LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Fallstudie inom informationssäkerhet

En undersökning av hur informationssäkerhet hanteras på ett globalt företag verksamt inom IKT

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Toni Dell Aquila

Theodor Nestler

Handledare: Miranda Kajtazi

Examinatorer: Markus Lahtinen

Benjamin Weaver

Fallstudie inom informationssäkerhet: En undersökning av hur informationssäkerhet hanteras på ett globalt företag verksamt inom IKT

Författare: Toni Dell Aquila och Theodor Nestler

Utgivare: Inst. för informatik, Ekonomihögskolan, Lunds universitet

Framlagd: Vårterminen 2018

Dokumenttyp: Kandidatuppsats

Antal sidor: 110

Nyckelord: Informationssäkerhet, Policys & Direktiv, Security Management

Sammanfattning:

Informationssystem är något som de flesta organisationer till stor del är beroende av i sitt dagliga arbete och på så sätt är även informationssäkerheten en viktig del för att organisationerna ska kunna skydda sina resurser på ett effektivt sätt utan att det hindrar arbetsflödet.

Studien uppmärksammar viktiga faktorer för hur ett företag arbetar med sin informationssäkerhet. Dessa faktorer har en direkt koppling till de teorier och studier som också beskrivs i studiens andra kapitel. Studien behandlar befintliga etablerade teorier och tidigare studier inom området. Denna teori jämförs med hur det i praktiken fungerar hos ett utvalt anonymt företag. Detta gjordes genom att först utföra en intervju med en av företagets säkerhetschefer för att sedan genomföra ytterligare intervjuer och enkätundersökningar baserade på den första intervjuns resultat samt interna dokument vilka rör säkerhetsarbetet som vi tagit del av.

Tre faktorer identifierades som särskilt viktiga för företagets arbete med informationssäkerhet: Väl konstruerade policys och direktiv, medvetenhet och slutligen ansvar. Genom att ha väl konstruerade policys och direktiv blir det tydligt och enklare för anställda att förstå vad som behöver göras och hur detta ska göras. Medvetenheten innebär att anställda är informerade om hur viktigt det är med informationssäkerhet och därmed engagerade i att efterfölja reglerna som finns, här är intern kommunikation en viktig bidragande faktor. Ansvar innebär att anställda är motiverade att ta sitt eget ansvar med att följa reglerna och hålla sig uppdaterade om informationssäkerheten.

Innehåll

1. Inledning ... 1
1.1 Bakgrund ... 1
1.2 Problemformulering ... 2
1.3 Frågeställning ... 2
1.4 Fallstudie ... 2
1.5 Syfte ... 2
1.6 Avgränsningar ... 3
2 Litteraturgenomgång ... 4
2.1 Upplägg av litteraturgenomgång ... 4
2.2 Riskanalys ... 6
2.2.1 Tillgångar ... 6
2.2.2 Hot ... 6
2.2.3 Sårbarheter ... 7
2.2.4 Attacker ... 7
2.3 CIA-triaden ... 8
2.4 Kritiska framgångsfaktorer ... 8
2.5 International Organization for Standardization ... 9
2.6 Security Management ... 10
2.6.1 Security Policys ... 11
2.6.2 Anställdas syn på informationssäkerhet ... 11
2.7 Ledning och organisationskultur ... 12
2.8 Kommunikation ... 13
2.9 Hot mot Informationssäkerheten ... 13
2.10 Silo inom säkerhet ... 14
2.11 Utmaningar inom informationssäkerhet – mänskliga faktorer ... 14
3 Metod ... 16
3.1 Metodval ... 16
3.2 Källkritik ... 17
3.3 Urval ... 17
3.4 Intervjustruktur ... 18
3.4.1 Pilotstudie ... 19
3.5 Enkät ... 22
3.6 Transkribering ... 23
3.7 Validitet ... 24

3.8 Etik 24
4. Resultat 25
4.1 Resultat av intervju med säkerhetschef 25
4.1.1 Informationssäkerhetsarbetet 25
4.1.2 Policys 26
4.1.3 Ledning – Ansvar – Kommunikation 26
4.1.4 Utmaningar 27
4.2 Resultat av intervjuer med chefer 27
4.2.1 Informationssäkerhetsarbetet 27
4.2.2 Policys 28
4.2.3 Ledning – Ansvar – Kommunikation 28
4.2.4 Utmaningar 28
4.3 Resultat av enkätundersökningar 29
4.3.1 Säkerhetschef 29
4.3.2 Managers 32
4.3.3 Anställda i Sverige 36
4.3.4 Internationellt anställda 39
5. Analys och Diskussion 43
6. Slutsats 49
6.1 Förslag till vidare studier 50
Bilaga 1 Enkät till Managers 51
Bilaga 2: Enkät till anställda i Sverige 53
Bilaga 3: Enkät till anställda internationellt 55
Bilaga 4: Transkribering av intervju med R1 57
Bilaga 5: Transkribering av intervju med R2 70
Bilaga 6: Transkribering av intervju med R3 75
Bilaga 7: Transkribering av intervju med R4 83
Bilaga 8: Information Security Policy vid företaget 88
Bilaga 9: Classification and handling of Information vid företaget 90
Bilaga 10: Information Security Management System vid företaget 99
Referenser 104

Tabeller

Tabell 2.1: Kategorisering av litteratur 4

Tabell 3.1: Respondenter 18

Tabell 3.2: Intervjuguide säkerhetschef (R1) 19

Tabell 3.3: Intervjuguide chefer 21

Tabell 3.4: Enkätundersökning 22

1. Inledning

Detta kapitel inleds med en övergripande presentation, där det i korthet redogörs för rapportens relevans och koppling till ämnet informationssäkerhet. Därefter presenteras aktuella problem inom området för att sedan resultera i det som rapporten huvudsakligen kommer att behandla och besvara. Sedermera kommer arbetet och dess ändamål att motiveras, för att slutligen ge en tydlig bild av det som ska avhandlas i kommande delar.

1.1 Bakgrund

Dagens organisationer är till stor del beroende av informationssystem för att kunna bedriva ändamålsenlig företagande. Informationssystemen medför att olika typer av risker måste kunna hanteras för att säkerställa att verksamheten inte drabbas av allvarliga konsekvenser (Bulgurcu et al, 2010). För att reducera riskerna använder verksamheter ofta tekniska lösningar, vilket förvisso förbättrar informationssäkerheten, men sällan eliminerar riskerna i sin helhet (Bulgurcu et al, 2010).

Studier påvisar att framgång inom området uppnås genom investeringar i både teknologi och personal (Bulgurcu et al, 2010). Den mänskliga faktorn är oftast den som enskilt utgör störst risk, vilket innebär att riktlinjer och policys måste finnas etablerade för att säkerställa att information inte hamnar hos tredje part (Bulgurcu et al, 2010). För att utforma ett regelverk som efterföljs behöver man förstå vilka motiverande faktorer som finns för anställda inom företaget.

Policy och riktlinjer utgörs av dokument vilka är vägledande för hur en organisation bedriver sitt arbete med informationssäkerhet. Dessa dokument tydliggör och definierar ansvarsområde samt beskriver hur verksamheten ska arbeta med informationssäkerhet för att detta ska vara i linje med affärsbaserade visioner och mål (Hönö & Eloff, 2002).

Svårigheter med att sammanställa ett sådant dokument förekommer då olika delar eller roller inom en verksamhet kan ha skilda åsikter i fråga om vad som anses vara av betydelse ur säkerhetssynpunkt. Detta tillsammans med den komplexitet som en välformulerad policy ofta innebär leder inte sällan till att ledningen utformar en policy efter fördefinierade mallar, kommersiellt tillgängligt material eller använder sig av policy liknande andra verksamheters (Hönö & Eloff, 2002). Det ligger i sakens natur att en policy som inte är utformad efter verksamhetens förutsättningar aldrig kommer leva upp till högsta nivå (Hönö & Eloff, 2002).

Kompetensen beträffande informationssäkerhet hos personer med ledande position inom ett företag, står i direkt relation till de strategier man har beträffande riskhantering och hur dessa bedrivs (Fenz & Ekelhart, 2009). Oberoende av den metodologi som tillämpas är syftet med riskhantering att värdera verksamhetskritiska tillgångar och sedan minimera riskerna så att dessa har en acceptabel risknivå (Fenz & Ekelhart, 2009).

Då informationssäkerhet ofta berör samtliga avdelningar av en verksamhet, kan det uppstå svårigheter med att avgöra vem eller vilka som är ansvariga för de olika delprocesserna som arbetet med framtagandet av en policy utgör. Detta är ytterligare ett moment som kan bidra till att policyn inte ringar in samtliga verksamhetskritiska aspekter.

1.2 Problemformulering

I dagsläget finns ett flertal teorier, metodologier, ramverk, standarder och koncept inom området för informationssäkerhet. Dessa baseras ofta på olika former av undersökningar där slutsatser kring ”best practices” kan variera. Detta skapar viss osäkerhet och lämnar plats för egna tolkningar i frågan, vilket kan innebära bristande informationssäkerhet vid tillämpandet av sådan metodik.

Problem som kan uppstå vid bristande informationshantering handlar bland annat om personlig integritet, säkerhetsklassat material, ekonomiska förluster och förtroende.

Större verksamheter kan även drabbas av så kallat silotänk där avdelningar arbetar med fokus på sin egen prestation, och bortser från faktorer som rör verksamheten i stort. Detta kan även innefatta aspekter som rör säkerhet och kan därför vara av intresse att titta närmare på.

1.3 Frågeställning

Hur förhåller sig arbetet med informationssäkerhet inom en organisation verksamt inom IKT med utvalda teorier inom området, och hur följer anställda de regelverk som finns uppsatta jämfört med hur organisationens ledning upplever att regelverken följs?

1.4 Fallstudie

Studien följer metoden för fallstudie då vi enbart valt att undersöka ett företag. Metodiken beskrivs mer ingående i kapitel 3. Anledningen till att undersökningen baseras på en fallstudie motiveras genom att den berörda organisationen opererar internationellt, har fler än hundra tusen anställda varav de flesta både arbetar och är utbildade inom området för IKT. Studien kommer att fokusera på olika nivåer och befattningar vilket bör förmedla ett brett spektrum av de synsätt på säkerhet som finns inom en del av miljön för IKT.

1.5 Syfte

Syftet med denna fallstudie är dels att granska utvalda teorier som finns inom området för informationssäkerhet, för att sedan jämföra valda delar med hur man arbetar med säkerhetsfrågor på ett internationellt företag. Vidare, kommer vi att undersöka anställdas syn och förhållningssätt till arbetsprocesser som involverar informationssäkerhet. Detta görs för att utröna hur individens tillämpning i det dagliga arbetet förhåller sig till de policys som finns uppsatta inom verksamheten. Med hjälp av den information som framkommer är vår förhoppning att kunna presentera faktorer inom en organisation som bidrar till både hög och

låg informationssäkerhet. Sedermera ska materialet i denna studie kunna användas för att utveckla arbetet inom olika organisationer verksamma inom IKT, när det gäller frågeställningar som rör anställda och skyddad data.

1.6 Avgränsningar

Arbetet avgränsas till ett specifikt företag och fyra av dess avdelningar vilka anses vara relevanta för ändamålet. Företaget bedriver verksamhet på olika platser runt om i världen, men på grund av begränsade resurser kommer vår undersökning främst vara inriktad på deras svenska filialer. Vi kommer i den mån det är möjligt att försöka utröna hur man arbetar med informationssäkerhet inom verksamheten i andra delar av världen.

2 Litteraturgenomgång

2.1 Upplägg av litteraturgenomgång

Här presenteras kort den valda litteratur och teori som det sedan redogörs mer för i kommande kapitel. Här presenteras även en uppdelning av dessa inom kategorier och deras relation till varandra. Syftet med detta är att ge en förståelse för relationen mellan de olika avsnitten hur och dessa är relevanta för studiens syfte och forskningsfråga.

Tabell 2.1: Kategorisering av litteratur

Kategori	Rubrik	Relevans
Informationssäkerhetsarbetet	Riskanalys	Riskanalys tar upp olika grundläggande delar av en riskanalys och innebörden av dessa för tex ett företag. Riskanalysen är en relevant del då denna kan användas som underlag för ett företags säkerhetsarbete, detta då analysen visar viktiga resurser och de hot som finns.
	CIA-triaden	CIA triaden beskriver en grundläggande modell för informationssäkerhet och är en relevant grund då dessa koncept genomsyrar flera andra delar i detta kapitel.
	Kritiska Framgångsfaktorer	Att identifiera kritiska framgångsfaktorer inom en verksamhet är av stor betydelse för att kunna uppnå de mål som finns uppsatta. Informationssäkerhet präglar alla nivåer inom en organisation och kan ofta härledas från de kritiska framgångsfaktorerna.
	ISO	ISO är en standard för hur bland annat företag bör arbeta gällande informationssäkerhet för att på ett bra sätt skydda sina resurser. Detta är högst relevant för forskningsfrågan och syftet då vi avser undersöka hur just ett företag arbetar med sin informationssäkerhet. ISO tas även upp i andra delkapitel i litteraturgenomgången.
Policys	Security Policys	Security Policys tar upp den mer praktiska tillämpningen av informationssäkerhetsarbetet. Detta sker i form av policys som beskriver olika regler och tillvägagångsätt för hur anställdas arbete ska utföras på ett sätt som är säkert. Detta är således ytterst relevant för studien då detta är vad de anställda faktiskt upplever i sitt dagliga arbete.
Ledning – Ansvar – Kommunikation	Security Management	Security Management beskriver informationssäkerhetsarbetet sett från ett ledningsperspektiv och de organisatoriska rollerna

		och system som bör finnas på plats för att övriga anställda inom organisationen ska kunna utföra sitt arbete och samtidigt inte bryta mot säkerheten. Vilket är relevant för studien då detta direkt påverkar det dagliga arbetet gällande informationssäkerhet inom organisationen.
	Ledning och organisationskultur	Organisationskultur har visat sig vara en stark bidragande faktor till hur information skyddas och hanteras inom ett företag. Chefer bör beakta detta i samband med att strategier för säkerhetsarbetet tas fram. Eftersom att denna uppsats till stor del bygger på information som framkommer vid intervju med säkerhetschef kan man anse att detta är relevant att redogöra för.
	Kommunikation	Kommunikation tar upp betydelsen av bra intern kommunikation inom organisationen. Detta är relevant då det är viktigt att där finns bra kommunikation gällande bland annat informationssäkerheten för att säkerställa att alla är på samma sida.
Utmaningar	Hot mot informationssäkerheten	Hot mot informationssäkerheten beskriver diverse hot som kan finnas gentemot en organisations informationssäkerhet och vad dessa kan bero på. Detta är relevant för studien då detta belyser vilka utmaningar som kan finnas för anställda i deras dagliga arbete i relation till organisationens informationssäkerhet.
	Silo inom Säkerhet	Eftersom information blivit en allt viktigare del av en verksamhet kan det vara intressant att förstå hur avdelningar som tidigare hanterade fysisk säkerhet nu även måste förstå hur information ska skyddas. Detta kan skapa viss silo-effekt och bör därför presenteras för att sedan kunna användas som underlag i diskussionsdelen.
	Utmaningar inom informationssäkerhet – Mänskliga faktorer	Genom att förstå hur människor ser på sig själv och den roll de har inom en organisation kan man hantera vissa av de svårigheter som kan tänkas uppstå när olika roller interagerar med varandra i arbetsprocesser. Av denna anledning är det viktigt att ur ett informationssäkerhetsperspektiv belysa de mänskliga faktorerna inom en verksamhet.

Relationen mellan de olika kategorierna kan ses genom att grunden för organisationens informationssäkerhet har en grund i de teorier och modeller som diskuteras i kategorin **Informationssäkerhetsarbetet** vilket sedan leder till den praktiska tillämpningen i form av **Policys.** Därefter flyttas fokuset på **Ledning – Ansvar – Kommunikation** där det istället handlar om hur man efterföljer dessa policys och vem som har ansvaret att följa dem. Här påpekas även betydelsen av bra kommunikation för att vidare se till att arbetet med informationssäkerhet är så bra den kan vara. Slutligen leder detta till **Utmaningar** där det kontinuerliga arbetet med att förbättra informationssäkerhet pågår. Dessa utmaningar kan då vara allt från bristfällig kommunikation inom organisationen, externa hot och liknande.

2.2 Riskanalys

Riskanalys är enligt LeVeque (2006) ett viktigt verktyg för företag genom att på ett effektivt sätt ge företaget ett bra mandat till att se över sina informationstillgångar. Detta kan inkludera att identifiera och vidare försäkra att tillgångarna är ordentligt säkrade från potentiella hot. I riskanalysen bör det framkomma värdet på tillgången som ska skyddas, hur stort hotet är och kostnaden för att minska hotet (LeVeque, 2006).

2.2.1 Tillgångar

Det första som behöver göras i en riskanalys är enligt Gollman (2011) att identifiera vilka tillgångar som ska skyddas. Detta kan vara hårdvara såsom datorer, servrar, telefoner, nyckelkort och så vidare.

Det kan även vara mjukvara såsom diverse operativsystem, applikationer, databassystem, programkod och så vidare (Gollman, 2011). Det kan också slutligen vara data och information som är tillgångar. Detta kan då vara kundinformation, patent och annan liknande information.

Identifierande av dessa resurser bör enligt Gollman (2011) vara en relativt enkel och systematisk uppgift, utmaningen i detta är att bestämma värdet på tillgångarna, detta är särskilt sant när det gäller information och data.

2.2.2 Hot

Ett hot är enligt Gollman (2011) en oönskad negativ påverkan av tillgångarna. Det finns flertalet olika sätt att negativt påverka tillgångar, till exempel:

- Någon kan låtsas vara en anställd för att få tillgång till tillgångar.
- Manipulering av data. Detta kan vara både sabotage eller ett sätt att öppna upp för vidare attacker genom att ändra inställningar för säkerhet och liknande.
- Spridning av information. Information från företaget sprids till personer utanför företaget. Detta kan vara till exempel affärshemligheter som antingen säljs eller delas av misstag.
- Denial of Service. Detta förhindrar åtkomst till tillgångarna. Till exempel kan ett företags web shop stängas ner vilket förhindrar kunder från att handla.

Man kan vidare kategorisera baserat på var hotet kommer ifrån, kan det komma inifrån organisationen? Är det utanför? Tidigare anställda och så vidare.

2.2.3 Sårbarheter

Enligt Gollman (2011) är sårbarheter svagheter inom system som antingen medvetet eller omedvetet kan användas för att skada företagets tillgångar. I ett IT system skulle sådana sårbarheter kunna vara dåliga lösenord, program med kända fel, svaga brandväggar och liknande.

Det är därför enligt Gollman (2011) viktigt att ha automatiska och systematiska processer eller system för att upptäcka sådana sårbarheter. Detta kan göras med mjukvara.

Det är även väsentligt att dessa program prioriterar de sårbarheter som har störst påverkan på företagets tillgångar. Till exempel är det viktigare att åtgärda en sårbarhet som kan ge åtkomst till forskningsdokument än en annan sårbarhet som bara ger tillgång till ett användarkonto utan behörigheter.

2.2.4 Attacker

En attack kan beskrivas som att hotet har blivit verklighet (Gollman, 2011). En attack kan gå igenom flera steg för att nå ett slutgiltigt mål, där de första stegen kanske inte är lika allvarliga. Det kan börja med att försöka få ett visst lösenord för att sedan jobba sig vidare in i systemen för att komma åt känslig information.

Hur farlig attacken är beror på ett fåtal faktorer, hur sannolik den är att hända, sannolikheten att den lyckas, och skadan som kan ske av attacken. Gollman (2011) beskriver den så kallade DREAD metoden för att beskriva attacker.

- Damage potential – Vilket relaterar till värdet av de påverkade tillgångarna.
- Reproducibility – Attacker som är enkla att reproducera är mer sannolika att ha kommit från egna miljön än utifrån.
- Exploitability – Beskriver vad som krävs för att genomföra attacken, vilken expertis, vilka resurser som krävs och så vidare.
- Affected Users – Hur många tillgångar som påverkas av attacken.
- Discoverability – Kommer attacken upptäckas?

2.3 CIA-triaden

En av de mer grundläggande modellerna inom informationssäkerhet är enligt LeVeque (2006) den så kallade CIA-triaden. CIA står för **Confidentiality, Intergrity** och **Availability**.

Confidentiality innebär hur informationen ska skyddas (LeVeque, 2006). Detta kan vara vem som får tillgång till informationen, vem som inte får tillgång och liknande. Men det kan även innebära hur den personliga integriteten ska skyddas. För att förenkla hur viktig informationen som ska skyddas är kan denna delas upp i kategorier, vilket då gör det enklare att prioritera och skydda de mest viktiga (LeVeque, 2006).

Integrity är hur informationen underhålls. Vilket innebär att informationen måste hållas uppdaterad, korrekt, trovärdig och upp till företagets standards (LeVeque, 2006). Ett sätt att försäkra sig om detta är att enbart låta auktoriserad personal modifiera denna typ av data.

Availability innefattar att användare och liknande alltid ska ha tillgång till informationen när det behövs (LeVeque, 2006). Vilket i sin tur innebär att alla underliggande system såsom säkerhet, lagring, åtkomst och liknande måste vara operativa för att tillgängligheten ska gälla. Det betyder även att det behöver finnas system som hanterar återhämtning vid olyckor och liknande som kan begränsa tillgången till data (LeVeque, 2006).

2.4 Kritiska framgångsfaktorer

Det primära syftet med att bedriva en verksamhet är att möta de förväntningar som finns hos aktieägare, kunder, anställda och affärspartners (Caralli, 2004). Genom att förmedla organisationens mål kan man ge konkret form åt syfte, vision och värderingar. För att leva upp till de uppsatta målen krävs en strategi för hur man på ett effektivt sätt uppnår delmål inom en viss tidsperiod. Dessa delmål omvandlas sedan till aktiviteter inom organisationens olika nivåer vilket säkerställer att hela verksamheten har en gemensam fokus på de uppdrag som ska utföras (Caralli, 2004).

Kritiska framgångsfaktorer (Critical successfactors, ”CSF”) definierar de områden som verksamheten är mest beroende av (Caralli, 2004). Dessa framgångsfaktorer beaktas noga av personer i olika chefspositioner i samband med att aktiviteter planeras vilka sedermera ska leda till att delmål uppnås. Ledning av säkerhetsarbetet inom en organisation är ett utav flera affärsrelaterade problem som måste hanteras för att uppnå organisationens mål. Oavsett om organisationens tillgångar är materiella eller immateriella behövs en strategi som kan implementeras, mätas och uppdateras i takt med att organisationen växer eller förändras. Effektiviteten av säkerhetsarbetet bygger till stora delar på hur väl den stödjer och anpassats till mål och CSF (Caralli, 2004).

En av de främsta uppgifterna för chefer på verkställande nivå är att hantera risker som är genomgående för hela verksamheten (Caralli, 2004). Av denna anledning måste strategier som rör säkerhet utformas och presenteras på ett sätt som fångar verkställande chefers uppmärksamhet, där risker och konsekvenser betonas. Genom ett sådant förfarande kan man fokusera på att skydda organisationens mest värdefulla tillgångar. Tillvägagångssättet med fastställandet av CSF inom verksamheter började under tidigt 80-tal och hade då ett brett användningsområde. På senare tid har denna metodik även börjat användas inom

verksamheter där informationssystem präglar organisationens dagliga verksamhet för att understödja värdeskapande processer i form av en kontinuerlig uppföljning av de olika faktorerna som anses vara mest kritiska för att nå framgång (Caralli, 2004).

Eftersom chefer definierar både mål och CSF inom en organisation skapas det starka förbindelser mellan dessa två, där man ofta kan härleda uppnådda mål eller delmål från en eller flera kritiska framgångsfaktorer (Caralli, 2004). Denna kardinalitet påvisar beroendet mellan mål och CSF samt betydelsen av CSF inom organisationer. Uppsatta mål inom en verksamhet är inte sällan ett resultat av system som mäter prestation och effektivitet. Detta kan leda till att fokus hamnar på vad man kan göra ifall dessa mål uppnås, istället för att skapa en strategisk plan för hur man bidrar till att målen verkligen uppfylls (Caralli, 2004).

Där finns ett flertal svårigheter med att implementera en strategi som rör säkerhetsarbete då verksamheter ofta tenderar att överlåta denna del till den tekniska avdelningen inom organisationen, vilket i sin tur leder till ett problem då denna avdelning sällan lyckas sammanfoga sitt eget arbete med de övergripande mål som blivit fastställda på verkställande nivå. I de fall då säkerhetsavdelningen eller delar av denna arbetar på konsultbasis, skapas ytterligare en barriär mellan verksamheten och säkerhetsfunktioner. Ett annat problem som arbetet med informationssäkerhet bidrar till, är det faktum att ett flertal ser det som en aktivitet som inte är värdeskapande eller bidrar till tillväxt (Caralli, 2004).

En verksamhet som förstår sina styrkor och svagheter vad gäller säkerhet och därefter är villiga att arbeta aktivt med dessa delar, har möjlighet att skydda verksamheten samtidigt som man kan bidra till att övergripande mål blir uppfyllda. Med rätt ledning kan detta arbete till och med leda till att man skapar sig konkurrensfördelar gentemot andra aktörer inom samma bransch (Caralli, 2004).

2.5 International Organization for Standardization

”International Organization for Standardization” eller ISO är en internationell icke-statlig organisation vars arbete omfattar industriell och kommersiell standardisering (ISO, 2018). ISO har flera olika kategorier av standarder inklusive en för informationssäkerhet, ISO/IEC 27000.

ISO/IEC 27000 är en familj av olika standards med syfte att hjälpa organisationer skydda sina resurser (ISO, 2018). ISO/IEC 27001 är den standard inom familjen som ger krav på *Information Security Management Systems (ISMS).* Ett ISMS är ett tillvägagångssätt för organisationer att hantera information eller resurser så att denna förblir säker.

I ISO/IEC 27001 tas det upp flera punkter väsentliga för studien, dessa är bland annat (ISO, 2013),

- Leadership and commitment
- Policy
- Organizational roles, responsibilities and authorities
- Actions to address risks and opportunities
- Information security risk assessment

Vidare föreslås olika åtgärder för att lösa de situationer som beskrivs i dokumentets diverse punkter (ISO, 2013).

Detta är upphovsrättsskyddat material som vi fått ta del av, varpå vi inte kan beskriva detta i mer detalj än det som är ”offentligt”. Fullständig dokumentation finns tillgänglig att köpa från ISO.

2.6 Security Management

Enligt Dieter Gollman (2011) är informationssäkerhet inte ett problem som enbart går att lösa med tekniska lösningar. Det måste finnas ansvar inom organisationer för att hantera och lösa sådana problem. Anställda måste följa de fastställda regler och lagar som finns, både inom organisationen samt nationella lagar (Gollman, 2011). Ansvaret att detta efterföljs ligger hos organisationens ledning.

Att skydda organisationens resurser, bland annat patent, finansiella data, kunddata, produktplaner och så vidare, är oerhört viktigt (LeVeque, 2006). Det är därför viktigt för organisationen att anställda är motiverade och engagerade i organisationen och därmed villiga att samarbeta och följa de uppsatta reglerna inom organisationen för att säkerställa informationssäkerheten (Gollman, 2011). Det kan dock förekomma att dessa regler och protokoll inte efterföljs av andra anledningar. Till exempel kan dessa protokoll och regler förhindra anställda från att på ett optimalt och effektivt sätt utföra sina arbetsuppgifter, detta kan då enligt Gollman (2011) leda till att dessa regler ignoreras eller kringgås för att då undvika hindren. Detta är särskilt sannolikt om dessa regler kommer från en annan avdelning i organisationen och inte från högre upp i organisationens ledning (Gollman, 2011).

Därför är det enligt Gollman (2011) och LeVeque (2006) viktigt för organisationen att ha etablerade ansvarsroller som då säkerställer att dessa regler efterföljs och har ledningens stöd för att vidare visa tyngden och betydelsen av dessa regler och protokoll. Ett exempel för att visa detta är att ha en grundläggande policy undertecknad av ledningen som del av anställdas handbok/manual med kort information om de grundläggande tankarna kring organisationens informationssäkerhet (Gollman 2011). Tanken är inte att alla ska bli säkerhetsexperter men det är viktigt att alla har en grundläggande uppfattning om varför säkerheten är viktig för organisationen och därmed dem själva. Det som även bör tas upp i denna grundläggande policy är vad som förväntas av de anställda och vilka metoder (good practice) de bör följa för att säkerställa informationssäkerheten i organisationen.

Vidare sätt att uppmuntra och öka medvetenheten gällande informationssäkerheten är att genomföra så kallade ”*Security Awareness*” (Gollman, 2011) program där denna information delges.

2.6.1 Security Policys

Enligt Gollman (2011) är Security Policys ett av de viktigare koncepten i informationssäkerhet. En Security Policy är en redogörelse som förklarar vad som ska skyddas och hur detta ska ske. Dessa policys kan vara generella regler såsom att anställda ska bära sina ID-brickor på ett synligt sätt, olika tillgång till lokaler beroende på vilken avdelning man jobbar och så vidare (Gollman, 2011). Det kan även vara mer specifika saker såsom hur vissa dokument ska hanteras, vilka som har tillgång till vilka dokument, hur får jobb email användas, lösenordshantering och liknande. Dessa policys kan verkställas genom exempelvis tekniska lösningar, såsom att mjukvara stoppar obehöriga användare från att få tillgång till dokument och liknande. Det kan även förekomma att det finns olika policys på plats baserat på vilken avdelning eller roll inom företaget man har (LeVeque, 2006), vissa avdelningar kan ha hårdare krav på säkerhet än andra.

Dessa policys ska enligt LeVeque (2006) vara utformade på så sätt att de inte blir ett hinder för anställdas arbete, men inte heller vara för slappa. Om de hindrar arbetet är det hög sannolikhet att anställda hittar genvägar runt dessa för att slippa krånglet och därmed utsätter organisationen för onödiga risker.

Som riktmedel för hur dessa policys ska utformas för bästa möjliga resultat, alltså att anställda finner förståelse och motivation att efterfölja dessa, föreslår LeVeque (2006) fyra viktiga punkter en policy ska innehålla för att uppfylla dessa mål.

- *Purpose* – Denna punkt bör beskriva syftet med policyn och vad den skyddar.
- *Scope* – Denna punkt beskriver omfånget för policyn, det vill säga vilka resurser som inkluderas i policyn. Det kan till exempel vara en policy som omfattar alla patent eller alla bärbara datorer. Samt vilka anställda som förväntas efterfölja denna policy.
- *Responsibilities* – Här beskrivs vilka anställda, genom roll, titel, avdelning och så vidare, som är ansvariga för att policyn efterföljs.
- *Compliance* – Här specificeras vilka åtgärder som kan tas om en anställd bryter mot dessa policys och regler.

2.6.2 Anställdas syn på informationssäkerhet

Då alla tekniska säkerhetslösningar behöver drivas och användas av personal är det omöjligt för ett företag att helt förlita sig på enbart tekniska lösningar (Chang & Lin, 2007). Detta då personal enligt Chang & Lin (2007) också är säkerhetsproblem. Det är därför viktigt med en bra security management policy och att dess tillämpning efterföljs av personalen på företaget.

För att säkerställa att företagets policys och regler efterföljs är det enligt Chang & Lin (2007) viktigt att företaget har en kultur och miljö som uppmuntrar säkerhetstänket.

