LUNDS UNIVERSITET

Institutionen för informatik | Kandidatuppsats 15 HP | SYSK 16 VT 2020

Informationssäkerhet inom organisationer

Attityder mot kunskap, policies och ansvarsfördelning

Författare: Mike Pham 950521

Handledare: Miranda Kajtazi

Examinator: Umberto Fiaccadori

Markus Lahtinen

Informationssäkerhet inom organisationer

Författare: Mike Pham. Institutionen för Informatik, Lunds universitet. 2020.

ABSTRACT:
Information security is only as strong as the weakest link. Although the technical, externally oriented efforts are of great importance, there is a predominant weakness when it comes to securing information assets; the individual user within an organization. Employees are often seen as the weakest link due to human error. Many of the security breaches that occur would not have been possible without intentional or unintentional efforts by employees. In order to ensure a safe environment within an organization, all departments must inevitably be ready to counter or neutralize potential threats. Employees in different departments must work together to be able to do this effectively. An organization without functioning security will have problems protecting their information.

The study gathers empirical data through a qualitative approach with interviews of three different companies to investigate how they relate to information security. A major problem is that an increase in security may have the opposite effect as the productivity within the organizations can suffer. After analyzing the interviews and linking the results with both literature and theory, the study demonstrated that companies should see the inclusion of information security as an iterative process and also take into account the balance between policies, education and responsibility perspectives. The results show that information security needs to be highly motivated by the management and there must be a continuous dialogue with the employees.

Keywords: Security values, IT operations, IT governance, information security, information security policy, digitalization, strategic security

1 Inledning

1.1 Bakgrund

Informationssäkerhet är ett begrepp som fortfarande saknar entydiga definitioner. I vissa fall kallas det informationssystemets säkerhet, i andra som digital säkerhet eller säkerhet i sig. Initiativ för informationssäkerhets reglering som Basel II, Sarbanes.Oxley Act har definierat det som "behovet av att skydda informationsresurserna och förhindra obehörig tillgång till organisationen" (Katsikas 2006). Det kan även hittas i termer som säkerhetshantering, affärssäkerhet, och listan fortsätter. Informationssäkerhet innebär således skydd av data och informationssystem från en illvillig tredje part, i form av att man skyddar systemet från modifiering, förstörelse och icke-auktoriserad tillgång. Informationssäkerhet är ytterst relevant i och med hur vanligt det är att privatpersoner såväl som företag använder sig utav datorer och informationssystem utav olika slag. Situationen var annorlunda för 30 år sen och problemen med hackare och andra fientliga tredje parter var näst intill obefintligt. Idag har situationen förändrats och att skydda information och tillgångar har blivit ytterst relevant (Andress, 2014).

När det kommer till informationssäkerhet så har studier främst riktat in sig på tekniska frågor rörande utveckling och genomförande av delsystem för säkerhet. Exempelvis avancerade tekniska metoder för att förhindra intrång i organisationssystem, upptäckande av DDoS, och mer avancerade lösningar för brandväggsskydd. Informationssäkerhet är bara lika stark som den svagaste länken. Anställda ses ofta som den svagaste länken på grund av mänskliga fel (Bulgurcu 2010). Även om de tekniska, externt inriktade insatser är av stor vikt, så finns det en övervägande svaghet när det kommer till att säkerställa informationstillgångar; den enskilda användaren inom en organisation. Många av de säkerhetsöverträdelser som uppstår skulle inte ha varit möjliga utan några avsiktliga eller oavsiktliga handlingar från anställda. Undersökningar tyder på att fler informationssäkerhets brott orsakas av insatser internt från anställda än utomstående hackare (Crossler R 2013). Forskning som undersöker operativa aspekter av informationssäkerhet har varit bristfällig.

Säkerhet över information kan därför vara nödvändig för organisationer idag, på grund av en rad skäl från tekniska till mänskliga fel. För att säkerställa en säker miljö inom en organisation, måste alla avdelningar oundvikligen vara redo att motverka eller neutralisera potentiella hot. Anställda inom olika avdelningar måste samarbeta för att effektivt kunna göra det. En organisation utan fungerande säkerhet kommer att ha problem med att skydda deras information. Säkerhet definieras som kvaliteten eller tillståndet för att vara säker och fri från fara. Detta kan uppnås med hjälp av tillämpningar av policyer, utbildning och utbildning av personal samt ökning av medvetenhet och teknik (Whitman & Mattord, 2012).

1.2 Problemområde

Enligt Whitman & Mattord (2012) har både styrelsen och IT avdelningen ansvaret att implementera informationssäkerhet som skyddar organisationens förmåga att fungera. De nämner många företagsledare och chefer avskräcker sig från att rikta sig till informationssäkerhet eftersom de uppfattar det som en tekniskt komplex uppgift, men i verkligheten har implementering av informationssäkerhet mer att göra med förvaltning än med teknik. Att hantera informationssäkerhet handlar mer om policy och dess utformning än med tekniken för dess implementering. Precis som att hantera löner har mer att göra med förvaltningen än med matematiska löneberäkningar.

Konsekvenserna av ett dataintrång är många. Enligt Campbell et al. (2003) så kan ett dataintrång, där hemlig data röjts, leda till en negativ reaktion från marknaden. Enligt Ismail (2018) finns flertalet konsekvenser med dataintrång utöver den finansiella biten. Däribland finns risken med ett företag som haft dataintrång att bli stämda av sina kunder men även skadat företagsrykte. Feinman (2015) nämner att inom sjukvårds-, finans- och handelsindustrin, så kan upp till en tredjedel av företagets kunder sluta göra affärer med företaget på grund av ett dataintrång. Utan data förlorar en organisation sin förmåga att leverera värde till sina kunder. Därför är skyddandet av data en kritisk aspekt av informationssäkerhet. Värdet på data motiverar angripare att stjäla, sabotera eller förstöra. Ett effektivt informationssäkerhetsprogram implementerat av ledningen skyddar integriteten och värdet av organisationens data (Whitman & Mattord, 2012).

Medvetna attacker inträffar när en individ eller grupp konstruerar och distribuerar programvara för att attackera ett system. Det mesta av denna programvara kallas malicious software eller malicious-code, eller

ibland skadlig programvara. Dessa komponenter eller program är utformade för att skada, förstöra eller förneka service till det riktade systemet. Framträdande bland historien med anmärkningsvärda förekomster av malicious-code är attackerna som utfördes av Mafiaboy på Amazon.com, CNN.com, ETrade.com, ebay.com, Yahoo.com etc. Dessa attacker varade ungefär fyra timmar, och rapporteras ha lett till miljontals dollar i förlorade intäkter (Whitman & Mattord, 2012).

Forskning har pekat på att mycket ansvar ligger på den enskilde individen i en organisation gällande informationssäkerhet. Bulgurcu et al. (2010) pekar ut den mänskliga faktorn som den svagaste punkten i informationssäkerhet och Safa et al. (2016) påpekar att angripare ofta inriktar sig på att utnyttja människor istället för att med teknologiska medel utföra ett dataintrång. Enligt Alotaibi et al. (2016) så inser fler företag att många dataintrång kan härledas till anställda och att de inte följde företagets säkerhets procedurer.

Safa et al.(2016) poängterar att kunskap om informationssäkerhet och uppmärksamhet angående rådande regler kan leda till ökad efterföljelse av reglerna. Alotaibi et al. (2016) framhäver att ISA (information security awareness) är en viktig del i huruvida informationssäkerhet regler efterföljs. Ens egna normer har även pekats ut av Al-Omari et al. (2013) och Blugurcu et al. (2010) som en faktor som påverkar efterföljandet av informationssäkerhets procedurer.

Den enskilde individens ansvar och Informations Security Awareness har utforskats grundligt och litteraturen verkar peka på att detta är en stor del i arbetet med informationssäkerhet. Tidigare nämnda litteratur går även in på metoder företaget kan använda för att öka ISA, däribland träningssessioner för informationssäkerhet och att man delar erfarenheter om ämnet (Safa et al., 2016). Alotaibi et al. (2016) framhäver att dåligt gjorda eller brist på träningssessioner leder till sämre ISA och ökat riskbeteende bland anställda.

1.3 Forskningsfråga

Frågeställning för detta examensarbete är formulerad på följande sätt:

Vilka säkerhetskriterier och förhållningssätt har säkerhetsansvariga i arbetet med IT säkerhet?

1.4 Syfte

Syftet med denna uppsats är att analysera hur organisationer arbetar kring policys, utbildning och ansvarsbegränsningar och balansen mellan dessa. Uppsatsen undersöker hur organisationer förhåller sig i arbetet med informationssäkerhet. Vidare är ambitionen att presentera var inom informationssäkerheten som det är otillräckligt som företag kan förbättra. Utifrån den information som inhämtas är det övergripande syftet att producera en uppsats som organisationer kan använda för att utöka sina kunskaper inom området, framförallt bättre förståelse för organisationers informationssäkerhetsstrategi.

1.5 Avgränsningar

Eftersom informationssäkerhet är ett brett område kommer arbetet avgränsas och förhålla sig till organisationers interna faktorer. Arbetet avgränsas ytterligare genom att i huvudsak fokusera på ansvarsroller hos både informationssäkerhetspersonal och användare. Vidare belyses ett antal teorier och ramverk som resulterar i en förbättrad informationssäkerhet. Uppsatsen riktar in sig på vad driftansvariga kan göra för att minska risken för ett dataintrång.

Uppsatsen kommer inte att gå in på juridiska krav som ställs om informationssäkerhet, då det inte är av intresse. Det är medvetet att juridik utgör en substantiell del av informationssäkerhet men för att uppsatsen inte skall bli alltför bred och komplex så utesluts juridiska krav och studien fokuserar mer på metoder och processer som driftansvariga kan använda för att motverka dataintrång.

2 Litteraturgenomgång

2.1 Information Security Awareness (ISA)

Som tidigare nämndes, ISA innebär, enligt Bulgurcu et al. (2010), en individs kunskap om säkerhetsrisker och dennes ansvar och roll relaterat till riskerna. I litteraturen återfinns många metoder som driftansvariga skulle kunna använda för att hjälpa användarna av ett informationssystem att öka ISA. Safa et al. (2016) nämner facilitering av kunskapsutbyte som ett hjälpmedel för att engagera folk inom området informationssäkerhet och att detta kan öka medvetenheten om informationssäkerhet. Denna typen av kollaboration och engagemang ökar användarnas kunskap om informationssäkerhet vilket i sin tur har en

positiv effekt på användarnas efterföljande utav informationssäkerhetspolicyn (ISP). Dessa aktiviteter bör faciliteras av driftansvariga (Safa 2016).

Shaw et al. (2009) menar att huruvida ett ISA-program lyckas beror på om den anställde erhåller tre former av kunskap: perception, förståelse och förutsägbarhet. Perception innebär att man bildar sig en förståelse över att ett hot existerar. Att ha bra ISA-perception kan öka chansen för att man bildar sig en korrekt bild över hotet i fråga. Förståelsen innefattar huruvida användare förstår och kan analysera farorna som en viss säkerhetsrisk kan medföra. Användare ska kunna tolka information och sålla bland information för att gå i rätt riktning. Förutsägbarhet går ut på att man ska kunna förutse riskerna. Om en användare kan förutse risker innan de sker så har denne uppnått den högsta nivån av förståelse om sin omgivning enligt Shaw et al. (2009). De understryker vikten av att en ISA-utbildning täcker dessa företeelser.

D'Arcy et al. (2006) skriver i likhet med Safa et al. (2016) att träningssessioner och att öka medvetenheten kring informationssäkerhet är bra för ISA. Både Alotaibi et al. (2016) och Safa et al. (2016) nämner att dåliga träningssessioner eller brist på dem kan leda till försämrad ISA hos slutanvändarna. Enligt Von Solmos & Von Solmos (2004) är en av de farliga fallgroparna inom informationssäkerhet att förbise hur viktigt ISA är. De menar att en informationssäkerhetspolicy kan fallera om denna komponenten inte finns med.

Harold & Krause (2010) menar att medvetenhet och träning är viktiga inte bara för informationssäkerheten men också för företaget i sig. De skriver att anställda inte vet vad de ska göra om ingen förklarar vad och hur de ska göra saker och ting. Teknologiska säkerhetslösningar blir värdelösa om personal inte utbildas i hur man använder teknologin korrekt och på ett säkert vis. Informationssäkerheten hänger alltså i mångt och mycket på personalens förståelse och medvetenhet kring ämnet. Företagets säkerhetspolicy kan inte efterföljas om anställda inte känner till dem. Likt föregående författare menar Harold & Krause (2010) att tränings sessionerna måste vara gedigna och väl genomtänkta för att vara effektiva. Detta skall vara pågående för att upprätthålla en god informations security awareness, och inte vara en dåligt genomförd engångsföreteelse. Harold & Krause (2010) menar att en säkerhetsutbildning inte bör vara en generell lösning som kan appliceras på alla situationer. När ett företag utvecklar sin utbildning procedur bör den anpassas

efter varje unik målgrupp som finns inom företaget i fråga och vikten av bland annat att skydda företagets och kundens information måste tydligt understrykas.

2.2 Chefers roll i arbetet med organisationens säkerhetskultur.

Harold & Krause (2010) betonar vikten av att ledningen i ett företag tydligt tar tar ansvar och ger sitt fullaste stöd till informationssäkerhetsarbetet. Johnston & Warkentin (2010) menar att en decentraliserad IT-styrning leder till större risker då alla användare är olika. Användarna varierar mycket i sin nivå av hotmedvetenhet och allvaret, samt kunskap om hur man styr och skyddar sina respektive datorer. Dessutom finns det betydliga skillnader mellan slutanvändare när det gäller åtkomstbehörighet, prioritering och motivation som i sin tur komplicerar efterföljandet av policys. Detta leder till att riskerna ökar om man lämnar mycket över ansvar till slutanvändarna. Harold & Krause (2010) belyser att ansvariga bör mäta hur väl säkerhetsmedvetandet inom företaget är för att kunna göra nödvändiga justeringar om problem upptäcks. Vidare menar Harold & Krause (2010) att ett företag kan mäta nuvarande kunskapsnivåer inom ämnet för att identifiera vilka grupper som inte besitter tillräckligt med kunskap. Där kan bland annat telefonintervjuer och enkäter göras.

Bulgurcu et al. (2010) menar att engagemang är en viktig faktor för att säkerställa att användare följer Informations Security Policy (ISP). Både Alotaibi et al. (2016) och Safa et al (2016) pekar ut avsaknaden utav träningssessioner eller bristfälliga sådana som ett problem som leder till ökad mängd avvikelser från ISP och mer riskfyllt beteende bland användare. D'Arcy et al. (2006) understryker också vikten av gedigna träningssessioner för bättre informationssäkerhet.

Vidare kan man se i tidigare litteratur att företagskulturen och huruvida en adekvat säkerhetskultur finns inom företaget har en stor påverkan. Detta understryks av både Bulgurcu et al. (2010) och Alotaibi et al. (2016). Ashenden (2008) och Chang & Lin (2007) skriver båda att företagskulturen har en märkbar inverkan på informationssäkerheten inom ett företag. Harold & Krause (2010) menar att ansvariga kan försöka integrera en säkerhetskultur i den rådande företagskulturen för att försöka komma tillrätta med detta.

Alotaibi et al. (2016) skriver att ett sätt att öka efterföljandet av informationssäkerhetspolicyn är att använda sig utav tekniska hjälpmedel såsom övervakningsprogram, och om anställda är medvetna om att de övervakas så minskar risken för avvikelser. D'Arcy et al. (2006) nämner också att övervakningsprogram kan minska risken för avvikelser från säkerhetspolicyn.

Både Bulgurcu et al. (2010) och Alotaibi et al. (2016) nämner hur säkerhetskulturen inom ett företag kan påverka informationssäkerheten. De nämner specifikt riskerna med en avvikelsekultur och så kallad shadow security som i sig själv kan späda på avvikelsekulturen. Shadow security definieras av Alotaibi et al. (2016) som en situation där en anställd följer de givna information säkerhetsreglerna på papper men i praktiken så utgör de en säkerhetsrisk. Ett exempel som beskrivs är när säkerhetspolicyn kräver ett komplext lösenord. En anställd kan då välja att skriva sitt lösenord på ett papper och ha pappret uppklistrat på sin datorskärm. Blugurcu et al. (2010) nämner också att avvikelser från ISP kan ske om anställda anser ISP leder till att deras produktivitet minskar. Ashenden (2008) poängterar också att företagskulturen har en stor påverkan vad gäller informationssäkerhet och svårigheten med att påverka den.

2.3 Den enskilde användarens roll i arbetet med informationssäkerhet

Safa et al. (2016) nämner att bristfällig erfarenhet och kunskap kring informationssäkerhet är stora problem bland enskilda användare. Bulgurcu et al. (2010) skriver att medvetenheten kring informationssäkerhet kan sättas i fokus genom antingen erfarenhet, till exempel att en användare får ett virus på sin dator, eller via externa källor såsom tidskriftsartiklar.

Alotaibi et al. (2016) menar att en användares situationella uppmärksamhet påverkar informationssäkerheten genom att en uppmärksam individ lättare kan upptäcka hot. Författaren fortsätter med att säga att användare bör hållas uppdaterade om de senaste utvecklingarna inom informationssäkerhet som ämne.

Enligt Alotaibi et al. (2016) så kan en anställdas nöjdhet och dennes vanor påverka informationssäkerheten. Det är mindre risk att en nöjd medarbetare skulle avvika från ISP och en användares vanor kan ha stora inverkningar på informationssäkerheten, i både negativ och positiv riktning. Vanorna kan dock påverkas av organisationen för att uppmana till sunda och korrekta vanor i enlighet med ISP.

2.4 Attityd & rationalitet gentemot ISP

Det påtalas ofta i de nämnda studierna att den anställda anses vara den svagaste länken inom informationssäkerhet, men anställda kan också vara viktiga tillgångar i försöket att minska risken relaterad till informationssäkerhet. Eftersom anställda som följer organisationens informationssäkerhetspolicy (ISP) och regler är nyckeln till att stärka informationssäkerheten.

Normer och attityd mot informationssäkerhet har också en inverkan. Al-Omari et al. (2013) går in på detalj om personers normer och hur dessa påverkar informationssäkerheten.

Al-Omari et al. (2013) menar att om en anställd känner en moralisk skyldighet att följa ISP så kan detta påverka dennes normer och vanor på ett positivt vis. Vidare nämner Al-Omari et al. (2013) att formalism, i form av skrivna regler och riktlinjer som ska vägleda en användare, påverkar efterföljandet av ISP och en anställds reflektion kring huruvida de fördelarna med avvikelser från ISP väger tyngre än de potentiella konsekvenserna för det. Blugurcu et al. (2010) omnämner detta genom att skriva att en användares attityd kring att följa ISP påverkas av användarens upplevda fördelar och nackdelar med att följa ISP och konsekvenserna av att inte följa ISP. Om användaren upplever att ISP sänker hens produktivitet så kan det leda till avvikelser från ISP.

Bulgurcu (2010) undersökte de rationalitetbaserade faktorer som får en anställd att uppfylla ISP: s krav när det gäller att skydda organisationens informations- och teknikresurser. Viktig förklaring var att en anställds attityd påverkas av förmånerna och kostnaderna av att följa policyn samt kostnaden för att avvika från policyn, dessa övertygelser påverkar användarens egna bedömning i huruvida de väljer att följa policyn eller inte. Safa et al. (2016) nämner att en motiverad arbetare som vill klättra upp i företagets hierarki är mindre benägen till att bryta mot ISP. Dessutom påverkas både attityd och bedömning positivt av ISA.
Alotaibi et al. (2016) menar också att vissa personlighetstyper är mer benägna till att avvika från ISP. Till exempel är det mer sannolikt att mycket extroverta och kompulsiva individer avviker från ISP än en medveten och villig individ.

2.5 Sanktion & belöningssystem

Von Solms (2004) skriver att upprätthållning av organisationens säkerhetspolicy är av största vikt. Att upprätthålla det kan göras på flera olika vis. D'Arcy et al. (2006) betonar vikten av att sanktionera beteenden som bryter mot informationssäkerhetspolicyn och Bulgurcu et al. (2010) instämmer med att hävda samma sak. Själva vetskapen om att sanktioner för felaktigt beteende existerar kan öka efterföljandet av informationssäkerhetspolicyn. Al-Omari et al. (2013) lyfter också effekterna av sanktioner genom att skriva att efterföljandet av informationssäkerhetspolicyn påverkas av huruvida en anställd anser att resultatet av att följa reglerna är bättre än att inte följa dem. Alotaibi et al. (2016) nämner att belöningar som ges till individer som följer reglerna är ett bra sätt att öka efterföljandet av regelverket. Chen et al. (2014) belyser också hur ett belöningssystem kan vara bra för att öka efterföljandet av reglerna.

Dessutom påverkar informationssäkerhet medvetenhet (ISA), som bildas av allmän ISA och ISP medvetenhet, anställdas attityd att följa säkerhetspolicy. Bulgurcu (2010) påpekar att en anställds ISA har ett direkt inflytande på attityden till efterlevnad av policys och spelar en huvudroll i att forma anställdas bedömning. Befintlig litteratur som framhäver vikten av ISA bekräftar att det har en stark påverkan på anställdas attityder till att följa säkerhetspolicy.

3 Metod

3.1 Metodval

För att fördjupa kunskapen inom forskningsområdet genomfördes en litteraturstudie med fokus på tidigare forskning inom informationssäkerhet. Litteraturstudien baserades på tidigare vetenskapliga artiklar som undersöker och diskuterar informationssäkerhet. Metoden för insamling av empiri är utifrån kvalitativ ansats. Individuella intervjuer med IT-ansvariga för de olika företagen utfördes där frågor ställdes om hur de arbetar för att motverka dataintrång. Intervjuerna är semistrukturerade med öppna frågor för att möjliggöra en större omfattning inom det valda ämne samt att möjligheten till följdfrågor och diskussioner leder till ett mer djupgående perspektiv än t.ex. en enkät. Denna metoden är mest lämplig för att se ett samband mellan individ och kontext enligt Jacobsen (2002). Intervjufrågorna riktades in på hur företagen arbetar med

IT-säkerhet utifrån ett strategiskt och tekniskt perspektiv, samt respondenternas egna perspektiv på informationssäkerhet. Resultaten av intervjuerna tillsammans med litteraturstudien användes som grund till diskussionen sedan sammanfattas en slutsats där författaren redogör hur väl den empiriska studien överensstämmer med litteraturstudien.

3.2 Urval av intervjupersoner

Fokuset ligger i att hålla en intervju med ett mindre företag som har några hundra anställda, ett medelstort bolag med några tusen anställda och ett stort, multinationellt bolag med tiotusentals anställda. På så vis kan man samla in data utifrån olika bolags storlekar och utifrån de olika erfarenheter intervjupersonerna i fråga har. Detta önskade urval mynnade ut i att tre intervjuer bokades med tre bolag utav olika storlekar. Med anledning av att de utvalda företagen vill förbli anonyma delvis för att informationssäkerhet är ett känsligt ämne och denna studien vill inte röja företagens procedurer, då intervjupersonerna går in på procedurer de använder inom sina respektive företag. På grund av detta togs beslutet att maskera samtliga företagsnamn och utelämna intervjupersonens efternamn för att hålla en röd tråd i uppsatsen. Företagsinformationen är sekundär data hämtad från respektive företags hemsida.

Företag 1 är ett världsledande bolag inom sin bransch med cirka 30000 anställda runt om i världen. Företaget arbetar med produktion av förpackningar och här intervjuades “Adam” med befattningen Information Security Education & Awareness Manager.

Företag 2 är ett IT-bolag med cirka 4000 anställda och respondenten “Björn” ansvarar för informationssäkerheten hos företaget. Företaget är ledande i Sverige och arbetar med konsultverksamhet inom IT, informationslogistik, teknisk R&D, mjukvarutjänster, industri och samhällsbyggnad.

Företag 3 är ett IT-bolag med cirka 300 anställda och där “Calle”, Chief Technical Officer (CTO) intervjuades. Nedan i resultat presenteras en sammanfattning av från intervjuerna.

3.3 Litteratur

För att utföra en litteraturgenomgång på området har sökmotorerna Google Scholar, Google Search och LUBSearch använts. Google Search har agerat som ett supplement till Google Scholar, för att finna mer material från bland annat väl beryktade tidningar och andra källor såsom företag verksamma inom informationssäkerhet, informationssystem och informatik. Då Google Scholar har en otroligt bred databas som innehåller tusentals artiklar användes olika sökord som “Security values”, “IT operations”, “IT governance”, “Information security”, “cyber security” , “Digitalization”, “Strategic security”. Med hjälp av sökorden hittades relevanta artiklar, böcker och studier som kunde användas som grund till uppsatsen.

Artiklarnas relevans och trovärdighet bedömdes kontinuerligt utifrån kvalité, publikationsansvarig, årtal och peer-review. Flertalet av böcker, artiklar och studier som uppsatsen valde att presentera är skrivna av professorer inom IT från Boston College m.fl. andra välkända lärosäten. Bulgurcu (2010) Information Security Policy Compliance, Safa (2016) Information security compliance model in organizations & Whitman (2012) Principles of Information Security 4th edition har varit viktiga inspirationskällor till rubrikerna i litteraturgenomgången. Vidare hittades även litteratur genom att söka vidare i de relevanta studiernas referenslista. Ambitionen för litteraturgenomgången var att djupdyka inom informationssäkerhet för att få en god förståelse inför den kommande datainsamlingen.

3.4 Intervju utformning

Intervjuguiden för de individuella intervjuerna strukturerades med öppna frågor, med inledningsvis allmänna frågor för att sedan fördjupas med följdfrågor och diskussioner. Innan varje intervju började ställdes grundläggande frågor om intervjupersonens befattning och vilket typ av företag hen jobbar för. Frågorna för den empiriska studien grundades utifrån kunskapen som erhålls från litteraturstudien samt frågeställningen kring arbetsmetoder och förhållningssätt av driftansvariga gällande informationssäkerhet. En semistrukturerad intervju genomfördes och således var frågorna inte en strukturerad checklista. Frågorna belyser vilket ämne som kommer att behandlas och utrymme finns för att ställa följdfrågor eller diskutera varje fråga djupgående. Jacobsen (2002) framhäver att en resultatrik intervju bör inte vara längre än en timme och kortare än 30 minuter. Med detta beslutades det att tidslängden för intervjuerna skulle vara ungefär 45

minuter. Då informationssäkerhet är ett känsligt ämne kommer företagsnamn utelämnas om så önskas av intervjupersoner.

3.5 Analysmetod

För att bearbeta den insamlade empiriska datan transkriberades de individuella intervjuerna. Jacobsen (2002) menar att fördelen med detta är att tydliggöra all information intervjuerna innehåller för att sedan kunna analysera datan på ett effektivt sätt. Efter inspelning och transkribering av samtalen med intervjupersoner används tematisk analys utifrån Braun och Clarkes (2006) motiveringar med syftet att identifiera gemensamma teman i intervju uppgifterna. Deduktiv analys har gjorts där teman identifieras och grundar sig på befintliga teorier för att sedan kopplas till vad som analyserats i intervjumaterialet. Datamaterial som samlats in organiseras och struktureras upp utifrån teman som gemensamt framträtt mellan intervjupersonerna. Dessa teman sammanställs som en resultatdel i en rapport. En av fördelarna med tematisk analys är att det är en flexibel metod och passar denna typ av deduktiv studie där intervjuer genomförs på en teknisk arbetsplats för att ta reda på vilka utmaningar de driftansvariga står inför i deras arbete med informationssäkerhet och att säkerställa att risken dataintrång förblir så minimal som möjligt.

3.6 Validitet och reliabilitet

Cohen, Manison och Morrison (2007) motiverar att ett av de mest praktiska sättet att uppnå större validitet är främst att minimera mängden av partiskhet mellan alla inblandade så mycket som möjligt. För att hålla intervjuerna opartiska avhålls förväntningar, attityder eller åsikter under intervjun och målet har varit att ställa neutrala frågor där respondenter själva får utveckla, motivera och förklara vad de upplever. Oppenheim (1992) hävdar att formulering är en särskilt viktig faktor i attitydfrågor snarare än faktiska frågor. Han föreslår att förändringar i formulering, sammanhang och betoning undergräver tillförlitligheten, eftersom det upphör att vara samma fråga för varje svarande. Ett sätt att kontrollera reliabilitet är därmed att hålla en strukturerad intervju med samma format och sekvens av ord samt frågor för varje respondent. Eftersom ett semistrukturerat intervjuformat har valts är det viktigt att inte ställa ledande följdfrågor för att inte äventyra validiteten och reliabiliteten.

3.7 Etik

I utförandet av undersökningen har ett etiska aspekter tagits i beaktning från Jacobsen (2002) centrala begrepp gällande etik. För att utföra studien på ett så etiskt vis som möjligt har det därför varit viktigt att respektera samtliga deltagares rätt till privatliv och anonymitet. Informationssäkerhet är ett känsligt ämne och frågorna har formulerats på en generell nivå som gör det möjligt för intervjupersonen inte behöver berätta något om deras bolags procedurer om denne inte vill. Vid begäran så kommer intervjuade företag och personer att inte benämnas med namn för att inte röja deras arbetssätt med informationssäkerhet.

4 Resultat

Sammanställning av intervjuresultat

4.1 ISA

För få resurser uppges vara en utmaning för arbetet med ISA. Adam (Företag 1) förklarar att organisationen måste kontinuerligt arbeta med utbildning procedurerna samtidigt som man måste titta på framtida strategier och vad som måste förbättras. Tid är en bristvara. Fokus har skiftat mot ISA, utbildning och kunskap på senare tid och alla större bolag har någon form av awareness-program igång men man har kommit olika långt. När det gäller informationssäkerheten så måste det enligt Adam (Företag 1) ta en avstamp i riskbedömning, man måste göra en riskanalys och utifrån den definiera sina infosec mål och var man ska lägga ribban.

Enligt Björn (Företag 2) finns alltid konfliktlinjer med att skicka folk på InfoSec utbildning och de står alltid i konflikt med att produktiviteten minskar. Tar du exempelvis 100 anställda ut från deras dagliga verksamhet och säger nu ska ni gå en halv dag på utbildning, ja då minskar produktiviteten. Det kostar pengar någonstans. Och då får man göra en värdering och bedömning och vi inom Företag 2 har valt att satsa på informationssäkerhet så vi avsätter pengar för att göra detta men det är inte alla företag som tycker det är värt det.

Enligt Calle (Företag 3) bestämmer IT avdelningen hur mycket utbildning som ska köras, när ska det göra, och hur mycket tid kan läggas på det. Det handlar om att vara proaktiv. De har satt det här programmet att

alla kör obligatoriskt 2 timmars introduktion och sen följer man upp 15-30 minuter per år. Utmaningen där är mest att se till att alla vet och hjälper alla att se det som obligatoriska moment och man följer upp det i företagets karriärsystem där man får bocka av att man gjort den utbildningen.

Företag 3 har dessutom phishing tester som komplement, och man undrar ifall man borde göra något annat också? Man kan göra hur mycket som helst. Man hade kunnat lägga ut veckans säkerhetstips. En fem minuters liten film. Men en film fem minuter tar en ganska lång tid att producera. Så en utmaning är att man ska veta var drar man gränsen? Hur mycket är lagom? Hur mäter vi att det här är framgångsrikt? Phishing testerna kan man mäta på lite grann. Det är jättesvårt att dra några slutsatser om det. Det är väl två utmaningar i all fall, att veta hur mycket är lagom och vad får vi tillbaka för det? Samtidigt tror Calle inte att ett företag i deras storlek behöver veta exakt hur mycket vi får ut av det. Han vet att utbildningen är viktig och att den tjänar sitt syfte och att den gör per automatik att företaget får färre incidenter för man skapar en ökad medvetenhet hos medarbetare. Så utmaningarna är väl lägga ribban lagom högt och se till att det upprätthålls och se till att ha bra innehåll. Företaget valt att producera sitt egna innehåll själva istället för att köpa in någonting och det är väl också någonting som tagit ganska lång tid att producera det materialet. Calle är väldigt nöjd att de gjort det för att anpassa det precis efter deras verksamhet.

4.2 Styrelsens roll i informationssäkerhetsarbetet

Företag 1 uppger att deras ledningsgrupp är helt med på arbetet med informationssäkerhet och de anser sig inte ha haft problem med att lösgöra resurser till informationssäkerhetsarbetet. Även den globala ledningsgruppen är med på arbetet. Företag 1 skapar diskussioner på sin Jammer, som är som ett facebook endast för företaget, om informationssäkerhet och sprider information om till exempel phishing mailen och hur många som klickade på den. Här kommer även ledningsgruppen in och lämnar likes och kommentarer på det som skrivs (Intervju 1). Företag 1 uppger också att de tror att det blivit vanligare att topp ledningen engagerar sig i informationssäkerhetsarbetet i och med att informationssäkerhet uppmärksammas i medier. Stora dataintrång publiceras flitigt i media. Det blir naturligt att andra bolag i världen uppmärksammar detta, blir oroliga och fokuserar på informationssäkerhet.

Björn (Företag 2) talar om att stöd från ledningen är A och O för att informationssäkerhet ska fungera i ett bolag oavsett om det är ett tremanna företag eller om man har tusen anställda. Högsta ledningens stöd och support är helt avgörande utan den så kommer man inte lyckas. Det är så pass viktigt. Informationssäkerhet kostar både i pengar och lite engagemang och har man inte högsta VDn eller styrelseledamöter som stöttar detta till 100 procent så kommer det inte bli bra. Ofta handlar det om att dessa personer kanske inte alltid förstår risker och vilka hot som finns ute på internet. Man tänker amen de har funkat bra hittills och bolag i Företag 2 storlek på ungefär 3000 anställda, får runt 50 000 phishing mejl om dagen. Det mesta klipps ju och stoppas av filter men 98 procent är automatgenererat där det är bots som bara trycker ut mejlen genom internet hela tiden. Vi har kanske tusentals hackings försök på vår yttre brandvägg där de flesta är automatgenererade men sen finns det vissa kriminella nätverk som sitter och letar efter sårbarheter i brandväggarna kanske från uzbekistan, ukraina, nordkorea, kina, iran, usa och mexiko. Whatever. Vi har fått hackningsförsök från Holland också så det kan komma varsomhelst ifrån. Och den här hotbilden tror jag inte VD och ledningar i bolag är så medvetna om alltid om vilket tryckt det är på våra bolag utifrån. Det är sanslöst tryckt.

Ja det är ju en utmaning och det är dem själva som är ansvariga ytterst för bolag och för infosec, det är VD som är ansvarig och han har i sin tur sitt ansvar att informera styrelsen om han behöver mer pengar för IT säkerhet.

Enligt Calle (Företag 3) är informationssäkerhetspolicy godkänd av styrelsen och de är informerade om vad som står i den och de har fått en briefing förra året gällande det säkerhetsarbetet som görs. Sen tror Calle generellt sätt kanske att man inte riktigt är medveten om hur viktigt arbetet är och man underskattar det lite grann innan det har hänt en incident som påverkar verksamheten ordentligt. Tyvärr. Det ligger lite i människans natur.

Företag 1 uppger att de säkerställer att ledningen har rätt kunskaper genom riktade träningsmoduler specifikt framtagna för dem. Vissa fattar ju att det här är en viktig fråga men det finns dem som inte inser hur mycket skit som finns ute på internet och hur mycket det är som vi blockar. Företaget blockar 99.9 procent av allting och det är ju en bra siffra men omfattningen är så himla stor att det trillar alltid igenom någonting.

Björn (Företag 2) anser att det inte finns tillräckligt med kompetens i styrelsen och det finns inga bra kurser eller utbildningar heller. Styrelseledamöter och ordförande har inte all tid i världen till att ägna sig åt detta, därför skulle det behövas ta fram små intensiva kurser på kanske 3 timmar. Bara så man får lite insikt om hur hotbilden ser ut och vad som händer ute på internet, men de typen av utbildning finns det inte mycket om. Det finns långa tekniska utbildningar men dessa riktar sig inte till styrelsen. Enligt Adam kommer informationssäkerhet kommer bara tas upp mer och mer med tiden. Det finns sårbarheter överallt och till och med en hiss har programvara som kan bli manipulerat hur enkelt som helst. Det kanske inte finns mycket att hämta där men det finns liksom överallt sårbarheter och det finns de ute på internet som är beredda på att störa och förstöra för skojs skull men det kommer ju mer och mer nu att det finns ekonomiska incitament för att hålla på med denna typen av brottslighet. Om man drabbas av det är det väldigt svårt att ställa dem tills vars, ofta går den genom proxyservrar i länder som inte har något fungerande rättssystem eller som kanske inte sparar loggar.

Företag 3 har en styrelse som enligt Calle är i alla fall tekniska nog i att jobba med ett mjukvarubolag och informationssäkerhet är en väldigt viktig detalj. Han är väldigt nöjd med styrelsen.

4.3 Sanktions- och belöningssystem

Adam (Företag 1) anger att de använder sig utav träningsmoduler som köps in från en tredje part i deras awareness och education-program och detta är en kontinuerlig process. Eftersom modulerna tar tid att utföra så kan man diskutera om man ska tvinga anställda att gå på ett visst antal träningar eller ska man engagera dem istället. I länder såsom USA så är dem väldigt hårda med straff men Företag 1 går mer på att det är mandatory och går via chefer och skickar påminnelser. Adam anser att det inte är hela världen om en anställd missar en träning. Däremot säger Adam att sanktioner och straff är mer applicerbart i större bolag medan i mindre bolag så är belöningar mer lämpligt. Företag 1 har däremot en slags sanktion om man klickar på flertalet simulerade phishingmail där man till slut får ett samtal med chefen.

Björn (Företag 2) tycker att belöningssystem fungerar garanterat. Man tror inte på att straffa bort felaktigt beteende. Organisationen består av högutbildade ingenjörer, systemvetare och civilingenjörer m fl. Det är

smarta och intelligenta människor, finns det inget tydligt mönster vid brott mot organisationens policyn och det inget ont uppsåt bakom utan då är det otydligt regelverk eller riktlinjer, eller pressad situation där man kanske gör avsteg gällande policyn för att rädda en kund, affär eller annan relation.

Calle (Företag 3) kallar detta för carrot eller stick. Han tror mycket på för det är nog det bästa sättet att få ett mer "positive reinforcement", att man uppmanar folk att göra rätt och det ska vara enkelt att göra rätt istället för att man tar genvägar och gör fel helt enkelt. Där fel kan vara lite subjektivt ibland. Ett exempel som han inte gjort men läst om och som han tycker är väldigt bra är att låsa sin dator när man lämnar skrivbordet vilket inte alla är så jättebra på. Istället för att kollegan kanske går in och skriver något tråkigt på din facebooksida eller någonting annat som får dig att förstå att det är en bra grej att göra. I deras företag använder de ett chattsystem, Microsoft Teams för exempelvis gruppdiskussioner. Det var någon någonstans som gjort en bot där man kan gå in i en olåst dator, öppna Teams-klienten och ge sig själv poäng. Det vill säga att man snor poäng från den vars dator man tar över. Sen spårar man och har en leaderboard där man ser vem har tjänat mest poäng på att jaga öppna datorer den här månaden till exempel. Och sen om man vill koppla ett pris till det eller vad man vill göra. Men det tycker Calle är ett jättebra exempel. Det är ett ganska konkret och ganska billigt sätt att öka medvetenheten och få med lite gamification.

4.4 Shadow security & företagskultur

Adam (Företag 1) hävdar att shadow security eller Shadow IT var ett problem förr för deras bolag. Icke-godkända appar användes då användarna ansåg att de inte hade rätt systemstöd för att utföra sina jobb. Organisationen övervakar också vilka molntjänster som kopplas upp genom en mjukvaruapplikation och nämner att de använder smart card och VPN för säker inloggning. Smart card har ett kortare lösenord och således rekommenderas alla medarbetare på Företag 1 att logga in i datorerna med smart card. Företag 1 anser att shadow security är ett organisatoriskt problem och inte bara IT-relaterat. De nämner också att många incidenter sker på grund av misstag och oavsiktligt. Regler måste vara balanserade då komplexa regelverk kan öka risken för misstag. Företaget har informationssäkerhetspolicy och procedurer som är obligatoriska att följa till skillnad från guidelines som är mer riktlinjer och mindre strikta enligt Adam.

Enligt Björn (Företag 2) är det största problemet med skugg-IT är att man använder molntjänster som ligger utanför företaget kontroll. Det vill säga att företaget har exempelvis sagt att vi ska använda oneDrive, Sharepoint eller annat och ändå finns det enheter ute i linjen som köper en Dropbox och gör på egen hand eftersom man tycker den är enklare, bättre, smidigare, snyggare. Och företaget har ingen kontroll över den information eller datan som ligger på den Dropboxen och som slutligen blir skugg-IT. Han skulle säga det är mer regel än undantag att det finns skugg-IT men hos vissa företag finns informationssäkerhet så djupt förankrat i kulturen, i väggarna så där förekommer det inte. Men i de allra flesta företag så finns skugg IT enligt hans bedömning.

Calle (Företag 3) tror väldigt mycket på att göra det enkelt att göra rätt. En anledning till att det blir shadow-IT eller att användaren hittar egna lösningar på problem. Det är ju för att man antingen har för tajt säkerhet så att folk inte kan jobba eller att det inte finns tillräckligt bra tekniska lösningar eller lösningar överlag för att man ska kunna jobba effektivt. Har man duktiga medarbetare så är de här för att jobba effektivt. Dem kommer hitta vägar runt allting för att kunna jobba effektivt. Det handlar mycket om att jobba med användarna för att bygga lösningar som är säkra att använda och som användarna vill använda. Sen kommer det där aldrig vara 100% utan man måste ibland säga nej för det blir för kostsamt att bygga enkelt och bra alla gånger. Men det måste vara en balans. Det måste vara tillräckligt enkelt att göra rätt.
Calle tar som exempel att anställda använder sin google docs och privata mail och cloud lagring. Kanske inte för att det är smidigare men mer av okunskap. Man kanske säger det är så här jag brukar göra men det är inte vad företaget använder. Där handlar det också om utbildning och se till att medarbetarna vet att det är detta som gäller och man måste använda dem här lagringsställen och man vet att det är minst lika bra. Det vill säga att man inte använder andra system av ren vana för man kan det utan man använder det som företaget säger man ska använda och att man vet hur det fungerar och vilka fördelar som finns med det.

Adam (Företag 1) diskuterar att kultur är olika i olika länder och organisationen försöker anpassa det så det fungerar för alla. Hela deras awareness-programmet handlar om att införliva säkerhet i det dagliga arbetet. Adam uppger även att det har varit problem med tekniska lösningar. Användarna avskyr när tekniska lösningar trycks ut som dödar produktiviteten eller gör datorn långsammare. Moderbolaget kommer med krav som inte är från informationssäkerhets gruppen hos Företag 1. Adam (Företag1) menade exempelvis när

det kommer till lösenord så finns det två olika skolor. Den ena säger att man ska ha så långa och komplexa lösenord och sedan byta de så ofta som möjligt. Och alla som jobbar med människor vet ju att så funkar det inte. Människor är inte konstruerade att komma ihåg den typen av lösenord och hela tiden byta. Och sen finns det den andra skolan som menar att det är bättre att ha ett långt komplext lösenord men som du kanske inte byter hela tiden. Du har det kanske i ett år. Det här med komplexa lösenord och tvinga anställda att kontinuerligt byta var 90 e dag som ofta är standard i branschen, det får ofta till följd att folk skriver det på post it lappar och lägger det under tangentbordet. Informationssäkerhet är väldigt komplext, det utvecklas ständigt och man måste anpassa skyddet efter hotbilden och kraven och man kan ju också skydda sig till tänderna men då blir det väldigt svårt för det är som ett dragspel. Säkerhetskriterier såsom komplexa lösenord som måste bytas leder till att användare börjar ta genvägar för de är arga på informationssäkerhet gruppen.

Björn (Företag 2) diskuterar två huvudområden, det första är bristande förståelse, organisationer förstår inte hotbilden och varför är det viktigt med säkerhetstänk. De andra är att alternativen kanske inte är helt optimala, då skapar vi företaget skugg-IT och dåligt säkerhetskultur. Vill företaget ställa krav, ha ordning och reda, hänvisa till regelverk, säkerhetspolicyn och så vidare, så ska det man hänvisar till först och främst fungera. Ofta är det så att man pekar på någonting som inte funkar så jättebra och då är människan så kreativ och tänker på andra snabba utomstående lösningar: “ja men här är ju dropbox/Slack” eller vad det nu kan vara som man tycker fungerar bättre och man använder då det. Så det är en kombination av bristande insikt och att alternativen som man har pekat på oftast inte är så bra.

Som Calle (Företag 3) nämnde tidigare om man anställer duktiga medarbetare så kommer dem vilja jobba så effektivt som möjligt och ibland kan det vara svårt under tidspress. När man kämpar mot klockan så blir det mycket enklare att avvika och ta genvägar. Att göra saker på fel sätt snarare än att göra det på rätt sätt. Det är ju en utmaning och det är en leveransorganisation där företaget dels måste vara väldigt noga vid hantering av deras kunders data. Samtidigt så finns en tidspress på medarbetare att leverera och prestera inom en viss tidsram och de jobbar med ett ganska stort antal individer som kommer direkt från skolan och har bara några få års erfarenhet.
Man kanske råkar tänka “Ska jag göra på det här sättet eller är det bättre att göra på det här sättet som tar längre tid? Någon sa att det var säkrare men hur viktigt var det?”

Enligt Calle så är en av deras större utmaningar med avvikelse kultur. Stress och tidspress.

En utmaning Calle ser med att införliva säkerhetskultur är att folk glömmer väldigt snabbt. Man måste påminna hela tiden, utbilda och göra folk medvetna om säkerhetstänk kontinuerligt. Det är ett lärande man måste ha hela tiden. Han menar att Företag 3 arbetar proaktivt istället för att vänta på att en incident sker. Till exempel så har man kört phishing tester internt där IT-avdelning skickar ut test med jämna mellanrum till alla medarbetare och följer upp resultatet. Vilka öppnade det, vilka rapporterade det, vilka ignorera det bara?

"Vi försöker tracka hur det går för oss. Det är faktiskt någonting som har blivit en kul grej, en liten snackis. Är det här ett test? Det har lett till att man är mycket mer medveten vad gäller just phishing."

- Calle (Företag 3)

Calle menar att det är en sak att lära ut säkerhet i teorin under en utbildning men sen när man väl sitter i sin kontorsstol och ska jobba praktiskt med det man har lärt sig, under tidspress, har många bollar i luften, många som skriker mot en. Det är stora utmaningar. Tidsbrist och att man glömmer bort.

4.5 Övervakningsprogram och tekniska skydd

Adam (Företag 1) beskriver att organisationen har diverse tekniska skydd men de anser att för två år sen så var det ett stort fokus på tekniska skydd hos bolag. Nu har fokuset skiftat mer mot awareness and education och inte bara teknik. Det måste vara en kombination av teknik och utbildning men att anställda är medvetna om risker är viktigt i slutänden. Tekniska skydd spelar ingen roll om en användare är omedveten och utför saker som innebär en risk.

Björn (Företag 2) beskriver att övervakningsprogram förekommer mest på de stora företagen, man granskar brandväggsloggar, surf loggar var folk har surfat lite så sporadiskt, att övervaka personalen minutiöst det kostar enorma pengar och det är inget företag som gör det, utan vad man gör är att man har lite intelligenta filters och om någon går in i vapen sidor, porrsidor eller drog sidor på internet så finns det logik i brandväggarna som klipper till och säger att det är en otillåten sajt. Sen finns det IDS, intrusion detection

system och IPS, intrusion prevention system men de är mer logik i nätverken som detekterar externa intrång och kanske inte så mycket internt, om var man surfar och så vidare.

Företag 3 använder en detekterings mjukvara på deras laptops som loggar varifrån man loggar in och jämför.

"Här har vi Nisse och han brukar sitta i stockholm men ibland är han nere i skåne. Men nu försöker han logga in från ryssland här och det är ju antagligen lite fuffens och det triggar ett larm."

- Calle (Företag 3)

Företaget har också multifaktorautentisering för alla medarbetare. Enligt Calle borde det vara standard. Man har även ett par andra skydd också där man tittar på avvikelser. Företaget har full disk kryptering på laptops. De kan dessutom spärra alla företagsmobiler och följa upp vilka applikationer man har vid behov.

4.6 Uppföljning och kunskapskontroll

Phishing mailen används som en kontroll över hur många som klickar på mailet. Björn (Företag 1) utvärderade informationssäkerheten när awareness-program påbörjades och följde upp med detta och på så vis se om programmet varit framgångsrikt. Phishing mailen har blivit en snackis och på så vis diskuteras säkerhetsfrågor inom bolaget. Att skapa engagemang inom frågan och att få folk att prata om det är viktigt, även när det gäller negativa företeelser.

Vad Adam (Företag 2) berättar är att det viktigaste med informationssäkerhet är det återkommande arbete där företag måste komma in i ett årshjul där man jobbar hela tiden med att definiera säkerhetsmål och man måste prata om säkerheten hela tiden i företaget. Det kan inte bara vara en fråga som lever sitt eget liv vid sidan om. Det ska upp på agendan och man måste lyfta upp det under viktiga möten.
Det kan man säkert göra, men här gör vi så kallade sårbarhetsanalyser där vi kontakter ett externt bolag så får de ett IP range eller adress till våra nätverk och så säger vi ni har en dag på er att hacka oss. Det ena är penetrationstest och det andra är sårbarhetsanalyser där de säger till oss om våra sårbarheter och vad vi måste

förbättra. Om vi går tillbaka till den frågan där om att skicka fiktiva phishingmejl enbart i syfte för att se hur många som eventuellt klickar på länkar skulle kunna vara ett sätt att få en lite grov uppfattning om hur mognadsgraden är i bolaget. De skickar ut simulerade phishing kampanjer för att testa kunskapen.

Calle (Företag 3) har en uppföljningsutbildning en gång om året för samtliga anställda som de ska ta fram innan sommaren. Företaget körde igång med det programmet förra året så det kommer bli 15-30 minuters refresher för samtliga. För Calle är en av utmaningarna ifall uppföljning skulle räcka en gång om året?

5 Diskussion

5.1 ISA

Litteraturstudien nämner att den svagaste länken för att upprätthålla informationssäkerhet är anställda inom organisationen. Mänskliga faktorn kan hota hela företaget eller avslöja känsliga och klassificerade data till obehöriga. För att förhindra detta behövs det kontinuerlig träning och utbildning av de anställda. Harold & Krause (2010) betonar vikten av ISA och att öka användarens kunskap och medvetenhet kring informationssäkerhet. Där finns självfallet ett ansvar bland användaren men driftansvariga har ansvaret att hjälpa till genom att informera, hålla i informationsmöten och träningssessioner vars syfte är att öka de anställdas ISA.

Resultaten i denna studien visar tydliga likheter i teori och företagens förhållningssätt till informationssäkerhet. På senare tid har företagens fokus riktat sig mot ISA, utbildning och kunskap. Företag 1,2 och 3 har alla någon form av awareness-program igång men man har kommit olika långt. IT avdelningar jobbar proaktivt och man bestämmer hur mycket utbildning som ska köras, när ska det göra, och hur mycket tid kan läggas på det. Vi ser att företag förstår vikten av utbildningen och att den tjänar sitt syfte vilket leder till att företag får färre incidenter för man skapar en ökad medvetenhet hos medarbetare. Utmaningen med förhållningssätten kring informationssäkerhet är att lägga ribban lagom högt, och se till att det upprätthålls.

Enligt Adam från företag 1 läggs inte tillräckligt med resurser på ISA. Än så länge verkar det som att Företag 1 har koll på vad man ska göra men har svårt med att leva upp till det. Björn (Företag 2) menar att finns alltid konfliktlinjer med att skicka folk på ISA utbildning och de står alltid i konflikt med att produktiviteten minskar. Informationssäkerhet kostar pengar. Det är inte många företag som gör den avvägningen. I litteraturen tar man inte upp de monetära kostnaderna av att ha en bra säkerhet. Detta är ett tydligt problem då företag kan tendera att ha kortsiktigt tänk när det kommer till ISA. De vill hellre spara pengar nu genom att dra in olika utbildningar än att spendera pengar och kanske spara en större summa pengar i framtiden genom att avvärja olika dataintrång. Enligt Calle från företag 3 bestämmer IT avdelningen omfattningen av utbildning som ska köras, när, och hur mycket tid som skall läggas. De har program som alla anställda kör obligatoriskt med 2 timmars introduktion och sen följer man upp 15-30 minuter per år. Här ser vi en centraliserad it-styrning som försöker stämma av slutanvändarnas kunskap och medvetenhet. Precis som litteraturen förespråkat. Harold & kruse skriver bl.a. att träningssessioner måste vara gedigna, och väl genomtänkta. Men det finns alltså en tolkningsfråga som kan ställa till det något. Vad är gediget och väl genomtänkt? Företag 3 kom med dessa insikter och hade som tidigare nämnts ett program med 2 timmars obligatorisk introduktion och sedan 15-30 minuter uppföljning varje år. Frågan är om detta är tillräckligt gediget och genomtänkt? I praktiken kan det vara svårt att försöka utveckla "gedigna och väl genomtänkta" träningssessioner. Det är alltså i praktiken svårt att få grepp om vad som i litteraturen är självklart. Sen kommer man också till problematiken som företag 3 lyfter fram: var ska man dra gränsen? Hur mycket är lagom?

“Så en utmaning är att man ska veta var drar man gränsen? Hur mycket är lagom? Hur mäter vi att det här är framgångsrikt?”

- Calle, företag 3

Granskar vi på resultaten av företags 3 arbete inom ISA och återkopplar vi detta till forskningsfrågan så kan vi se att deras förhållningssätt gällande ISA och utbildning är att lägga ribban lagom högt och se till att det upprätthålls och se till att ha bra innehåll.

5.2 Styrelsens roll i informationssäkerheten

Harold & Krause (2010) betonar vikten av att ledningen i ett företag tydligt tar tar ansvar och ger sitt fullaste stöd till informationssäkerhetsarbetet.
Adam uppger att företagets ledningsgrupp är helt med på arbetet med informationssäkerhet och de anser sig inte ha haft problem med att lösgöra resurser till informationssäkerhetsarbetet. Även den globala ledningsgruppen är med på arbetet. Vi ser också en öppen dialog hos Företag 1 för diskussioner med anställda via Jammer, som är som ett socialt nätverk endast för företaget, om informationssäkerhet och sprider information om till exempel phishing mailen och hur många som klickade på den. Här kommer även ledningsgruppen in och lämnar likes och kommentarer på det som skrivs. Detta är i enlighet med litteraturen där Harold & Krause (2010) förklarar att ansvariga bör mäta hur väl säkerhetsmedvetandet inom företaget är för att kunna göra nödvändiga justeringar om problem upptäcks. Företag 1 uppger också att de tror att det blivit vanligare att topp ledningen engagerar sig i informationssäkerhetsarbetet i och med att informationssäkerhet uppmärksammas i medier. Stora dataintrång publiceras flitigt i media. Det blir naturligt att andra bolag i världen uppmärksammar detta, blir oroliga och fokuserar på informationssäkerhet.

Björn från företag 2 förklarade att högsta ledningens stöd och support är A och O, utan den så kommer man inte lyckas. Informationssäkerhet kostar både i pengar och lite engagemang och har man inte högsta VDn eller styrelseledamöter som stöttar detta till 100 procent så kommer det inte bli bra. Problemet ligger i att dessa personer kanske inte alltid förstår risker och vilka hot som finns ute på internet.

Calle (Företag 3)förklarade att styrelsen informeras om vad som står i deras informationssäkerhetspolicy och att de får en briefing från förra året gällande säkerhetsarbetet som gjort. Sen tror Calle generellt sätt att ledningen inte alltid är riktigt medvetna om hur viktigt arbetet är och man underskattar det lite grann innan det har hänt en incident som påverkar verksamheten ordentligt.

Här ser vi att styrelsen tar ett ansvar vilket instämmer med litteraturens rekommendationer. Styrelser har det främsta ansvaret och bör vara medvetna om riskerna och hot. Alla tre företagen instämmer om att det är viktigt att man har ledningens stöd för att it-säkerheten ska fungera.

Adam säkerställer att ledningen har goda kunskaper genom riktade träningsmoduler specifikt framtagna för dem. Han menar att många förstår att det är en viktig fråga men det finns dem som inte inser hur mycket faror som finns ute på internet och hur mycket det är som blockeras.

Björn (Företag 2) är medveten om bristande kompetens i styrelsen och företaget har inga bra kurser eller utbildningar som riktar sig mot styrelsen heller. Styrelseledamöter och ordförande har inte all tid i världen till att ägna sig åt detta, och han diskuterar att det behövas ta fram små intensiva kurser på kanske 3 timmar.

5.3 Sanktion och belöningssystem

I litteraturen nämns det att upprätthållning av organisationens säkerhetspolicy är av största vikt och att det kan göras på flera olika vis (Von Solms 2004). Både D'Arcy (2006) & Bulgurcu (2010) betonar vikten av att sanktionera beteenden som bryter mot informationssäkerhetspolicyn. Däremot nämner Alotaibi et al. (2016) att belöningar som ges till individer som följer reglerna är ett bra sätt att öka efterföljandet av regelverket. Chen et al. (2014) belyser också hur ett belöningssystem kan vara bra för att öka efterföljandet av reglerna.
I resultaten ser vi att Företag 1 förhållningssätt lutar sig mer åt sanktionssystem men man ser också fördelarna med ett belöningssystem. