondenterna informerades om att deras namn inte nämns då det gäller full anonymitet.

Genom att vi följde CUDOS-kraven och använde boken av Oates (2006) säkerställde vi att forskningen genomfördes på ett etiskt sätt. Ingen av den data som samlades in manipulerades och det resultat som rapporten mynnade ut i bygger endast på objektiv analys av denna data. Ytterligare en viktig del som lyfts av Oates rör respekt för människors rättigheter där man

som forskare bör vara medveten om, och ta hänsyn till de ekonomiska, sociala och politiska faktorer som kan komma att påverka forskningen och resultatet. Vi var här medvetna om att intervjuobjekten kommer från olika bakgrunder och att de haft olika förutsättningar i deras arbete, speciellt eftersom vissa av dem har ledarpositioner inom deras företag och andra inte. Sammanfattningsvis följde vi dessa etiska riktlinjer och säkrade arbetets trovärdighet och forskningsobjektens integritet.

3.3 Databearbetning och analys

3.3.1 Transkribering

Efter att intervjuerna genomfördes transkriberades de för att tydliggöra vilka svar som respondenterna gav. Detta gjordes genom att koda svaren i olika teman och subteman för att förenkla samt tydliggöra vilka ämnen de olika svaren lyfter. Genom att transkribera kommer forskaren ännu närmre sin data genom att ta den från tal till text vilket leder till en ytterligare upprepning av informationen (Denscombe, 2018). Enligt Denscombe (2018) finns det tre olika sätt att transkribera, dessa tre sätt är konversational transkribering, ordagrann transkribering samt redigerad transkribering. Konversational transkribering innebär att hänsyn tas till hur respondenten svarade på en fråga, till exempel vilken tonart som personen hade när den svarade på frågan. Ordagrant transkribering innebär att varenda ljud som görs i intervjun även finns med i texten, till exempel pauser eller om respondenten säger “eh…” och annat. Redigerad transkribering innebär att man inte skriver ner alla ljud samt pauser som uppstår under intervjun. Denna rapport använde sig av *redigerad transkribering* då betoning samt bakgrundsljud inte var några aspekter vi forskare ansåg var viktiga för syftet med rapporten. Transkriberingen gjordes omedelbart efter att varje intervju genomförts. Detta för att säkerställa att informationen och våra egna tankar nyligen är dokumenterade, samtidigt som det gav en ökad precision gällande vilken respondent som uttrycker vad. Denna noggrannhet var särskilt viktig då samtalsämnen och frågor till viss del varierade mellan intervjuerna varpå individuell och omedelbar bearbetning och analys blev av största vikt.

3.3.2 Dataanalys

Dataanalys är en process som handlar om att samla, bearbeta samt tolka olika data och information för att kunna stödja frågeställningar inom forskning samt ligga till grund för slutsatserna i en rapport eller artikeln (Denscombe, 2018). Författaren lyfter att det finns flera steg i processen av dataanalys. Dessa fyra är: datainsamling, dataförberedelse, dataanalys och slutsatser. Datainsamlingen handlar om att samla på sig den data som kommer vara väsentlig för rapporten. Detta kan göras på olika sätt men i följande rapport gjordes det främst genom intervjuer. Dataförberedelse handlar om bearbetningen av datan och informationen samt att göra datan läsbar för användning och för att det ska bli lätt att kunna förstå den i texten. Själva dataanalysen innebar att framställa och använda sig av de metoder som är centrala och passande för att kunna analysera den data och information som framkommit i tidigare steg. Slutsatser innefattar att från resultatet som dataanalysen bidragit med förklara hur detta relaterar till forskningsfrågorna och syftet med rapporten.

I och med att det var intervjuer som genomfördes för att framställa datan i denna rapport är det en kvalitativ dataanalys som är central för arbetet. För att ta reda hur vi på bästa sätt skulle använda oss av kvalitativa metoder vände vi oss till Ahrne & Svensson (2015). Författarna beskriver olika sätt att minska, argumentera samt dela upp den datan som genererats av det kvalitativa arbetssättet. Dessa var de olika stegen för att analysera kvalitativ data på ett sätt som underlättar för både forskaren samt läsaren för att göra det enkelt att tolka och förstå. Det första steget är att dela upp datan i mindre koder för att de olika svaren av olika respondenter hamnar inom samma tema. Det blir därför enklare att se vilken data som är relevant för vilken forskningsfråga. Nästa steg enligt Ahrne & Svensson (2015) är att minska insamlingen redan innan den samlas in. Detta för att undvika att samla in större mängd data än vad som egentligen behövs. På grund av detta var samtliga av de frågor som ställdes till respondenterna relevanta för arbetet. Nästa steg är att argumentera för varför datan är relevant och här använde rapporten sig av empirin i samband med datan från intervjuerna och litteraturgenomgången för att skapa en relevans mellan dem. Här argumenteras det för varför datan är relevant för rapportens frågeställningar och syfte (Ahrne & Svensson, 2015). Slutligen argumenterade vi för våra slutsatser samt försvarade dem och dess relevans. Genom att koppla de funna resultaten till tidigare forskning inom området gav det en grund för slutsatserna och uteslöt att det var rena spekulationer. Sammantaget är det en analysmetod för att öka trovärdigheten och validiteten i studien och som av Denscombe (2018) beskrivs som kodning.

Ytterligare en analysmetod som användes var tematisk analys, vilket innebar att identifiera olika teman och mönster i de olika intervjuerna för att kunna dela upp respondenternas svar. Detta för att enkelt kunna se vilka områden som lyfts i de olika intervjuerna och om det fanns genomgående likheter mellan dem. Denna analysmetod underlättar för att kunna uppfatta likheter i ämnena som lyfts för att sedan kunna analysera dessa och implementera dem i rapporten.

3.4 Metoddiskussion

Att valet föll på att främst använda sig av en kvalitativ datainsamlingsmetod berodde på det djup och den komplexitet denna strategi möjliggör i analysen. Att genomföra intervjuer innebar att vi fick direktkontakt med företag inom en vald bransch vilket medförde att verkliga händelser och upplevelser kunde studeras på ett, enligt oss, mer intressant plan. Vi var dock medvetna om att valet av metod medförde såväl möjligheter som begränsningar. Om valet istället fallit på en kvantitativ studie, exempelvis enkäter, hade utfallet blivit helt annat. Detta hade medfört en mer objektiv syn på fenomenet då fokus istället hade riktats mot numeriska data. Enkäter bygger på frågor som ställs med redan tidigare angivna svarsalternativ vilket resulterar i att respondentens möjligheter att ange ytterligare information minimeras. Vi valde därför istället att använda oss av semistrukturerade intervjuer med öppna frågor där intervjuobjekten fick möjligheten att nämna information som inte tidigare var planerad. Denna data kan vid intervjutillfället upplevas som intressant och givande för studien i helhet och som förbisetts vid en enkätundersökning.

Vidare kan argumenteras för att vi genom vår kvalitativa datainsamlingsmetod arbetade efter vad Rienecker och Jörgensen (2018) namngett som *interpretivism*. Inom denna ansats antar forskaren att det finns en subjektiv dimension i vår uppfattning av verkligheten där författarna förklarar att man inom denna ansats vill förstå sociala fenomen på ett djupare sätt. Dock har vi, som tidigare nämnts, dessutom genomfört en litteraturgenomgång för att få en grund att stå på i arbetet. Vi har där tagit del av tidigare rapporter, artiklar och forskning inom området för att kunna jämföra och dra slutsatser mellan detta och den data som samlas in i intervjuerna för att hitta samband. Då denna genomfördes har vi som forskare försökt vara objektiva då vi inte utgått från några av våra enskilda åsikter eller tankar vid urvalet av litteraturen.

Om vi istället valt att följa den *positivistiska* ansatsen hade vi som forskare istället utgått från objektiva mätningar, observationer och verifierbar fakta för att försöka eliminera subjektivitet och bias (Rienecker och Jörgensen, 2018). I denna studie vill vi förstå det digitala samhälle företag inom cybersäkerhetsbranschen verkar inom och hur Covid-19 påverkade arbetsklimatet i form av riskhantering och informationssäkerhet. På grund av detta ansågs det mer relevant och intressant för studiens utfall att istället använda oss av en kvalitativ forskningsmetod än av kvantitativa, numeriska värden och statistik. Dock var vi medvetna om att komplettering med kvantitativa data kunnat bidra med positiva inslag i studien men med tanke på tidsbegränsningen för studien i helhet (10 veckor) samt studiens omfattning valdes detta bort.

Samtidigt som intervjuer erbjuder en effektiv och bred datainsamlingsmetod som kan användas för att få ett djup och en komplexitet i rapporten, finns det en del nackdelar. Det var exempelvis väldigt tidskrävande. Förutom att planera och genomföra intervjuerna behövde dessa sedan transkriberas och analyseras. Kontroll och analys av texten var tidskrävande och krävde många timmars arbete. Ytterligare ett krav för att få det att fungera var att respondenterna hade, eller tog sig tid för att genomföra intervjuerna. Då vi skickade ut mail och bad om 1-1,5 timmes intervjuer svarade många att de endast hade 30 minuter, eller i bästa fall en timme att avsätta. En annan nackdel, eller kanske snarare svårighet, med intervjuformatet var formuleringen av frågor. Vi hade redan innan en grundläggande förståelse för ämnet men då vi skulle prata med experter inom området krävdes en djupare kunskap för att kunna ställa de rätta frågorna som dessutom genererar relevant data som kan bidra till att fylla syftet och besvara frågeställningen. Detta är av yttersta vikt då hela arbetet och dess utfall bygger på den data som samlas in från dessa.

4. Empiri

Empirin bygger på insamlade data från de intervjuer som genomförts vilka transkriberades och kodades för att kunna utläsa likheter och olikheter mellan de insamlade svaren. Majoriteten av de frågor som ställts, vilka finns under *Bilaga A*, bygger på data från litteraturgenomgången där målet var att bekräfta eller ifrågasätta den tidigare forskningen inom området för att besvara frågeställningen. Rubrikerna nedan är baserade på dessa frågor varpå svaren anges och summeras därefter under vardera rubrik. Dock insåg vi redan efter

andra intervjun att samtliga frågor inte hann ställas innan den avsatta tiden för intervjun var över, och därav valdes ett antal frågor ut som ansågs vara centrala för studiens syfte. Det var ett krav att dessa frågor skulle ställas till samtliga respondenter, medan de övriga frågorna ställdes om det fanns tid och om samtalet rörde sig i en viss riktning. Vi insåg dessutom att vi lyckades uppnå ett bättre djup i svaren, och därmed i analysen, om vi fokuserade på att ställa följdfrågor snarare än att strikt hålla oss till de förutbestämda frågorna som fanns i frågeformuläret.

De respondenter som medverkade återfinns i *tabell 1* under rubrik *3.2.2 Urval*. De som valdes ut och kontaktades för intervjun arbetar inom ett ganska brett spektrum men samtliga arbetar med någon form av intern riskhantering, antingen i form av att de ansvarar för anställda och deras exponering för olika risker eller genom att de ansvarar för hela företagets riskhanteringsstrategi. Något som väldigt snabbt märktes var just känsligheten gällande ämnet. Risk, och kanske främst intern riskhantering, kan anses vara ett relativt känsligt ämne att prata om. Därav lades det stor vikt på att redan i början av intervjun göra klart för respondenterna att de endast ska berätta sådant de känner sig bekväma med och de pressades heller inte att svara på frågor de inte ville. Ytterligare en sak vi märkte redan efter två intervjuer var att ingen av respondenterna ville att deras företagsnamn skulle finnas med i arbetet. På grund av detta togs beslutet att detta inte skulle nämnas alls för någon av de medverkande.

Ahrne & Svensson (2015) lyfter vikten av att sortera, minska och argumentera som ett arbetssätt då detta leder till att de viktigaste delarna av respondenternas svar kan väljas ut från intervjuerna. Vidare är vår data läsbar i löpande text med några citat längs vägen. Citat kommer att användas då detta klarlägger respondenternas tankar mer personligt och det blir enklare att tolka dem. Allt detta görs genom att följa Rieneckers (2018) rekommendationer vilket handlar om att underlätta för analysen och diskussionen som i sin tur leder till att datan kan utvärderas på ett bra och systematiskt sätt.

4.1 En proaktiv approach till riskhantering

Medvetenhet och utbildning pekas ut som den absolut viktigaste delen när det kommer till proaktiv riskhantering hos majoriteten av respondenterna. Alla respondenter utom en förklarade att de i företaget genomförde obligatoriska utbildningar och certifieringar antingen kvartalsvis, halvårsvis eller årsvis. En av de typer av utbildningar som kommer på tal är *Security Awareness Trainings* vilket tyder på att företaget aktivt arbetar med att förhöja medvetenheten hos sin personal. Både respondent 1 och respondent 2 förespråkar *scenariobaserad* utbildning i arbetet, ‘vad gör vi om X eller Y inträffar, vilka ska kontaktas och hur ska de påverkade enheterna isoleras?’. Respondent 2 menar att de utsätts för attacker varje dag, och att antalet attacker bara ökar och ökar för varje år som går. Genom att ha väl definierade policys och riktlinjer menar respondenten att de lyckas avvärja dessa i den mån att inget betydande påverkat företaget så vitt hen kan minnas.

Något annat som tas upp rör den *behovsanpassade* utbildningen. Med detta menas den utbildning som genomförs då något omfattande händer i världen som med all sannolikhet kommer påverka risklandskapet för företaget, likt exempelvis Covid-19 eller kriget i Ukraina. Enligt respondent 1 har dessa händelser lett till insikten att världsordningen inte är stabil längre och att det inte går att förutsätta att allt bara fungerar som det ska. Även respondent 2 lyfter kriget där hen beskriver hur detta satt fingret på hur mycket saker som kan förändras över en natt.

Dock måste företaget dessutom backa upp med en stabil och omfattande IT-infrastruktur för att reducera skadorna om det skulle vara att någon medarbetare gör fel, antingen medvetet eller omedvetet. Att arbeta proaktivt beskrivs vara oerhört viktigt då det kostar ofantligt mycket både tid och pengar att reparera och komma tillbaka från ett exempelvis ett dataläckage. Två av respondenterna lyfter Coop som exempel där de beskriver att det handlar om enorma summor innan företaget helt återhämtat sig. Både respondent 7 och 9 förklarar dessutom att riskarbetet bör implementeras genom hela organisationen, och respondent 7 menar att en holistisk approach bör appliceras där riskfrågor bör kunna röra sig hela vägen upp och ner samt åt sidorna på ett smidigt sätt.

När det kommer till människan i förhållande till det proaktiva arbetet anser majoriteten av respondenterna att det i slutändan är människan som anses vara den största risken, både medvetet och omedvetet. Det är i slutändan en individ som sitter och tar beslut om vad hen ska eller inte ska göra och det spelar ingen roll hur mycket säkerhetsmekanismer som införs eftersom de alltid kan ‘overridas’ av människans agerande. Dock lyfter respondent 4 en lösning på detta problem där hen menar att företag genom att kontrollera tillgångarna som en individ har kan markant reducera risken att något oväntat eller oönskat inträffar. Hen berättar hur företaget arbetar efter en ‘Zero trust-princip’ vilket innebär att en individ inte ska ha fler tillgångar än vad som behövs exakt när dessa behövs. Med tillgångar menas i detta sammanhang data, anställda ska endast ha tillgång till exakt den data som behövs för att göra sitt jobb. Även respondent 2 och 8 menar att de arbetar efter denna princip, men företaget som respondent 2 arbetar på gör det endast när det kommer till den data som är som mest känslig.

Att arbeta efter denna princip anses skydda såväl företaget som individen då medarbetaren vet exakt vilken data denne har tillgång till. “...behöver inte vara rädda 24 timmar om dygnet 365 dagar om året utan bara de 2-3 dagarna man arbetar med den absolut känsligaste informationen…” - Respondent 4. Detta i sin tur resulterar i att företaget inte behöver införa lika omfattande säkerhetsmekanismer då möjligheten att känslig data läcker ur reduceras, samtidigt som intresset för hackare att genomföra en attack minskas.

Respondent 3, som istället tryckte på teknikens bidrag till företagets proaktiva riskhantering ansåg att människan alltid kommer göra fel och att de därför måste se till att det rätta tekniska skyddet för att inte det ska få förödande konsekvenser finns. Hen berättar att en regel de arbetar efter är att det för varje policy, instruktion och riktlinje ska finnas en teknisk lösning.

För att ha ett proaktivt tillvägagångssätt finns det enligt denna respondent fem förmågor företag måste besitta; identifiera, skydda, upptäcka, svara och till sist återhämtning.

Ytterligare något som skiljde sig åt respondenterna emellan var om tillit och/eller kontroll ska tillämpas. Några menade att tydliga riktlinjer, policys och regler bör finnas för vad individen får och inte får göra samt bör och inte bör göra. Andra menade att de snarare bör arbeta med tillit till sina medarbetare, att arbeta med stöttning och lärande och att "göra det lätt att göra rätt". Både respondent 7 och 9 nämner vikten av att arbeta med en säkerhetskultur snarare än en uppfostran. Företagsledningen ska värna om sina medarbetare och få dem att vilja göra rätt både för sig själva och företaget i helhet. Här är det till stor del företagsledningens och chefernas ansvar att skapa detta.

När det kommer till vilken av de fyra proaktiva riskhanteringsmetoderna respondenternas företag använde sig av skilde det sig även här. Vissa arbetade med alla fyra, vissa arbetade med alla utom en, vissa arbetade med en eller två av dem medan några inte visste vilken av de olika metoderna som användes. Något värt att nämna var dock något som lyftes av respondent 2 då hen berättade att *unsupervised machinelearning* ökade markant. Detta innebär att algoritmer ständigt ligger och övervakar nätverket och larmar om ett avvikande beteende identifieras. företag letar alltså risker i det de inte vet.

Samtliga respondenter var överens om att proaktiv riskhantering är en förutsättning för att överleva i dagens föränderliga samhälle. De menar att digitaliseringen går i en rusande fart och att företag behöver vara förberedda att agera om något skulle hända. "Jag skulle säga såhär att det är en förutsättning att jobba proaktivt/…/världsordningen är inte så stabil längre och att man kan inte ta det förgivet att allting bara funkar som det ska." - Respondent 1. Då risk inte alltid behöver vara något negativt förklarar respondent 7 att ett proaktivt arbetssätt erbjuder möjligheten att välja hur risken ska hanteras, vilket kan innebära positiva konsekvenser för företaget i längden. Dock anser samtliga respondenter att den reaktiva delen även den är av stor betydelse eftersom saker faktiskt inträffar, oavsett hur mycket förberedelse som sker innan. Vidare var samtliga respondenter överens om att både människan och den tekniska infrastrukturen är viktigt att ta i beaktning då företag arbetar med proaktiv riskhantering, inte bara i informationssäkerhets- och cybersäkerhetsföretag utan i samtliga organisationer i samhället. Dock fanns det meningsskiljaktigheter då det kom till vilken av dessa två komponenter som anses vara viktigast. De flesta av respondenterna anser att kunskapshöjande aktiviteter såsom utbildning och medvetenhet bland personalen är det som främst bidrar till den proaktiva riskhanteringen, medan respondent 3 väldigt tydligt menade att tekniken är det som spelar absolut mest roll.

4.2 De största utmaningarna är..?

Det var många lika utmaningar som respondenterna såg i deras företag. En av utmaningarna som framkommer i flera intervjuer är att det nästan inte är ett enda företag som vet vilken data företaget har och på grund av det vet de inte heller hur den ska skyddas. Om detta kopplas ihop detta med andra utmaningar som finns är det en brist på kunskap om data och

information som är den största utmaningen som vi kan komma fram till från alla respondents svar. Brist på kunskap leder till en osäkerhet i sitt skyddande vilket skapar en utmaning för företagen eftersom de är sårbara utan något skydd. En brist på kunskap är väldigt skadligt och det visas redan i rekryteringsprocessen i vissa företag. Respondent 3 tog upp att kunskap är något som hamnar under radarn när nya människor ska anställas i ett företag:

"Jag satt mig och googlade på avhandlingar om hur man bygger en ledningsgrupp och kunskap och erfarenhet var inte centrala delar av 11 000 arbeten /…/ Här är problemet med Sverige idag, vi är inte ett meritokratiskt samhälle. Det är helt andra saker som spelar in än kunskap och erfarenhet, det spelar ingen roll om vi är rätt person till rätt uppgift." - Respondent 3

Detta är en utmaning för företagen och det är att bristen på kunskap leder till att individen inte har medvetenhet om vad som krävs för att skydda företaget. Brist på kunskap kommer också ofta från högt uppe i företaget vilket skapar ett missförstånd i företaget då ledningen tror att det går bra men i verkliga fallet är det kaos hos nätverk- och serviceteknikerna. Kraven som ställs av de högre upp i företagen som inte besitter kunskap för att ta kunskapsbaserade beslut gällande säkerheten gör att det blir svårt att implementera deras krav i säkerhetsprocesser.

Ytterligare utmaningar som lyfts i de olika intervjuerna är själva digitaliseringen samt ansvar. Digitaliseringen går fort vilket gör att företagen ständigt måste anpassa sig, och om de inte gör det på rätt sätt leder det till att de kan försvinna i branschen och andra företag som lyckas hänga med tar större plats. Respondenterna håller med om att digitaliseringen både är bra och dålig då det gör att de får tillgång till flera verktyg som kan hjälpa deras verksamhet, å andra sidan gör det att krav från kunder och samarbetspartners förändras ofta vilket måste följas för att inte förlora dem. Ansvar är dessutom en utmaning gällande vem som har ansvar om någonting går fel, vem har rätt att skylla på vem om till exempel en phishing-länk klickas på. Även om det var en individ som klickade på länken är det oftast ledningens ansvar då det är de som inte har gjort sitt jobb gällande utbildning vilket då ofta leder till intrång. Detta är en utmaning som dök upp en del under intervjuerna då många av respondenterna var med i ledningen på företaget de jobbar på.

4.2.1 Människans roll i sammanhanget

"Kedjan blir aldrig starkare än den svagaste länken, [...], den svagaste länken är oftast individen och människan…" - Respondent 1. Likt vad som tidigare diskuterats lyfter samtliga respondenter att individen och människan är en av de största säkerhetsriskerna inom företaget, om än från olika perspektiv. Några av respondenterna lyfter risken att människor medvetet gör saker för att skada företaget, antingen för att denne drivs av en övertygelse av något slag, att medarbetaren är arg på sin arbetsgivare eller är öppen för att ta emot mutor. Dessutom menar respondent 6 och 7 att arbetsmiljön kan bidra till att medarbetaren drar sig till gemenskaper, alkohol eller droger vilket i sin tur kan bidra till att individen i sig blir en säkerhetsrisk. Andra lägger större vikt på medarbetarens omedvetna handlingar, att denne gör något med goda intentioner men dåliga påföljder.

Detta problem kan hanteras, eller i alla fall reduceras, genom att reducera individens tillgångar. Respondent 4 förklarar att många organisationer ger sina anställda för mycket tillgångar eftersom de utgår från att de inte kommer göra någonting skadligt för företaget. Respondenten förklarar vidare att många medarbetare läckt information till hackare, media eller kollegor antingen medvetet eller omedvetet, ofta på grund av att individen har tillgång till information som hen inte förstår är känslig och behöver skyddas. Även respondenterna 7 och 8 lyfter tillgångar då de pratar om individen och dess påverkan på risk och att det behöver ställas krav på vem/vilka som kan komma åt systemen.

Även missförstånd kan resultera i enorma säkerhetsrisker. Detta lyfts både av respondent 7 och 3, dock från olika perspektiv. Respondent 7 menar att missförstånd gällande vilka risker som faktiskt är aktuella kan resultera i att fokus läggs på fel saker och att svårigheten är att "få alla med". Respondent 3 fokuserar istället på de tekniska delarna där hen förklarar att man måste säkerställa att de tekniska skyddsmekanismer som implementeras fungerar som de ska, att personalen får den rätta utbildningen gällande hur den ska användas, konfigureras och förvaltas.

4.2.2 Hur viktig är tekniken

Ett genomgående tema i alla intervjuer är att tekniken är viktig ja, men det är inte viktigare än individerna i företaget. Teknik kan användas för att underlätta för företaget när en länk klickas på genom att då analysera länkens innehåll, men det viktigaste är att individen i företaget inte ska befinna sig på den platsen från första början och inte kunna klicka på den länken. Alltså, tekniken ska finnas där som en sista säkerhetsåtgärd men samtidigt ska företag kunna förlita sig på den vilket gör det till en viktig del, men inte det viktigaste.

Den grundläggande tekniken som finns hos dessa företag är brandväggar för att se till att ingen kommer in i systemen när anställda är på kontoren. Detta är en teknisk lösning som gör det svårare för cyberbrottslingarna att komma in i systemet. Här lyfter även några av respondenterna vikten av Port Shuffling, vilket förklaras i kapitel *2.1 Begreppsdefinition*, som en viktig och central del av brandväggar för att skydda sig effektivt. Dessutom är tvåfaktorsautentisering även en teknisk säkerhetsåtgärd som finns som ett proaktivt arbete. Detta är något som varje respondent lyfte som en teknisk fördel när det kommer till att skydda sig proaktivt. Tvåfaktorsautentisering gör att företag vet om att det är rätt person som tar sig in i känsliga dokument och system och det är ett väldigt säkert sätt att logga in då inte bara lösenord krävs vilket kan vara enkelt för cyberbrottslingar att knäcka.

Vidare lyfter respondenterna att det finns olika tekniska ramverk företag bör känna till och förhålla sig till men inte leva efter då det kan leda till problem då de blir för fyrkantiga i sina tekniska lösningar. Ett exempel, som lyfts av respondent 3, är Critical Security Controls (CC20) vilket innebär 20 olika kontroller där alla intrång med öppen data från de senaste 10-20 åren stoppas in för att ta reda på vad som faktiskt hade förhindrat de intrången. Ett väldigt bra sätt att hålla koll på hur företag ska skydda sig och vad de kan ta för

säkerhetsåtgärder, men inte leva efter då det kan leda till förlusten av den mänskliga förmågan i företagen.

4.3 Utbrottet av Covid-19, vad är fortsättningen?

Temat i alla intervjuer var att utbrottet av Covid-19 gjorde att riskerna mot företagen ökade och med det även säkerhetsåtgärderna. Detta var någonting som blev väldigt svårt att hantera då det kom lite från ingenstans. Kontor stängdes ner, folk permitterades och slutade samt motivationen minskade för att jobba då många föredrar att jobba på plats. Detta var inne i företagen men det påverkade även relationerna med kunder att de inte kunde ses. “Det blev inte lika personligt och givande att ses på Zoom istället för IRL” - Respondent 9. Själva övergången till att arbeta hemma gick dock smidigt för majoriteten av företagen vi intervjuade. Detta var på grund av att de är företag inom IT/Cyber-branschen vilket var en fördel då de redan vet hur tekniken fungerar, och dem var dessutom redan vana med att jobba på distans. Dock var det väldigt svårt med själva nätverken hemma hos sina medarbetare. Det var detta företag var oroliga för, i och med att företagsledningen inte har någon koll på hur säkert de anställdas nätverk är hemma. Detta var en negativ sak på grund av att företag var tvungna att öppna upp system och dokument för att få tillgång till dem hemifrån vilket är skadligt då det lockar till sig cyberbrottslingar. En sak som infördes eller redan fanns innan Covid-19 hos nästan varje företag vi intervjuade, och som tidigare diskuterats, var tvåfaktorsautentisering vilket innebär en mycket säkrare inloggning och de vet vem det är som loggar in.

Några av våra respondenter svarade att de blir attackerade väldigt ofta dagligen och de flesta märker en skillnad på antal attacker innan och efter pandemin. Detta för att digitaliseringen gjorde att drastiska åtgärder var tvungna att tas och om företag inte lyckades med det kan det fortfarande vara skadligt för sitt företag att jobba på distans, utanför brandväggarna. Flera av respondenterna beskrev dessutom att de tror att företagen kommer fortsätta arbeta i detta hybridläge där medarbetaren kan välja att arbeta hemifrån eller på den fysiska arbetsplatsen.

De lärdomar som dök upp oftast i dessa intervjuer var att hoten blev reella. Innan har företag sett på cyberhot som något fiktivt, något som de vet finns där men eftersom de själva inte har blivit påverkade av det, “finns de inte”. Detta har ändrats sedan pandemin när allt fler blev attackerade och med det blev hoten verkliga. I början av pandemin var det svårt att hänga med och det var en långsam start för att kunna göra just det, men med tiden och all ny teknik som kommer dagligen och bättre sätt att skydda sig internt och externt har det bara blivit bättre med tiden. Efter att hoten har blivit mer verkliga har det gått bra för många av företagen som jobbar med säkerhet då företag som inte finns i den branschen också anser att hoten är mer reella. Detta kan ses på antalet fler proaktiva uppgifter dessa företag efter pandemin jämfört med innan.

Respondent 3 nämnde vidare att digitaliseringen exploderade med pandemin vilket gjorde att cyberattacksbranschen gick om all droghandel i världen gällande pengar 2021. Detta gjorde att flera företag råkade ut för cyberattacker med att de blev sårbara. Följden av pandemin nu

är att företag måste vara ännu säkrare än vad de var innan och att ha koll på sin IT. Om detta inte görs kommer företag att falla då de råkar ut för cyberattacker. Detta då en cyberattack gör att ett företag, enligt respondent 3, står stilla i 23 dagar utan att kunna arbeta. Vidare förklarar respondenten att det sedan tar i snitt 287 dagar att återhämta sig från en cyberattack vilket kommer att kosta väldigt mycket pengar. Därför är det viktigt att vara förberedd på att attacker nu förekommer mycket oftare än innan pandemin.

5. Analys

5.1. Ett ökat behov av proaktiv riskhantering

Något som tidigare diskuterats är omvärldens, framförallt IT-världens, omformning och omorganisering till följd av digitaliseringens framfart. Detta är dessutom något som kom upp under i princip samtliga intervjuer där respondenterna diskuterade att allt går snabbare och snabbare, nya risker uppstår för varje dag som går vilket ställer högre krav på ett mer agilt arbetssätt och riskhantering. Dessutom tror många av respondenterna att detta bara kommer fortsätta och accelerera vilket resulterar i att såväl företag som individer behöver lägga mer tid och energi på förarbetet, det vill säga den *proaktiva riskhanteringen.* Covid-19 gjorde att processen ökade i takt och omfång betydligt mer vilket märktes då antalet attacker ökade markant, även mot informations- och cybersäkerhetsföretagen. Detta berodde på övergången till att arbeta hemifrån då det innebar att medarbetaren numera satt och arbetade bakom sin hemrouter och på sitt hemnätverk och inte bakom företagets omfattande infrastruktur och brandväggar.

Många kanske trodde att allt skulle övergå till det “normala” då pandemin lagt sig och smittan minskat, att anställda skulle flytta tillbaka till kontoret, men så verkar inte vara fallet. Majoriteten av respondenterna sade uttryckligen under intervjuerna att de tror att anställda kommit in i en form av “nytt normaltillstånd” där individen själv får välja varifrån de bedriver sitt arbete. Respondent 2 använde ordet “hybridläge” för att beskriva detta där hen poängterar fördelarna med att arbeta efter denna struktur. Vissa uppgifter kan anställda helt enkelt utföra på ett mer tidseffektivt sätt om de får arbeta ostört i hemmet snarare än på ett kontor där anställda kanske blir störd av sina kollegor. Dock medför detta, vilket tidigare nämnts, en ökad hotbild och fler risker. Risker som inte tidigare ansetts vara risker uppstår, både rörande den teknik som används och medvetenheten hos den enskilda individen. Detta i sin tur medför att företagen behöver vara bättre förberedda för att kunna agera innan en oönskad risk inträffar.

Ytterligare en viktig faktor, vilken tidigare diskuterats, är kunskapen och förståelsen gällande vilken typ av data företaget har tillgång till. Det gäller att veta exakt vilken man har, vilken data som behöver skyddas, hur den ska skyddas och varför. Flera av respondenterna, bland annat respondent 2 och 4, beskriver att detta är ett av de största problemen när det kommer till riskhantering, för hur ska företag skydda det de inte vet vad det är? Under intervjuerna framkommer dessutom att detta är ett flerdelat problem eftersom data idag kan ses som en av

företagets viktigaste tillgångar då den data ett företag besitter i sin tur kan omvandlas till betydande konkurrensfördelar om den förvaltas och används på rätt sätt. Av den anledningen blir det därför en strävan att samla på sig så mycket data man bara kan. På grund av digitaliseringens enorma framfart växer därmed detta problem, att företag inte har koll på vilken data de har, då datamängderna ökar för varje år som går (Grossman & Pedahzur, 2020). Allt eftersom tiden går, och datamängden ökar, ökar dessutom riskerna exponentiellt om detta problem inte tas itu med. Företag och organisationer måste göra förarbetet, även fast det känns tungt och mycket, med att arkivera, klassificera och sortera data, för att göra det tydligt vilken av denna som faktiskt behöver skyddas.

Då intervjuerna genomfördes ställdes frågan vilken av de fyra proaktiva riskhanteringsmetoderna av Rajan (2022) som eventuellt föredrogs och användes på företaget. Några av respondenterna menade att alla fyra var lika effektiva och viktiga för företagets proaktiva riskhantering, andra förespråkade endast en eller två av dem medan vissa inte visste vilken som användes. Något som dock kom upp i intervjuerna var vikten av utbildning, det vill säga personalutbildning, vilket är den metod som absolut störst andel av respondenterna menade att de värderar väldigt högt. Man kan därför anta att denna metod är den som respondenterna, men också Galarita (2022) anser vara mest effektiv. Galarita (2022) beskriver nämligen att en form av minimumkrav för de som jobbar med informations- och cybersäkerhet är att genomgå en utbildning relaterad till det område man jobbar inom vilket kan jämföras med de behovasanpassade- och scenarioanpassade utbildningar som diskuteras i avsnitt *5.2 Hur ska man hantera den största risken- medarbetaren?* Vidare uttryckte en av respondenterna att de arbetade med *unsupervised machinelearning* vilket innebär att algoritmer ständigt ligger och övervakar nätverket och larmar om ett avvikande beteende identifieras. Företag letar alltså risker i det de inte vet och kan därför jämföras med metoden *proaktiv övervakning av nätverk och slutpunkt*. Respondenten menade att denna typ av strategi ökade markant, och kanske är det denna metod som i framtiden kommer ersätta personalutbildning som den mest effektiva riskhanteringsmetoden.

Risk behöver dock inte alltid vara något negativt, det är “en oväntad påverkan på mål” som en av respondenterna uttrycker det. Att arbeta med proaktiv riskhantering innebär alltså inte att endast reducera sannolikheten att en risk inträffar, utan även att ta vara på de möjligheter som kan uppstå till följd av en risk. Detta beskrivs dessutom av Hopkins (2018) där författaren menar att risker ibland resulterar i nya möjligheter vilka företag kanske missat om de endast behandlade risk som något dåligt. En proaktiv riskhantering medför att företag får tid på sig att hantera riskerna på det sätt som i längden blir mest gynnsamt för företaget. Genom att arbeta med riskhanteringen på ett *holistiskt* sätt, vilket lyfts av några av respondenterna, kan riskfrågorna röra sig på ett smidigt sätt genom hela organisationen. Detta medför i sin tur att en risk som ses som oönskad eller dålig av en avdelning, men kanske inte av en annan, kan omprövas och eventuellt hanteras annorlunda då flera olika personer och därmed perspektiv appliceras.

5.2. Hur ska företaget hantera den största risken- medarbetaren?

I nästan samtliga av intervjuerna beskrivs medarbetaren vara det största hotet mot företagens säkerhet. Oavsett hur mycket teknisk infrastruktur, brandväggar och VPN-teknik som implementeras kommer människans agerande och beslut alltid kunna bidra till risker, både medvetet och omedvetet. Just *medvetenhet* beskrivs ha en avgörande roll, då individers kunskap och förståelse, både gällande vilken data företaget har och vilka cyberhot som finns, bidrar till den allmänna riskhanteringen i företaget. Detta lyfts både av Ghann m.fl. (2022) och Alsmadi m.fl. (2022) där de diskuterar individens medvetenhet, dock i förhållande till övergången att arbeta på distans efter Covid-19.

Artiklarna och deras fokusområde är trots detta av intresse då IT-världen ritar om sig. Bara för att distansarbetet fick ett explosionsartat uppsving i och med pandemin betyder inte detta att alla företag kommer gå tillbaka till att arbeta från deras fysiska kontor, utan många kommer att behålla distansarbetet som ett alternativ för sina anställda, vilket diskuterades i föregående avsnitt. I både artikeln av Alsmadi m.fl. (2022) och Ghann m.fl. (2022) beskrivs medvetenheten hos individen öka i betydelse då medarbetaren arbetar hemifrån, något som dessutom tas upp nästan av samtliga respondenter. I intervjuerna lyfts två olika komponenter som extra viktiga när det kommer till medvetenhet; medvetenhet om vilka *data* företaget har, och vilka *hot* som finns. Varför dessa komponenter är viktiga lyftes under avsnitt *5.1 Ett ökat behov av proaktiv riskhantering.*

5.2.1 Omedvetna risker

Som tidigare nämnts finns det två typer av risker, medvetna risker och omedvetna. De omedvetna riskerna är de som uppstår trots individens goda avsikter- eller som respondent 1 uttrycker det, goda intentioner med dåliga påföljder. Exempel kan vara att en individ råkar klicka på en länk som råkar innehålla ransomware, företag kan bli utsatt för en phishingattack eller på något annat sätt råka bli hackad eller manipulerad till att avslöja eller ge ifrån sig information. Något som lyftes av flera av respondenterna var människans brister, ingen är perfekt och alla gör misstag, men genom att kontinuerligt arbeta med att höja individens medvetenhet kan företag reducera sannolikheten att en attack skulle lyckas.

För att göra detta uttrycker nästan samtliga av respondenterna att de arbetar med diverse olika former av utbildning. De två typer som konkret lyfts är *scenariobaserad* utbildning och *behovsanpassad*. Den förstnämnda av dessa, scenariobaserad, behandlar enskilda scenarion och vad en individ bör och inte bör göra om det sedan skulle inträffa. Detta görs för att förbereda medarbetaren att vara handlingsberedd om en attack inträffar. Den andra, behovsanpassad, genomförs om något betydande skulle hända i omvärlden, såsom exempelvis Covid-19 eller kriget i Ukraina. Det kan dessutom handla om företagets leverantörer och om någon av dessa utsatts för ett intrång vilket ställer högre krav på medvetenhet och förberedelse. Respondent 7 lyfter detta där hen beskriver att dataläckaget som Coops leverantör utsattes för resulterade i att hotakörerna fick tillgång till andra bolag och verksamheter (Toresson, 2021). Ytterligare en typ av utbildning som lyfts är *cyber security awareness programs* vilket lyfts av både respondent 1 och i artikeln av Alsmadi m.fl.

(2022). Att genomföra dessa typer av utbildningar kontinuerligt är något som resulterar i en ökad medvetenhet, fokus och kvalitet vilket i sin tur bidrar till en bättre proaktiv riskhantering.

5.2.2 Medvetna risker

När det kommer till *medvetna* risker behöver dessa hanteras på ett annat sätt. Dessa risker uppstår genom att en medarbetare medvetet gör något för att skada det egna företaget, antingen på grund av att de är arga på sin arbetsgivare eller för att de kan vara öppna för att ta emot en muta. Ett sätt att hantera denna risk på rör ledarskap. Respondent 6 och 7 diskuterar detta under intervjun där respondent 6 uttrycker att ledarskapet på ett sätt är en säkerhetsrisk eftersom sättet att bedriva ledarskap antingen bidrar till en god eller dålig arbetsmiljö. Medarbetare som vantrivs på arbetsplatsen kommer med all sannolikhet vara mer öppna att göra saker som kan skada företaget än de som trivs och känner sig inkluderade. Även respondent 9 nämner detta där hen nämner begreppet *säkerhetskultur*. Att arbeta med en god och trivsam kultur är med andra ord ett sätt att proaktivt arbeta med säkerhet för att reducera sannolikheten att en medarbetare medvetet utgör ett hot och därmed en risk.

Båda dessa typer av risker, medvetna och omedvetna, kan dock hanteras genom att arbeta med *tillgänglighet* och *Zerotrust-principen.* Detta lyfts av flera av respondenterna där de diskuterar hur reducerad tillgänglighet av data bidrar till en större säkerhet för såväl den enskilda medarbetaren och företaget i stort. Genom att reducera tillgångarna till att endast finnas tillgängligt för exakt den individ som behöver det exakt när hen behöver det minskar både hotbilden av individen och konsekvenserna av den skada som kan inträffa (NIST, 2013). Dessutom bidrar detta till ökad spårbarhet eftersom företaget numera vet exakt vart det eventuella dataläckaget ägde rum. Mer om detta diskuteras i kapitel *5.3 Kontroll eller Tillit.*

Slutligen lyfts dessutom *missförstånd* som en av de mänskliga faktorer som bidrar till ökad risk. Detta lyfts av både respondent 3 och 7, dock från olika perspektiv, men trots detta finns argumentet att en lösning på problemet skulle behöva komma uppifrån. Ledningen är den som behöver ta det största ansvaret både gällande att "få alla med på tåget", att se till att allt fungerar som det ska och att alla får den rätta utbildningen för att hantera de tekniska skyddsmekanismer som finns. Detta argument styrks dessutom av Hopkins (2018) och de punkter som presenteras i kapitel *2.4 Risk och riskhantering.* I dessa lyfts gemensamma processer, kommunikation och ledningsbeslut som centrala element för att reducera risken att något oväntat ska inträffa som påverkar företaget negativt. Givet detta kan de olika typer av missförstånd som lyfts av både respondent 3 och 7 hanteras av ledningen genom en tydlig, utarbetad och konkret strategi vilken sedan på ett begripligt och klart sätt kommuniceras nedåt i företaget.

5.3. Kontroll eller tillit

Något som dök upp i intervjuerna och som vissa respondenter inte var ense om var om och hur företag ska arbeta med kontroll och/eller tillit. En del av respondenterna anser att visa tillit till sina medarbetare är något som bör göras för att de ska kunna lära sig samt utvecklas,

De andra respondenterna tyckte å andra sidan att tydliga regler, riktlinjer och policys bör etableras för att det ska vara tydligt för medarbetarna vad de får och inte får göra, det vill säga kontroll. Det finns alltså inget tydligt tema för respondenterna, men det var ett begrepp som dök upp då och då i intervjuerna som handlar om just kontroll och/eller tillit, nämligen Zero Trust. Denna modell är lösningen på ett av de problem som beskrivs av respondenterna. Genom att kontrollera de tillgångar som en individ har reduceras de risker som är oväntade eller oönskade.

Zero Trust-modellen var som tidigare nämnts ett återkommande tema i intervjuerna och respondent nummer 3 lyfte detta som en lösning på problemen som finns gällande kontroll och tillit hos olika företag. Modellen innebär att man genom att kontrollera de tillgångar som en individ har på företaget, minskar risken att de blir attackerade (NIST, 2013). Efter intervjuerna kom vi fram till att Zero Trust är ett bra verktyg att använda för att skydda sig proaktivt gällande kontroll och tillit. Detta backas upp, och förklaras ytterligare, i litteraturgenomgången under rubrik *2.6 Zero Trust-modellen* där vi lyfter hur Zero Trust fungerar.

5.4. Hur Covid-19 förändrade risklandskapet

I intervjuerna var det många av respondenterna som nämnde att de blir ofta blir attackerade och i samband med det märker de ett ökat antal attacker under och efter Covid-19 jämfört med innan. Alawida m.fl. (2022) beskriver att det var vanligt att företag utsattes för det i samband med pandemin enligt då det i artikeln framkommer att det finns ett samband mellan utbrottet av Covid-19 och ett ökat antal cyberattacker samt cyberbrottskampanjer. Detta backades i sin tur upp med förklaringen om att det ibland kunde vara 3-4 attacker som ett företag utsattes för dagligen. Det finns alltså ett samband mellan det som respondenterna svarar att de har upplevt och vad forskningen faktiskt säger vilket gör att det är väldigt viktigt att ha de ökade attackerna i åtanke då de arbetar idag, och måste därmed vara beredd på att skräddarsy sin säkerhet för att skydda sig mot dessa hot.

Vidare lyfts det i artikeln att det finns, och alltid kommer finnas en koppling mellan kriser, pandemier och andra globala kriser och antal cyberattacker i världen (Alawida m.fl., 2022). Detta är något som respondenterna håller med om och de vill även trycka på att digitaliseringen är en del av händelser som främjar cyberattacker och cyberbrottskampanjer. Detta för att digitaliseringen "exploderade" med pandemin och stora summor av pengar strömmade in i cyberattacksbranschen. I och med den stora summa pengar som strömmade in och de 1108 attackerna i USA 2019 (baserat på statistiken i artikeln av Alawida et. al., 2022) till 1872 attacker 2020 är det tydligt att hoten ökar med händelser som påverkar digitalisering och därför är det extremt viktigt att skydda sig på rätt sätt, vilket ytterligare förklaras i *kapitel 5.2 Hur ska den största risken, medarbetaren, hanteras?*. Pandemin har alltså både förändrat hoten och ökat dem. Detta leder till att skyddet som företag måste ha för att kunna stå emot attacker har helt nya krav på sig, vilket kan ses som en utmaning för dagens företag.

Pandemin har, som tidigare nämnts, ändrat på hur företag ser på att jobba hemifrån, både på ett positivt sätt men också negativt. Respondenterna lyfter att det inte fanns så mycket att påverka gällande säkerheten till en början då de anställda gick från att jobba på arbetsplatsen som har brandväggar och skydd för att ingen ska ta sig in till att istället arbeta hemifrån. Ghann m.fl. (2022) förklarar att användningen av internet, på grund av distansarbetet, har ökat sedan pandemin och det blir allt viktigare med medvetenhet av de anställda för att kraven på säkerhet ska hållas under ett distansarbete. Med pandemin började mycket handla om individen och att de måste vara medvetna om hur deras agerande kan påverka att risken för företaget ökar, i samband med att hotaktörerna blivit mer sofistikerade och bra på att utnyttja företags säkerhet. Efter Covid-19 fick hotaktörerna dessutom mer både makt och inflytande i cybersäkerhetsbranschen (Alsmadi m.fl., 2022). Detta kopplat till en av respondenternas svar att med Covid-19 har även det uppstått en ny bransch för cyberkriminella som liknar vilken vanlig bransch som helst. De har semester, löner, organisationsmodeller och pensionssystem. Detta gör att de har exakt samma förutsättningar som andra företag vilket gör det mycket värre. Denna utveckling är den största risken som uppkommit med Covid-19 och den kommer inte att försvinna inom den närmaste framtiden.

6. Diskussion

Då vi påbörjade studien hade vi egentligen ingen uppfattning om hur företag inom informations- och cybersäkerhetsbranschen konkret arbetar med just proaktiv riskhantering. Vi misstänkte dock att det skulle handla mycket om teknik och teknisk infrastruktur, men märkte relativt snabbt då vi påbörjade litteraturgenomgången att mycket fokus låg på medarbetaren och dess kunskap och medvetenhet. Denna “hypotes” stärks ytterligare då vi påbörjade intervjuerna då nästan samtliga respondenter ansåg att individen var det absolut största och farligaste hotet mot företaget och därmed också den största risken. Både i artikeln av Ghann m.fl. (2022) och Alsmadi m.fl. (2022) lyfts individen fram som det största hotet vilket som sagt stämmer överens med majoriteten av respondenternas svar. Då vi dessutom valde att ta utgångspunkt i Covid-19 pandemin och dess påverkan på företagen ur ett riskperspektiv hade vi även här en idé om vad för typ av svar vi skulle få. Attackerna har, som vi trodde, ökat markant i och med den snabba övergången till att arbeta hemifrån vilket både framkommer i den tidigare forskningen av Alawida m.fl. (2022) och Glassberg (2020) samt under intervjuerna. Något vi dock inte räknat med, och som förvånade oss, var gällande okunskap. För det första att det finns så otroligt många företag som idag inte vet vilken data de har, var den data de har finns lagrad eller vilken av datan som behöver skyddas och hur. Detta framkom i flera av intervjuerna då respondenterna ombads beskriva de största hoten från ett riskperspektiv. För det andra förvånades vi av bristen på kunskap kring den generella riskhanteringen, att det är sådan brist på tydliga riktlinjer och policys gällande hur företag och dess anställda ska agera under pressade situationer, vilket dessutom lyfts i boken av Hopkins (2018). Då vi påbörjade studien antog vi att båda dessa faktorer, okunskap gällande datan samt okunskap gällande riskhanteringen i helhet, var självklarheter. Därav förvånades vi då det framkom att dessa ansågs vara några av de allra största riskerna för de medverkande företagen.

Något som dock skiljde sig åt respondenterna emellan, och som även det delvis förvånade oss under intervjuerna, var vilken av de proaktiva riskhanteringsmetoderna av Rajan (2022) företaget använde sig av. Dessa skiljde sig åt markant, men en gemensam nämnare för majoriteten av de som visste vilken företaget använde sig av och som därmed kunde svara på frågan var *personalutbildning.* Att arbeta med denna metod går i sin tur att koppla till det som beskrevs i stycket ovan, nämligen att människan och dess medvetenhet är en otroligt stor bidragande faktor till företagets totala riskhanteringsstrategi. Vi kan därför konstatera att denna metod är en av de främsta när det kommer till proaktivt riskhanteringsarbete idag, både baserat på tidigare forskning och på respondenternas svar.

Ytterligare något värt att nämna är respondenternas delade åsikter gällande teknikens roll i sammanhanget. Majoriteten ansåg som sagt att medarbetaren är det viktigaste, att få denne att känna sig inkluderad för att inte medvetet göra något för att skada företaget, samt att utbilda och lära upp genom kunskapshöjande aktiviteter för att öka medvetenheten. Nästan alla respondenter menar alltså att det inte spelar någon roll vilken teknik eller vilket skydd som implementeras eftersom människan alltid är den som tar det slutgiltiga beslutet gällande hur företag ska agera. Respondent 3 argumenterade helt tvärt emot detta då hen menade att företag absolut bör lägga mest tid och kraft på den tekniska infrastrukturen eftersom "människan alltid kommer göra fel". Vi som forskare blev först ställda av detta, att alla utom en person säger nästan samma sak. Då vi började fundera och reflektera kom vi dock på en faktor som kan ha avgörande effekt på respondenternas svar, nämligen deras bakgrund. Nästan alla av de vi intervjuade arbetar med "mjuk" IT, de är försäljare och konsulter och arbetar främst med andra människor. Respondent 3 kommer från en teknisk bakgrund som programmerare, något hen själv beskrev. Därav tror vi att detta kan vara det som avgjorde vilken typ av svar vi fick på frågorna och behöver tas med i beaktning i studien. Det kan dessutom ses som en förbättringsmöjlighet till framtiden, att göra en mer noggrann bakgrundskontroll på de utvalda respondenterna för att få så mycket bredd i svaren som möjligt.

Slutligen vill vi nämna de begränsningar vi stött på under arbetets gång. Då vi valde vilket problemområde vi skulle studera insåg vi ganska snabbt att det är ett relativt känsligt ämne, speciellt då vi dessutom valde att genomföra en kvalitativ intervjustudie. För det första är företags riskhantering något som de kanske inte vill skylta med i en publik studie, vilket märktes under intervjuerna då vi noterade att många drog sig för att svara på vissa frågor. Vi fick kommentarer som "jag vet inte om jag får säga det här men…" och "det här är ju otroligt känslig information vi har att göra med…". För det andra uppstod vissa svårigheter då vi kontaktade våra potentiella respondenter. Samtliga av de vi intervjuat arbetar på stora företag, och vissa av dem sitter dessutom på höga positioner inom dessa. Därav låg ett samtal med oss kanske relativt lång ner på deras prioriteringslista då de redan sitter med fullspäckade scheman.

Denna studie har varit en ögonöppnare för oss, och förhoppningsvis för dig som läser den. Proaktiv riskhantering anses inte bara vara viktigt, utan rentav avgörande för hur ett företag inom informations- och cybersäkerhetsbranschen lyckas hantera de risker som uppstår. Med

den rätta förberedelsen kan företag vända en risk som först ses som något negativt till att istället bli en möjlighet. Dock är det viktigt att poängtera att även den reaktiva säkerheten är av stor vikt, företag behöver tydliga riktlinjer och policys för hur de ska agera om något trots proaktivt arbete faktiskt inträffar. I majoriteten av studien har dessutom mycket fokus legat på människan och individen, men det är givetvis avgörande med teknisk infrastruktur också.

6.1 Vidare forskning

Som tidigare nämnts är informations- och cybersäkerhet ett område under utveckling. Digitaliseringens framfart ställer allt högre krav på företag, både gällande anpassning och agilitet till nya hot och risker, men också förmågan att kunna ta tillvara på de möjligheter som uppstår. Ett intressant område för vidare forskning hade därför kunnat vara de möjligheter som risk kan medföra för företag i en informations- och cybersäkerhetskontext. Vidare uttryckte, som tidigare nämnts, en av respondenterna att unsupervised machinelearning används mer och mer för att proaktivt detektera hot. Även detta område kan därav vara både intressant, och spännande att dyka djupare i. Slutligen kan ytterligare ett förslag på vidare forskning innefatta hotaktörerna. Eftersom mycket handlar om att attackerna genomförs på deras villkor hade en intressant synvinkel gällande vidare forskning vara att undersöka närmare hur de tänker som individer samt som organisationer.

7. Slutsats

Denna studie var ämnad att besvara frågan hur företag inom informations- och cybersäkerhetsbranschen bör arbeta internt för att främja en proaktiv riskhantering av såväl interna som externa risker. För att besvara denna någorlunda breda frågeställning ville vi först ta reda på hur de utvalda företagen bedriver sitt riskarbete idag, samt hur deras arbetssätt och strategi eventuellt förändrats efter utbrottet av Covid-19 då arbetet förflyttades till att bedrivas på distans. Vi visste redan innan att det kan bli svårt att komma fram till ett exakt svar på denna fråga, det vill säga ett rätt eller fel när det kommer till det proaktiva riskarbetet, men vi anser att lyckats besvara frågan i den mån det är möjligt. Vi är dessutom medvetna om de eventuella begränsningar som präglar studien gällande såväl tid och kunskap, och därav bör slutsatsen i arbetet endast betraktas som ett bidrag eller komplement till den tidigare forskningen inom området.

Baserat på analysen av empirin och litteraturgenomgången är det dock vissa punkter som är extra viktiga för att främja ett gott proaktivt riskhanteringsarbete. Dessa punkter kan ses som riktlinjer eller förslag för hur företag kan arbeta proaktivt med risk och har sammanfattats nedan för bättre förståelse och konkreta propositioner:

- Använd de fyra mest vanliga arbetssätten, personalutbildning, etiska hackare, jaga hot och proaktiv övervakning av nätverk och slutpunkt, gällande det proaktiva arbetet för att minska risken för oönskade och oväntade attacker. Av dessa fyra är *personalutbildning* den absolut viktigaste för att skapa medvetenhet och öka säkerheten på det proaktiva planet.

- *Medvetenhet* är något extremt viktigt att ha inom företaget, både gällande vilka hot som finns men också vilken data som ska skyddas inom företaget. Väldigt ofta vet inte företag vilken data de har som bör skyddas och detta är något av extrem vikt att vara medveten om. Detta kan i sin tur kopplas till punkten ovan då detta kan lösas med kontinuerlig utbildning baserat på verkliga scenarion, det vill säga såväl scenarioanpassad som behovsanpassad utbildning. I och med att hoten blev reella med Covid-19 bör även medvetenheten öka i samband med händelser som denna för att kunna skydda sig proaktivt. Att ha medvetenhet om hur en cyberattack och cyberbrottskampanjer påverkar ens företag gällande pengar det kostar, tid som verksamheten blir förlamad, hur det påverkar personal och hur företaget går tillväga efter det är essentiellt för att kunna bedriva ett proaktivt cybersäkerhetsarbete.
- Ytterligare något som anses centralt då det kommer till riskhantering, eller riskreducering, rör *ledarskapet*. Hur ledarskapet bedrivs kan både ses som en risk och en riskreducering då det kommer till individens vilja att skada, eller inte skada företaget. Genom att arbeta med inkludering och bra kommunikation för att få alla införstådda i såväl arbetsprocesserna som kulturen anses detta bidra till en lägre risk gällande de medvetna risker en individ kan tänkas utgöra. Ledarskap har en liten del i analysen och empirin men det är en del som vi anser är värd att nämna i slutsatsen.
- *Zero Trust* är en modell som är ett väldigt bra verktyg för företag. Genom att använda sig av Zero Trust minimeras risken att en attack börjar internt av en anställd till exempel. Genom att se till att de anställda bara har tillgång till det som de arbetar med i företaget eller hos kunder minskar risken att attacker lyckas. Zero Trust innebär till exempel att en anställd på ekonomiavdelningen bara ska ha tillgång till det som är relevant till ekonomi och den anställdes arbetsuppgifter exakt då denne utför dessa.
- I och med att digitaliseringen utvecklas och ställer *nya krav* på företag vilket i sin tur ställer nya krav från hotaktörerna är det viktigt att ha en föränderlig riskhantering. Hoten ändras och på grund av det måste även den proaktiva riskhanteringen göra det i takt med hoten. Genom att ändra sitt arbete samt hålla koll på hoten kommer företaget bli bättre beredd att kunna bemöta dessa hot för dagen och framtiden. Med Covid-19 exploderade digitaliseringen och hotaktörer började få mer makt på marknaden. Då pandemier och globala kriser ökar hoten och riskerna för företag är det viktigt att alltid vara förberedd, att inte låta beredskapen gå i “ebb och flod”, utan att konstant vara redo att ändra den nuvarande säkerhetsstrategin för att minska risken att cyberattacker lyckas.
- Människor är väldigt viktigt, vilket lyfts i samtliga punkter, men man får heller inte bortse från teknikens bidrag till det proaktiva riskhanteringsarbetet. Med Covid-19 gick arbetet över till distans vilket efter det har normaliserats. Detta innebär att de anställda inte längre sitter på kontoret med skyddade IP-adresser och bra brandväggar utan istället sitter hemma på ett nätverk som ofta inte är av lika bra kvalitet. För att behålla säkerhet utanför brandväggarna är det viktigt att införa verifieringsskydd såsom *tvåfaktorsautentisering*. Genom att införa detta ökar skyddet när någon ska ta sig in i känsliga system eller dokument. På grund av de säkerhetsåtgärder som tvåfaktorsautentisering medför är detta ett väldigt bra verktyg att använda för att framtidssäkra företags riskhantering.

Genom att följa dessa punkter förhöjs beredskapen och därmed företagets proaktiva riskhantering i stort. Dock får man, som tidigare nämnts, inte heller bortse från teknikens bidrag eller det reaktiva arbetet. En omfattande teknisk infrastruktur måste finnas vilken dessutom är väl införstådd av samtliga medarbetare i företaget. Anledningen till att tekniken fått mycket mindre utrymme i arbetet beror på att majoriteten av respondenterna ansåg att individen spelar en större roll. Gällande det reaktiva måste det finnas tydliga, väl kommunicerade riktlinjer och policys för exakt hur företag ska agera om något oväntat och/eller oönskat inträffar. Att arbeta fram dessa redan innan en risk inträffar kan å andra sidan ses som en del av det proaktiva arbetet.

Sammanfattningsvis konstateras det att ett proaktivt arbetssätt är en *förutsättning* för dagens företag. Både Covid-19 och kriget i Ukraina är tydliga exempel på världsomfattande händelser som bevisar att världsordningen inte alltid är så stabil som man kanske kan anta, och att företag konstant behöver vara förberedda på det oväntade. Genom att anta en holistisk och proaktiv strategi för riskhantering och ständigt anpassa sig till det komplexa och dynamiska cybersäkerhetslandskapet kan informations- och cybersäkerhetsföretag inte bara förutse hot, minimera skador och skydda sina tillgångar utan även ligga i framkant för att möjliggöra en tryggare och mer pålitlig digital framtid i stort.

Referenser

Ahrne, G., & Svensson, P. (2015). *Handbok i kvalitativa metoder* (Andra upplagan). Liber AB, Stockholm.

AngelOne. (5 augusti, 2022). *Difference between Risk Appetite, Risk Capacity and Risk Tolerance!* https://www.angelone.in/blog/how-to-do-risk-profiling-understanding-the-difference-between-risk-appetite-risk-capacity-and-risk-tolerance

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University – Computer and Information Sciences, 34* (10), 8176-8206. DOI:10.1016/j.jksuci.2022.08.003

Alsmadi, D., Maquosi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. *KYBERNETES.* DOI:10.1108/K-08-2022-1104

Berenhaut, S., K., Caroll, E., T., Crouse, M. & Fulp, W., E. (2014). Analysis of network address shuffling as a moving target defense. *2014 IEEE International Conference on Communications*. Hämtad den 17 april 2023 från 10.1109/ICC.2014.6883401

Bhingarkar, A. (2021, 24 juni). *Implementing Zero Trust Architecture on Azure Hybrid Cloud.* DZone. https://dzone.com/articles/implementing-zero-trust-architecture-on-azure-hybr

Bhanderi, D., Bhut, T., Kavathiya, M., Kaur, H. & Mehta, M. (2023). Impact of Two-Factor Authentication on User Convenience and Security. *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) Computing for Sustainable Global Development (INDIACom), 2023 10th International Conference on. :617-622 Mar, 2023*. Hämtad den 29 maj från https://ieeexplore-ieee-org.proxy.mau.se/document/10112421

Cains, M. G., Flora, L., Taber, D., King, Z., Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis, 42* (8), 1643-1669. DOI: 10.1111/risa.13687

Cheng, R., Tong, J., Wu, K. & Xu, H. (20 april, 2023). Design and Implementation of the Zero Trust Model in the Power Internet of Things. *Hindawi*. Hämtad den 18 april 2023 från https://doi.org/10.1155/2023/6545323

Cisa. (u.å.). *Stop Ransomware- Guidance and Resources.* Hämtad 28 mars 2023 från https://www.cisa.gov/stopransomware

Cisco. (u.å.). *What is Malware? Introduction.* Hämtad 28 mars 2023 från https://www.cisco.com/site/us/en/products/security/what-is-malware.html

Chaturvedi, R., Chakravarthy, K. & Williams, M. C. (2020). *Cybersecurity Risks in a Pandemic*. Hämtad 16 februari 2023 från https://www.jmir.org/2020/9/e23692/

Denscombe, M. (2018). *Forskningshandboken - För småskaliga forskningsprojekt inom samhällsvetenskaperna* (Fjärde upplagan). Studentlitteratur AB, Lund.

Elgan, M. (20 oktober, 2021) *What is proactive Cybersecurity?* SecurityIntelligence. https://securityintelligence.com/articles/what-is-proactive-cybersecurity/

Enisa. (u.å.). *What is "Social Engineering"?* Hämtad 28 mars 2023 från https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

Ericsson, M., Almukaynizi, M., Soumajyoti, S., Nunes, E., Shakarian, J., & Shakarian, P. (2021). *Exploring Malicious Hacker Communities - Toward Proactive Cyber-Defense (s. 183-188).* Cambridge University Press. DOI: 10.1017/9781108869003 https://www-cambridge-org.proxy.mau.se/core/books/exploring-malicious-hacker-communities/4A6543BCF8703B8F7784309569093A85

FBI. (u.å.). *How can we help you.* Hämtad 28 mars 2023 från https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise

Galarita, B. (2022, 8 november). *Information Security Vs. Cybersecurity: What's The Difference?* Forbes. Hämtad 20 mars 23 från https://www.forbes.com/advisor/education/information-security-vs-cyber-security/

Ghann, P., Tetteh, E. D., & Doe, N. P. (2022). The Impact of Covid-19 on Cybersecurity. *International Journal of Recent Contributions from Engineering, Science & IT, 10* (1), 67-75. DOI: 10.3991/ijes.v10i01.27889

Glassberg, J. (2020, 19 mars). *Are remote workers a security risk to your business?* The Business Journals. Hämtad 2 mars 23 från https://www.bizjournals.com/bizjournals/how-to/technology/2020/03/are-remote-workers-a-security-risk-to-your.html

Grossman, J. & Pedahzur, A. (2020). Political Science and Big Data: Structured Data, Unstructured Data, and How to Use Them. *Political Science Quarterly, 135* (2), s.225. DOI: 10.1002/polq.13032

Hadnagy, C. (2018) *Social Engineering : The Science of Human Hacking*. John Wiley & Sons, Incorporated. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/malmo/detail.action?docID=5436552

Hopkin, P. (2017). *Fundamentals of Risk Management- Understanding, evaluating and implementing effective risk management* (4th edition). Kogan Page.

Huang, Shuai, Zhang, Xu, Xu, Yu och Antwi (2020). A New System Risk Definition and System Risk Analysis Approach Based on Improved Risk Field. *IEEE TRANSACTIONS ON RELIABILITY, 69* (4), 1437-1452. DOI:10.1109/TR.2019.2942373

Hyder, M. F. & Ismail M. A. (29 januari 2021) Securing Control and Data Planes From Reconnaissance Attacks Using Distributed Shadow Controllers, Reactive and Proactive Approaches. *IEEE Access, 9*, 21881-21894. DOI:10.1109/ACCESS.2021.3055577

IBM. (u.å.). *How Industry 4.0 technologies are changing manufacturing.* Hämtad 13 februari 2023 från https://www.ibm.com/topics/industry-4-0

Malwarebytes. (u.å.). *Hacking.* Hämtad 28 mars 2023 från https://www.malwarebytes.com/hacker

Nationalencyklopedin. (u.å.). *Risk.* NE.se. Hämtad 28 februari 2023 från https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/risk

NIST. (4 augusti 2013). *Developing a Framework to Improve Critical Infrastructure*

Cybersecurity. The National Institute of Science and Technology. Hämtad 7 maj 2023 från https://www.nist.gov/system/files/documents/2017/06/05/040813_forrester_research.pdf

Oates, B.J. (2006). *Researching Information Systems and Computing* (Första upplagan). SAGE Publications Ltd, London.

Orre, C. J. (2023). *Etik & Kritik.* [PowerPoint presentation]. Canvas. https://mau.instructure.com/courses/13420/pages/forskningsetik-and-etik?module_item_id=489478

Polisen. (2020). *Nätfiske, phishing – skydda dig*. Hämtad 28 mars 2023 från https://polisen.se/utsatt-for-brott/skydda-dig-mot-brott/bedrageri/natfiske-phishing-/

Rajan, S. (2022, 11 mars). *What is proactive vs reactive cyber security?* LinkedIn. Hämtad 27 mars 2023 från https://www.linkedin.com/pulse/what-proactive-vs-reactive-cyber-security-saravind-rajan/?trk=pulse-article

Rienecker, L., & Stray Jörgensen, P. (2018). Att skriva en bra uppsats (Fjärde upplagan). Liber AB, Stockholm.

Ryan, J. J. C. H. Kamachi, C. (2015). Chapter 2- Types of Malicious Messages. I Ryan, J. J. C. H. & Kamachi. C (Red.), *Detecting and Combating Malicious Email* (s. 11-36). Syngress.

Roos, M. (2022, 28 mars). *Microsoft Teams- 5 år senare.* Edgeguide. Hämtad 2 mars 2023 från https://edgeguide.se/2022/03/28/microsoft-teams-5-ar-senare/

SOU 1998:15. *Distansarbete.* Hämtad 2 mars 2023 från https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/1998/09/sou-1998115-/

Singh Lallie, H., Shepherd, L. A., Nursec, J. R.C., Eroland, A., Epiphanioua, G., Maple, C. & Bellekense, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Elsevier, 105.* DOI: 10.1016/j.cose.2021

SISA. (2021). Processbeskrivning av arbetsgruppens arbete med förslag till ny ämnesdefinition SISA 2021 [Working Paper]. Svenska informationssäkerhetsakademin.

Säkerhetskollen. (u.å.). *Phishing/Nätfiske.* Hämtad 28 mars 2023 från https://sakerhetskollen.se/artiklar/phishing

Säkerhetspolisen. (2020). *Informationssäkerhet*. Hämtad 29 maj 2023 från https://sakerhetspolisen.se/download/18.310a187117da376c6601d43/1636446528314/Vagledning-Informationssakerhet_2020.pdf

Threat Intelligence (19 april, 2023) *Proactive Cybersecurity - What Is It, and Why You Need It*. Hämtad 27 mars 2023 från https://www.threatintelligence.com/blog/proactive-cybersecurity

Toresson, J. (14 juli, 2021). *It-attacken mot Coop – detta har hänt.* SVT Nyheter. https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant

Bilaga A

Intervjuguide

INLEDNING

- Vilken position har/hade du inom företaget?
- Hur länge har du haft/hade du denna position?
- Vad jobbar företaget med?
- *Vad är cybersäkerhet för dig?*
- *Vad är informationssäkerhet för dig?*
- **Kan du berätta om de största utmaningarna ni har gällande er informations- och/eller cybersäkerhet och arbetssättet för att klara av dem utmaningarna?**
- Vilka är de vanligaste/största hoten och riskerna mot företags säkerhet idag?
- **Vilken roll spelar individer i företagets interna, proaktiva riskhantering? Vilket ansvar har ni på ett privat plan?**

VAD VAR FÖRETAGETS STRATEGI INNAN COVID-19?

- Innan Covid-19, hade ni någon plan för incidenter och för att hantera dem om det uppstår? I så fall, hur fungerade den?
    - (Proaktiv eller reaktiv)
- Skedde mycket av arbetet hemifrån eller fysiskt på företaget?
- **Vad var de största skillnaderna du upplevde med övergången till att arbeta hemifrån?**
    - **Hur upplevde dina kollegor det?**
- **Kan du se ett samband mellan pandemins utbrott och antalet cyberattacker som genomfördes?**
    - **Vad berodde detta på tror du?**
    - Vilka nya utmaningar uppstod sett ur ett risk- och säkerhetsperspektiv?
- **Hur ofta utsätts ni för cyberattacker och vad beror det på? Om inte, vad är anledningen till att ni inte utsätts för det i ert arbete?**
- Då vi gått igenom tidigare litteratur påstås det att antalet fysiska attacker såsom dokumentläckage och skimming drastiskt minskat, medans attacker som ransomware och malware ökat- är det något som märkts av enligt dig?
- **Då ni övergick till att arbeta hemifrån, och kanske delvis fortfarande gör, hur arbetar du personligen med att förebygga "attacker" mot dig (som i sin tur kan skada företaget?)**
    - **Vilken roll spelar individen (individens *medvetenhet)* i företagets proaktiva riskhantering?**
    - **Fick ni någon form av utbildning när det kommer till personlig säkerhet vid övergången till distansarbete?**

VILKEN STRATEGI ARBETAS EFTER IDAG?

- Vilken typ av riskhanteringsstrategi använder ni just nu?

    - *Om reaktiv*- Har du/ni övervägt att implementera en proaktiv strategi?
    - **Vad anser du fördelarna är med proaktiv vs reaktiv riskhantering**
    - Har denna förändrats efter distansarbetet som följde av Covid-19?
    - Hur kan denna förbättras?
- Vilka rutiner och processer har ni just nu för att hantera risker, finns det något sätt att analysera om dessa processer följs?
- Har ni någon strategi för incidenter och för att hantera dem om det uppstår? I så fall, hur fungerar den?
    - (Proaktiv eller reaktiv)
- Hur följer ni upp på eran strategi gällande cybersäkerhet och vilka ingripande gör ni för att förbättra den över tid?
    - Hur adapterar ni strategin gällande cybersäkerhet för att möta nya hot och säkerhetsrisker som uppstår?
- **De fyra största metoderna att arbeta med proaktiv cybersäkerhet är Personalutbildning, etiska hackare, jaga hot och proaktiv övervakning av nätverk och slutpunkt. Vilken av dessa metoder förespråkar ni och använder? (Kan vara flera)**

VILKEN STRATEGI BÖR IMPLEMENTERAS?

- **Utifrån din erfarenhet, vilka utmaningar ser du med att genomföra samt upprätthålla en proaktiv riskhanteringsstrategi?**
- Hur mäter ni effektiviteten av eran riskhanteringsstrategi och vilken typ av data använder ni för att analysera just det?
    - Kan denna förbättras? Isåfall hur?

KONKRETA LÄRDOMAR

- Vilka är de viktigaste och främsta lärdomar som ni har fått från tidigare incidenter?
    - Hur har ert riskarbete utvecklats från dessa lärdomar?
- **Vilka lärdomar tog ni med er från situationen som uppstod till följd av Covid-19?**
- Vilket/vilka är de största hoten för informations- och cybersäkerhetsbranschen idag?
- Hur planerar ni att förbättra och utveckla er cybersäkerhet (riskhantering?) i framtiden? Om ni inte arbetar proaktivt med det, är det något som ni vill implementera?