Enligt Ashenden (2008) har företagets Information Security Manager en viktig roll i arbetet med att utveckla företagets säkerhetskultur. Denna roll innebär enligt Ashenden (2008) inte bara att driva tekniska lösningar utan bör istället uppmuntra kommunikation och dialog med annan personal och användare av systemen på företaget. Det finns dock utmaningar med ett sådant tillvägagångssätt, till exempel om chefen (manager) uppmuntrar personalen till att själva ta mer ansvar och beslut om säkerheten, gentemot en striktare kontrollerande miljö, kan detta till en början leda till initiala händelser som kan ha negativ påverkan på

informationssäkerheten. Detta är dock något som bör förbättras över tid efter att lärdomarna av dessa misstag har lärts in (Ashenden, 2008).

2.7 Ledning och organisationskultur

Då informationssystem ständigt används som stöd inom organisationer blir frågor som rör informationssäkerhet allt viktigare (Chang & Lin, 2007). Detta gäller i synnerhet verksamhet som bedrivs inom den tekniska sektorn. De stora mängder data som lagras i elektronisk form behöver inte alltid vara en tillgång, utan kan även vara ett orosmoment då verksamheten blir sårbar vid händelse av att informationen missbrukas. Under de senaste åren har företag fokuserat på den tekniska aspekten av informationssäkerhet genom att använda sig utav detekteringssystem, kryptering och kontroll av åtkomst. Detta har bidragit till att datorstyrda attacker blivit färre, men påvisar samtidigt att de finansiella förlusterna trots allt inte minskat när man beaktar all informationshantering inom organisationen (Chang & Lin, 2007). Detta beror sannolikt på att organisationen inte arbetat med riskhantering internt, och att medarbetares engagemang varit lågt i arbetet med informationssäkerhetssystem. Den kultur som råder inom företaget är den enskilt viktigaste faktorn som styr ifall man når framgång, eller ifall man misslyckas med informationshanteringen. Med anledning av detta bör chefer beakta organisationskulturen i samband med att strategier för informationshantering tas fram (Chang & Lin, 2007).

Eftersom informationsteknologi blivit en integrerad del av modernt företagande har detta lett till att informationssäkerhet blivit en nyckelkomponent vad gäller planering och förvaltning (Chang & Lin, 2007). Antalet digitala transaktioner har ökat tack vare Internet vilket medfört att frågor som rör sekretess, integritet och tillgänglighet av information blivit allt viktigare att bemöta och hantera. En undersökning som gjordes utav ”Information Security Magazine” år 2002, vilken var baserad på 2196 anställda som arbetade med informationssystem, påvisades att 32 procent av problemen med informationshantering berodde på antingen auktoriserade användare eller organisatoriska faktorer och att det främst är vårdslöshet som orsakat problem. Detta är således omständigheter som till stor del kan elimineras med hjälp av att rätt säkerhetskontroller identifieras, implementeras och underhålls (Chang & Lin, 2007).

Ett effektivt kontrollsystem kan vara komplicerat och resurskrävande vilket många företag inte klarar av att bemästra (Chang & Lin, 2007). I en sådan situation kan man med fördel använda sig utav standarder som finns framtagna för informationssäkerhet. En sådan är ISO17799 som antogs som internationell standard år 2000 (se kapitel 2.5). Även om denna standard inte ger några garantier för absolut säkerhet är det en bra grund för att implementera och vidareutveckla säkerhetsfunktioner inom en verksamhet. Arbetet med informationssäkerhet inkluderar dels tekniska lösningar, dels de människor som ska hantera tekniken. En väl utformad strategi för informationshantering handlar om att inkludera tekniken och människorna i den organisationskultur man befinner sig i (Chang & Lin, 2007).

2.8 Kommunikation

Enligt Ingelmo Palomares et al (2018) är intern kommunikation inom företaget en viktig komponent för flera aspekter av företagets välmående. Bland annat bidrar bra kommunikation till ökad arbetsglädje, ökad prestanda och liknande. Vidare är den interna kommunikationen viktig för att säkerställa att anställda utför de arbetsuppgifter de blivit tilldelade och driver företagets konkurrenskraft. Det är även viktigt att denna kommunikation är integrerad i ledningsstrukturen och i hur ledning arbetar med sina anställda (Ingelmo Palomares et al, 2018). Företagets interna struktur och även kultur spelar en viktig roll för hur effektiv den interna kommunikationen är.

Genom att använda och integrera sociala verktyg in i de mer traditionella ledningssystemen (Management Systems) möjliggör man för att enklare öppna upp för anställda att enklare dela sin expertis och idéer och så vidare (Ingelmo Palomeras et al, 2018). Detta kan då enligt Ingelmo Palomeras et al (2018) leda till ökad produktivitet, underlättar för öppen innovation, informationsdelning, engagemang och så vidare. Det är dock en del hinder på vägen som kan göra det svårt att implementera ett bra sådant här socialt verktyg, bland annat kan anställdas syn på arbetsklimatet eller kulturen inom företaget förhindra denna typ av kommunikation. Detta kan då exempelvis vara relationen mellan chefer och anställda. Det kan även leda till att anställda inte lyckas ”koppla ifrån” detta sociala nätverk/verktyg på sin fritid och då bli stressade och utbrända på grund av detta.

2.9 Hot mot Informationssäkerheten

Hot mot en organisations informationssäkerhet kan komma från flera olika källor (Gollman, 2011), bland annat kan det vara interna hot, det vill säga avsiktliga eller oavsiktliga handlingar som kan riskera organisationens informationssäkerhet. Det kan även vara externa hot såsom andra organisationer, hackers och så vidare.

Enligt D’Arcy et al. (2009) är ett av de största hoten mot organisationens informationssäkerhet internt missbruk av informationssystem (IS) resurser. Enligt studien är ca 50-75% av alla incidenter relaterade till informationssäkerhet grundade på faktorer från inuti organisationen. På grund av denna höga andel interna hot mot säkerheten är det därför viktigt att förstå hur dessa kan minimeras (D’Arcy et al, 2009).

De interna hoten mot organisationen kan som nämnts vara avsiktliga eller oavsiktliga. Enligt Wall (2013) kan de avsiktliga hoten vara bland annat anställda som egentligen jobbar för ett annat företag eller tredje part och då ”spionerar” åt detta företag, eller gör detta för egen vinning. Det skulle även kunna vara missnöjda anställda som vill hämnas. De oavsiktliga hoten kan då vara anställda som råkar göra misstag som i sin tur kan riskera informationssäkerheten (Wall, 2013). Ett ytterligare exempel på oavsiktliga hot kan vara att anställda inte följer de uppsatta regler och policys som finns och därmed riskerar säkerheten. Genom detta agerande riskerar anställda att kunna bidra till läckor av känsliga data (Wall, 2013). Att anställda inte följer dessa utsatta policys kan bland annat bero på antingen bristfällig kunskap om de utsatta regler och policys som finns eller att den anställde väljer att kringgå dessa i alla fall för sin egen bekvämlighet (Wall, 2013). Det är även möjligt att dessa policys kringgås för att lättare kunna utföra sina arbetsuppgifter (Gollman, 2011).

När det gäller externa hot kan dessa bland annat grunda sig i bristande kunskaper från anställda eller brist på medvetenhet om informationssäkerheten och vad som sägs utanför företagets ”mark” (Wall, 2013). Bland annat kan företaget utsättas för risker genom att anställda oavsiktligt avslöjar information, använder sig av ”dåliga” lösenord eller aldrig uppdaterar dessa, använder sig av offentlig post för att skicka och leverera känsliga data/material.

2.10 Silo inom säkerhet

Under 90-talet förändrade organisationer sitt förhållningssätt till vad som ansågs vara tillgångar inom verksamheter (Rahman & Donahue, 2010). Tidigare hade man betraktat tillgångar som fysiska föremål vilka fanns inom organisationens besittning (Rahman & Donahue, 2010). Dessa skyddades med hjälp av bland annat kameraövervakning, vakter och inpasseringskort (Rahman & Donahue, 2010), och avdelningarna som ansvarade för säkerheten bestod ofta av personer med tidigare bakgrund inom rättsväsendet. Med hjälp av teknologins utveckling skapades nya kommunikationsvägar vilket medförde att man började bli införstådd med att information var organisationens största tillgång (Rahman & Donahue, 2010). För att skydda informationen från obehöriga bildades avdelningar med inriktning på informationssäkerhet (Rahman & Donahue, 2010). Med tiden visade det sig att traditionellt säkerhetsarbete och informationssäkerhet började växa samman i olika former vilket medförde utmaningar för organisationerna. Konvergens är den term man använder sig av när man talar om både informationssäkerhet och fysisk säkerhet inom en verksamhet, och definieras som ”en trend med inverkan på globala företag där man identifierar risker och ömsesidigt beroende mellan affärsfunktioner och processer inom företaget samt hur aktiviteter bör utvecklas för att hantera dessa risker” (Rahman & Donahue, 2010). En betydande anledning till att arbeta konvergent är det faktum att hot i någon mening riktade mot ett företag ofta berör hela verksamheten. På så vis kan man säkerställa att nödvändig information når alla berörda parter (Rahman & Donahue, 2010).

2.11 Utmaningar inom informationssäkerhet – mänskliga faktorer

När man talar om utmaningar i form av mänskliga faktorer måste man beakta både personens roll inom verksamheten samtidigt som personens personliga egenskaper såsom inställning och uppfattning (Ashenden, 2008). Med detta som utgångspunkt kan man titta på samtliga individer inom en organisation, från användare till säkerhetsansvarig och styrelsemedlemmar. Tillsammans skapar dessa personer en företagskultur vilket kan definieras som ett mönster av antagande som personer inom företaget kommer använda sig utav för vägledning i situationer de inte är bekanta med sedan tidigare. Enligt Ashenden (2008) finns det tre olika dimensioner av organisationskultur, dessa är observerbart beteende av individer, normer samt attityd och uppfattning. En individ inom en organisation kan förenklas till något som är en kombination av personlig och social identitet tillsammans med den affärsrelaterade roll man blivit tilldelad (Ashenden, 2008).

Den primära utmaningen som präglar allt företagande är att verksamhetens resurser ska fungera på ett sätt där de ständigt presterar på sitt maximala (Ashenden, 2008).
Termen ”resurs” innefattar allt från ekonomi, egendom och människor till organisationens struktur, hur processer är implementerade och hur relationer inom verksamheten fungerar.

Utmaningen i att få dessa resurser till att fungera blir ännu svårare i takt med en globaliserad marknad, samt ny teknologi och den hastighetsökning som tillkommer med detta. Organisationer har nu förstått att en av de kritiska faktorerna är att integrera kunskap. Dessvärre är stora delar av den kunskap som finns inom en organisation dold och endast tillgänglig för de individer som besitter den. Enligt Ashenden (2008) kan detta hanteras genom att anställda inom organisationen kan få olika roller vid olika tidpunkter för att på så vis få åtkomst till rätt information och kompetens vid en given tidpunkt. Detta kan dock leda till konflikter och ett utdraget beslutsfattande men kan hanteras genom att man skapar en obalans i form av begränsad tillgång till finansiella resurser. Ett sådant tillvägagångssätt leder till att man skapar en form av nätverksstruktur och frångår den hierarkiska modellen (Ashenden, 2008).

Området för informationssäkerhet har breddats de senaste åren, från att ursprungligen ha handlat om den tekniska aspekten av IT-säkerhet, till att sedan komma att handla mer om hur man skyddar organisationen i sin helhet (Ashenden, 2008). Informationssäkerhet handlar inte uteslutande om att värna om integritet och sekretess, utan även att kunna kontrollera att information utbyts och sprids på rätt sätt inom en miljö som anses vara utsatt för förändring och påfrestning. Då informationssäkerhet utvecklas till en inbyggd funktion inom organisationer och existerar i någon form på varje nivå krävs det en väldefinierad strategi för dess hantering (Ashenden, 2008).

ISO 27001 definierar förvaltning av informationssäkerhet som ”den del av det övergripande förvaltningssystemet, baserat på en affärsstrategi, som etablerar implementerar, driver, övervakar, granskar, underhåller och förbättra informationssäkerheten.”. Standarden anger även att detta inkluderar ”organisatorisk struktur, policies, planerandet av aktiviteter, ansvar, utövning, procedurer, processer och resurser. Denna standard implementeras för att säkerställa att det finns ett konsekvent sätt att bemöta frågeställningar som rör informationssäkerhet. Genom att använda sig utav denna standard kan man försäkra aktieägare om att arbetet med säkerhet hanteras på ett effektivt sätt (Ashenden, 2008).

3 Metod

3.1 Metodval

Metodiken för denna studie är till en del baserad på "*Case Study Research"* av Robert K. Yin (2014) då studien till stor del uppfyller definitionen av just en fallstudie. Yin (2014, s. 16-17) tar upp definitionen i två delar,

1. *A case study is an empirical inquiry that*
    - *investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when*
    - *the boundaries between phenomenon and context may not be clearly evident*
2. *A case study inquiry*
    - *copes with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result*
    - *relies on multiple sources of evidence, with data needing to converge in a triangulating fashion, and as another result*
    - *benefits from the prior development of theoretical propositions to guide data collection and analysis.*

I linje med denna definition (Yin, 2014) är vår studie en fallstudie. Detta då flera av punkterna direkt uppfylls i studiens metodik och diverse kapitel. Då flertalet av punkterna i ovanstående definition (Yin, 2014) direkt uppfylls i studiens metodik och diverse kapitel är vår studie således en fallstudie. Bland annat är studien i ett nutida sammanhang på ett isolerat fall, det vill säga ett specifikt företag. Studien sammanfogar flera data-punkter såsom kvalitativa undersökningar, kvantitativa undersökningar, samt sekundärdata i form av företagets interna dokument. Vidare har dessa undersökningar och resultat en direkt koppling till den litteraturgenomgång som gjorts i kapitel två samt de interna dokumenten (bilagor 8-10).

För att samla in data baseras metoden på en kvalitativ undersökningsmetod men har även inslag av kvantitativa undersökningar (Jacobsen, 2002). De kvalitativa undersökningarna valdes för att bidra med bredare och djupare insyn inom ämnet och vidare bidra med inblick i studiens frågeställning. Den kvalitativa undersökningen består av ett fåtal intervjuer med individer som bedömts som viktiga för studiens syfte, detta då de bland annat har positioner inom företaget direkt relaterade till informationssäkerhet samt ansvarspositioner, plus en studie av företagets dokumentation rörande informationssäkerhet. Intervjuerna följer en semi-struktur vilket öppnar upp för en mer öppen diskussion och tillåter på så sätt respondenterna att själva leda till det som de anser vara viktigt för frågan. Frågorna är upplagda på så sätt att de guidar respondenterna till de ämnen och situationer vi vill undersöka, detta lämnar även utrymme för förtydligande och uppföljande följdfrågor vid behov.

Bakgrunden till intervjufrågorna har en deduktiv ansats (Jacobsen, 2002), vilket då innebär att frågorna är baserade på teori för att därmed guida oss fram till ”rätt” frågor under empirin. Dessa teorier och litteraturen ger en grund till att vidare analysera det empiriska resultatet.

De kvantitativa undersökningarna görs för att få en generell överblick över vilken uppfattning som finns på företaget rörande säkerhetsfrågor. Dessa frågor baseras även de på de teorier och litteratur från kapitel två, samt den information som framkommer vid intervju med en av

företagets högre säkerhetschefer samt delar av företagets dokumentation rörande informationssäkerhet (se kapitel 3.7). Detta för att bättre anpassa frågorna till den faktiska situationen hos företaget. Detta ger oss en möjlighet att kunna analysera och jämföra teorin med företagets fastställda policys samt då hur dessa upplevs och efterföljs i praktiken.

3.2 Källkritik

De källor som använts har varit en kombination av kurslitteratur, vetenskapliga artiklar, och övrig litteratur inom området. De vetenskapliga artiklarna har framkommit genom sökningar i bland annat databaser som LUBsearch och GoogleScholar. Då dessa artiklar har publicerats i etablerade vetenskapliga journaler och finns i LUB databasen anses dessa som trovärdiga källor.

Vidare värderas källorna för att fastställa deras kvalité och värde för att säkerställa deras kvalité och relevans för studien. Denna källvärdering följer den metod som föreslås enligt Rienecker & Stray Jörgensen (2014).

3.3 Urval

Då studien är baserad på informationssäkerheten i relation mellan teori och verklighet hos företag är studien begränsad till enbart ett företag. Det valda företaget för studien valdes då de har en prominent marknadsposition i den globala IKT marknaden och väletablerad informationssäkerhet och IT säkerhet. Valet att enbart studera ett (1) företag gjordes då detta ger oss möjligheten att gå mer djupgående och kvalitativt än om vi hade studerat flera företag. Urvalet av respondenter gjordes baserat på roll och avdelning inom företaget. Viktigast för studien var respondenten med rollen som säkerhetschef för företaget i fråga. De övriga respondenterna har ledande/ansvarsroller för avdelningar såsom: Forskning, Patent samt Produktutveckling. Alla med påtagliga behov av hög informationssäkerhet.

Enkäterna är gjorda som onlineformulär för att förenkla spridningen samt löpande kunna avläsa inskickade svar. Respondenterna för dessa är de anställda inom de olika avdelningar vi genomfört intervjuer med för att bättre kunna jämföra och analysera skillnaderna i hur det ska fungera och hur det faktiskt fungerar i praktiken. Vidare gjordes även en enkät för chefer inom företaget för att se hur de tror anställda agerar i situationerna beskrivna i enkäten.

Detta ger en tydlig blick om hur ledningen tror sina anställda agerar jämfört med hur de faktiskt agerar.

De respondenter vi hade till våra intervjuer presenteras i följande tabell.

Tabell 3.1: Respondenter

	Roll	**Datum för intervju**	**Var**	**Längd**
Respondent 1	Säkerhetschef	2018-04-12	Företagets lokaler	1:04:27
Respondent 2	Ansvarig mjukvaruutveckling + Platschef	2018-04-19	Företagets lokaler	19:18
Respondent 3	Forskningschef	2018-04-19	Företagets lokaler	30:55
Respondent 4	Director of Patents (*förkortat pga. säkerhetsskäl)*	2018-04-20	Företagets lokaler	10:14

3.4 Intervjustruktur

De personliga intervjuerna utformades på ett sätt där ledande frågor kunde undvikas i den mån det var möjligt. Detta gav utrymme för respondenten att på eget bevåg utveckla svar och tankegångar kring de frågeställningar som behandlades vid en given tidpunkt.

Frågorna i intervjun kan delas upp i sex kategorier, se tabell 3.2 & 3.3. Dessa kategorier baseras på kategorierna från Upplägg av litteraturgenomgång (kapitel 2.1). Den första raden inom “kategori” avser respondentens bakgrund och personens roll inom företaget. Efterföljande rader är baserade på den teori och litteratur som undersökts och är indelade i olika kategorier baserat på vilket område de avser. Slutligen en avslutande kategori som ställs öppet ifall det är något respondenten vill berätta eller liknande.

Genom att kategorisera frågorna blir det enklare att dra kopplingar till teorin och litteraturen samt att få en tydlig struktur vid redovisning samt analys av resultat.

Intervjuerna följer inte konsekvent de frågor som förberetts då frågorna kan ha kommit i annan ordning samt att vissa oplanerade följdfrågor har tillkommit.

Intervjuerna genomfördes enskilt i företagets lokaler enligt önskemål. Intervjuerna spelades in för att senare kunna transkriberas (se kapitel 3.6).

Det genomfördes fyra intervjuer, den första intervjun var med en av företagets säkerhetschefer. Denna intervju var en mer djupgående pilotstudie och längre än de andra och var en bidragande faktor till hur frågor utformades till de andra respondenterna samt enkätundersökningen. På grund av detta följer två intervjuguider (tabell 3.2 & 3.3), en till Respondent 1 (R1), dvs säkerhetschef och en till övriga respondenter (R2, R3, R4).

3.4.1 Pilotstudie

Syftet med en pilotstudie är att samla in data i begränsad omfattning för att sedan använda resultaten för vidare forskning i större skala. Pilotstudier inom samhällsvetenskaplig forskning kan även innebära förprövning av ett visst forskningsinstrument. Studien kan baseras på antingen kvalitativa eller kvantitativa metoder (Tejlingen & Hundley, 2001). Med hjälp av den information som framkommer vid djupintervju med säkerhetschefen för det företag som undersöks, kommer frågeformulär att utformas. På så sätt kommer nyckelfrågor kunna identifieras på ett tidigt stadium. Frågorna som ställs vid djupintervjun baseras i stora delar på den teori som presenteras i denna uppsats. Enligt van Teijlingen & Hundley (2001) ökar sannolikheten för framgång i huvudstudien när man använder sig av en pilotstudie.

Tabell 3.2: Intervjuguide säkerhetschef (R1).

Kategori	**Frågor**	**Motivering & Teori**
Bakgrund	Kan ni börja med att berätta om er roll inom företaget och vad ni jobbar med?	Syftet med detta är att få en inblick i området respondenten jobbar med och hur detta skulle kunna relateras till informationssäkerhet.
Informationssäkerhetsarbetet	Hur ser ni på arbetet med informationssäkerhet inom organisationen? Kan ni ge oss en bild av hur företagets ledning ser på informationssäkerhet? Görs det regelbundna revisioner av informationssäkerheten?	Syftet med denna fråga är att få en bild av hur organisationens arbete med informationssäkerhet ser ut och upplevs.
Policys	Kan ni berätta hur ni arbetar med policys inom företaget? Har ni olika ”lager” av säkerhet? Kan ni ge exempel på specifika policys/direktiv? Hur utformas dessa?	Dessa frågor ställdes för att ge oss en bild av hur företaget arbetar med sina policys och direktiv, och då hur dessa framställs.

Ledning – Ansvar – Kommunikation	Vem eller vilka ansvarar slutligen för informationssäkerheten? Hur säkerställer ni att policys och riktlinjer/direktiv fastställs? Hur motiveras anställda att följa dessa	Detta ger en inblick i hur ansvaret för informationssäkerhet fördelas inom organisationen samt hur anställda motiveras att efterfölja detta.
Utmaningar	Upplever ni att avdelningarna har svårigheter att kommunicera med varandra på grund av säkerheten? Vilka svårigheter finns det med att arbeta med informationssäkerhet inom ett globalt företag? Vilka konsekvenser kan bruten informationssäkerhet innebära? Hur ser ni på avsiktliga och oavsiktliga hot?	Syftet med dessa är att få en inblick i vilka utmaningar det finns, dels för en säkerhetschef samt för en organisation i helhet gällande informationssäkerhet. Samt hur dessa utmaningar kan hanteras. Dessa frågor berör även kapitel 2.4 Silo inom säkerhet och utmaningarna som beskrivs där.
Avslut	Har ni något ni vill avsluta med?	Syftet med detta är ett ge respondenten en möjlighet att ge input på något vi kan ha missat att fråga, något som behöver förtydligas eller liknande.

Tabell 3.3: Intervjuguide chefer.

Kategori	**Frågor**	**Motivering & Teori**
Bakgrund	Kan ni börja med att berätta om er roll inom företaget och vad ni jobbar med?	Syftet med detta är att få en inblick i området respondenten jobbar med och hur detta skulle kunna relateras till informationssäkerhet.
Informationssäkerhetsarbetet	Hur ser ni på arbetet med informationssäkerhet inom organisationen?	Syftet med denna fråga är att få en bild av hur organisationens arbete med informationssäkerhet ser ut och upplevs.
Policys	Kan ni berätta hur ni arbetar med policys inom företaget?	Dessa frågor ställdes för att ge oss en bild av hur företaget arbetar med sina policys och direktiv. Samt hur dessa upplevs.
Ledning – Ansvar – Kommunikation	Hur upplever ni att er avdelning inom organisationen tillämpar de regler som fastställs?	Detta ger en inblick i hur ansvaret för informationssäkerhet fördelas inom organisationen samt hur anställda motiveras att efterfölja detta.
Utmaningar	Upplever ni på er avdelning att ni har svårigheter med att kommunicera med andra avdelningar på grund av säkerheten? Vilka konsekvenser kan bruten informationssäkerhet innebära? Hur ser ert samarbete med InfoSec avdelningen ut?	Syftet med dessa är att få en inblick i vilka utmaningar det finns, dels för en säkerhetschef samt för en organisation i helhet gällande informationssäkerhet. Samt hur dessa utmaningar kan hanteras. Dessa frågor berör även kapitel 2.4 Silo inom säkerhet och utmaningarna som beskrivs där.
Avslut	Har ni något ni vill avsluta med?	Syftet med detta är ett ge respondenten en möjlighet att ge input på något vi kan ha missat att fråga, något

		som behöver förtydligas eller liknande.

3.5 Enkät

För att undersöka anställda och deras tillämpning av policys och säkerhetsfrågor skapades enkäter baserat på den information som framkommit vid intervju med säkerhetschef och de dokument som vi fått ta del av (bilaga 7). Totalt finns det tre enkäter, en för anställda i Sverige (E1), en för anställda i övriga länder (E2) samt en för avdelningschefer (E3). E1 och E2 är identiska med varandra bortsett från att man i E2 ombeds namnge det land man arbetar i. Detta behövs för att kunna härleda ursprunget som i senare skede kan påvisa skillnader eller likheter mellan olika länders syn på informationssäkerhet. I E3 är frågorna ställda till avdelningschefer där de omformulerats för att undersöka vad cheferna tror deras anställda kommer att svara.

Enkäten fylls i online och distribueras till respondenterna via email. I detta email finns en paragraf med en kort introduktion till studien där vi presenterar oss och delger bakgrund och syfte. Här förtydligas även att enkäten är helt anonym och frivillig.

Tabell 3.4: Enkätundersökning.

Kategori	**Fråga**	**Motivering**
Arbete med informationssäkerhet	8. How easy is it to communicate issues with InfoSec management? 9. What's your general impression of the security policies and directives?	Syftet med frågorna är att få en bild av hur organisationens arbete med informationssäkerhet upplevs och hur kommunikationen med management om problem upplevs.
Policys	2. If you find a USB without knowing its origin (like employee parking), what are the chances that you would plug it in to your work station? 3. If you keep confidential (RED) data on your USB drive, how often do you encrypt it?	Dessa frågor ställdes då de ger en bra inblick i hur företagets direktiv och policys efterföljs.
Ledning – Ansvar – Kommunikation	4. How often do you use public networks on your work-laptop? (Starbucks, Espresso-House, Trains etc)	Frågorna ger en inblick i hur anställda inom företaget agerar i olika situationer baserat på omdöme, ansvar och vad de fastställda reglerna anger.

	7. Do you ever skip security directives to easier perform your work tasks? 1. How often do you use external drives such as USB for both private and business use? (same unit) 5. How often do you work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotellobby etc) 6. How often do you work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotellobby etc) 10. How did you asses the threat level of opening this link and email?	

3.6 Transkribering

För att underlätta arbetet med att skriva ner informationen som givits under intervjuerna och för att vidare underlätta vid arbetet av jämförelser och analysering av resultaten transkriberas intervjuerna. Detta underlättar även vid sökandet av data från intervjuerna. Transkriberingen är inte en exakt återkoppling av intervjun utan innehåller små ändringar i syfte att underlätta för läsaren, detta kan vara bland annat förtydliganden gällande vissa förkortningar och liknande. Det kan även förekomma att hela stycken tagits bort då respondenterna har möjlighet att gå över transkriberingen och ta bort eventuella bitar som de egentligen inte vill delge, vilket är naturligt då studien handlar om informationssäkerhet.

Vidare har vissa delar redigerats för att säkerställa att företaget och respondenterna hålls anonyma, detta kan då vara att de under intervjun namngett företaget och vi istället i transkriberingen skriver ner det som *företaget.* Annat exempel kan vara att det diskuteras produkter eller forskningsområden väldigt unika för företaget vilket då har antingen strukits helt eller ersatts med ”XXX” eller liknande. Återigen görs detta för att inte riskera att det avslöjas vilket företag denna studie gjorts hos.

3.7 Validitet

För att säkerställa validiteten av vår studie har vi grundat empirin i det teoretiska ramverket som fastställts i föregående kapitel. Detta ramverk tar upp relevanta teorier och metoder för att ge bra inblick i hur informationssäkerhet kan eller bör fungera i praktiken. De empiriska undersökningarna har sin grund i detta ramverk, vilket vidare fastställer studiens validitet. För att undvika frågor som kan upplevas som vinklade, eller ett försök att guida respondenten till ett visst svar, är frågorna så neutralt ställda som möjligt, och vi har under intervjuprocessen en så neutral inställning som möjligt. Vi har alltså på så sätt inte aktivt försökt leda till specifika svar.

Det finns dock en risk att respondentens svar inte är helt sanningsenliga. Detta kan bero på flera olika saker, bland annat kan det vara så att respondenten försöker framstå bättre än vad den egentligen är, eller vill ge en annan blick på hur verksamheten fungerar. Respondentens svar stämmer kanske inte med dennes faktiska handlingar. Det kan också vara så att respondenten ger svar som denna tror att vi vill ha för studiens skull. Detta är något som är svårt för oss att vidare validera då vi inte har någon vidare insyn i företaget och kan inte jämföra med andra källor. Det kan även vara så att svaren inte heller är sanningsenliga på grund av bristande kompetens inom området, eller att frågan rör ett känsligt område som inte vill delges.

För att vidare säkerställa validitet och möjlighet att återkoppla med förtydliganden har respondenterna tillgång till transkriberingen av sin intervju. Här har de även möjlighet att be vissa områden strykas om dessa skulle innehålla känsliga punkter som inte bör delges i denna studie. Detta är så klart naturligt känsligt då studien innefattar informationssäkerhet.

Gällande anonymiteten av företag och respondenter i studien är detta på grund av ämnets känsliga natur, det vill säga informationssäkerhet. Därför är det naturligt att ett företag inte vill att det blir allmänt känt hur de jobbar med informationssäkerhet, det är därför på deras begäran denna anonymisering har gjorts. Speciellt då detta område är för dem ett av de känsligaste områdena för deras affärsmodell. Dokumenten (bilaga 8-10) vi har fått ta del av är konfidentiella och får bara spridas inom företaget, undantaget gjordes för oss baserat på att dokumenten anonymiserades och viss känslig information tagits bort. Även resultatet av intervjuerna och enkäterna bedöms som känsligt och man vill inte att det framgår vare sig vilka personerna (respondenterna) eller företaget är.

3.8 Etik

Genom att ta hänsyn till de etiska aspekterna som presenteras av Jacobsen (2002) säkerställer vi en etisk grund för studien. Det som tas i åtanke vid intervjuer och enkäter är att: garantera att deltagandet är frivilligt, rätten till privatliv/anonymitet och kravet att på ett korrekt sätt presentera data från intervjun.

Detta säkerställs genom att i intervjun förklara för respondenten studiens syfte och frivilligt deltagande. Här förklaras även att intervjun är anonym och alla eventuella kopplingar till både företaget och respondentens identitet kommer strykas. Vi ger även möjlighet att senare gå igenom transkriberingen för att vid behov göra revideringar för att vidare säkerställa anonymitet eller spridandet av känslig information.

4. Resultat

I detta avsnitt redogörs för de svar som respondenterna har givit. Resultaten presenteras i kategorier baserat på vilken respondent det är samt till vilken kategori från intervjuguiden (tabell 3.2/3.3) som frågorna/resultatet tillhör.

Resultatet presenteras även genom omskrivningar och våra egna formuleringar för att ge en tydligare bild av det som sagts. Transkriberingar av intervjuerna som resultaten baseras på finns som bilagor (4, 5, 6 & 7).

4.1 Resultat av intervju med säkerhetschef

4.1.1 Informationssäkerhetsarbetet

Verksamheten är uppbyggd på ett sådant sätt att alla inom säkerhetsorganisationen är involverade i arbetet med informationssäkerhet. Utöver detta finns där en speciell avdelning som explicit hanterar informationssäkerhet och agerar länk mellan övriga grupper i sådant som rör just informationssäkerhet. Avdelningarna inom säkerhetsorganisationen är uppdelade på följande sätt;

- Threat and Vulnerability Management
- Crisis Management
- Security Incident Management
- Business Continuity Management
- Information Security Management
- Personnel Security
- Physical Security
- Sourcing Security
- Security Awareness, Training & Education
- Sales Support
- Security Governance
- Privacy

Avdelningarna listade ovan tillhör antingen gruppen “Information Security” eller “Security Operations”. Group Security Organization är det styrande organet globalt och består av Chief Security Officer (CSO), regionala chefer samt vissa stödjande roller på olika nivå. Organisationen i sin helhet är indelad i så kallade “market areas” vilka består utav Europa, Latinamerika, Asien tillsammans med Oceanien, och sedan Indien för sig. Arbetet med säkerhet styrs centralt uppifrån för att sedan komma ner en nivå på varje “market area”. Varje land eller kluster av länder rapporterar till respektive “market area” som i sin tur rapporterar till Group Security Organization. Global information security board är den högsta instansen för informationssäkerhet och här hanteras sådant som eskalerats vidare från lokal nivå. Group compliance hanterar konsekvenser för personal som brutit mot interna regler.

Inom verksamheten finns klassificeringarna “public”, “internal” och “confidential”. Det finns planer på att införa “strictly confidential”, vilket det enligt respondenten finns behov utav. Väldigt mycket hamnar inom ramen för “confidential” och därav kan det uppstå svårigheter

med att värdera vad som bör prioriteras mest. Den information som måste skyddas till varje pris kallas för GIA (global information assets) och utgör cirka 5% av all den information som finns inom verksamheten. På fråga om hur respondenten ser på arbetet med ledningsgrupp säger personen i fråga att samarbetet är mycket gott och känner ett extremt stöd, vilket även är en förutsättning. Vidare säger respondenten att personal i allmänhet har gott engagemang och bra förståelse för att verksamheten måste skydda sin information. Det arbete som görs inom området för informationssäkerhet följs upp och utvärderas av ledningsgruppen på lokal nivå.

4.1.2 Policys

I intervjun fastställs det att arbetet med policys och direktiv som de också kallas internt (viss skillnad internt) är enormt viktigt. Arbetet med detta anses vara viktigt då mycket av företagets aktiviteter omfattar patent, forskning och liknande information som då innebär stora förluster för företaget om dessa skulle spridas.

Inom företaget räknas policy de fåtal övergripande "regler" eller information om hur saker och ting ska göras (Bilaga 8). Dessa övergripande policys genomsyrar hela organisation och alla har ett ansvar att följa dessa. Meningen med dessa policys är att förtydliga vad som är målsättningen med säkerheten, "vad är det man vill uppnå?".

Direktiv är mer detaljerade och konkreta än policys och kan då vara saker som hur anställda ska hantera sina datorer och liknande (Bilaga 9). Direktiven är tillvägagångssätt för hur policys ska uppnås. Dessa direktiv är konstruerade med "purpose, scope, compliance och responsibility (Kapitel 2.6.1) i åtanke, men även confidentiality, integrity och availability, den så kallade CIA-triaden (Kapitel 2.3).

Dessa direktiv och policys är skrivna av företagets Chief Information Security Officer (CISO) och direkt godkända av företagets VD.

4.1.3 Ledning – Ansvar – Kommunikation

Enligt respondenten är det den enskildes ansvar att efterfölja de policys och direktiv som är uppsatta. Företagets ledning har ansvaret att hålla dessa direktiv uppdaterade och relevanta men själva ansvaret att leva upp till reglerna är upp till de anställda. För att vidare säkerställa att anställda har koll på de olika direktiven och policys har företaget obligatoriska program eller träning i informationssäkerhet där anställda då lär sig och testar sin kunskap om informationssäkerhet. Detta görs för att få de anställda mer medvetna om hur viktig informationssäkerheten är och hur viktigt det är att efterfölja direktiven.

Företaget anordnar även andra evenemang för att lyfta upp informationssäkerhetens betydelse, detta genom så kallade "security awareness" dagar, meddelanden på skärmsläckarna, artiklar på intranätet och liknande. Dessa dagar och evenemang uppskattas enligt respondenten av medarbetarna.

4.1.4 Utmaningar

Utmaningar med informationssäkerheten inom företaget kan bland annat vara hur man säkerställer att anställda följer de uppsatta direktiven och policys. Det görs bland annat kontroller men det är också viktigt att folk rapporterar incidenter och liknande. Det kan vara saker som gjort omedvetet eller till och med medvetet på grund av tidspress, detta kanske inte alltid rapporteras.

Arbetet med Informationssäkerhetsavdelningen är därför en viktig roll för att säkerställa att båda parterna är på samma sida och upplever direktiven på liknande sätt. Eventuella svårigheter eller brister med säkerheten är därför viktiga att kommunicera mellan avdelningarna.

Det nämns ytterligare att det finns kulturella utmaningar. Då företaget är globalt är det inte alla områden i världen som tar säkerheten lika seriöst som det kanske görs i de svenska avdelningarna, vilket då innebär en utmaning. Detta kan till exempel vara att rapportering inte alltid görs och liknande.

Andra utmaningar kan vara samarbetet med IT säkerheten, där det ibland är otydligt vem som har ansvaret för vissa funktioner och implementering arbeten.

4.2 Resultat av intervjuer med chefer

4.2.1 Informationssäkerhetsarbetet

Samtliga respondenter påpekar hur viktigt arbetet med informationssäkerheten är. Företaget ligger i framkant vad gäller utveckling av ny teknologi vilket gör att verksamheten är konkurrensutsatt. Detta innebär att intern klassificering av information är av stor vikt för att förstå informationens karaktär. Mail med känslig information ska krypteras när valda avdelningar kommunicerar för att försvåra intrång. Vidare krävs det att information som rör patent hemlighålls för att rymmas inom den juridiska ramen vad det gäller immaterialrätten. Respondenterna berättar i olika utsträckning om att anställda utbildas inom informationssäkerhet kontinuerligt och att det sedan sker uppföljning på detta. R3 berättar om hur personen i fråga upplevde att informationssäkerheten riskerades att sättas ur spel när man tillät anställda att använda mobiltelefoner för att skicka jobbrelaterade email och att synkronisera kalendrar mm. Genom att testa säkerheten på ett sätt som respondenten inte vill delge, kunde uppenbara risker hittas. Samma person anser att det måste finnas en balans mellan vad som kan anses vara bekvämt och den information som ska skyddas, men att det test som utfördes pekade på att man beaktat bekvämlighets-aspekten i allt för stor utsträckning. Rapporteringssystem för bruten informationssäkerhet finns, men används i liten utsträckning enligt respondent R1 och R2. Man arbetar även proaktivt genom att försöka jobba efter scenario som kan uppstå för att kunna hantera kriser som uppstår. På fråga om hur respondenterna ser på samarbete med andra avdelningar svarar de att de upplever att det inte finns några större svårigheter så länge alla anställda följer reglerna. R4 poängterar att alla avvikelser ska rapporteras till säkerhetschefen.

4.2.2 Policys

Arbetet med policys inom de olika avdelningar vi varit hos är ungefär likadant, de har uppsatta direktiv och regler för hur olika arbetsuppgifter eller procedurer ska gå till, och det är den enskildes ansvar att efterfölja dessa. Det görs träningsprogram och liknande evenemang för att hålla personal uppdaterade och informerade om informationssäkerhetens betydelse.

Vissa av avdelningarna är mer "medvetna" och tar säkerheten på mer allvar än andra, detta då deras roll inom företaget hanterar mer känslig data än andra, men alla avdelningarna har samma förväntningar och krav på att efterfölja reglerna. Citat från respondent 4 (Bilaga 7)

> "*...vi arbetar så som dessa policys och föreskrifter säger. Alla får samma grundläggande utbildning, krypterade mail och sådana saker, följa policyn helt enkelt det är så vi arbetar med dem, vi följer dem och får lära sig hur det ska fungera."*

Liknande formuleringar eller tankar runt arbetet kring policys och direktiv går igen hos övriga respondenter. Policys och direktiv är något som förväntas att följas i arbetsuppgifterna och inget som aktivt kontrolleras hela tiden utan är snarare en del av vardagen eller rutinen, det är i vissa fall när något är oklart eller osäkert som det kanske dubbelkollas vad som är rätt tillvägagångssätt.

4.2.3 Ledning – Ansvar – Kommunikation

Det nämns i intervjuerna att ansvaret ligger hos varje anställd att efterfölja reglerna och att det är viktigt att vara medveten om betydelsen av informationssäkerheten. Det nämns även i intervjuerna vikten av att rapportera incidenter till korrekt instans och på så sätt bidra med att förbättra säkerheten. Tillämpningen av dessa regler på avdelningarna upplevs som att de följs, med sannolikhet för visst mörkertal av mindre incidenter som inte rapporteras. I stora drag upplevs det som att arbetet med direktiv och policys görs på ett bra sätt.

4.2.4 Utmaningar

Ytterligare diskuteras det konsekvenserna av vad bruten informationssäkerhet skulle kunna innebära för företaget. I de flesta fallen skulle bruten säkerhet på en av avdelningarna kunna innebära stora förluster för företagen. Till exempel en sådan incident kunna innebära att patent eller patentfamiljer "försvinner" vilket då kan innebära stora monetära förluster. Det skulle även kunna leda till stämningar och liknande.

Ytterligare utmaningar kan vara direktiven och policys kanske inte alltid hänger med i omvärldens utveckling och då kanske halkar efter och därmed inte alltid täcker upp alla hot. Detta kan till exempel vara införandet av "*Bring your own device"*, det vill säga att anställda kan ta med sina egna enheter såsom laptops, telefoner och liknande och använda dessa inom arbete. Det kan också vara nya tekniker eller sociala trender såsom molntjänster och eller sociala medier.

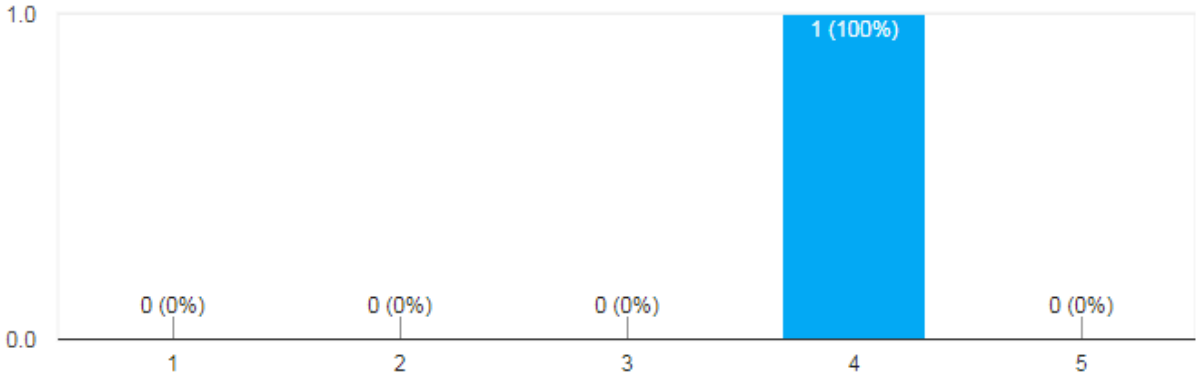
En utmaning som föreslogs kunde vara svårigheter att kommunicera med andra avdelningar inom företaget på grund av de olika säkerhetskrav och liknande som finns, detta var dock inte något som stämde överens med verkligheten. Respondenterna upplever inga problem att kommunicera eller arbeta mellan avdelningar på grund av säkerheten.

4.3 Resultat av enkätundersökningar

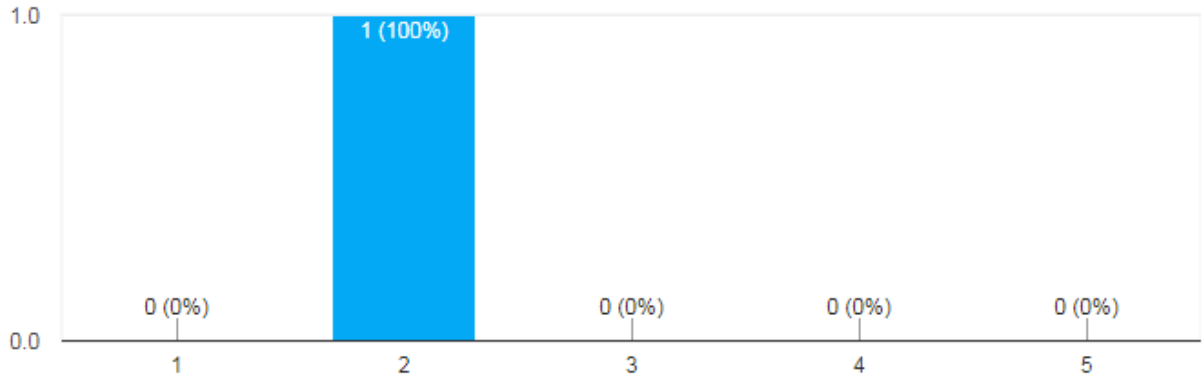
I detta avsnitt redogörs för de svar som framkommit av enkätundersökningarna. Resultaten presenteras i kategorier baserat på vilken grupp av respondent det är. Resultaten presenteras I form av stapeldiagram.

4.3.1 Säkerhetschef

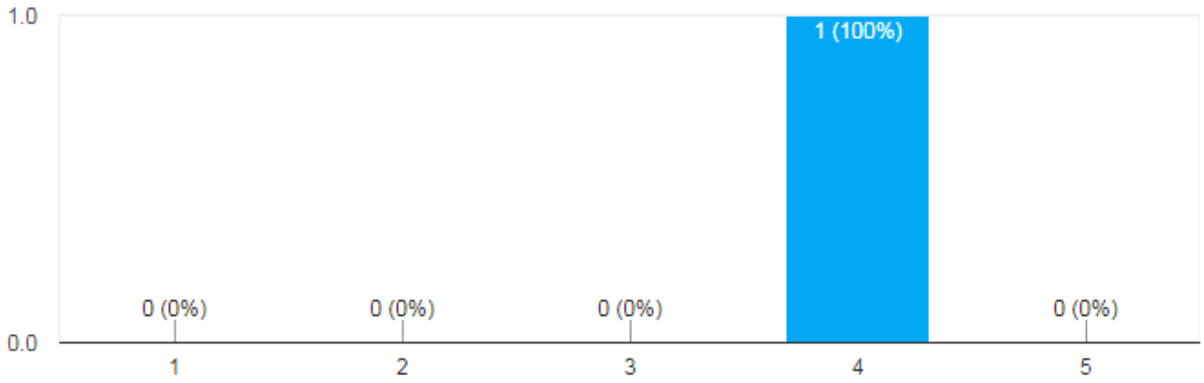
1. How often do you think employees use external drives such as USB for both private and business use? (same unit). Där 1 är *Never* och 5 är *Very Often.*



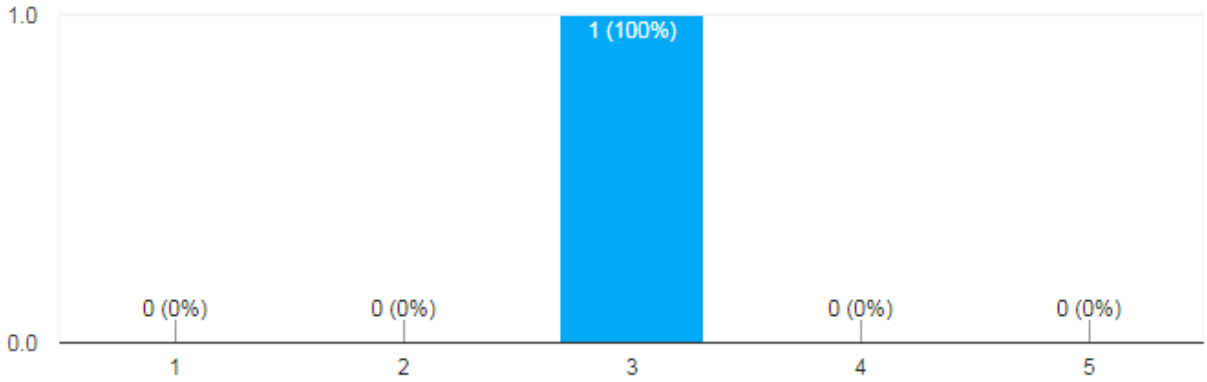
2. How do you think employees act if they find a USB without knowing its origin (like employee parking), what are the chances that they would plug it in to their work station? Där 1 är *No Chance* och 5 är *High Probability.*



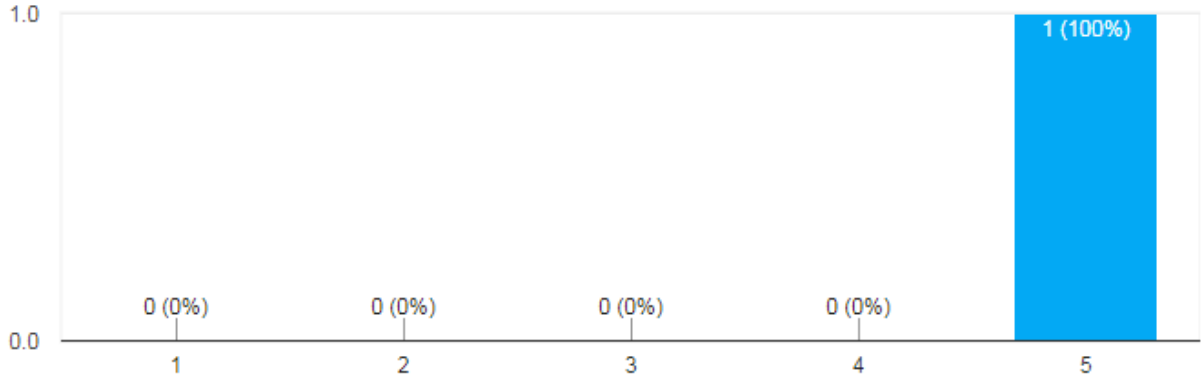
3. If employees keep confidential (RED) data on a USB drive, how often do you think they would encrypt it? Där 1 är *Never* och 5 är *Very Often.*



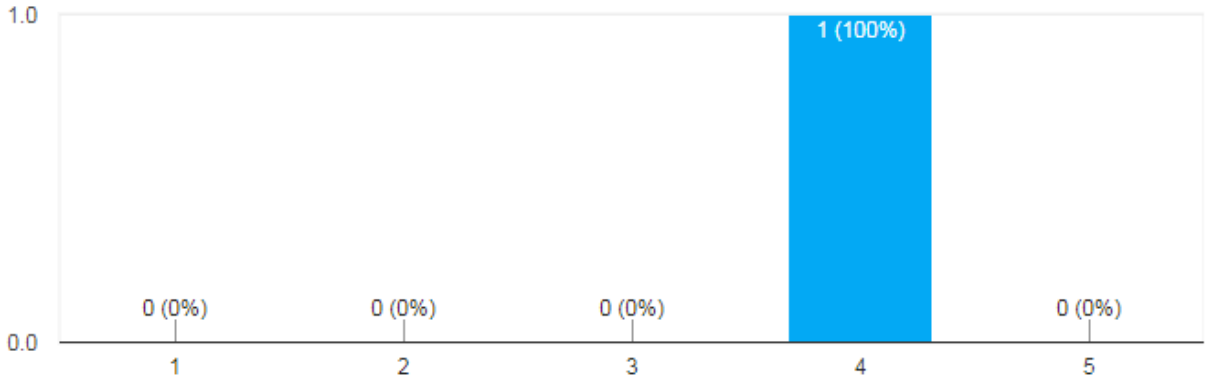
4. How often do you think employees use public networks on their work-laptop? (Starbucks, Espresso-House, Trains etc). Där 1 är *Never* och 5 är *Very Often.*



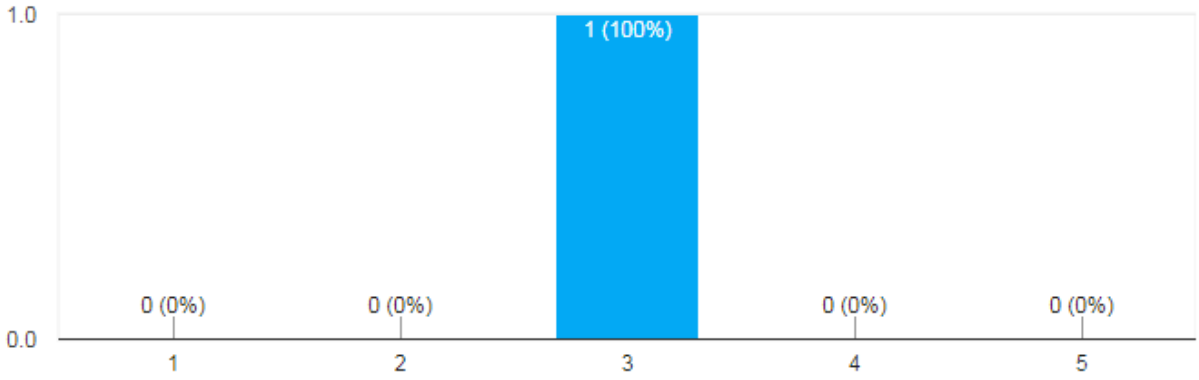
5. How often do you think employees work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



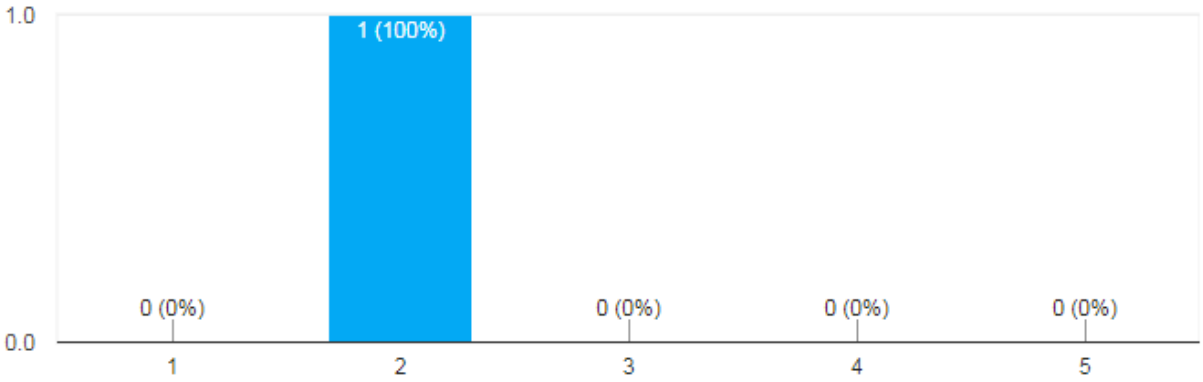
6. How often do you think employees work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



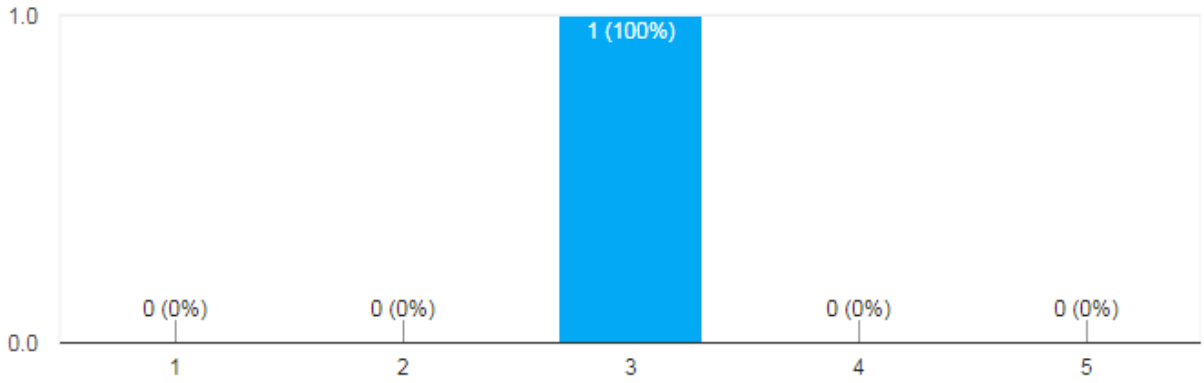
7. How often do you think employees ever skip security directives to easier perform their work tasks? Där 1 är *Never* och 5 är *Very Often.*



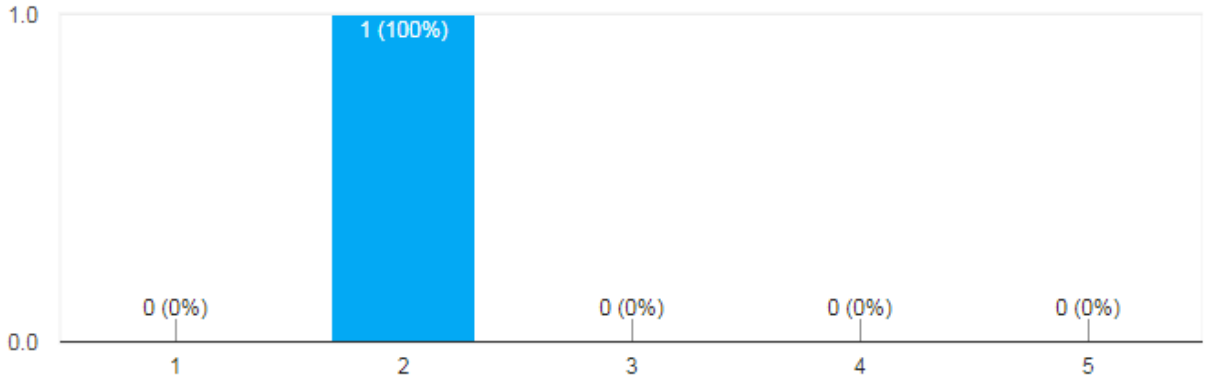
8. How easy you think employees find it to communicate issues with InfoSec management? Där 1 är *Hard* och 5 är *Very Easy.*



9. What do you think employees general impression of the security policies and directives are? Där 1 är *Bad* och 5 är *Great.*

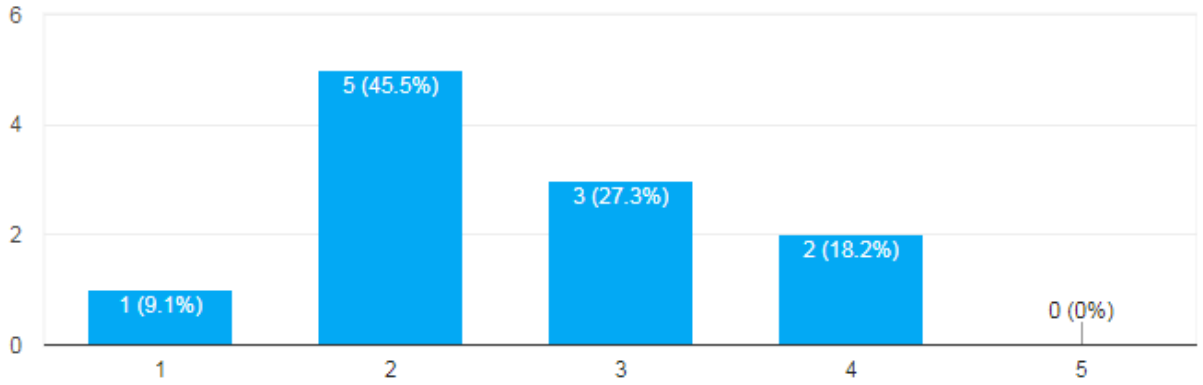


10. How do you think employees assessed the threat level of opening this link and email? Där 1 är *No Risk* och 5 är *High Risk.*

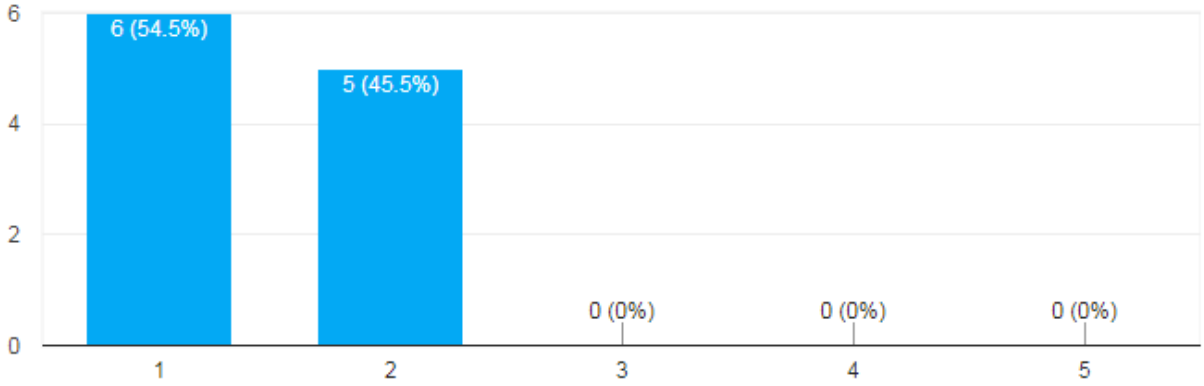


4.3.2 Managers

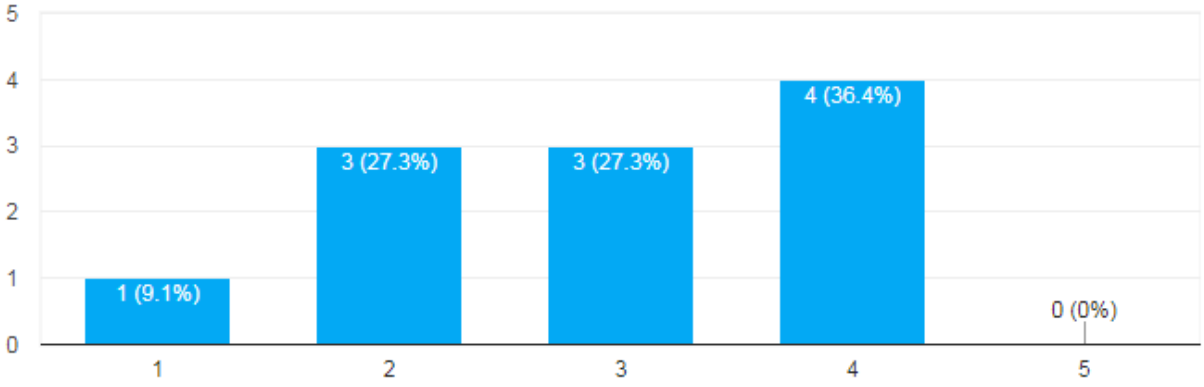
1. How often do you think employees use external drives such as USB for both private and business use? (same unit). Där 1 är *Never* och 5 är *Very Often.*



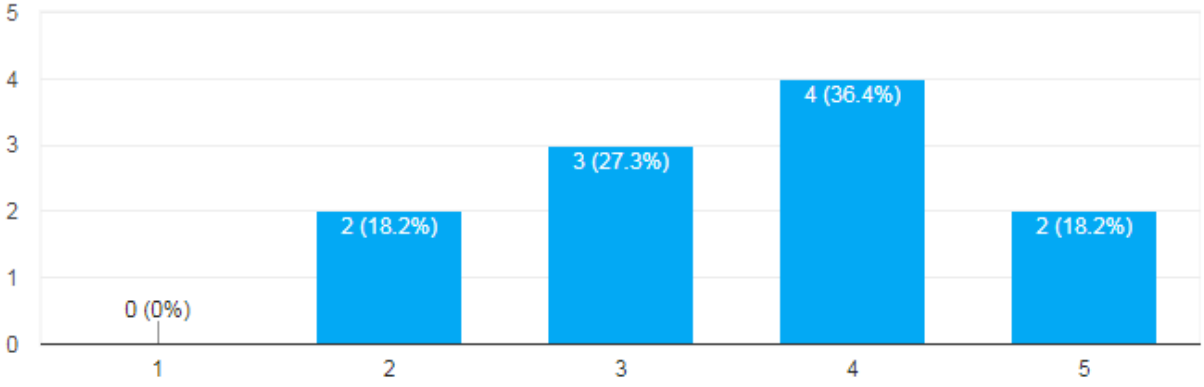
2. How do you think employees act if they find a USB without knowing its origin (like employee parking), what are the chances that they would plug it in to their work station? Där 1 är *No Chance* och 5 är *High Probability.*



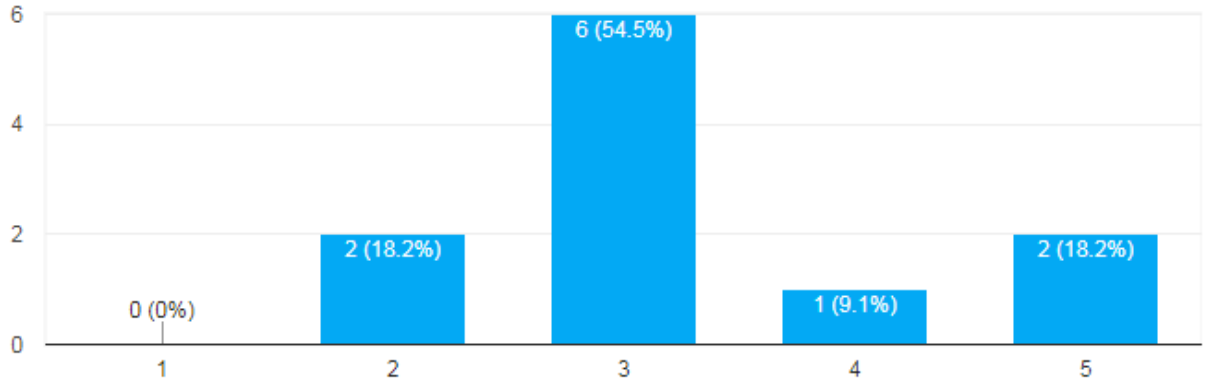
3. If employees keep confidential (RED) data on a USB drive, how often do you think they would encrypt it? Där 1 är *Never* och 5 är *Very Often.*



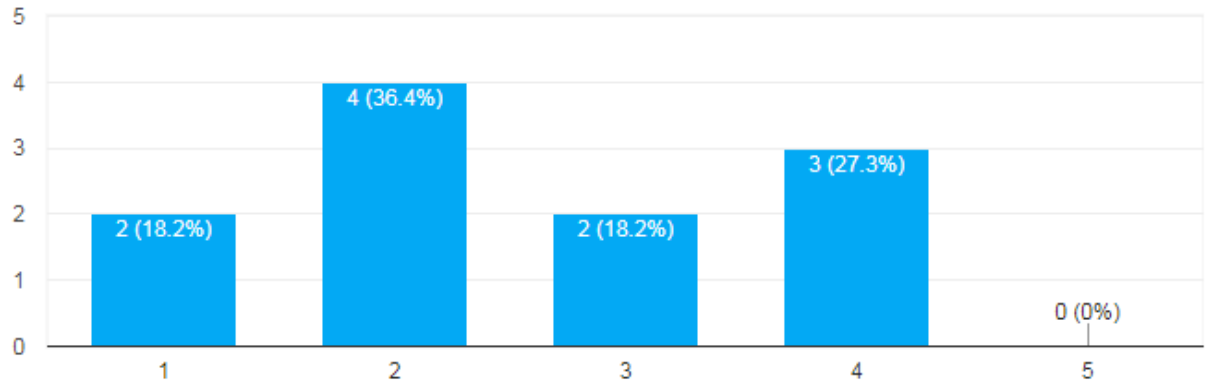
4. How often do you think employees use public networks on their work-laptop? (Starbucks, Espresso-House, Trains etc). Där 1 är *Never* och 5 är *Very Often.*



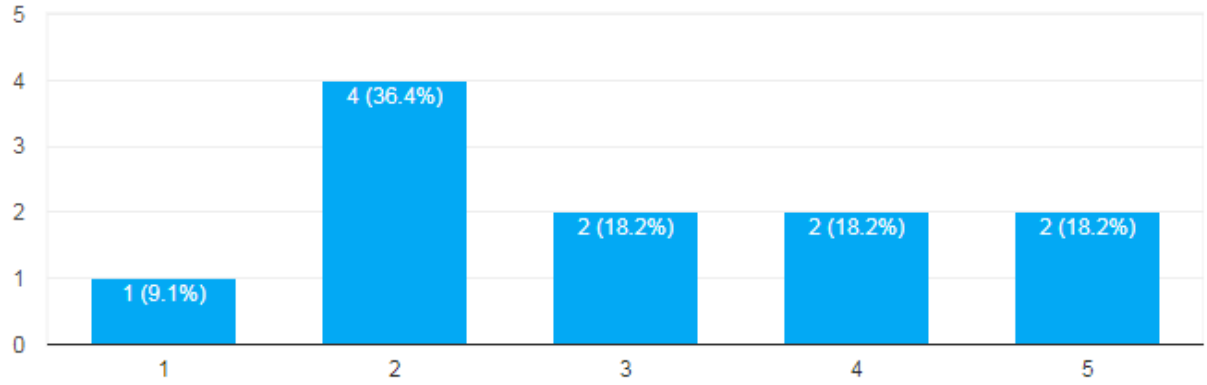
5. How often do you think employees work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



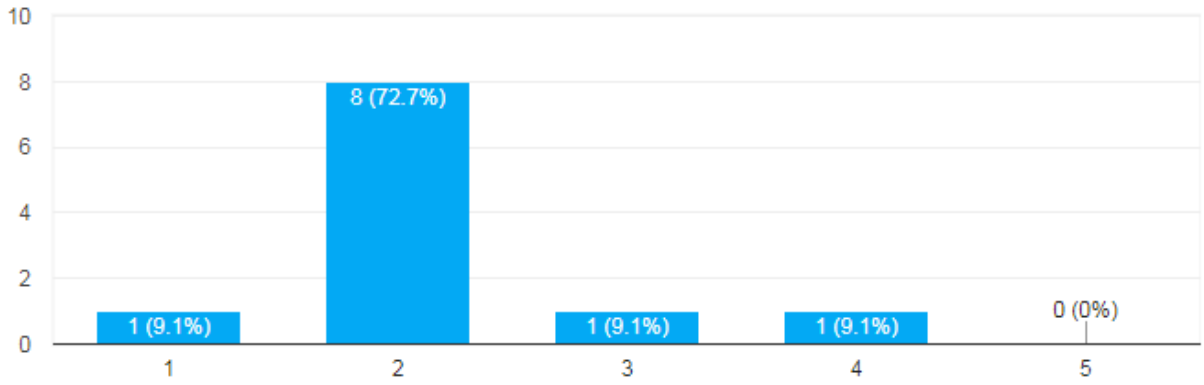
6. How often do you think employees work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



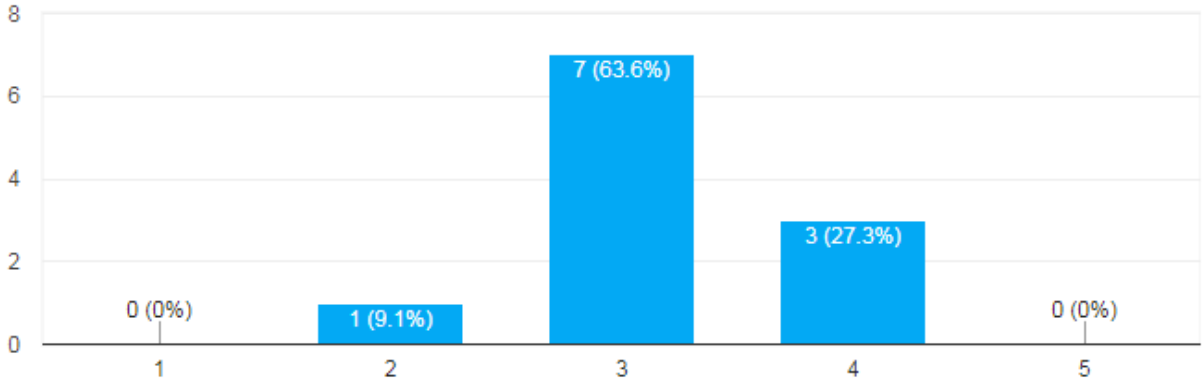
7. How often do you think employees ever skip security directives to easier perform their work tasks? Där 1 är *Never* och 5 är *Very Often.*



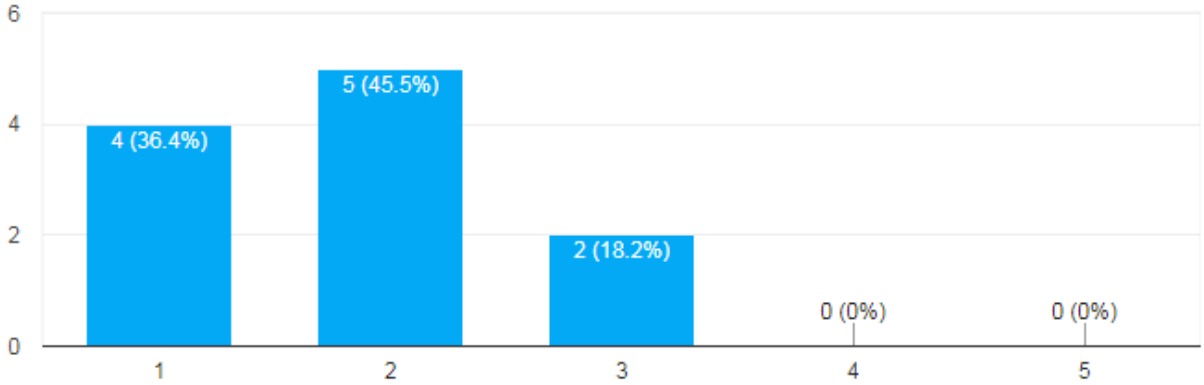
8. How easy do you think employees find it to communicate issues with InfoSec management? Där 1 är *Hard* och 5 är *Very Easy.*



9. What do you think employees general impression of the security policies and directives are? Där 1 är *Bad* och 5 är *Great.*



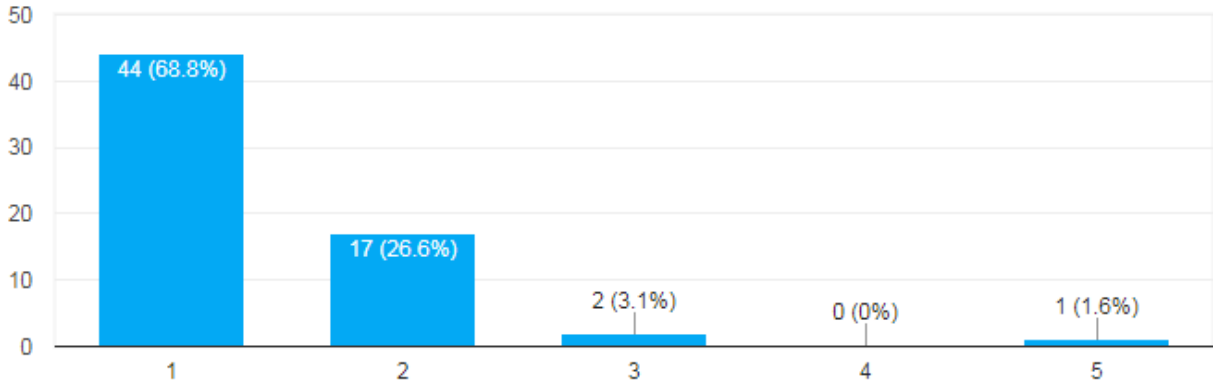
10. How do you think employees assessed the threat level of opening this link and email? Där 1 är *No Risk* och 5 är *High Risk.*



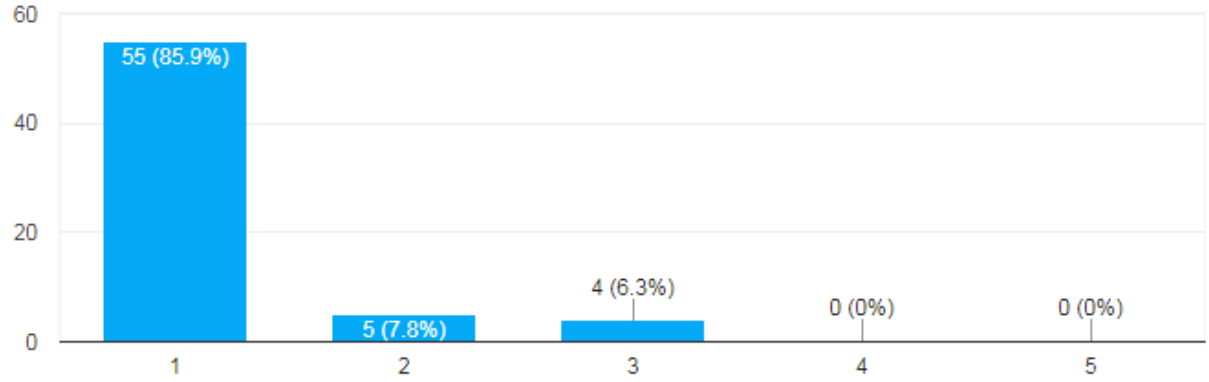
4.3.3 Anställda i Sverige

Nedan presenterar vi våra resultat från enkätundersökningen med anställda i Sverige.

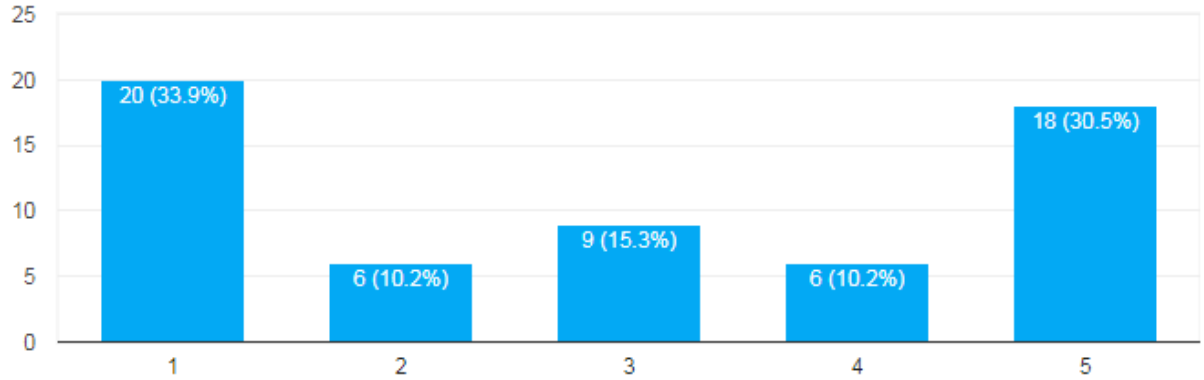
1. How often do you use external drives such as USB for both private and business use? (same unit). Där 1 är *Never* och 5 är *Very Often.*



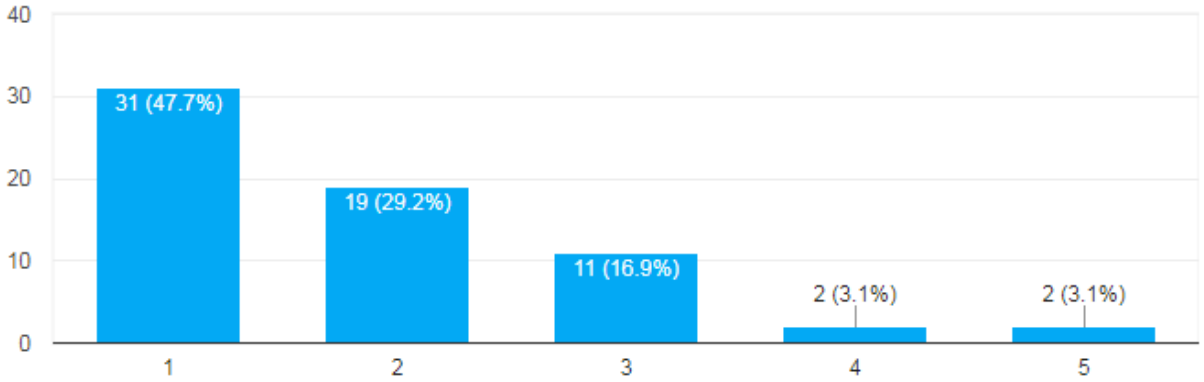
2. If you find a USB without knowing its origin (like employee parking), what are the chances that you would plug it in to your work station? Där 1 är *No Chance* och 5 är *High Probability.*



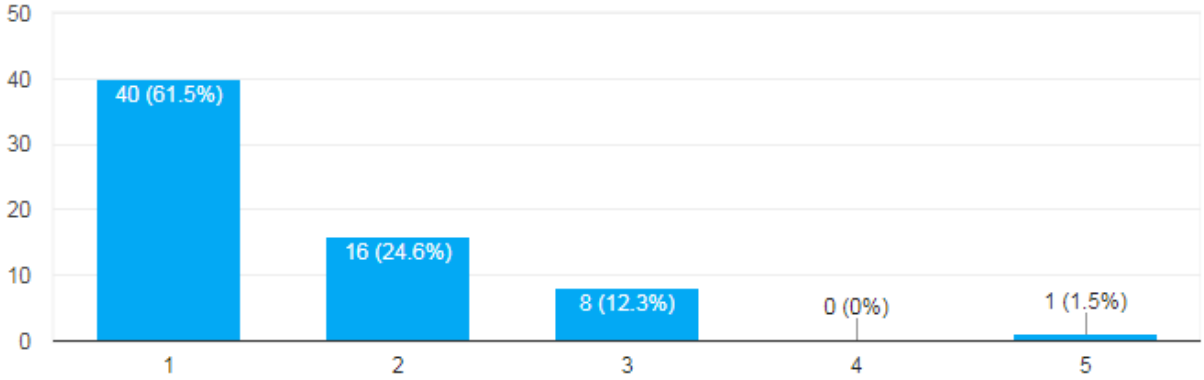
3. If you keep confidential (RED) data on your USB drive, how often do you encrypt it? Där 1 är *Never* och 5 är *Very Often.*



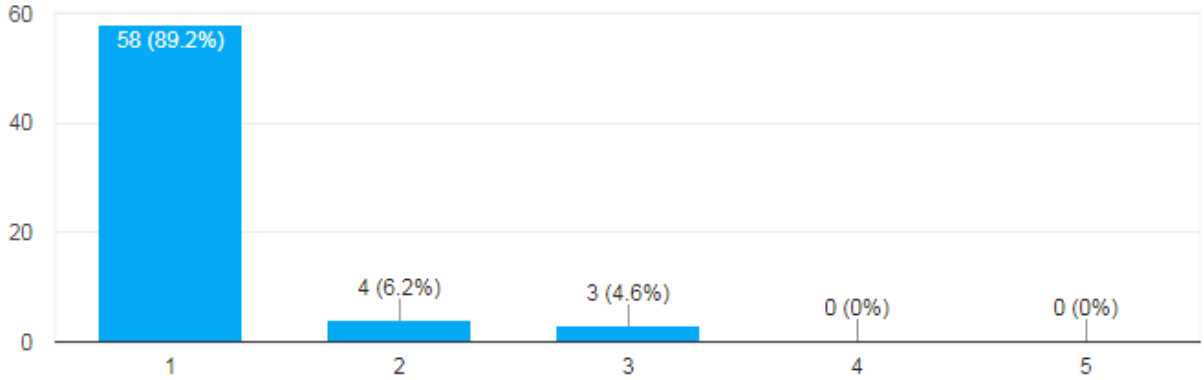
4. How often do you use public networks on your work-laptop? (Starbucks, Espresso-House, Trains etc). Där 1 är *Never* och 5 är *Very Often.*



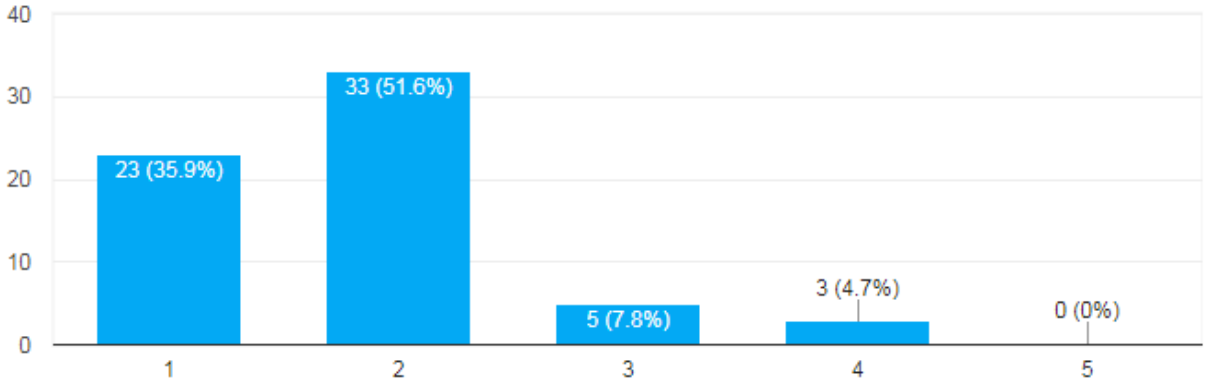
5. How often do you work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



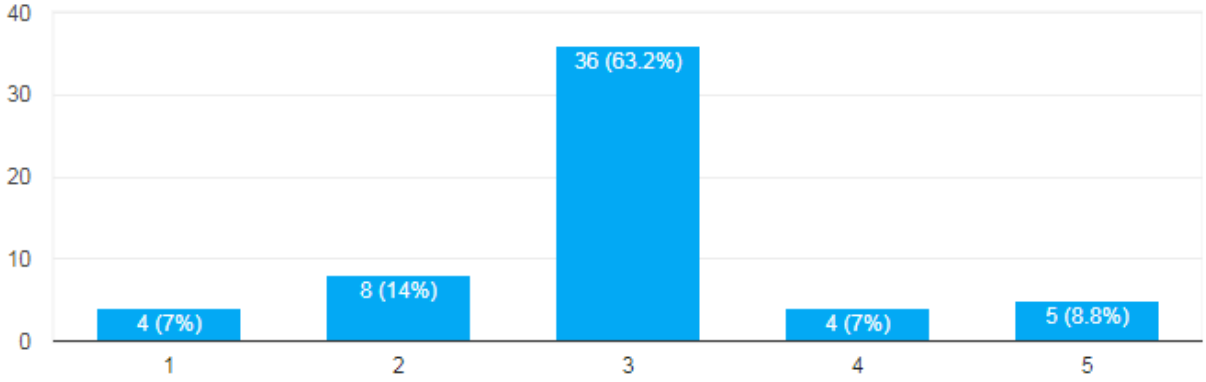
6. How often do you work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



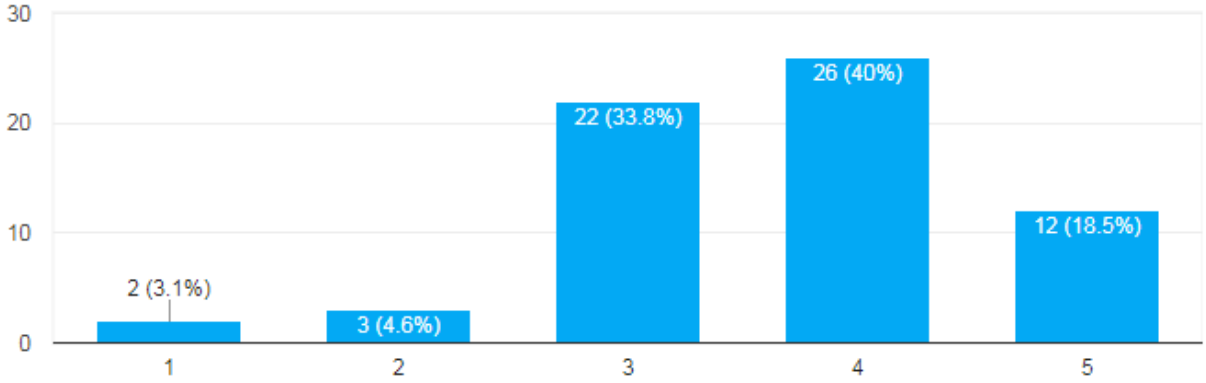
7. Do you ever skip security directives to easier perform your work tasks? Där 1 är *Never* och 5 är *Very Often.*



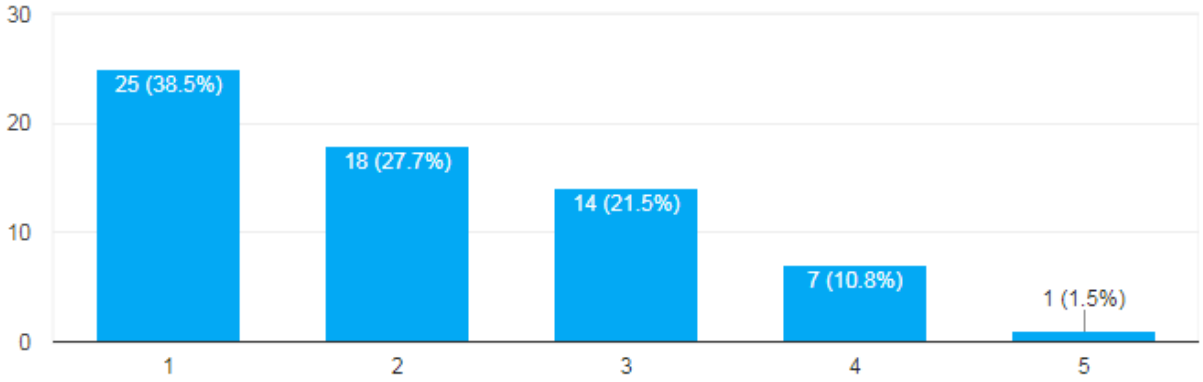
8. How easy is it to communicate issues with InfoSec management? Där 1 är *Hard* och 5 är *Very Easy.*



9. What's your general impression of the security policies and directives? Där 1 är *Bad* och 5 är *Great.*

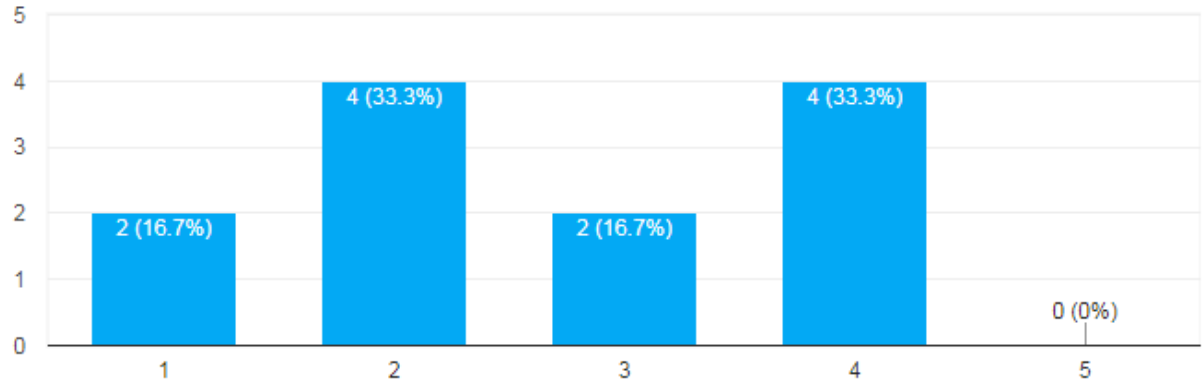


10. How did you assess the threat level of opening this link and email? Där 1 är *No Risk* och 5 är *High Risk.*

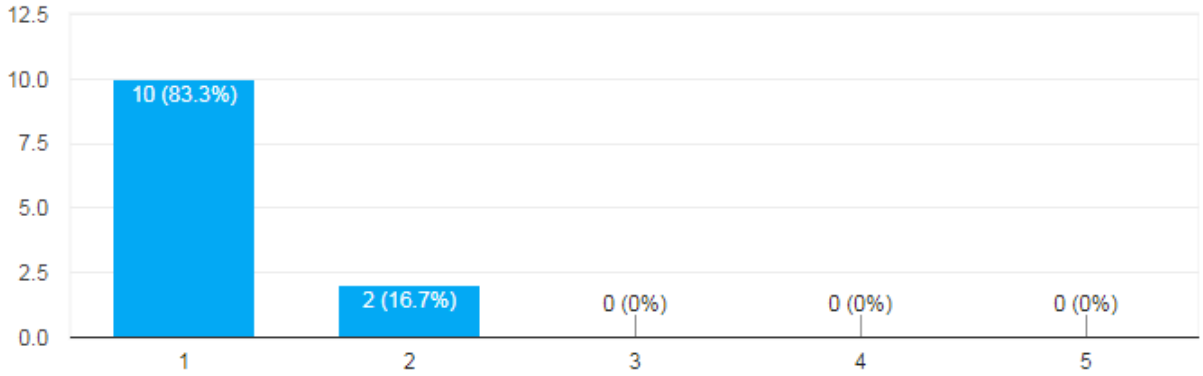


4.3.4 Internationellt anställda

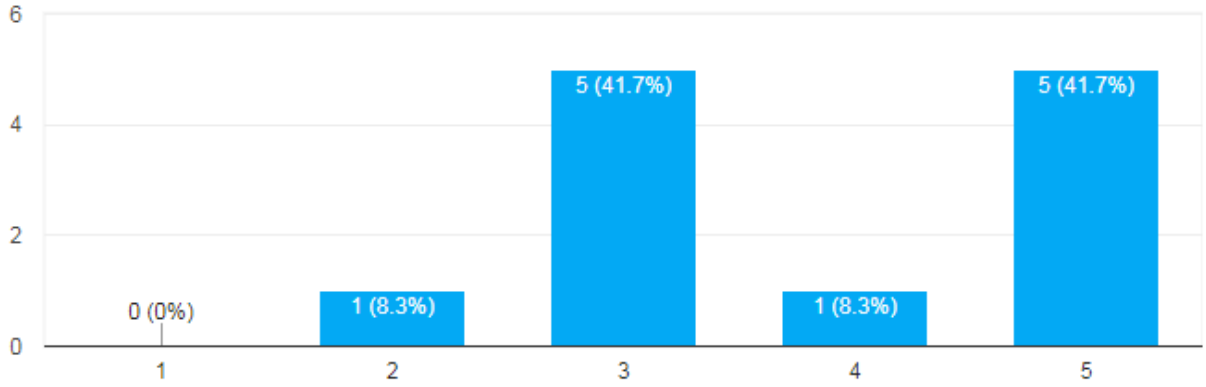
1. How often do you use external drives such as USB for both private and business use? (same unit). Där 1 är *Never* och 5 är *Very Often.*



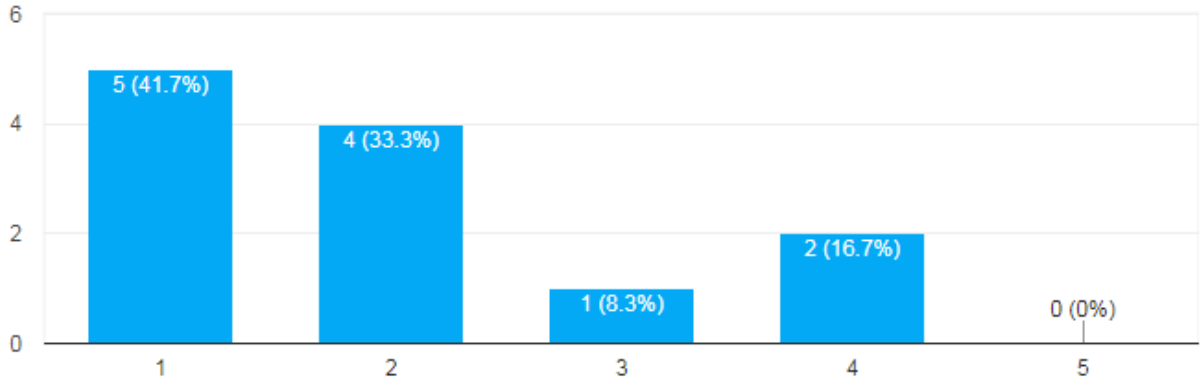
2. If you find a USB without knowing its origin (like employee parking), what are the chances that you would plug it in to your work station? Där 1 är *No Chance* och 5 är *High Probability.*



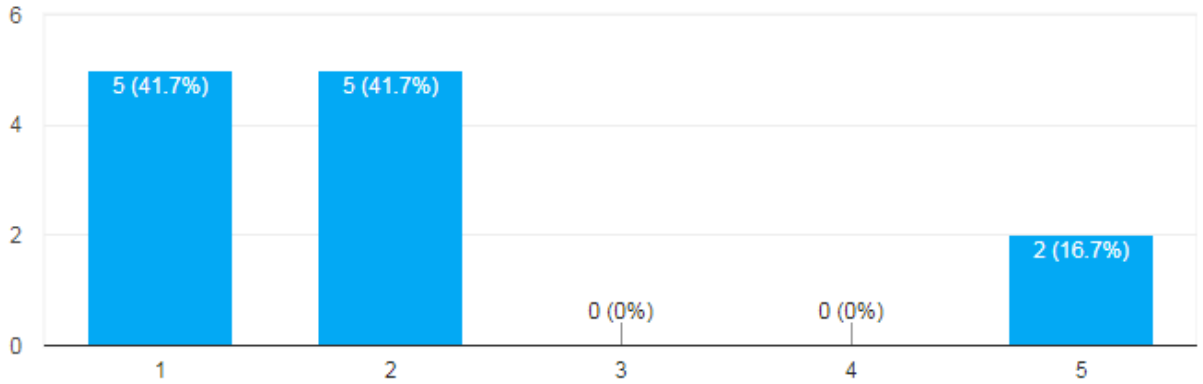
3. If you keep confidential (RED) data on your USB drive, how often do you encrypt it? Där 1 är *Never* och 5 är *Very Often.*



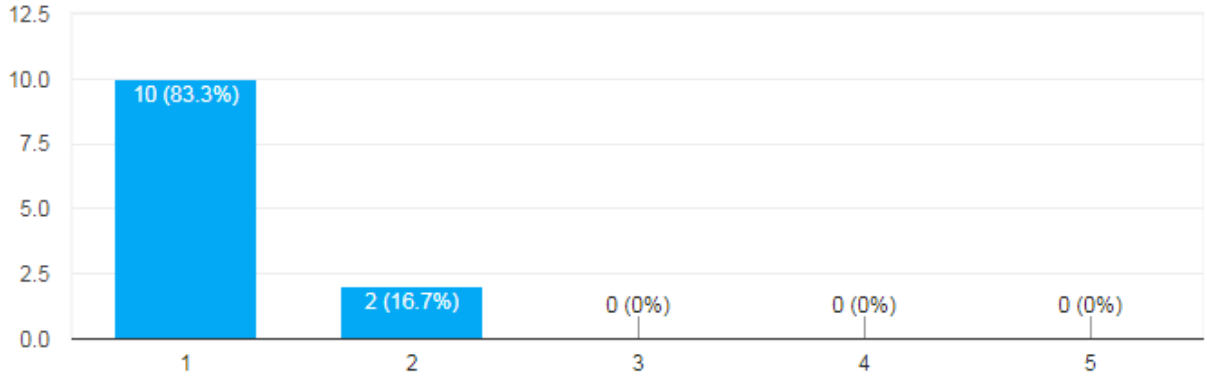
4. How often do you use public networks on your work-laptop? (Starbucks, Espresso-House, Trains etc). Där 1 är *Never* och 5 är *Very Often.*



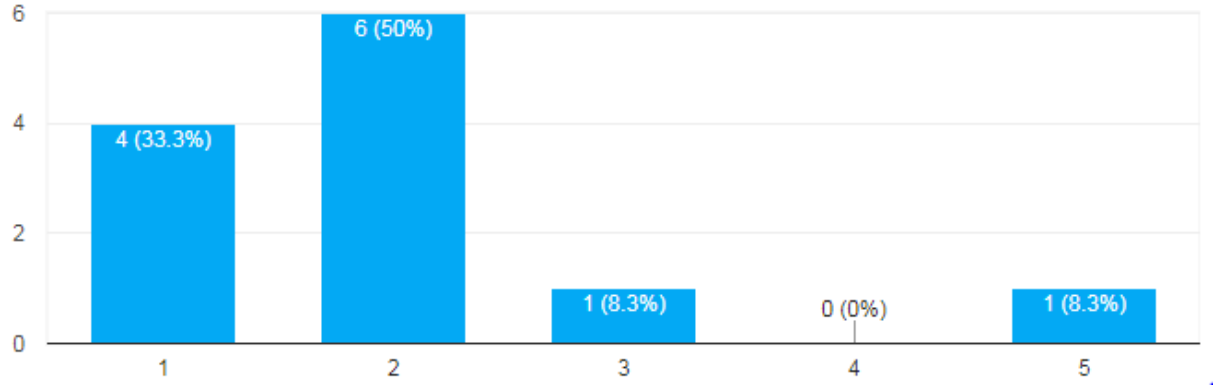
5. How often do you work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



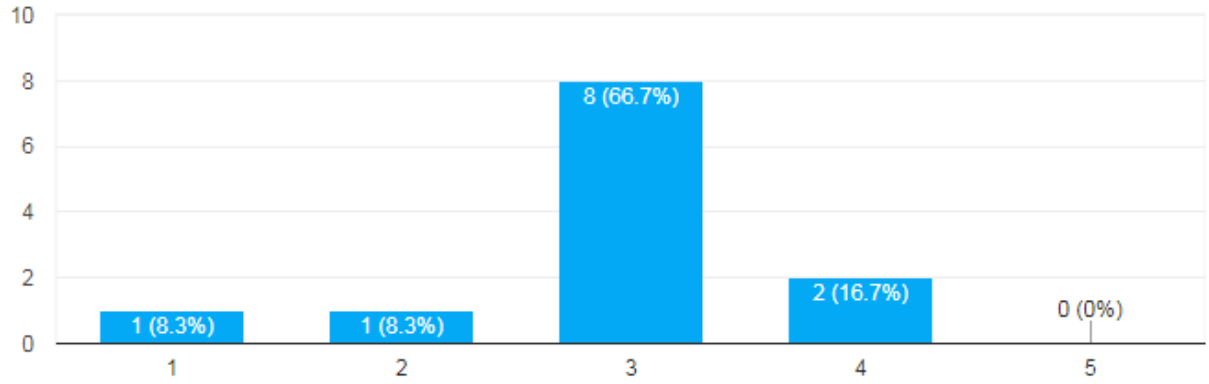
6. How often do you work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotellobby etc). Där 1 är *Never* och 5 är *Very Often.*



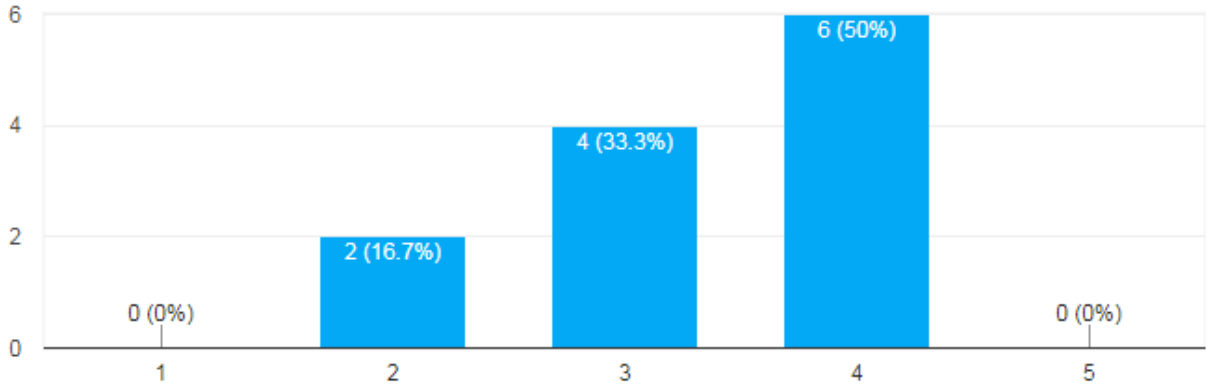
7. Do you ever skip security directives to easier perform your work tasks? Där 1 är *Never* och 5 är *Very Often.*



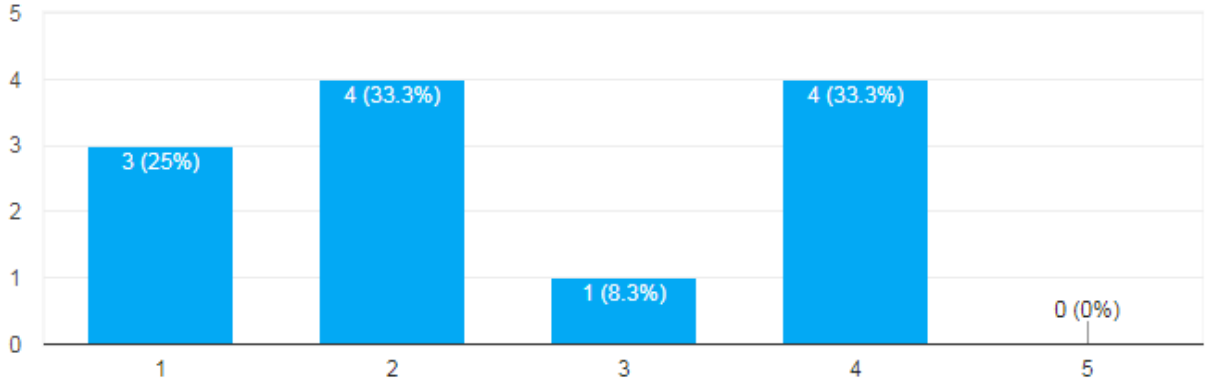
8. How easy is it to communicate issues with InfoSec management? Där 1 är *Hard* och 5 är *Very Easy.*



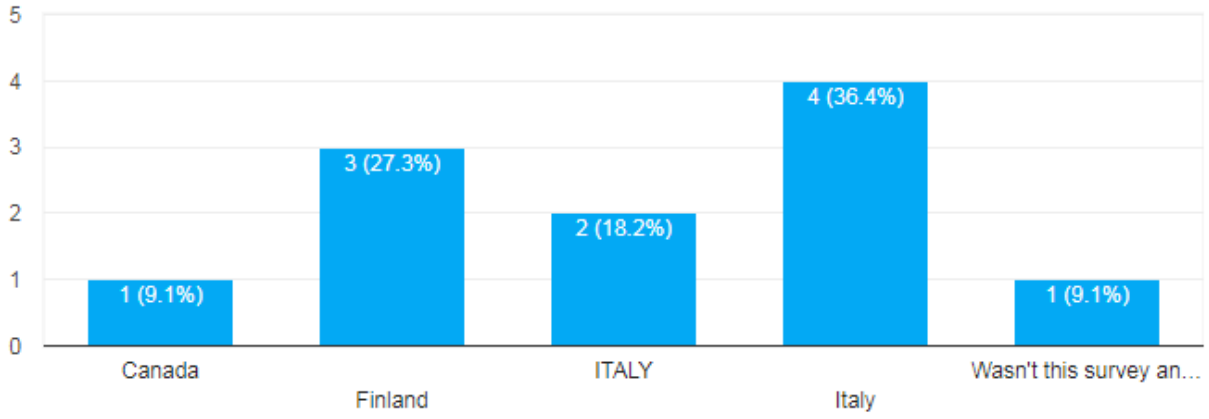
9. What's your general impression of the security policies and directives? Där 1 är *Bad* och 5 är *Great.*



10. How did you assess the threat level of opening this link and email? Där 1 är *No Risk* och 5 är *High Risk.*



11. In which country are you employed?



5. Analys och Diskussion

Enligt den teori som presenterats i kapitel 2 finns det flera nyttiga lärdomar om hur informationssäkerheten hos ett företag eller organisation kan eller bör se ut. Till exempel i avsnitt 2.6 presenteras policys och dess viktiga roll inom informationssäkerheten. Denna betydelse av policys har fått genomslag i företaget där nästan hela säkerhetsarbetet baseras på just dessa policys eller direktiv som de även kallar dem. Bland annat nämns det av Säkerhetschef på företaget, Respondent 1, att dessa policys har skapats med flera av de punkter som Gollman (2011) och LeVeque (2006) tar upp, men även en viss grund från CIA modellen (kapitel 2.3). Detta ger intrycket att företaget har skapat sina policys och direktiv på ett efterforskat sätt och baserat dessa på väl etablerade modeller och teorier. Ett annat verktyg som använts inom säkerhetsarbetet är enligt R1 riskanalyser. Att göra riskanalyser (se kapitel 2.2) är ett bra sätt för en organisation att få ordning på sina resurser och att se till att dessa är säkra från hot (LeVeque, 2006). Detta är något som R1 också diskuterar att de försöker bli bättre på att göra regelbundet. Enligt R1 är det svårt att göra en bra riskanalys och framförallt bedöma hotbilder mot säkerheten då företaget bland annat är en så stor och komplex organisation.

Att deras policys och direktiv skapats på ett efterforskat sätt förstärks ytterligare i deras arbete med att upprätthålla dessa regler. Detta arbete görs genom att nya anställda bland annat går kurser eller utbildningar inom informationssäkerhet och hur företaget arbetar med just upprätthållandet av säkerheten. Dessa kurser görs även regelbundet av alla medarbetare, vilket är obligatoriskt, för att underhålla detta säkerhetstänk men även att för att kontinuerligt kunna uppdatera programmen med ny information och regler. Detta då det bland annat kommer nya tekniker och liknande som kanske inte omfattas av nuvarande säkerhetsregler. Ett exempel på detta gavs av Respondent 3 (R3) och var införandet av *Bring Your Own Device* (BYOD). Detta innebar nya utmaningar för säkerhets organisationerna inom företaget och är ett bra exempel på hur företaget behövde hålla sig moderna med hur arbete utförs, men även att inte låta detta påverka säkerheten. Detta system med BYOD är däremot inte helt perfekt som påpekats av R3, men det behöver finnas en balans med vad som är praktiskt och hjälpande för arbetet och vad som är bidragande till bättre säkerhet, men kanske då ett hinder för effektivt arbete.

Vidare förstärks motivationen med att upprätthålla och efterfölja de uppsatta regler och policys genom så kallade *"Security Awareness"* program/dagar där bland annat informationssäkerhets organisationen inom företaget lyfter säkerhetens betydelse och bidrar med övrig information och hjälp inom detta. Användandet av security awareness program är också en direkt koppling till den teori som presenterades i kapitel 2, mer specifikt av Gollman (2011) där just dessa program är bra redskap för att motivera anställda om betydelsen med att följa företagets regler inom säkerhet. Ytterligare sätt att lyfta betydelsen av informationssäkerhet och för att motivera anställda att följa reglerna inom detta är enligt Gollman (2011) och LeVeque (2006) att detta informationssäkerhetsarbete har stöd från företagets ledning, vilket är fallet i denna studie. Bland annat undertecknas dessa regler av företagets VD. Engagemanget från medarbetare runt säkerheten är därför en viktig komponent för att få en framgångsrik eller välmående informationssäkerhet.

Ansvaret för att följa reglerna ligger däremot till största del hos den enskilde anställde inom företaget, detta enligt samtliga respondenter. Just därför förlitar sig företaget på att göra en del kontroller men även till stor del att anställda själva rapporterar incidenter relaterade till

säkerheten. Detta kan då leda till en del utmaningar för säkerhetsorganisationen, bland annat finns där sannerligen ett stort mörkertal av incidenter som inte rapporteras, men även att man kanske inte kan hitta grunden till dessa incidenter och hitta åtgärder för att lösa dem. Det kan till exempel vara brist på kunskap, dåligt utformade regler som därmed är hinder för arbete eller liknande. Därför är kommunikationen mellan informationssäkerhets organisationen och resten av företaget väldigt viktig. Det påpekas även att det kan finnas en del kulturella skillnader i hur säkerheten uppfattas, både mellan avdelningar men även i andra länder då företaget är internationellt. Ett sätt att kommunicera, utöver security awareness dagarna, har varit att lägga ut meddelanden och liknande på anställdas skärmsläckare som då belyser aktuella problem eller antalet incidenter och liknande.

Innebörden av tydlig kommunikation och upplysning av gällande policys och direktiv bidrar även till att mängden oavsiktliga interna hot (kapitel 2.9) kan minska. Enligt D'Arcy (2009) kommer majoriteten av hoten mot informationssäkerheten inifrån organisationen, och kan då enligt D'Arcy (2009) och Wall (2013) till exempel vara brist på kunskap om befintliga regler och procedurer, eller att dessa är konstruerade på ett sätt som hindrar den anställde från att jobba effektivt och därmed kringgås. Det kan även vara vanliga misstag som görs. Just oavsiktliga misstag nämns av en del respondenter och att dessa kanske inte nödvändigtvis rapporteras utan att de istället enbart informerar den "skyldige" om vad som faktiskt gäller. Detta kan grunda sig i att kunskap som finns inom verksamheten är "dold" och att endast ett begränsat antal personer känner till viss information. Kunskapen är således inte integrerad i inom verksamheten i tillräckligt stor utsträckning (Ahsenden, 2018).

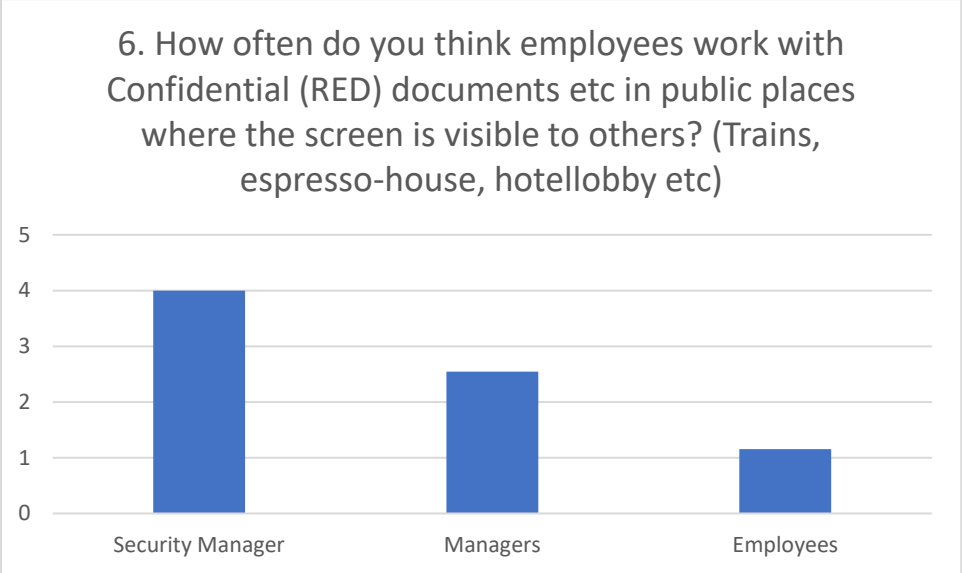
Vidare om hur policys och direktiv uppfattas och efterföljs, allmänt säkerhetstänk och liknande diskuteras nedan. Denna diskussion baserar sig på de resultat som fåtts från enkätundersökningen (kapitel 4.3) som i sin tur baseras på information given av en av företagets säkerhetschefer (R1) och interna dokument från företaget (bilagor 8-10).

Genom att till en början titta på resultaten av enkätundersökningarna som anställda i Sverige genomfört, och vad säkerhetschefen (R1) tror att anställda i Sverige kommer att svara, kan vi påvisa en del skillnader mellan den uppfattning som säkerhetschefen har, och hur det ser ut i realiteten. Tilläggas bör att ansvarig för informationssäkerheten ensam besvarat den enkät som används som referensmall, och att vi av den anledning endast har ett perspektiv som ställs mot de resultat som framkommit via anställda. Vidare kan man anta att R1 behövt generalisera när uppskattningar gjorts om personalens medvetenhet beträffande informationssäkerhet. Verksamheten har ett flertal avdelningar där arbetsuppgifternas karaktär varierar, vilket även betyder att synen på informationssäkerhet kan se olika ut beroende på vilken avdelning som avses.

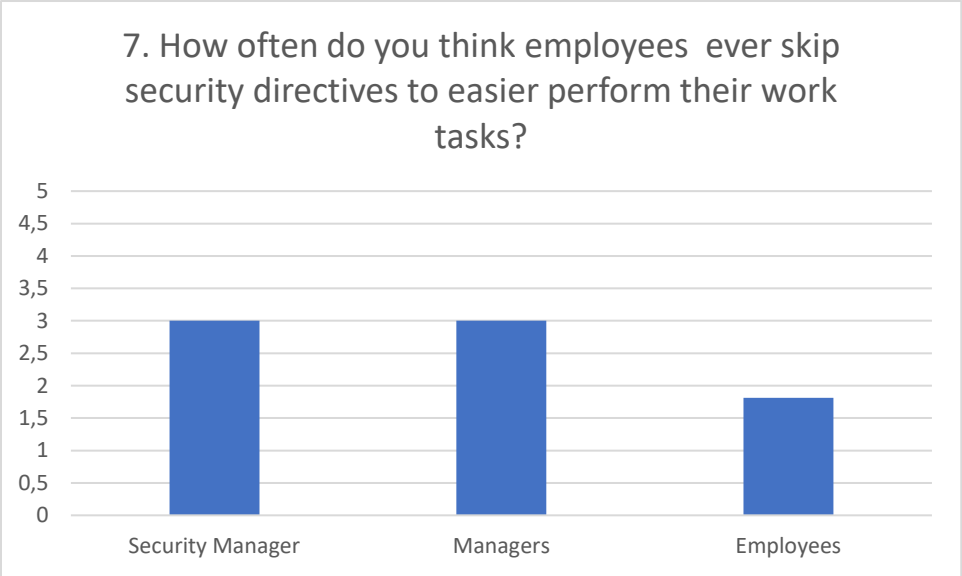
Frågorna som undersökningen är baserad på är starkt knutna till den policy som finns inom företaget, och bekräftar dels att regelverket i vissa delar efterlevs bättre än vad säkerhetschefen trott på förhand, samtidigt som det i andra delar finns uppenbara brister i hur anställda hanterar den information som finns inom organisationen.

Anställda använder sällan eller aldrig USB-stickor för både privat - och arbetsrelaterade uppgifter, vilket tyder på att det finns en stark medvetenhet om att lagringsmedium i sådant format kan påverka informationssäkerheten. Dels kan det vara så att minnet i större utsträckning kan försvinna om det används vid olika tillfälle, samt att man vid privat bruk eventuellt inte har samma riskmedvetenhet som under arbetstid, vilket kan göra att skadlig kod överförs till minnet, för att sedan föras vidare till arbetsdator. Med samma utgångspunkt får man anta att anställda inte kopplat in USB-stickor med okänt ursprung i sina arbetsdatorer.

Nästa betydande skillnad rör konfidentiell information med högsta säkerhetsklassning och hur detta lagras, enligt resultaten av fråga 3. Närmare 60 procent av respondenterna svarar med siffran 3 eller lägre, medan säkerhetschefen svarat med en fyra på den femgradiga skalan. Detta visar dels på att säkerhetsklassad information ofta lagras i klartext men även att anställda eventuellt inte är införstådda med policyn, eller att de väljer att frångå de uppsatta riktlinjerna avsiktligt. På fråga om hur ofta anställda använder publika nätverk för arbete visar det sig att dessa används i mindre utsträckning än vad R1 trott. Anställda arbetar även med känslig information på sina arbetsdatorer i offentliga miljöer i långt mindre utsträckning än vad säkerhetschefen anger på fråga om vad denne tror. Detta visas i diagrammet nedan där staplarna visar medelvärdet på respondenternas svar.



Skillnader mellan R1:s uppfattning och anställdas åsikt påvisas även i viss utsträckning genom svar på fråga sju där endast cirka 12 procent av respondenterna anger “tre” som svarsalternativ, vilket även är den siffra R1 svarar med. Övriga respondenter har angett siffran “ett” eller “två” på fråga om hur ofta de väljer att kringgå rutiner för informationssäkerhet för att underlätta för sina egna arbetsuppgifter. Detta står i motsats till vad som framkommit på fråga om hur ofta anställda krypterar information med högsta säkerhetsklassning. Bilden av hur anställda kommunicerar med ansvariga för informationssäkerhet överensstämmer ganska väl med hur R1 ser på saken. Vidare väljer anställda att svara att de ser positivt på policys och riktlinjer. Detta visas i diagrammet nedan där staplarna visar medelvärdet på respondenternas svar.

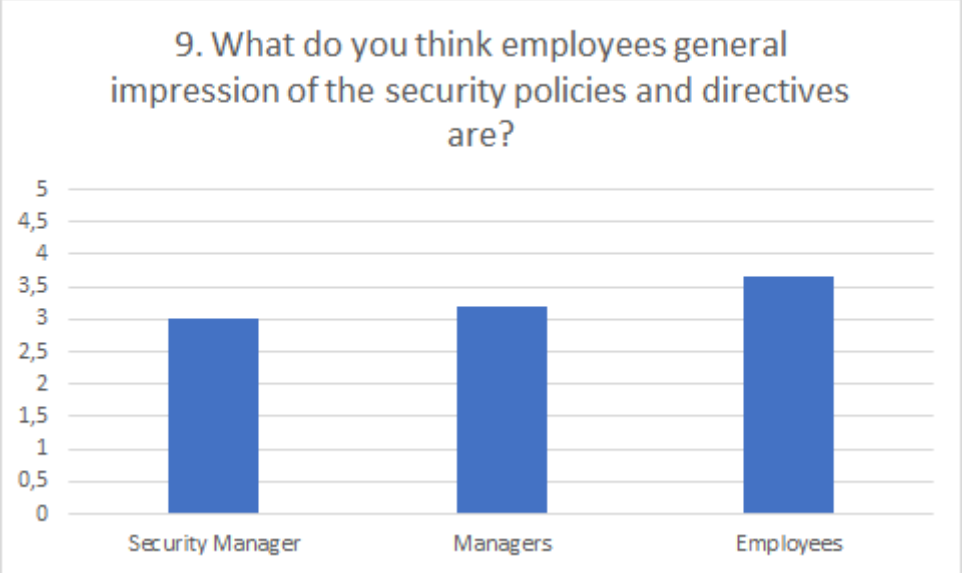


När man tittar på hur chefer besvarat frågor om hur de tror att anställda arbetar när det kommer till informationssäkerhet kan man se att dessa svar generellt överensstämmer bättre med de hur det ter sig i verkligheten, än de resultat som framkommit i samband med att säkerhetschefen fått göra sina antaganden om anställda och dess informationshantering. Väljer man att granska siffrorna närmare i enskilda frågor kan man även se att chefer tenderar till att utgå från att anställda hanterar säkerheten sämre än vad de faktiskt gör. Undantaget är frågan som rör dokument som är klassificerade som "röda" i fråga nummer tre.

Anledningen till att säkerhetschefens uppfattning skiljer sig åt markant mot hur anställda faktiskt arbetar kan grunda sig i att R1 endast arbetar med säkerhetsfrågor och har väldigt hög medvetenhet om hur konsekvenser kan påverka verksamheten i stort. Det kan även vara så att en person som arbetat med säkerhetsfrågor under en längre tid har ett visst mått av misstänksamhet mot personer och hur dessa i sin tur hanterar känslig information. Personen i fråga och dennes syn på informationshantering kan även ha färgats av de utlandsvistelser som omnämns vid intervjun, där det framkommer att man har ett helt annat förhållningssätt till informationssäkerhet än i Sverige. Det faktum att avdelningschefer på ett bättre sätt kunde förutspå anställdas svar på enkätundersökningen kan grunda sig i att de har en bättre personkännedom då de arbetar med varandra på daglig basis.

Vid en närmare granskning av de interna dokumenten (bilaga 8-10) ser man att den bild av policys, direktiv och liknande som målades upp av framförallt respondent 1, men även av övriga respondenter, stämmer bra överens med det som framkommit i resultatet. Bland annat finner vi en tydlig struktur över de regler och direktiv där det på ett enkelt sätt framkommer vad som förväntas av den anställde samt övrig nyttig information gällande företagets informationssäkerhet såsom ansvariga chefer och så vidare.

Beträffande diskrepansen mellan varför det i vissa fall skiljer sig med hur ledning (managers) upplever sina anställdas syn på informationssäkerheten och hur de arbetar med denna, och hur de anställda faktiskt arbetar kan detta bland annat bero på icke tillfredsställande kommunikation mellan just ledning och anställda. Detta kan bland annat ses i resultaten på frågorna 8 och 9 i enkäten. Diagrammen nedan visar medelvärdet av respondenternas svar.



Här kan vi då se att chefer tror att anställda har det svårt att kommunicera informationssäkerhets problem med just avdelningen för detta, och anställda har svarat i snitt medel, vilket i och för sig inte är särskilt bra, men bättre än vad cheferna trodde. Den interna kommunikationen är något som borde vara av hög prioritet då det annars riskeras att få negativa effekter genom hela organisationen, detta är något som Ingelmo Palomares et al (2018) bland annat diskuterar (se kapitel 2.8). Den interna kommunikationen kan även ha en inverkan på arbetsklimatet och kulturen inom en organisation (Ingelmo Palomares et al, 2018). Detta kan bero på att organisationen inte når ut till medarbetare med det fortlöpande arbetet som görs beträffande informationssäkerhet, vilket beskrivs av R1. Utbildningar som hålls kanske inte uppfattas som givande och viljan att ta till sig ny information kan därav bli begränsad. Detta kan resultera i att medarbetarnas engagemang vad gäller

informationssäkerhet förblir relativt låg på de avdelningar som undersökts (Chang et al. 2007). Det kan även vara så att chefer inte beaktat organisationskulturen när man tagit fram strategier, policys och riktlinjer för hur informationshanteringen ska se ut (Chang et al. 2007). En annan anledning till att anställda inte tycker att kommunikationen fungerar fullt ut med ledningen, kan vara att kritiska framgångsfaktorer inte beaktats i samband med att strategier för säkerhetsarbetet tagits fram av personer i chefsposition. På så sätt har arbetet inte genomsyrats av CSF och de mål som verksamheten satt upp (Caralli, 2004).

6. Slutsats

Frågeställningen som uppsatsen avser besvara lyder:

> "*Hur förhåller sig arbetet med informationssäkerhet inom en organisation verksamt inom IKT med utvalda teorier inom området, och hur följer anställda de regelverk som finns uppsatta jämfört med hur organisationens ledning upplever att regelverken följs?*"

För att besvara denna fråga började vi studien med att undersöka tidigare material och den teori som finns inom området informationssäkerhet. Dessa teorier, litteratur, tidigare undersökningar från vetenskapliga journaler och liknande skapade en grund för fortsättningen av studien. Efter att denna teoretiska grund skapats arbetades det fram en metodik för hur datainsamlingen skulle gå till, alltså de intervjuer och enkätundersökningar vi gjort, samt de interna dokument vi fick ta del av. Denna metodik baserades även den på befintligt material såsom kursböcker inom just metodik för skrivandet av uppsatser och liknande. Den första intervjun som gjordes baserades på den teoretiska grunden (kapitel 2) och utgjorde senare en grund tillsammans med de interna dokumenten (bilaga 8-10) för hur resterande intervjuer och enkätundersökningar utformades. Detta då den första intervjun gjordes med en säkerhetschef från företaget och dennes kunskap och insyn var då tillsammans med de interna dokumenten kring ämnet instrumentala för att kunna ställa relevanta frågor i resterande intervjuer och enkäter.

Vi har hittat viktiga faktorer som visar hur företaget och dess anställda arbetar med informationssäkerhet, och därmed besvarar forskningsfrågan som följande:

Företagets väl konstruerade policys och direktiv ger en tydlig bild över vad den anställde ska tänka på och göra i sitt dagliga arbete för att efterfölja att informationssäkerheten uppehålls. Genom att ha dessa policys och direktiv konstruerade på detta tydliga sätt minskar risken för missförstånd och misstag hos anställda. Det är även viktigt att dessa policys och direktiv täcker de potentiella hoten och riskerna som kan finnas.

Medvetenhet är nästa faktor för hur företaget arbetar med informationssäkerhet, denna faktor är viktig då den till del överlappar med de andra faktorerna. Med medvetenhet menar vi att både anställda och ledning inser vikten av bra informationssäkerhet och förstår dess roll och betydelse i det dagliga arbetet. Detta gäller då alltså både att vara medveten om de uppsatta reglerna och att vara medveten om det ansvar man som anställd inom företaget behöver ta för att säkerställa att man gör sin del av arbetet med informationssäkerhet. Vidare är även bra intern kommunikation en viktig del av detta då det direkt påverkar hur medvetna både ledning och anställda är om diverse problem som kan finnas angående informationssäkerheten, och även hur synen på detta arbete uppfattas i företaget.

Ansvar är därmed nästa faktor som visar på hur företaget arbetar med informationssäkerhet. Det påvisas flera gånger i resultaten att eget ansvar är en stor del av informationssäkerheten inom företaget. Detta ansvar innebär då att man som anställd har en skyldighet till företaget att både vara medveten om de uppsatta reglerna som finns samt att efterfölja dem. För att påpeka detta ansvar och för att öka medvetenheten har företaget diverse aktiviteter som ska få anställda att vara mer medvetna om säkerhetsarbetet och de interna reglerna.

Slutsatsen som vi drar är således att de tre faktorerna om väl konstruerade policys och direktiv, medvetenhet och ansvar är bland de viktigaste för hur organisationen i fråga arbetar med informationssäkerhet på ett lyckat sätt. Dessa tre faktorer har varit vanligt förekommande i de kvalitativa undersökningarna och resultaten från de kvantitativa undersökningarna påvisar även detta samband.

Genom att ta hänsyn till dessa faktorer kan man förvänta sig ett bra resultat gällande arbetet med informationssäkerhet inom en organisation. I så fall bör även det motsatta gälla, om företaget inte tar hänsyn till faktorerna lär informationssäkerheten därmed bli lidande.

Dessa faktorer ligger även i linje med den teoretiska grund som presenterats i början av arbetet vilket påvisar att dessa faktorer även kan förekomma inom andra stora företag verksamma inom IKT.

6.1 Förslag till vidare studier

Studien undersöker enbart hur ett företag arbetar med informationssäkerhet och hade därför kunnat breddas till att undersöka flera företag, exempelvis inom olika branscher och av olika storlek, och dra paralleller och jämförelser däremellan, och på så vis kontrollera att de tre framtagna faktorerna är relevanta i samtliga fall.

Vidare hade fler avdelningar inom företaget kunna undersökas. Genom detta hade ett större antal anställda besvarat enkätundersökningar vilket lett till att även dessa avdelningar fått ge sin syn på informationssäkerheten inom verksamheten. I nuläget undersöks endast avdelningar där man kan anta att arbete med informationssäkerhet är en del av den dagliga verksamheten. Genom att bredda undersökningen till att omfatta hela organisationen hade förmodligen nya och intressanta aspekter kunna behandlas.

Bilaga 1 Enkät till Managers

Följande enkät skickades som ett google docs formulär online. Företagets namn samt Respondent 1 namn har reviderats till ”*företaget”* samt R1.

10 Questions regarding InfoSec - Manager

Hi,

Thank you for taking time to answer these questions regarding *företagets* Information Security.
These questions have been approved by R1 (Security Operational Manager at *företaget*) regarding what can or can't be discussed.
All of this is 100% anonymous and voluntary.

These questions are part of our Bachelor Thesis work in Information Security / Informatics where we are investigating the relation between InfoSec theory - practice from management perspective and its practice from employee level.

These questions are for the manager perspective, how you as managers think the average employee would act, not how they should.

Thanks again for taking time to do this.

Best regards
Theodor Nestler & Toni Dell Aquila

1. How often do you think employees use external drives such as USB for both private and business use? (same unit)

Never 1 2 3 4 5 Very Often

2. How do you think employees act if they find a USB without knowing its origin (like employee parking), what are the chances that they would plug it in to their work station?

No Chance 1 2 3 4 5 High Probability

3. If employees keep confidential (RED) data on a USB drive, how often do you think they would encrypt it?

Never 1 2 3 4 5 Very Often

4. How often do you think employees use public networks on their work-laptop? (Starbucks, Espresso-House, Trains etc)

Never 1 2 3 4 5 Very Often

5. How often do you think employees work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotel lobby etc)

Never 1 2 3 4 5 Very Often

6. How often do you think employees work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotel lobby etc)

Never 1 2 3 4 5 Very Often

7. How often do you think employees ever skip security directives to easier perform their work tasks?

Never 1 2 3 4 5 Very Often

8. How easy you think employees find it to communicate issues with InfoSec management?

Hard 1 2 3 4 5 Very Easy

9. What do you think employees general impression of the security policies and directives are?

Bad 1 2 3 4 5 Great

10. How do you think employees assessed the threat level of opening this link and email?

No Risk 1 2 3 4 5 High Risk

Bilaga 2: Enkät till anställda i Sverige

Följande enkät skickades som ett google docs formulär online. Företagets namn samt Respondent 1 namn har reviderats till ”*företaget”* samt R1.

10 Questions regarding InfoSec – Employee

Hi,

Thank you for taking time to answer these questions regarding *företagets* Information Security.
These questions have been approved by R1 (Security Operational Manager at *företaget*) regarding what can or can't be discussed.
All of this is 100% anonymous and voluntary.

These questions are part of our Bachelor Thesis work in Information Security / Informatics where we are investigating the relation between InfoSec theory - practice from management perspective and its practice from employee level.

These questions are for the manager perspective, how you as managers think the average employee would act, not how they should.

Thanks again for taking time to do this.

Best regards
Theodor Nestler & Toni Dell Aquila

1. How often do you use external drives such as USB for both private and business use? (same unit)

Never 1 2 3 4 5 Very Often

2. If you find a USB without knowing its origin (like employee parking), what are the chances that you would plug it in to your work station?

No Chance 1 2 3 4 5 High Probability

3. If you keep confidential (RED) data on your USB drive, how often do you encrypt it?

Never 1 2 3 4 5 Very Often

4. How often do you use public networks on your work-laptop? (Starbucks, Espresso-House, Trains etc)

Never 1 2 3 4 5 Very Often

5. How often do you work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotel lobby etc)

Never 1 2 3 4 5 Very Often

6. How often do you work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotel lobby etc)

Never 1 2 3 4 5 Very Often

7. Do you ever skip security directives to easier perform your work tasks?

Never 1 2 3 4 5 Very Often

8. How easy is it to communicate issues with InfoSec management?

Hard 1 2 3 4 5 Very Easy

9. What's your general impression of the security policies and directives?

Bad 1 2 3 4 5 Great

10. How did you assess the threat level of opening this link and email?

No Risk 1 2 3 4 5 High Risk

Bilaga 3: Enkät till anställda internationellt

Följande enkät skickades som ett google docs formulär online. Företagets namn samt Respondent 1 namn har reviderats till ”*företaget”* samt R1.

10 Questions regarding InfoSec – International Employee

Hi,

Thank you for taking time to answer these questions regarding *företagets* Information Security.
These questions have been approved by R1 (Security Operational Manager at *företaget*) regarding what can or can't be discussed.
All of this is 100% anonymous and voluntary.

These questions are part of our Bachelor Thesis work in Information Security / Informatics where we are investigating the relation between InfoSec theory - practice from management perspective and its practice from employee level.

These questions are for the manager perspective, how you as managers think the average employee would act, not how they should.

Thanks again for taking time to do this.

Best regards
Theodor Nestler & Toni Dell Aquila

1. How often do you use external drives such as USB for both private and business use? (same unit)

Never 1 2 3 4 5 Very Often

2. If you find a USB without knowing its origin (like employee parking), what are the chances that you would plug it in to your work station?

No Chance 1 2 3 4 5 High Probability

3. If you keep confidential (RED) data on your USB drive, how often do you encrypt it?

Never 1 2 3 4 5 Very Often

4. How often do you use public networks on your work-laptop? (Starbucks, Espresso-House, Trains etc)

Never 1 2 3 4 5 Very Often

5. How often do you work with Internal (YELLOW) documents in places where the screen is visible to others? (Trains, espresso-house, hotel lobby etc)

Never 1 2 3 4 5 Very Often

6. How often do you work with Confidential (RED) documents etc in public places where the screen is visible to others? (Trains, espresso-house, hotel lobby etc)

Never 1 2 3 4 5 Very Often

7. Do you ever skip security directives to easier perform your work tasks?

Never 1 2 3 4 5 Very Often

8. How easy is it to communicate issues with InfoSec management?

Hard 1 2 3 4 5 Very Easy

9. What's your general impression of the security policies and directives?

Bad 1 2 3 4 5 Great

10. How did you assess the threat level of opening this link and email?

No Risk 1 2 3 4 5 High Risk

11. In which country are you employed?

Bilaga 4: Transkribering av intervju med R1

Intervjun började med att respondenten kort introducerade sig själv och hade även förberett en kort power-point presentation som introduktion till hur företaget arbetar med säkerhet. Därefter följde vi upp med frågor.

Respondenten har haft möjlighet att göra revideringar och borttagning av text i transkriberingen för att skydda bland annat företagshemligheter och liknande som skulle kunna avslöja företaget.

Indragen text efter ”-” är vi som pratar.

Jag heter X och jag kör säkerheten här lokalt och i XXX, och sen så kör jag krishantering i Europa och Latinamerika och kommer även att köra threat analysis smått, ganska nytt område inom företaget och vi har inte det på banan ännu och vet inte riktigt hur det ska gå till men ska ha någon lösning på det.

Vad det gäller informationssäkerhet så är alla som jobbar i säkerhetsorganisationen dem är involverade med informationssäkerhet, sen har vi en specifik grupp som är mer involverade i informationssäkerhet. Som driver, precis som jag driver krishanteringen så finns det någon annan som driver informationssäkerhet då, i det här *MarketArea*-teamet, och jag kommer in lite mer på det här hur fördelningen av uppgifter går till men generellt så är det alla anställdas ansvar att hantera information i enlighet med policys och så.

Jag har några slides här som jag tänkte visa lite här innan ni kör igång och ställer frågor

- Okej

Så i företaget så har vi delat in säkerhetsområdet i tolv delområden. och då informationssäkerhet är ett. i övrigt så är det som jag var inne på Threat & Vulnerability management, crisis management, BCM (Business Continuity Management).

Personal security, Physical security, Sourcing security. Security Awareness. Sales support, security governance och privacy.

Och då är samtliga områden indelade i Security Operations och informationssäkerhet. Och informationssäkerhets delen omfattar då informationssäkerhet, privacy, BCM och övriga område har vi lagt i security operations.

Fokus just nu i informationssäkerhet är BCM och det är privacy. Privacy självklart då med hänsyn till GDPR och så vidare. Så har varit mycket fokus på det under 2017 och fortsatt fram här då innan maj och därefter. BCM har varit lite spretande globalt sett, i vissa delar av världen har vi legat ganska högt med implementeringen av detta medan andra delar har varit lågt och vissa har dels implementerat det mest basala, så är läget och vad gäller informationssäkerhet så kan jag komma in på det lite senare.

- Får jag bara ställa en fråga X? På förra sliden, kan du lite mer förklara BCM?

Ja, med Business Continuity Management, det är alltså, sånt som det händer incident nu, för tillfället men den ordinarie organisationen kan hantera detta, vi behöver inte tillföra speciella resurser eller support utifrån, utan händer detta på en enhet A så hanterar enhet A detta. Egen personal och egna resurser. Men skulle de inte lyckas med detta utan det eskalerar, fortsätter förvärra situationen då övergår det till krishantering och då tillsätter vi resurser och eller personal.

- Och då blir du inblandad?

Ja, just det.

Den globala staben då, group security organisation, vi har en CSO (*Chief Security Officer)* naturligtvis, och sen har vi då leads för dem områdena som syns där. Informationssäkerhet och security operations och sen är där vissa advisor fattningar också då som stödjer generellt.

Nu står det regional security director här men det är struket, det finns ingen region längre utan det är istället market areas. Och då är det Europa och Latinamerika som vi är inne på då, Asien med Oceanien och Indien är en.

- Kan man säga att det är variationer på säkerheten baserat på regionerna eller är det mer centralt styrt från början och sen implementerat i regionen eller är det lite olika per market area?
- Dvs, styrs säkerheten centralt av gruppen och sen…

Ja juste, detta är då centrala teamet och därefter har vi på varje market area, det är alltså geografiska områden, sen har vi på business area områden säkerhetsorganisationer.

- Men dem där regionala kan vi säga, organisationerna svarar till den centrala säkerhetsorganisationen?

Ja just det, precis. Och sen går det till vidare så att, country eller cluster of countries rapporterar då till market areas och under där så har vi ner på site-nivå. I Sverige har vi säkerhet organisationer på alla siter, i princip, där är några kontor som har något separat. Men det har dem inte på många platser, säg Afrika till exempel, där har man cluster of countries där en eller ett par säkerhets managers som svarar för ett helt område. I huvudsak så har större R&D som kräver högsta säkerhetsklassificeringen security managers. Detta är alltså säkerhetsorganisationen som har till uppgift att ge styrningar, rådgöra, kontrollera, uppföljning och så vidare att organisationer följer förståelserna.

Sen security governance det bildas då av security boards och högsta instans för informationssäkerhet är då Global Information Security Board (GISB). Sen har dem ett core-team som består av några av dem här deltagarna och leds då av CISO, Chief Information Security Officer. Här hanteras allting som kommer underifrån i organisationen, hanteras av

detta sen är det då beslutsfattning i GISB och det leds av CFO och drivs av CSO. Det är högsta instans av informationssäkerhet. Vi har även privacy core team. Sen är det order på att varje business area och varje market area dem måste ha security management boards. Sen är det upp till dem att bestämma om man måste ha även på lägre nivå. Till exempel om underenheter också behöver, men det är upp till dem själva att bestämma.

- Dem här är egentligen en lokal variant av den översta klassen så att säga? Är detta en lokal variant av…

Ja just det, exakt. Det går igenom hela organisationen, dem här security management boards. Befattningshavare är, vi kommer till det här längre fram, nästa slide här. Återkommer jag till det. Men det är rätt. Det är lokala (*varianter)* av högsta det organet GISB.

Vi har specifika grupper som leder security governance, crisis management, compliance & investigation och privacy. Så på gruppnivå som vi är inne på är det GISB som är högsta organ och sen så market area, customer unit och siter.

Krishantering är ett eget separat team och group compliance, det är dem som beslutar om konsekvenser av felaktigt beteende hos personalen. Är det någon som ska få löneavdrag och liknande, vad det nu kan vara.

Här är en standard agenda för den här security management board och detta är då för stad XXX och leds av site ledaren, och som security managern driver och sen är där då representanter från alla viktigaste enheterna. Och målet är alltså “Secure that XXX Security Governance concept will support the protection of customer’s interests, XXX brand, people and information. Security shall be a part of day-to-day business operations.” Och sen är det då en stående agenda.

Ja, informationssäkerhet 2016/2017 har det pågått ett ganska omfattande arbete med att, först och främst inventera all informations “assets” och klassa detta. Och i företaget gör vi klasserna: Public, Internal, Confidential. Vi har då 3 klasser. Där är ett förslag på en fjärde, Strictly Confidential, men för tillfället är där 3. Och det finns behov den fjärde klassen, tycker jag. Om man bara har confidential, då är det väldigt mycket som hamnar i den klassen. Och så kan det bli svårt det här just med att prioritera vad är som verkligen behöver skyddas. Och det var med i det här arbetet då att ta fram vad är det, det verkligt skyddsvärda. Det är jättemycket information som är viktig, men vad är den kritiska informationen som vi måste skydda till varje pris? Och det kallar vi då global information assets, GIA. Och det motsvarar typ 5% av all information inom företaget. Till exempel *Patent* ingår där.

Och i det här arbetet ingick också att när man har tagit fram och gjort en riskinventering och registrerat dem som är very high och high, bedömt risker då, skulle alla av dessa, 100% alltså,

ha åtminstone förslag på lösning, vad ska vi vidta för åtgärder för att öka säkerhetsnivån inom dem här områdena? Ett omfattande arbete som pågått under 2 års tid.

Företaget är inte globalt certifierade i ISO 27001 men är "aligned with". Och det är delar som är certifierade fullt ut och det pågår ett omfattande certifieringsarbete just nu.

Okej, det var en kort introduktion. Ni kan få ta del av detta efteråt. Ni kan köra igång och ställa frågor.

- Finns risk att vissa frågor överlappar med det som redan sagts.

Det gör ingenting. Absolut, jag kan kanske inte svara på allting nu men kan då ta reda på det sen och så kan vi komplettera på så sätt.

- Sen kommer du få möjlighet att ta del av allt vi har skrivit och se om det är något du vill ta bort eller ändra. Så om det är något du säger nu som du kanske ångrar dig om sen så stryker vi det och så vidare.
- Då kör vi igång: Ledningen, hur ser dem på och tycker dem det är viktigt med säkerhetsarbetet eller är det lite second-hand?

Nej jag tycker det är väldigt gott, extremt bra stöd från ledningen när det gäller säkerhet överhuvudtaget och absolut informationssäkerhet. och det är nästan en förutsättning skulle jag säga. Det gör också att personal i allmänhet, det finns alltid dem som faller utanför men personal i allmänhet tycker jag har väldigt bra engagemang och förståelse för att "Ja det är faktiskt så här att vi måste skydda vår information".

- Gör ni revisioner av informationssäkerheten? Har ni någon form av kontinuerlig uppföljning av ert arbete löpande, eller hur?

Ja, just det. Om ni kommer ihåg den här jag visade om med Security Management områden, så är detta del inom security management maturity model som vi har kört och där man kvartalsvis, man sätter upp årliga mål och därefter är det kvartalsvis rapportering upp till "group". och där man gör en bedömning då som sen utvärderas av group så att, det är nogsam uppföljning på att dem här målen nås.

- Och du nämnde kort innan om policys, hur tar ni fram dessa? Hur arbetar ni med policys?

Det är ju övergripande policys som group tar fram och vi kan ju titta på … (*bläddrar fram ett dokument)*

- Kan man säga att ni har olika lager av policys?

Ja i respektive så högst upp så ligger en policy som styr det övergripande. Vad är målsättningen? Vad är det vi vill uppnå med säkerheten inom det här området? Därefter kommer direktiv som säger hur ska vi gå tillväga för att uppnå den policyn? för att uppfylla den här policyn? Och sen efter det så kommer instruktioner som är på detaljnivå, och reglerar hur det ska gå till.

- Kan det vara anställda hur dem hanterar sina datorer?

Exakt.

- Är det någon speciell modell ni följer för att utforma dem här? Har ni ett ramverk när ni sätter dem här eller beroende på vad ni gör?

Vi kan titta på ett exempel här… *(bläddrar fram dokument)*

- Har ni till exempel, purpose, scope och såna grejer?

Jaha, ja exakt

- Så dem har en tydlig uppbyggnad?

Ja just det. Så här har vi policyn i informationssäkerhet och det är då CISO som är författare och det är CEO som har godkänt. Och här ser man då CIA, confidentiality, integrity och availability.

- Ni har inte olika strikta beroende på vilken avdelning och så?

Nä, detta är det övergripande som är samma för alla.

- Vem eller vilka är det som slutligen är ansvariga för informationssäkerheten?

Fatta beslut om olika ärenden inom informationssäkerhet, det är dom här security management boards så det är alltså inte någon enskild, men att uppfylla alla policy, direktiv och instruktioner är den enskildes ansvar. Det går inte att komma ifrån det. Det går inte att hävda att "jag visste inte" eller motsvarande. Det är allas ansvar.

- Oavsett var i organisationen man befinner sig?

Japp

- Ok.
- Fanns det exempel på sådana direktiv och instruktioner i dokumentet?
- Hade du exempel på direkta direktiv på instruktioner och policys?
- Om det är något basic som inte är alltför hemligt?
- Typ, till exempel "installera inte tredjepartsprogram" på din laptop, någon sådan grej.

Kan vi … Jag vill ogärna dela hela dokumentet men jag kan kanske göra utdrag….

Jag kan ju visa…

- Om du kan visa någon väldigt basic…

Om ni ser här och läser rubrikerna så ser ni att…

- Det finns specifika grejer här.

Ja exakt

Och…

- Det är det här jag menar om de här är nivåbaserade så att säga, till exempel om det är någon här som inte applicerbar på till exempel på HR men är mer viktig för patent.

Ja men de är fullständigt… Dom gäller alla.

- Det gäller alla OK

Ja just det. Sen är det kanske viss verksamhet på X som inte använder sig av vissa system eller motsvarande och då blir det inte applicerbart.

- Ok vad bra.
- Hur säkerställer ni att policy och riktlinjer efterlevs, hur kontrollerar man en sådan sak?

Det är inte helt enkelt, det är det inte.

Och det sker ju som jag var inne på tidigare, det sker kontroller fortlöpande men vi är också i behov av att folk rapporterar att det sker oegentlighet.

Det är omöjligt att ha sådan koll alltså på allt som händer i verksamheten. Så att nej, säg att det händer inga liksom felaktigheter eller brott här, jo det händer varenda dag. Folk som gör fel antingen medvetet eller omedvetet. Ofta vad det gäller tidspress och annat gör att folk gör fel som dom ska inte skulle gjort egentligen, om de hade tänkt efter lite innan.

- När du nämner rapportering, finns det risk eller tror du att någon i en annan del eller region att någon eller avdelning och exempelvis en överordnad där väljer att inte rapportera vissa saker som någon underställd honom har råkat eller gjort, för att skydda sig själv och sitt rykte?

Ja absolut. Så är det.

- Det förekommer?

Jag vet mycket väl, jag har själv jobbat i Kina till exempel och jag vet i kontakt med kollegor från andra håll i världen också att… ja det är väldigt olika med det här kulturella hur man ser på säkerhet och vilja att rapportera. I Kina vad det ju liksom en skymf… Massa konstiga grejer som… Jag kom dit för då hade dom haft alltså över ett år utan att ha någon security manager på deras huvudkontor i Bejing. Och så... Ja men jag kan fylla upp där ett halvår då, så åkte jag dit och insåg herregud, det är ju helt fantastiskt hur det går till här alltså och jag träffade några andra svenskar där som förklarade att nej det är ju så, vi kan ju inte lägga ut vad som helst till Kina för att vi litar inte på dom helt enkelt. Så att… Jätte märkliga grejer. Just det här, rädslan att rapportera någon. Nej det är… Men då får man också komma ut och se och… Vi är väldigt självkritiska här (*Sverige*) och tycker vi är inte så bra. Men sen när man kommer ut och ser, ja men herregud det är ju små detaljer vi håller på och finslipar på medans här försvinner ut information här helt okontrollerat. Nej, det är känsligt alltså.

Jag kan ta ett annat exempel… Jag var på den här "XXX" nu i stad XXX.

Och det var första gången jag kom dit där och då är det ju en security manager, hon leder den här från år till år, och sen får hon hjälp av någon som och stödjer. Och det var likadant där, vi hittade massa felaktigheter, beteende för folk och så vidare men hon menade på att nej… Det här tar vi inte upp. Det är för känsligt. Amen sluta herregud, det är tvärt om. Vi måste ta upp det och visa att här är fel som ni gör. Undvik detta till nästa år. Så att det är ju olika kulturer alltså.

- Hur motiverar man anställda till att följa detta?

Ett sätt som jag tycker vi kan använda oss mer av är att faktiskt sprida information om incidenter som har inträffat. Inte att lägga locket på och vara hålla på det inom säkerhetsorganisationen. Nej vi visar det för folk i organisationen att detta har hänt. Gör inte det. Vi kommer att upptäcka det. Så att, gör inte det.

- Sådana security awareness program?

Ja det kör vi ju mycket. Och vi ha ju de mandatory "mandatory e-learning training", både säkerhet med betoning på informationssäkerhet och en separat för privacy. Och sedan kör vi ju... Jag vet inte ni sett de interna skärmarna här? Vi kör ju konstant varje månad slides som rullar som vi byter varje månad. Men det finns alltid security awareness meddelande som rullar på skärmarna.

- Det är ganska intressant tillämpning, jag har inte tänkt på det tidigare.

Ja just det, och vi har fått liksom bekräftelse på att det går in också. För kör vi till exempel den här månaden att nu kör vi om rapportering av säkerhetsincidenter så kan man se att det ökar, rapporteringen alltså. Kör vi ett annat ämne så hör folk av sig med frågor eller synpunkter inom det här ämnet. Man har progress där. Sen har vi då en årlig security awareness dag, och förra året hade vi "cyber security week", men åtminstone en dag per år då vi kör ett heldags program med intervjuer som läggs upp på nätet, artiklar som rör säkerhet, skärmsläckare, ja vi brukar ha någon quizz och lite sånt här, ställa upp ett bord på en central plats och möta folk och diskutera säkerhet med dem. Och ja… Så att det tycker jag har fått rätt bra genomslag.

- Den här e-learning grejen du nämnde innan, hur ofta gör man den? Gör man den bara en gång?

Den behöver man bara göra en gång men den uppdateras… Jag tror det är minst vart tredje år. Så då kommer det en ny. Ibland blir det med kortare intervall när vi satsar på något nytt, som vi ska köra in, det kom en ny förra året och en 2016. Så där var det kortare intervall.

- Är det något nytt ni har börjar med, sådana här evenemang kring informationssäkerhet?

Ja nu ska vi se, hur många gånger har vi kört det? Tre eller fyra gånger. Så tre eller fyra år har vi hållit på. Lite olika inriktning respektive gång. Men det är något som ligger konstant i programmet.

- Tas det emot positivt av övriga medarbetare?

Jag tycker det. Jag tycker vi fått bra genomslag. Man märker på engagemanget på deltagare i quizzar och sådant här och som kommer och lyssnar. Det är inget mandatory utan det är på frivillig basis alltihop. Hela dagen har programpunkter men alla kommer naturligtvis inte på allt, och det är inte meningen heller. Att ge folk olika möjligheter att delta i någonting av detta här under dagen. Och sen de här intervjuerna som brukar vara med CSO CISO läggs upp på nätet om man inte skulle kunna se dem just den dagen.

- Hur ser samarbetet ut mellan de som håller på med informationssäkerhet och de som håller på med säkerhet inom mjukvara och hårdvara?

Det är något vi kunde blivit bättre på. IT security avdelningen de hamnar mitt emellan security och IT och sedan har vi IT security. En nivå ner så att säga, men med pilar både från IT och säkerhet. Och ibland är det sådana här… Ja meningsskiljaktigheter vem som har ansvar och inte.

- Blir det någon form av silotänk där?

Ja, och det har varit... Senaste året har det varit mer motsättningar än tidigare och lite oklara direktiv när det har varit tal om att det är med att outsourca och lägga information i molnet. Olika lösningar… Vem som egentligen är ansvarig för det här alltså. Det har varit oklara...och ovilja att egentligen från högsta ledningen att faktiskt klara ut hur ska vi ha det?

Jag har varit involverad i ett projekt här vad gäller *patent* management system, de skulle ersätta flera andra system. Då var den grundläggande frågan här naturligtvis är att vi har tre leverantörer här som erbjuder, två av dem erbjuder både molnlösning och on premises, och den tredje har bara molnlösning. Jaha, vad gäller egentligen? Kan X nu lägga *patent* som är klassat som GIA (*Global Information Assets*), det mest skyddsvärda vi har, kan vi lägga det i molnet? Och det satt långt inne innan det kom ett klart besked på det här. Och där upplevde jag att vi har informationssäkerhet, vi har IT, vi har IT security och vi har verksamheten själva som är informationsansvariga. Ni är ansvariga för er information. Ni äger den. Informationssägaren säger - vi vet inte, vi har inte den kompetensen, vi har inte den

kompetensen att göra en bedömning om detta är säkert nog. IT security vill inte ta ansvar att författa beslutet, informationssäkerhet det kom inte klart besked, det kom inget klart besked därifrån. Men frågan är utklarad nu i alla fall.

- Jobbar IT säkerhet inom samma typ av modell som du visade oss tidigare, eller har de en egen tillämpning för sin del av verksamheten?

Ja de har sin egen tillämpning. De ingår inte i det här som jag visar. Utan det är informationssäkerhet.

- Hur ser du på hur lätt eller svårt det är att få igenom förändringar av till exempel policy och liknande. Om du skulle införa en ny policy eller direktiv?

Nej det gör vi inte över huvud taget på den här nivån.

Policy är bara på gruppnivå.

- Om vi pratar mer direkta direktiv, hur är det att få in en ny sån till exempel?

Ja men det är typexempel på global... Det gäller…

- Så att driva in en ny sån är omöjligt? Hur enkelt är det att få igenom sånt förslag?

Jättesvårt att säga, du menar om vi här lokalt skulle komma på att här finns en brist som måste styras upp?

- Ja precis.

Då får man eskalera det i det här systemet och jag har aldrig varit med om det har hänt. Utan det är top down som gäller liksom. Här detta gäller…

- Det är lite av en hierarki?

Ja absolut.

- Och övriga avdelningar inom denna enhet, hur upplever ni att de följer allting?

Ja det skiljer sig åt från avdelning till avdelning. Om vi tar *patent* är de väldigt medvetna, väldigt hög security consciousness, sen kan det vara andra som är mindre mottagliga och ska jag säga något generellt såhär skulle jag säga till exempel H&R och…

- Sales?

Tack. De är ju värst.

- Upplever ni att avdelningar har svårt att kommunicera med varandra på grund av säkerheten, att de är rädda att prata emellan, exempel att *PATENT* har svårt att prata med forskningen för att de inte är säkra på vad man får prata om?

Jo det tycker jag man märker att sånt inträffar och ibland kan även alltså security requirements ge upphov till att försvåra verksamheten för business alltså. Det är uppenbart. Ja men vänta nu här, ska vi följa dessa bestämmelser kan vi inte göra ett effektivt jobb. Och då är man lite farligt ute. Det är jättelätt att sitta och bestämma generella policys som låter jättebra, men om verksamheten inte köper det, om verksamheten märker att nej det här går inte, vi kan inte jobba effektivt om vi ska uppfylla dessa regler, då kan det ge upphov till att man börjar att….

- Tumma lite på det…

Just det

.

- Lite genvägar…

Det här är helt sjukt, det kan vi inte uppfylla

Ja men nästa grej då detta skulle vi kunna uppfylla men det skiter vi i…

- Kommuniceras detta till er?

Det finns både och, det finns sådana som är väldigt öppna och kommer och säger till att man gör fel. -”Vi följer inte bestämmelser för att kunna göra vårt jobb”....

Jättebra då kan man eskalera detta, påtala att det är problem.

Men sen vet jag andra som inte gör det, utan som “ah blanda inte in säkerhet för det blir bara massa problem”.

- Svårigheter med att jobba globalt med säkerhet?

- Du nämner kulturella skillnader.

Borttaget 51:50 - 56:57 pga känslig information framkommer

- Kan det förekomma konsekvenser för en hel avdelning om informationssäkerheten bryts?

Det kan ju ge upphov till att man förlorar en hel patentfamilj, vilket alltså då är värderat till hundra miljoner. Om den här informationen läcker innan patent är inlämnade då kan X man förlora hela patentfamiljen.

- Har ni erfarenhet av stulna patent internt?

Det finns kända case som ni kan kolla mer på Google.

Jag känner till ett case, en ungersk hacker som lyckades sno en massa information från X, och han var lite skruvad, och den här människan han gjorde det i syfte att söka jobb på företaget, så han ville visa hur duktig han var. Men dåvarande chefen här lyckades få förtroende skapat med den här killen och de bestämde ett möte på X. Han hade förberett så att SÄPO var med och tog honom där. Och sen åkte han in på var det nu var, sex år eller någonting.

- Finns det även fall där anställda har tagit patent i ren illvilja?

Inte som jag känner till.

Du menar interna stölder av information?

Ja det har förekommit. Jag kan inte hänvisa till specifika fall, men ja information försvunnit från interna, det har det gjort.

- Avsiktliga och oavsiktliga hot, hur upptäcker ni dessa? Hur ser du på det?

Just den här biten som vi behöver utveckla. Threat analysis, där är vi alltså inte tillräckligt bra. Det var såhär faktiskt att för två år sedan rekryterade man en ny förmåga på group level som skulle sätta igång arbetet på allvar internt här. Men vederbörande kom från UD och hade jobbat på SÄPO och inom MUST och hade en mycket gedigen bakgrund, men tyckte ändå att det blev för komplext. Det var lättare på UD där det var internationella hotbilder, men nu mot en sån komplex organisation så är det hotbilder som kan vara stater, enskilda kriminella, aktivister och så vidare. Det blir så mångfacetterat så vederbörande tyckte att det var roligt att göra något annat. Det pågår fortfarande rekryteringsarbete på den. På “market area” nivå där

jag ingår för Europa och Latinamerika så ska vi köra igång något arbete med detta. Men som svar på din fråga, ja det är väldigt svårt och vi är inte jätteduktiga på det.

Samtalet fortsätter ca 3 min med generell information

Bilaga 5: Transkribering av intervju med R2

Respondenten har haft möjlighet att göra revideringar och borttagning av text i transkriberingen för att skydda bland annat företagshemligheter och liknande som skulle kunna avslöja företaget.

Indragen text efter ”-” är vi som pratar.

- Vi håller på med examensarbete som handlar om informationssäkerhet där vi tänkte titta på hur ett globalt företaget jobbar med informationssäkerhet, både hur företaget jobbar, jämföra olika perspektiv inom verksamheten men även titta på lite hur de teorier som finns kring ämnet, hur det står sig mot hur ni jobbar på företaget.
- Vi kommer inte nämna företagets namn i arbetet, allting är anonymt och så. Säkerhetschefen (*Respondent 1*) har gått igenom frågorna och så, så att inget läcker ut så att säga, han får även tillgång till arbetet sen och kan kolla igenom att…

Så han gör en check sen?

- Ja precis

Då känner jag mig trygg. Shoot.

- Kan ni börja med att berätta om din roll i företaget och vad ni jobbar med?

Jag har två jobb, jag ansvarar för vår mjukvara utvecklingsavdelning här i xxx där vi utvecklar xxx och sen platschef också, så det betyder att jag liksom håller ihop det som har med företaget här i xxx och alla organisationer här. så att i mitt operativa jobb som mjukvara utvecklingschef så är det mycket liksom stötta team, massa utvecklare o hjälpa framåt. Platschef jobben är allt från säkerhet, facilities, externa kontakter med närings team, med kommun liksom, så det är en ganska annorlunda roll. Och vi som site, som man säger, ska kunna ha rätt kompetens för framtiden, så det ska hjälpa företaget fram. Det är väll kort om min roll.

- Hur ser ni på arbetet med informationssäkerhet inom företaget?
- Som platschef?

Men det är extremt viktigt det har säker r1 sagt också, liksom. Vi har ju rätt mycket processer kring det här eftersom vi jobbar med det senaste tekniken och så klart är vi konkurrensutsatta och så, så det är väldigt viktigt att vi är försiktiga och noggranna med vilken information vi går ut med och, alltså vilka klassificeringar vi har. Så det är det vi lever på, uppfinna nya saker, nya idéer, ny utveckling och vi vill ju vara först och då man kan ju inte läcka saker så att någon annan kan sno de idéerna liksom. Så det är viktigt

- Och hur arbetar ni med dem här säkerhetsdirektiven ni har? Hur ser ni på dem?

Vi arbetar på flera sätt, det är både hur man lagrar information, hur man skickar information. Finns ju liksom så att alla på företaget, det finns mandatory, man måste gå säkerhet och datautbildningar, och det följs upp så att man kollar att alla verkligen gör det. För det handlar ju om kunskap, så det ena handlar om att förmedla kunskapen, hur gör jag? Vilken information kan jag lagra? Vad kan jag skicka? Vad gäller? Så det är väll det, och det sker ju ganska mycket centralt, det är inget vi gör sådär lokalt liksom här utan det är företaget i stort. Men vi följer upp lokalt att alla går den utbildningen och så. Det är väll det ena sen har vi ju liksom på företaget, vi går igenom vi har möte kring säkerhet, uppföljning, vi har processer om något går fel, så rapporterar detta in i ett system, så blir det uppföljning, feedback och åtgärder utifrån vad det är för något. Så att så vi jobbar vi och där har ju jag kontakt med r1 framförallt, på dem sakerna om det skulle vara något. Sen har vi även proaktivt med att vi har en grupp som jobbar med liksom, iscensatta scenarion, om detta händer vad gör vi då? Vi tränar på, om det är en kris eller om något skulle hända. Detta drivs ju av R1, han har kanske berättat lite?

- Aa lite.
- Hur tycker du att just din avdelning jobbar, tillämpar de reglerna som finns uppsatta?
- Är det liksom en stor del av vardagen eller är det mer att det finns där? Tänker ni aktivt, nu ska vi göra så då måste vi kolla på dem här reglerna och så?

Nä inte att man måste kolla på regler, utan jag tror att vi förväntas, förväntas att man följer liksom, det är mer om det är något särskilt att man tänker vad är det som gäller här? I det dagliga så förväntar vi oss att lagra inte information där du inte ska, skicka inte mail med känslig information liksom, till någon extern. Alltså, vissa saker känns ju så självklart med det kan faktiskt bli fel ibland. Du krypterar informationen och sådär. Skulle säga det är väll mer om det är något speciellt… till exempel nu har vi ID över hela detta, (*Tidigare så var hela)* byggnaden företaget, det betyder att vi hade företagets säkerhetsanordning liksom skal runt hela huset, i entréer och så. Nu har vi inte det vilket gör att halva byggnaden är extern. Så vi har ju gått ut till exempel med att vi har lunchmatsal som inte är en personalmatsal längre utan den är öppen för andra med så tänk på vad vi pratar om på lunchen, vi har en extern stor aula i källaren där vi har seminarier och vi har kanske, för nån vecka var produktledningen där och berättade om vår produktportfölj. Då får vi tänka extra för det kan ju smita in någon om vi inte är uppmärksamma, så då har vi kontroll vid dörren. Så är det något extra får man tänka till ur säkerhetsaspekten här, hur ser vi till att vi, att vi följer så att vi inte riskerar att information läcker eller så.

- Och upplever ni att det är svårt att kommunicera med andra avdelningar, till exempel både inom här i *staden* eller övriga siter på grund av säkerheten?

Nä det tycker jag inte.

- Inte svårt att dela information eller liknande?

Nä inte alls faktiskt, inget hinder om man är på någon annan site eller om man är i ett annat land heller. Jobbar ju väldigt globalt. Ser ingen begränsning i det faktiskt.

- Ser du några svårigheter med informationssäkerhet på din avdelning?

Hmm, vad skulle det vara…

- Någon utmaning liksom?

En utmaning är kanske medvetenheten, nu har vi anställt rätt så många nya så det krävs liksom, det ingår ju utbildningen man får när man börjar. Det är en viktig del liksom, men jag tror det krävs kanske lite extra av oss som har varit här ett tag att trycka på det, att komma ihåg att nämna det, det som är naturligt och självklart för någon som jobbat länge är kanske inte det för någon som är ny, så det är kanske en utmaning.

- Hur skulle ni hantera eventuella svårigheter?

Öka medvetenheten liksom, och prata om det, ha det på agendan…

- R1 nämnde security awareness dagar, mer sånt?

Ja precis, det har vi också någon gång om året och så. Eller nån vecka tror jag det är lite extra fokus på säkerhet. Det gäller ju egentligen varje dag, det är lätt att göra ett misstag, alltså kanske inte lätt med det vanliga men ibland, det kan vara, säg att du har nån konsult, så är det något med mail-adresser och så, att man faktiskt kollar när man skickar viktigt information. Det finns ju en risk att man gör fel, inte medvetet men att man råkar göra något. Det gäller att man har säkerheten högt i sitt… DNA? Vet inte riktigt hur jag ska säga.

- Skulle du säga att det finns policys eller direktiv som är i vägen för arbetet?

Det kan vara en utmaning att, våra IT system kanske inte är 100%, kanske inte är tydligt, vad kan jag lagra den här informationen? Är det säkert? Jag tror faktiskt, där finns en utmaning som vi brottas med, vår IT avdelning liksom, allting är mer molnbaserat, vad är det du kan lägga där och inte. Är det säkert? Det är ju deras ansvar men man känner lite, det är en utmaning.

- Har ni reflekterat över vilka konsekvenser det kan innebära om informationssäkerheten bryts för er avdelning?

Aa absolut, det är liksom som, kommer det i fel händer kan det vara enorm skada för vår affär, så är det ju. Det är väldigt viktigt och jag tror man ska vara, man måste vara på sin vakt faktiskt. Vilket kanske tas för givet men jag tror man måste vara det. Man ska vara lite

misstänksam, det är faktiskt folk som aktivt försöker liksom komma åt information. Så att, ja…

- När du säger, aktivt, menar du att någon skulle söka arbete här för att sen kunna…?

Det kan hända, det vi gör ordentliga checkar på när vi anställer, om vi misstänker något sånt, att det är från konkurrerande verksamhet eller så. Men det kan vara mer att man kan bli kontaktad via mail, telefon eller något att någon försöker komma åt information eller ja… så man ska vara misstänksam, och det ingår i den säkerhetsutbildningen, med phishing och liksom, är det något som sticker ut ska man reagera på det. För vi sitter på mycket information.

- Har du någon uppfattning om hur mycket det bryts mot protokollen? Både stora och små saker? Händer det dagligen att någon skippar på någon liten grej?

Det som rapporteras har vi koll på, i det här vad det nu heter systemet. Det har vi månadsuppföljning på om det är avvikelser och så. sen är det svårt att säga vad som inte rapporteras. Där, jag tror absolut det finns massor med saker som inte rapporteras, till exempel nu när ni kommer in, nu följde vi ju allt, ni har visitkort och så men det kan vara besökare som kommer in, och man går iväg och tar kaffe liksom, men det är ju inte okej faktiskt. Men om du känner någon och tycker lite liksom, ja då kan det bli lite slappt, och sånt rapporteras nog kanske inte. Så att, så därför gäller det ändå att ha medvetenhet, ett öga på det.

- Händer det att er avdelning väljer att inte rapportera något till InfoSec?

Nä inte medvetet? Inte vad jag känner till iaf. Nä men det är liksom, nä det man ser, om det är något liksom eller. Jag är inte medveten om något som inte rapporterats.

- Har du jobbat något med andra Market Areas (*andra regioner*)?

Aa lite grann…

- Upplever du att det är någon skillnad med hur de ser på infosäkerheten? Jämfört med hur vi upplever den här?

Jag kan inte säga att det är så, men jag kan ju liksom, jag är nog extra misstänksam i XXX, så kan jag säga. Att det är slappare där.

- Ungefär det svar vi fick från R1 också.

Aa R1 vet ju för han har varit där på kontrakt.

- Aa vi snackade om det sist.

Men jag kan nog, när jag har varit där också så kanske känna, men jag har inga bevis. Men jag upplever kanske att vi är mer strikta här på det. Det skulle kunna vara så men jag vet inte…

- Du har ingen statistik på det?

Haha, nä och jag har inget case liksom där jag kan peka på… Jag har frågat, ansvarig i XXX men han förnekar liksom, vi har jättehög säkerhet här. Men jag är fortfarande misstänksam…

- Jo R1 gav oss den bilden också.

Jo så att det är ju ett issue faktiskt, det borde jag ta med R1 faktiskt.

- Hur tycker du att samarbetet med InfoSec avdelningen ser ut? Är det bra samarbete där ni kan kommunicera öppet med varandra eller är det mer så att dem liksom bestämmer?

Nä alltså, vi har ju inte så mycket issues så jag är väldigt glad att R1 är här, han har ju inte bara en *lokal* roll, men är det minsta lilla säkerhetsfråga eller så, så är det R1 jag går till och han kan hjälpa till att reda ut det. Vi hade ju vår VD här på besök. Det var en lärdom liksom, inte bara att förbereda allt med det utan även säkerhetsaspekten av att ha VDn här på besök, det var en helt annan dimension. Då var det jätteskönt att ha R1 här: Behöver jag XXX och så vidare, hur funkar detta? Och kan kunde dra i det, så vi har jobbat tillsammans. Men det är lite upp och ner vid behov eller om det är något särskilt.

- Känner ni att ni får ha input på dem direktiv och policys som finns? Till exempel den här policyn är jättejobbig och funkar inte så bra för oss, kan vi ändra på detta?

Har faktiskt inte försökt, jag förlitar på mig på att det ja…

- Accepterar den liksom?

Aa, skulle det vara något som är… men jag tycker inte det är något konstigt. Man brukar kunna förändra saker men brukar krävas lite energi, och den energin kanske man inte har i så fall riktigt. Men jag har inget jag kan peka på liksom som jag känner det här måste jag driva till förändring.

- Det var alla frågor egentligen, vi hade ju en lång intervju med R1 som låg till grund för detta.

Perfekt

- Tack så mycket för tiden, tack för allt…

Bilaga 6: Transkribering av intervju med R3

Respondenten har haft möjlighet att göra revideringar och borttagning av text i transkriberingen för att skydda bland annat företagshemligheter och liknande som skulle kunna avslöja företaget.

Indragen text efter ”-” är vi som pratar.

- Som du säkert vet håller vi på med examensarbete i informatik och vi tänkte titta på informationssäkerhet och vi har gjort ett litet formulär där vi tänkte undersöka hur era anställda ser på informationssäkerhet och där har vi även till er som är avdelningsansvariga, till er tänkte vi omformulera frågorna så att dessa ställs på ett sätt där ni får besvara hur ni tror att era anställda kommer att svara.

Ja…

- Theodor hade X mail förutsätter jag, så vi tänkte skicka formuläret…

Hur ska dem fylla i detta här?

- Det är Google forms
- Vi har gått igenom frågorna med X, så du kan dubbelkolla med honom ifall du inte litar på oss…
- Arbetet går ut på att vi jämför säkerhets...informationssäkerhet i teori och hur det fungerar här..
- Men även en jämförelse på hur olika avdelningar arbetar.

Men då blir det så att jag mailar ut en länk till alla mina anställda…

- Ja precis jag kommer maila ut länken till dig sen
- Sen kommer du få ett formulär där du får frågorna formulerade lite annorlunda

Ja det blir bra

- Sen har vi fått information från X att du har mer internationell utsträckning kan man säga

Ja jag har personal i Italien, Kanada, Finland,

- Så vi undrar ifall det finns möjlighet att du skickar ut ytterligare ett formulär till de som är internationella så att vi har statistik på hur det fungerar i Sverige och internationellt

Är det på engelska eller svenska?

- Engelska

Ja visst det kan jag göra

- Vi snackade med R1 förra veckan och då fick vi fram att det var ganska stora kulturella skillnad mellan hur olika länder ser på informationssäkerheten.

Ja om man till exempel tar mitt gäng i X och mitt gäng i X, de är väldigt olika. Det är nästan...Kommer ni kunna se varifrån…

- Nej det kommer vi inte
- Vi har ett formulär från Sverige och ett internationellt
- Vi ser ju bara vad folk svarat anonymt

Man ska kanske inte krångla till det för mycket.
Det är inga problem att skicka ut formulär till de utanför Sverige

- Hur många tror du kommer kunna besvara det? Eller hur många kommer du kunna skicka det till ungefär?

80 personer ungefär.
Men hur många som svarar har jag ingen aning om.
Men jag har 80 medarbetare ungefär, snart 90

- Det är helt anonymt och företaget nämns inte någonstans
- Alla frågor har vi gått igenom med R1 och han har godkänt allting
- Tack för att du ställer upp

Det är lugnt.

- Kan ni berätta lite om eran roll inom företaget?
- Vad ni jobbar med?

Jaha, jag är forskningschef på företaget, ansvarig för X och X. Det är det enklaste svaret. Det finns ett betydligt längre namn. Och jag har då suttit på X research som är den centrala forskningsavdelningen på företaget. Research är cirka 700 personer. Totalt är företaget ca 100 000 så detta är bara en pyttedel av företaget. Men det är vi som står för hälften av alla patent. Så att vi är så att säga uppfinnarverkstan. Jag har då personal i *flera länder*. De jobbar med olika saker, (*går in i detalj vad de arbetar med, därmed struket.)*

- Så du nämnde att ni hade 50% av patenten ungefär.

X research ja.

- Hur ser ni då på arbetet med informationssäkerheten inom er avdelning?

Det är ju, vi är ju tillhör en speciell kategori, personalkategori som har strängare krav på konfidentialitet än andra. Det finns ju vissa datormiljöer som används som vi inte får använda, dom anses inte säkra.
Vi har också sedan flera år tillbaka en sträng regel att allting som är patent eller *research*-relaterat ska krypteras i mailform. Så att vi har ganska stränga krav på oss. Och det beror ju på att vi är utsatta för, det vi gör, den information vi har är väldigt attraktiv för andra. Och värdefull.

- Så är det ju.
- Kan du berätta lite om hur ni arbetar med policys och riktlinjer inom er avdelning?
- Direktiv och sådana grejer.

Vi har ju inga egna, de finns ju för hela X research.

- Hur tillämpas dessa hos er?

Ja... Det är ju till exempel lagringslösningar vi inte använder. För att vi är inte…
Men annars är det ju...Jag såg att ni nämnde USB stickor här (*syftar på formuläret som skrivits ut på papper i demonstrativt syfte*)...jag har aldrig sett någon policy om USB bland våra policys.

- Den var hämtad från era policys faktiskt.

Ja… Men den har inte… Jag har varit här så länge så att när jag fick anställningsintroduktion på företaget var inte USB stickan uppfunnen än.
Men det är möjligt att de nyanställda får någon form av introduktion till detta idag.

- Många av de frågorna var baserade på… Vi fick ett utdrag på de riktlinjer som finns av R1, så vi plockade lite därifrån.
- Får jag fråga, när du säger att USB stickan inte var uppfunnen än… Kan du se det som ett problem att tekniken växer om eller går för fort för säkerheten ska hinna med, att ni som är kvar är kvar i gamla rutiner…
- Eller det är inget problem kanske?

Jo det tror jag att det är. Jag kan känna att.. Jag är ganska säkerhetsmedveten… jag gjorde lumpen inom svenska underrättelsetjänsten så jag har det lite i blodet. Jag jobbade även ett tag där. Jag kan känna att när vi till exempel började med ”bring your own device” på företaget, så kunde du ha mail på telefonen. Och då kunde jag ju känna att det här är inte säkert liksom. Vad fan... Jag provade att göra lite olika grejer, jag vill inte berätta vad. Men jag kunde göra saker som jag kände att nej detta ska man inte få lov, detta är inte säkert. Och det har ju

fortsatt, så jag har känt ibland att på något vis har convenience och efficiency gått före security. Och det finns ju naturligtvis alltid en balans. Man kan ju inte stanna upp i hela bolaget för att man har så rigorösa… Man kan inte låta säkerhetskraven låta gå ut över affärerna för mycket. Lite grann, men inte för mycket. Men i det fallet tyckte jag att kompromissen var alldeles för långt åt ena hållet. Jag blev lite bestört över hur lätt det var att göra saker man inte borde kunna göra. Allting från att kopiera sin kalender automatiskt upp till Google, sådana här grejer. Eller att kunna hämta hem en fil från någon intern drive på mobilen och sådana saker. Att det lagrades lokalt och ifall någon snodde min mobil var det okrypterat. Och jag vet inte om det var ett medvetet val eller okunskap och där kände jag jakten på enkelheten hade gått ut över säkerheten.

- Fick du något gehör för dina åsikter?

Nej jag bråkade inte om det.

- Har du någon gång upplevt att säkerhetsdirektiv och liknande är i vägen för arbetet.

Nej inte på X. Däremot på X var det så. Vi fick ju knappt komma åt Internet. Det fixade ju sig sen, men när bolaget precis bildades år X, då ärvde vi över X infrastruktur. Och den var ju 80-tals nivå på. Så där fick vi inte, där var i princip… Man skulle ansöka om man skulle ha tillgång till Internet på sin jobbdator. När man sedan hade ansökt om det, YouTube var spärrat, gmail var spärrat och sådana här saker. Det kom man inte åt alltså. Det ansågs inte ha med jobbet att göra. Sen att vi la upp våra marknadsföringsmaterial på Youtube det hade dom ju inte fattat. Det fanns massor med andra grejer. Datorn var tillstängd och tillknäppt på alla möjliga sätt, USB-portar var urkopplade. Den policyn var framtagen för fabriksmiljö, produktionsmiljö. Där jag kan respektera att man har extrema säkerhetskraven, jag menar som i X krav var ju fabriker, står sådana still kostar det ju miljarder per vecka. Det är okej, men i kontorsmiljö blir det absurt. Speciellt om man jobbar med marknadsföring och skulle lägga upp saker på Corporate-blogg det funkade ju inte. Där var de i vägen. Men på här på X har jag nog aldrig känt så, jag har alltid känt att det nästan vara lite förvånansvärt enkelt att göra saker. Det är mycket frihet under ansvar.

- Hur upplever du att just din avdelning tillämpar de här reglerna, känner alla som du känner eller?

Det tror jag inte. Jag är nog lite gammaldags. Jag är tror att nyare medarbetare tycker det är helt naturligt. Medans jag...Som till exempel vår corporate firewall släpper igenom alla möjliga protokoll. Inte bara HTTP… Det där kan jag ju tycka är lite förvånansvärt. Medans alla yngre förmodligen tycker att det bara ska vara så. De tycker att det inskränker deras personliga integritet att inte kunna använda egna appar på sin dator på jobbet.

- Tycker du att ni har svårt att kommunicera med andra avdelningar inom företaget, pga säkerhet?

Nej aldrig. Det skulle väl vara, i en del fall lägger man upp filer på Sharepoint. Man har intern Sharepoint för min enhet där man sparar presentationer, månadsrapporter och sådant som man kanske då vill dela med annan. Då är kanske default inställningar att det bara är min avdelning, då måste man gå in och lägga till användare och sådant. Det är sådana extra handgrepp ibland. Men det är inget hinder som sådant.

- Jag tänkte mest ifall ni vill diskutera något med X (*annan avdelning)*, men så vet ni inte riktigt vad vi får prata om och vad vi inte får prata om.
- Så att otydligheter vad man får kommunicera? Känsliga data liksom.

Nej jag tror att så länge man krypterar mailen så kan man skriva vad man vill.

- Ser du några utmaningar med informationssäkerheten på er avdelning?
- Finns där några svårigheter eller liknande du kan nämna?
- Är ni begränsade på något sätt?

Nej det tycker jag inte.

- Om ni skulle hitta någon eventuell svårighet eller utmaning hur skulle detta hanteras?

Jag hade ju nog… Det beror lite på vilken karaktär…

- Det blir lite hypotetiska frågeställningar här…
- Men om vi skulle säga att någon del av säkerhetsaspekter var ett hinder, hur skulle du hantera en sådan utmaning?

För det första, går den att kringgå eller inte. Är det ett mekaniskt problem att du faktiskt inte kan skicka den här informationen fysiskt, eller är det så att det kanske bara är olämpligt.

- Olämpligt snarare, det går men det tar extra energi och tid att göra det.

Ja, jag vet inte om jag kan komma på något sånt fall. Det kan ju vara så att du kanske inte fysiskt kan skicka en fil av viss typ. Alltså man jobbar ju runt det då. Ta till exempel att man inte får skicka .exe-filer som attachment internt. Och det är ju av goda skäl. Men om du nu behöver göra det kan du ju skicka dom via Skype istället, eller på en USB-sticka. Det finns ju en väg runt det. I övrigt så känner jag inte att det finns några regler egentligen som hindrar oss. Och skulle jag stöta på dem så, det beror på karaktären. Enklaste fallet går jag till min chef och vill ha ditt godkännande för det här då det är ett avsteg från vår policy. I andra fall måste jag kanske gå till IT-sektionen och be dem öppna en port i brandväggen, något mekaniskt alltså. Det beror på hindrets karaktär.

- Har du reflekterat vilka konsekvenser bruten informationssäkerhet kan få för er avdelning om något inträffat?

Ja det kan vara alla möjliga saker, det kan vara att ett patent blir ogiltigt eller att vi tappar en konkurrensfördel eller att vi blir stämda, eller ja det finns ju hundratals tänkbara konsekvenser. Sen kan de ju vara stora och små. Ett ogiltigt patent kan vara båda "äh det spelar ingen roll", eller så kan det vara katastrof.

- Har du någon uppfattning om hur ofta det händer att inom er avdelning, att både stora eller små protokoll bryts?

Hur ofta man bryter mot policy?

- Mm…

Jag misstänker att det sker varje dag.

- Det är lite det vi är ute efter.

Jag skulle tro det…

- Hur ofta rapporterar ni sådant?

Vad jag vet så har det inte rapporterats en enda säkerhetsincident de senaste två åren.

- Kan det vara så att ni väljer att inte rapportera ibland, för att behålla ert rykte?

Nej… Sen måste man definiera säkerhetsincident också. Att någon använder privat USB-sticka är ju inte en säkerhetsincident. Däremot bryter det mot policyn. En incident är när man upptäcker någonting när man till exempel har blivit utsatt för någonting. Och det tror jag inte har hänt, vad jag vet. Policybrott, vi håller ju inte på och Lex-maria anmäler oss själva.
Men jag känner som sagt inte till en enda incident i min enhet sedan den bildades för två år sedan.

- Skönt.

Det kan vara så att någon av mina underchefer varit utsatt för något och anmält detta men de har de inte berättat för mig.

- Du upplever inte att det är skillnad internationellt i informationssäkerhets-kultur?

Det tror jag inte.

- Som att i Sverige är det striktare medans någon annanstans är det slappare?

Nej jag tror inte det. Möjligtvis skulle vara lite striktare i X (*annat land)* eftersom att de sitter i samma lokaler som vårt säkerhetsfolk?

- Hur ser samarbetet ut med avdelningen för informationssäkerhet?

Det har vi inte.

- Ni har inte input på direktiv och regler på, vi pratade tidigare om utmaningar, om det finns något problematiskt med att ni kom med input?

Nej vi har haft lite tur på research, som jag sa finns det lagringslösningar som vi inte får använda, och det var då av säkerhetspolicyskäl, och det har vi inte gjort heller. Men det finns andra organisationer som liknar oss till karaktären som fått lov att göra det. Men då har de blivit belagda med restriktioner på hur man får använda. Och dessa restriktioner är oanvändbara. Det går inte att jobba på. Denna organisation har tagit stöten mot IT-säkerhetsorganisation och förändrat reglerna. Och sen åtnjuter vi de här nya förbättrade reglerna, så vi slapp ta stöten. Men vi kunde betrakta på avstånd hur de slogs på våra vägnar lite. Men överhuvudtaget har vi ganska privilegierad roll på det viset att när vi skriver programvara går detta inte ut i produkten utan används som underlag för att sedan utveckla produkter. Så att vi… Vårt arbetsmaterial skickas inte runt i bolaget och lagras inte i några stora system. Vi har en friare roll på det viset. Å andra sidan skriver vi underlag för patent och har massa sådana saker som är jättevärdefulla och hemliga och viktiga. Så att på det viset så behöver vi ju sköta det här med IT-säkerhet ordentligt. Och vi kanske också är en måltavla mer än andra.

- Var det allt för oss kanske?
- Ja det tror jag
- Vi hade en rätt mycket längre intervju med R1 där vi fick mer övergripande information om hur arbetar med säkerhet. Detta var mer en uppföljning på det.
- Är där något du vill tillägga som du tror kan ge oss nytta?

Nej… Vi är ju i en ganska snabbrörlig bransch, och det gör ju att den här kompromissen mellan säkerhet och bekvämlighet ibland måste förskjutas lite. Ibland måste vi prioritera bekvämligheten för att hinna med. Om vi blir långsammare, väldigt stor del av vår konkurrenskraft är snabbhet. Det gäller kanske ännu mer för när vi höll på med X. Det var en snabbare bransch. Men även med X så går det ju rätt fort. Vi jobbar ju inom forskning och det blir väl så att det vi gör kommer inte ut i produkter med det samma utan det kan ta både tre, fyra och sju år innan saker vi har tagit fram kommer ut i en produkt... Men, och då är det kanske viktigt att man faktiskt, problemet med att jobba så långt in i framtiden, är att om en konkurrent får nys om idéerna har han ganska gott om tid på sig för att kopiera och göra likadant. Får en konkurrent reda på att X kommer lansera en produkt, då spelar det ingen roll och han kan inte agera, de kan inte göra det på tre veckor liksom.

Därför har olika delar av organisationen olika säkerhetskrav. Jobbar man med en produkt som ska ut om ett halvår är det kanske inte viktigt att det är supersäkert, superhemligt. Konkurrenter kan inte göra mycket med den här informationen. Medans vi som arbetar på

5,6,7 års sikt måste hålla hårt i vår information. Läcker den, det är jättevärdefulla ledtrådar för våra konkurrenter. Men å andra sidan så stannar information hos oss i väldigt stor utsträckning. När vi, vi tar ju ofta idéerna ganska långt, så när de första rönen kommer om någonting, det är ingen på produktutveckling som är intresserad av att prata med oss om grejer som vi kommit på, som kommer användas om 7 år.

"Jobba ni vidare det låter bra, men stör inte oss för vi ska få ut en produkt om 6 månader". Så att vi har liksom inte något jättebehov av att sprida vår information inom företaget som är på så lång sikt. Sen när vi har jobbar med det i två, tre år och vi har en prototyp och något som faktiskt produktutvecklarna faktiskt vill ha och är intresserade av, skisser och ritningar och diagram, då är det herrens känsligt för då är det liksom närmare en produkt. Det finns någon slags känslighetsskala kan man säga. Det är vi gör nu är grundläggande, när vi gjorde X för 7 år sedan, då var jättehöga krav på informationssäkerhet. Ju närmare lanseringsdatum man kom ju lägre blir krav på säkerhet.

- Kan man säga att det är linjärt?

Ja det kan man säga. Det kan vara svårt att ha policy i ett bolag som tar sådana hänsyn det kan man inte gärna göra. Man kanske får han en eller två nivåer, eller tre. Så till exempel viss information får inte lagras alls på våra interna drivers. Vi har ett speciellt digitalt valv där vi lägger in sådant.

- Är det där ni lägger gamla prototyper och gammalt material som ni har tagit fram?
- Lagras det eller där ser man inte lika stor vikt vid det?

Nej… Sen har det visat sig gynnsamt, ett tag pratades om att ha retention policy, att man skulle liksom, alla skulle spara allt arbetsmaterial X antal år, och allt som var äldre än så skulle förstöras. Men det blev liksom aldrig något av det där. Och jag har ju material i min dator som är 20 år gammalt en del. Det har ju visat enormt värdefullt, I rättsfall till exempel, patenttvister. Men det är tveeggat svärd. Det kan vara så att det är jätteskadligt för X det som jag har lagrat på min dator. Det vet man inte i förväg. Så det är också lite besvärligt. Men vi har ingen retention policy idag vad jag vet.

Bilaga 7: Transkribering av intervju med R4

Respondenten har haft möjlighet att göra revideringar och borttagning av text i transkriberingen för att skydda bland annat företagshemligheter och liknande som skulle kunna avslöja företaget.

Indragen text efter ”-” är vi som pratar.

- Hej tack för att ni ställer upp på denna intervjun, allting som sägs kommer vara anonymt, företaget (*namnet på företaget)* kommer inte nämnas någonstans.
- Kan ni börja med att berätta vad ni jobbar med och er roll inom företaget?

Jag jobbar på företagets Patentavdelning (*ändrat till patentavdelning för att undvika ”avslöjande”)*, i princip patentavdelningen, mitt ansvar är att jag är Director of Patents *(förkortar ner till patents)* och ansvarig för hur immaterialrätt hanteras i alla företagets externa gränssnitt såsom, samarbeten, tekniksamarbeten, standardisering, kontakter med kunder, underleverantörer, open source, mergers and acquisition dvs inköp och säljning av bolag och sådana saker. Aa, allt där immaterialrätt kommer i samspel med företaget, med externa kontakter. Före detta chef för patentavdelning i XXX (*lokalt)* i ungefär 15 år.

- Hur ser ni på arbetet med informationsäkerhet inom organisationen?

Tror att vi är väldigt medvetna på patentavdelning, vi är nog en av de organisationer som tar det på väldigt stort allvar. Det är säkert olika från person till person, det är väldigt viktigt för oss i och med att patent och immaterialrätt måste verkligen hållas hemligt. Dels för att det finns formella regler kring patent som kräver att det måste vara hemligt rent juridiskt, dels att det är väldigt känsliga företagshemligheter vi sysslar med inom immaterialrätten.

.

- Och kan ni berätta hur ni arbetar med policys, direktiv och regler inom informationssäkerhet på just er avdelning?

Ja, enkelt, vi arbetar så som dessa policys och föreskrifter säger. Alla får samma grundläggande utbildning, krypterade mail och sådana saker, följa policyn helt enkelt det är så vi arbetar med dem, vi följer dem och får lära sig hur det ska fungera.

- Och hur upplever ni att er avdelning tillämpar de reglerna som fastställs?

Jag upplever att min avdelning, vår avdelning, följer det bra, det är vad jag tror i alla fall.

- Upplever ni att ni på er avdelning har svårt att kommunicera med andra avdelningar på grund av de säkerhetsdirektiv som finns?

Faktiskt inte, jag upplever det som att inom företaget så förstår folk detta och följer detta bra. Gör man inte det så förklarar vi för dem och företaget har bra krypteringssystem och regelverk, vi är röd avdelning så vi har saker och ting stängda och så vidare.

- Och vilka utmaningar eller svårigheter ser du med informationssäkerheten på er avdelning?

Utmaning är ju att väldigt mycket av det vi sysslar med är hemligt, men om man följer regelverken och policys så är det ju inte svårt utan det är ju bara att tänka efter så att man följer alla regelverken helt enkelt.

- Och hur skulle du hantera en eventuell svårighet eller utmaning inom info sec?

Beror ju naturligtvis på vad det är för utmaning, om det skulle vara något som bryter mot regler eller sådana saker så får man ju åtgärda det, se över de verktyg och processer man använder om man kan förbättra. Eller om det är individer som bryter så får man påtala detta för dem, det kan vara så att de inte förstått eller inte bryter mot det medvetet. Naturligtvis anmäler man allt sånt till säkerhetsansvarig.

- Vad för konsekvenser skulle en sådan incident kunna leda till?

Det skulle kunna leda till i patents fall att vi förlorar patenträttigheter till specifika patent eller patentportföljer, det är ju väldigt hemliga affärer väldigt mycket, så det skulle kunna påverka oss i olika förhandlingar om information läckte ut. Stor skada skulle verkligen kunna leda till rent monetärt, pengar, skulle förlora licensförhandling och liknande.

- Har du någon uppfattning det händer att det sker incidenter? Både stora och små?

På vår avdelning?

- Mm,

Nästan aldrig skulle jag säga numera. Folk har högt medvetande inbillar jag mig

- Händer det att ni inom avdelningen väljer att inte rapportera situationer där någon brutit mot en policy eller riktlinjer och så vidare?

Nä om man bryter mot policy eller riktlinjer så anmäler man det till säkerhetsansvarig så klart, och det gör vi.

- Gäller detta även små grejer som användning av USB-minnen på inkorrekt sätt?

Ja… man kan väll säga så här, i regel så förklarar man för folk, om man bedömer att det inte är någon skada skedd och om man gjort något omedvetet så kan man börja med att se till att folk gör rätt om det är en mindre sak. Ibland kanske man bara berättar, utan att formellt anmäla.

- Upplever du att det är kulturella skillnader hur folk ser på säkerheten?

Det tycker jag nog, om man ser på kulturellt mellan avdelningar och så. även om jag sa att vi inte har några problem med att jobba mot andra så kan det vara så att vissa avdelningar kanske inte alltid förstår när man jobbar mot andra, det kan ju finnas individer, skulle nog inte säga det är mycket kulturellt, det kan vara kulturellt i sådan mån att vad det är för typ av arbete man har om man inte jobbar med känsligt område, även om väldigt mycket är känsligt men vi är känsligare, så kan det vara en kulturell skillnad att folk inte förstår det hela… men det är då man får förklara och upplysa varför, om folk bara förstår varför brukar det inte vara några problem.

- Upplever du att det är regionala skillnader?

Inte upplevt det och tror inte det, men… ja…

- Till exempel asien och hur dem ser på säkerheten jämfört med europa?

Skulle nog säga att det är nog en skillnad om man ser utanför vår avdelning och kanske inte inom företaget, där är vi rätt duktiga på det. om man ser på andra kontakter inom vissa länder, när man jobbat med externa patentbyråer i kina så har de inte riktigt förstått det här med varför ska saker och ting vara hemliga på det här sättet, de kanske ser det på så att… men internt har jag inte upplevt det.

- Hur ser ert samarbete med informationssäkerhet avdelningen ut?

Ser bra ut, vi får information från dem och vi informerar dem om det skulle vara något, frågar om vi behöver hjälp med att lösa någonting. Det kan till exempel vara kryptering mot externa kontakter… hur man ska hantera något, exempelvis när vi på vår avdelning, hemligaste kategorin, den typen av information man har som är i den klassen inte lagras på molnet och sådana saker, vi (*företaget)* har ju ganska mycket standardlösningar som inte fungerar kanske när just vi (*patentavdelningen)* har saker som är så hemliga, då får man kontakta dem och se hur man ska lösa de här sakerna och då får de kanske ligga på IT avdelning. IT avdelning är kanske en sån avdelning som inte förstår det här med hemligt. De ska göra allting snabbt, enkelt och billigt får de på sig. och när vi då säger att det är hemligt så förstår de det men har kanske inte en färdig lösning och då tar vi ju hjälp av säkerhetsansvarig att ligga på och försöka hitta bra lösningar.

- Har ni någon input på de direktiv och policys som finns? Ni får diskutera dem med info-sec?

Ja jo, det är om det är… ett: om det är vad menar man med det här, hur ska man tolka saker och ting. Till exempel just det här med att vi rent fysiskt är en röd zon, men även när det gäller data/information hur man ska hantera den så har vi kontakt med dem gällande de bitarna, det är väl det som är frågan? Typ?

- Ja... eller om det är någon sort policy som är i vägen när ni jobbar, om ni kan diskutera detta?

om det skulle vara något som krånglar till det så tar man ju upp det men jag upplever inte det. vissa saker kanske man skulle göra lite, till exempel att vi inte får lagra på molnet och att när de då effektiviserar IT miljön ibland glömmer bort att det finns hemliga saker ibland… men det är inte policyn i sig utan det är med… ja, implementering. annars tycker jag de ställer upp och hjälper till, om det behövs

- Finns det vissa fall där du känner att efficiency och bekvämligheten har gått före säkerheten?

Nej det tycker jag inte. Jag tycker också att företaget har hittat en ganska bra nivå när det gäller att använda, man har… jag har ju jobbat länge på företaget och vi har ju hela tiden varit en röd zon och då var det ganska krångligt i början när vi hade datorer som inte kopplade upp på internet i princip… när det var svårt med kryptering och sånt på den tiden… det var väldigt mycket besvärliga arbeten med krypteringsnycklar och sådant. då var det mycket jobbigare, nu för tiden har vi mycket smidigare lösningar… det är klart, ibland så blir det ett litet extra moment där man ska ha "det"... till exempel att folk ska komma in på vår avdelning, så måste de ringa på, de måste bli insläppta av någon och så, men det är inget jätteproblem kan jag inte påstå, det är bara att se till att man gör det… till exempel om jag hade haft två examen arbetare inne på min avdelning så släpper jag dem inte ur sikte…

- Okej… Tack så mycket för att du har svarat på de här frågorna, vi återkommer om det skulle vara några kompletterande frågor eller så...Vi kommer även återkomma på mail med den enkäten vi tidigare diskuterat…

Tack så mycket.

Bilaga 8: Information Security Policy vid företaget

1 Policy

This policy applies to all individuals performing work for Company X, under the staff management of Company X, whether as an employee of Company X or a subcontractor, or as a private contractor, who have been granted access to Company X's non-public Information, or other Information on Company X's behalf.

Company X's Information Security Policy is as follows:

- The confidentiality of information in Company X must be maintained at all times. Information shall never be disclosed to unauthorized parties.
- Access to information will be provided on a need to have basis and in line with the business requirements.
- Information systems used or provided by Company X must ensure the integrity of the information stored in them. Information assets must be protected from unauthorized modification or tampering.
- Monitoring of Company X's information assets and threat landscape shall be in place to ensure that the appropriate protection level is maintained.
- Information assets must be available when needed by the business. Tools, policies and procedures must be implemented and exercised to ensure that sufficient protections regarding business continuity and disaster recovery are in place.

The responsibilities relating to the handling of information within Company X, including that of our customers and partners, is outlined in our Code of Business Ethics and detailed in Company X's ISMS. Failure to adhere to this policy, or associated steering documents & frameworks, may lead to Company X operating with unnecessary risks, not in compliance with local laws and legislation or in breach of customer contracts.

Exemptions to this policy must be approved by the Group Information Security Board.

2 Responsibility

The Group Information Security Board (GISB), chaired by the Chief Financial Officer, is the top level governance board for Information Security, and is supported by Market Area, Local and Business Area specific security management boards.

The Chief Security Officer (CSO) has the responsibility to define, steer and control the overall security governance within Company X and act as the driver of the GISB. The CSO is the senior advisor to the Company X Leadership Team on security matters.

The Chief Information Security Officer (CISO) is responsible for maintaining the Information Security Management System (ISMS) as well as describing and defining specific

responsibilities throughout the organization. Information security controls are also defined by the CISO, but are implemented by applicable functional areas.

It is the responsibility of everybody in Company X to manage information risks within their area of responsibility. Risks or issues should be escalated according to the framework described in the Information Security Management System Group Directive and Information Security Requirements Group Instruction.

Group Security provides tools and methods that can be used as part of every employee's work to ensure that risks to the information that Company X relies on can be managed in an effective way.

Bilaga 9: Classification and handling of Information vid företaget

Classification and handling of Information

Abstract

All documents must be classified and labeled in accordance with the confidentiality of the information. The classification is based on the business impact for Company X if the information is wrongfully disclosed. Information classification, handling and protection are critical components of information security governance.

Classification can be applied to information that is printed, written on paper, stored and processed electronically, transmitted, shown as film or clips, or spoken in conversation.

Application

This instruction is applicable for all information owned by, or in the custody of Company X, and to all individuals performing work for Company X, whether as employees, outsourcing partners, subcontractors or external workforce.

All workforce must adhere to this instruction and classify, label and handle information accordingly.

Non-employees shall be informed by the hiring/contracting department of this instruction and sign appropriate non-disclosure agreements.

Purpose

The purpose of this Instruction is to define the rules and responsibilities that must be applied within Company X regarding classification, labeling and handling of information assets.

Contents

1 Instruction..... 3
2 Responsibility 3
3 Information classification 4
3.1 Classification levels 4
3.2 Labeling..... 5
3.3 Other labeling 5
3.4 Information produced and classified by third party 5
3.5 Changes in classification 5
3.6 Access Control 6
4 Handling of information..... 7
5 Contact for this instruction 9
6 References 9
7 Change information 9

1 Instruction

Company X's workforce has access to information owned by Company X or entrusted to us by third parties. Such information may be confidential and wrongful disclosure could cause damage to Company X, our customers, our workforce or partners.

The term information refers to any collection of information that is printed, written on paper, stored and processed electronically, transmitted, shown as film or clips, or spoken in conversation.

To ensure relevant, consistent and cost-efficient protection of information within Company X globally the level of security should be optimized and differentiated in accordance with the confidentiality and the value of the information.

2 Responsibility

The Information Owner is responsible for providing general guidelines on classification and labeling of the Information Assets within their area of responsibility.

Further, the Information Owner is responsible for ensuring that the information is handled in accordance with the classification as well as for deciding on who is authorized to access the information. This responsibility includes informing personnel about applicable rules and procedures.

Anyone creating or handling information in Company X is responsible for applying classification and labeling of information according to the guidance provided by the Information Owner, and for ensuring the correct handling of the information throughout its life cycle.

The receiver of information owned by a third party is responsible for classifying the information.

System owners must ensure that their systems support the classification levels. Systems must meet the security requirements for storage of information at the different classification levels.

Group Security is responsible for providing the framework for information security and the general requirements on the handling of information for the different classification levels.

3 Information classification

All documents must be classified and labeled in accordance with the confidentiality of the information. The classification is based on the business impact for Company X if the information is wrongfully disclosed. Where there are no general guidelines provided, the information should be assessed by the creator in regards of its confidentiality and handled accordingly.

3.1 Classification levels

There are three classification levels in Company X: Public, Company X Internal and Company X Confidential.

3.1.1 Public

Public is used for information that is deemed for external publication, like press releases, information on web sites for the general public, etc.

All external publication or disclosure of Company X information shall be approved by an authorized Company X body or officer and/or approved spokesperson. Group Function Communications is responsible for appointing all Company X spokespersons.

Information will only be classified as Public and relabeled after the decision has been taken to publish the information externally.

Information that is intended for publication is often confidential up to the release, and shall be handled accordingly.

Public Information should be protected to ensure the integrity and availability of the information but have no restrictions regarding distribution.

3.1.2 Company X Internal

Company X Internal is information intended for internal use or for limited distribution to third parties.

Company X Internal provides the baseline protection for the information and should be used for most information produced in Company X. Company X Internal is accessible widely within Company X but should only be distributed externally under NDA.

This information could cause limited harm to Company X should it be wrongfully disclosed to unauthorized parties.

3.1.3 Company X Confidential

Company X Confidential shall be used for information that needs additional protection, and where availability should be limited internally. Company X Confidential shall only be available to authorized persons and only be distributed externally under NDA.

Personal Data as stated in the Data Privacy directive, XXX, or confidential documents entrusted to Company X by a third party must always be classified as Company X Confidential.

This is information which if it is disclosed to unauthorized persons, can cause noticeable or severe damage to business operations or to individuals.

3.2 Labeling

All documents must be labeled according to its classification with Public, Company X Internal or Company X Confidential. Electronically stored or processed information should be labeled according to the classification where technically feasible.

3.3 Other labeling

Non-public information that is intended to be shared with external parties should be labeled according to its classification with the addition of "Commercial in confidence", e.g. Company X Internal – Commercial in Confidence.

3.4 Information produced and classified by third party

Company X regularly handles information that is produced and classified by a third party. When in Company X custody the information shall be handled and classified in the corresponding way.

Any information entrusted to Company X that is classified as sensitive by a third party should be, regardless of its labeling, be classified as Company X Confidential and be labeled and handled accordingly, any other information should be handled as agreed upon.

Legal or regulatory requirements may in specific cases lead to other types of labeling being applied to Company X information by third parties such as government departments. In these cases a special instructions on how to handle this information should be provided. These labels are only applicable for the specific information and in the context described.

3.5 Changes in classification

The confidentiality of information can change during its life cycle. The Classification label should always reflect the current level of confidentiality.

Changes of classification shall be approved by the Information Owner. In some cases part of the information in the scope will keep the confidentiality and care must be taken when declassifying and relabeling documents.

Information that is classified as Company X Confidential shall not be declassified or distributed without approval from the Information Owner.

3.6 Access Control

Access shall be granted on a need-to-know basis and be limited accordingly. Accesses must be reviewed by the Information Owner regularly.

More information on access control can be found in Group Directive XXX Authorizing access to physical and information assets, and in the Quick Start Guide.

4 Handling of information

The classification level determines the handling requirements for the information. Non-public information, regardless of what media it is stored on must be protected from unauthorized access. Electronically processed, stored and transmitted information that is non-public has restrictions regarding access, handling, communication and disposal or destruction.

Non-public information that is printed or written on paper has restrictions regarding access control, storage, distribution and destruction of the information.

Non-public Information spoken in conversations or over phone shall be protected from unintended disclosure.

The minimum restrictions for handling information according to its classification are listed in this quick chart of handling requirements[1]. Further restrictions may be introduced by the information Owner.

Handling Area	Handling requirement	Public	Company X Internal	Company X Confidential
Documents	External publication or release	If approved by an authorized Company X body or officer and/or approved spokesperson	Only after reclassification by Information Owner.	Only after reclassification by Information owner.
	Sharing information with customers and external parties	No requirements	If authorized and commercial agreement (NDA) is in place. Apply "Commercial in Confidence"	If authorized and commercial agreement (NDA) is in place. Apply "Commercial in Confidence"
	Printing	No requirements	Pull printing	Pull printing or local printer
	Storage in green zone	No requirements	Safe, secure cabinet or vault	Safe, secure cabinet or vault
	Storage in yellow zone	No requirements	Locked offices or furniture	Safe, secure cabinet or vault
	Storage in red zone	No requirements	Suitable for performing day-to-day operations	Locked offices, furniture or cabinet
	Storage outside Company X premises	No requirements	Kept under surveillance or concealed in a secure place	In safe or under surveillance
	Destruction and disposal	No requirements	Document containers for recycling in yellow/red zones	Shredder or document containers for secure recycling in yellow/red zones

Communication	E-mail Internal	No requirements	Labeled	Encrypted

1 The restrictions in the quick guide are the comprehensive selection of requirements in the ISMS regarding confidentiality and handling of information.

	E-mail External	No requirements	Labeled	Encrypted
	Delivery by postal services	No requirements	Internal post – Open envelopes Public post – Sealed envelopes	Internal post – Sealed envelopes with marking in open envelope Public post – Not allowed Courier – Sealed and signed envelopes, confirmation of receipt
	Traveling and hand carriage	No requirements	Keep in sight. Use locked suitcases if possible	Supervised and in locked suitcase. Electronically stored information should be encrypted
	Teleconference	No requirements	No requirements.	E/// bridge should be used.
	Company X controlled Device	No requirements	Encrypted hard drive	Encrypted hard drive
	Private devices	No requirements	Authorized devices, should be encrypted	Authorized devices and encrypted

Workstations, Devices and Services	Third party devices	No requirements	Should be avoided	Not allowed
	Cloud or Internet storage	No requirements	Any approved services	Centrally approved services
	USB	No requirements	Should be encrypted	Encrypted or kept locked in safe, supervisors' approval needed
Equipment	Company X export controlled Equipment on travel	Under surveillance or in locked room	Under surveillance or in locked room, encrypted hard drive	Must be approved by Sensitive Business Areas Board and /or Trade Compliance Approved. Under surveillance or in locked room, encrypted hard drive, Supervisors' approval.

5 Contact for this instruction

Head of Information Security, GFFI Group Security.

6 References

Group Policy, XXX, Information Security

Group Directive, XXX, Information Security Management System

Group Directive, XXX, Classification of Information

Group Directive, XXX, Data Privacy

Group Directive, XXX, Authorizing access to physical and information assets

Quick Start Guide

7 Change information

2014-07-08, The framework for Information Security is being remodeled; as part of this work the Instruction and Directive on classification and handling of information are updated.

The main change from the previous Instruction is that classification is done in regards of confidentiality. The classification schema needs further review, and this instruction will be updated to reflect these changes.

Bilaga 10: Information Security Management System vid företaget

Information Security Management System

Abstract

This document describes Company X's Information Security Management System (ISMS) and the demands on Company X in terms of adherence to Information Security requirements in customer contracts, as well as Company X policies/directives/instructions and regulatory requirements related to Information Security.

The ISMS defines the governance for Information Security Management within Company X, including the structure, processes, roles and responsibilities and controls in accordance with the Company X Group Management System (XGMS).

Application

This directive applies to all Company X operations where Information Assets are handled and across all Company X Business Processes.

Purpose

Information Security shall be managed in accordance with Company X's ISMS to ensure that Company X's wanted position and security strategy is met, Information Assets are protected, and that security acts as a business enabler.

The purpose of this directive is to:

1. Enable the efficient and effective management of Information Security within all of Company X's operations and across all Company X Business Processes where Information Assets are handled to safeguard Company X's Information Assets, and those of our customers and partners.
2. Describe the ISMS, and its associated roles and responsibilities.
3. Ensure compliance with a set of common baseline requirements.

1 Directive

The ISMS defines the governance for Information Security Management within Company X, including the structure, processes, roles and responsibilities and controls in accordance with the Company X Group Management System (XGMS) [1]. The ISMS is applied to all Company X's operations and across all Company X Business Processes where Information Assets are handled.

Responsibilities, controls and the associated requirements [6] are defined by Group Security, following Company X Information Security Strategy [3] and according to the ISO 27000 family of standards, international best practices and the wanted position of Company X.

1.1 Information Security Management System

The Information Security Management System [2] includes a framework to support the following activities:

1. Criticality Assessment - Identification of protection value for Information Assets.
2. Information Security Requirements - Stating the requirements to achieve the protection level needed.
3. Information Security Risk Assessment - Information Security Risk Management in existing operations.

1.2 Criticality assessment

Information Assets, i.e. an entity or group of entities of information that has a value and is essential for the organization and its operations, should be assessed in order to evaluate the business need for protection of the information.

The protection value is defined through the Criticality Assessment resulting in a Protection Profile [7].

1.3 Information Security Requirements

Based on the Protection Profile the implementation of controls may be carried out in different ways provided the controls and requirements defined by Group Security are met [6].

Additional control sets may be used within Company X, however no other controls or requirements may be introduced that reduce or remove control objectives stated in [6] without prior authorization from Group Security.

Requirements that are listed as part of a control are mandatory, unless noted otherwise.

1.4 Information Security Risk Management

Risks to Company X Business must be managed. The Information Security Risk Management process [8] is used to manage risks regarding Information Security in order to achieve an acceptable risk level. Risks assumed shall be justifiable in relation to business objectives. Information Security Risk Management in Company X is aligned with Company X's Risk Management Policy [5].

Information Security Risk Management is a continual process of planning and performing risk assessments, reporting on activities and mitigating risks. Risk assessments must be carried out according to methodology stated in the Information Security Risk Assessment Instruction [8].

Information Security Risk Management must be performed if there is a risk of significant

Business Impact. Examples are;

1. When there is a change or an activity where information security risks can emerge that have an impact on Company X ability to carry out the strategic plan and business obligations.
2. When new information, or a new information processing system, is introduced to Company X, either in terms of a project, in- or outsourcing, merger & acquisition, or through other circumstances.
3. When internal or external activities will lead to a change in the existing information processing environment.
4. When the loss, disclosure or denial of access to an Information Asset would cause danger to any person, damage to Company X, Company X's partners or customers, a loss of business or impact on revenue, workforce moral or Company X's brand.

Information Security Risk Management activities that extends to other parts of the organization shall be coordinated between the relevant BU and Regional Security Management Boards. Information Security Risks that cannot be handled through such coordination shall be escalated to Group Security.

1.5 Protection of Global Information Assets

Global Information Assets (GIAs) are critical Information Assets that could have a business impact on Company X on a global scale, such information requires a higher level attention to ensure their protection.

As a part of the Information Security Risk Management the information Owner is responsible for identifying GIA candidates within their area of responsibility.

Identified GIA candidates should be presented to the Group Information Security Board (GISB) for qualification. The decision if the information asset should be regarded as a GIA is made by the GISB.

When an information asset is qualified as a GIA, a GIA Owner will be appointed and the GIA

is registered in the Information Asset Registry (IAR) managed by Group Security.

The GIA Owners appointed by Group Security have the delegated responsibility from Head of Group Function, Region or a Business Unit for establishing and driving the risk management for the GIAs. This responsibility includes creating a plan for carrying out the risk assessments, ensuring the execution of the plan and reporting on the activities.

The plan and the conducting of the risk assessments should be reported annually to Group Security.

2 Information Security Governance

The Group Information Security Board (GISB) is responsible for ensuring that Information security is governed throughout all of Company X. Any Security Management Board (SMB) in the organization should be able to show an escalation path to the GISB to ensure that Information Security concerns can be addressed at the appropriate level.

The Security Organization on different levels (Group, Regional and Local) is responsible for the corresponding level adherence to the ISMS and for supporting the organization in security related activities, e.g. security risk management.

Regional and Local Security staff shall ensure that the ISMS is adhered to within the scope of their region, operations or cross functional unit.

Business Units and Regions each have Security Management Boards (BUSMBs, RSMBs) that are responsible for providing support to their respective units. In addition, these SMBs may be supported by Local Security Management Boards (LSMBs) for specific units that require additional security support.

Group Security is the owner of the ISMS and responsible for defining the frameworks, roles and responsibilities, controls, requirements, as well as providing supporting processes, methods, and tools. Group Security is further responsible for measuring the control effectiveness of the Information Security Management through KPIs.

Group Security monitors the control execution and effectiveness across the organization to ensure that the correct security posture is maintained.

3 Responsibilities

3.1 Heads of BU, Regions and Group Functions

Heads of BU, Regions and Group Functions are accountable for setting the priorities for Information Security Management within their area of responsibility in accordance to the directives in the ISMS.

They are further responsible for establishing, documenting and maintaining a delegation of risk ownership, information ownership and such internal procedures and control mechanisms that are required to comply with the ISMS.

3.2 Risk Owner

Managers on all levels are responsible for setting the scope of the Information Security Management within their area of responsibility and for initiating Information Security Risk Assessments. Additionally they have the authority to make risk decisions and to escalate risks.

They are further accountable for execution of the risk mitigating activities and for setting the forms for follow-up of risk mitigation plans.

3.3 Risk Handler

The Risk Handler is a temporary role assigned in the Risk Assessment [8] and it includes responsibility for planning the risk mitigating activities and for follow-up on the execution of the risk mitigation plan.

3.4 Information Owner

Managers on all levels are responsible for managing the information security risks within their area of responsibility and for conducting the Criticality Assessment in order to define the Protection Profile for the Information Asset [7].

3.5 Line Managers

It is the responsibility of all line managers to ensure the alignment with the ISMS and that the requirements [6] are met within each person’s area of responsibility and adhered to by the Company X workforce.

3.6 Group Security

Group Security is the owner of the ISMS and responsible for defining the frameworks, roles and responsibilities, controls, requirements, as well as providing supporting processes, methods, and tools.

Referenser

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010), Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 3, p. 523. doi:10.2307/25750690

Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. *AsiaCCS*. doi: 10.1145/1533057.1533084

Höne, K., & Eloff, J. (2002). Information security policy — what do international information security standards say?. *Computers & Security*, *21, p.* 402-409. doi:10.1016/S0167-4048(02)00504-7

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107-124. doi:10.1057/sj.2012.1

D'Arcy, J., Hovav, A. and Galleta, D. F. (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20, 1, 79–98.

Rahman, S., & Donahue, S. E. (2010). Convergence of Corporate and Information Security. *International Journal Of Computer Science And Information Security, Vol 7, Iss 1, Pp 63-68 (2010)*, (1), 63.

Chang, S.E., & Lin, C-S. (2007). Exploring organizational culture for information security management. *Industrial Management and Data Systems*. 107. 438-458. 10.1108/02635570710734316.

Ashenden D. (2008). Information Security Management: A Human Challenge?, *Information Security Technical Report*. doi: 10.1016/j.istr.2008.10.006

Ingelmo Palomares, M., Navarro, C., & Sanz Lara, J. Á. (2018). Determining factors of success in internal communication management in Spanish companies. *Corporate Communications: An International Journal*, *23*(3), 405-422. doi:10.1108/CCIJ-03-2017-0021

Caralli, Richard., Stevens, James., Willke, Bradford., & Wilson, William. (2004). *The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management* (CMU/SEI-2004-TR-010). Retrieved August 09, 2018, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=7129

van Teijlingen, E. R., & Hundley, V. (2001). The importance of pilot studies. *Social Research Update*, (35), 1.

ISO (2018) ISO/IEC 27001:2013 Available Online: https://www.iso.org/standard/54534.html [Accessed 8 May 2018].

ISO (2018). About ISO. Available Online: https://www.iso.org/about-us.html [Accessed 8 May 2018]

Rienecker, L., & Stray Jørgensen, P. (2008) *Att skriva en bra uppsats*. 2nd ed. Malmö: Liber.

Jacobsen, D.I. (2002). *Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*. Lund: Studentlitteratur.

Gollmann, D. (2011): *Computer Security*, 3rd ed. Wiley

LeVeque, V. (2006): *Information Security – A Strategic Approach*. Wiley

Yin, R. (2014): *Case study research: design and methods*. 5th ed. London: SAGE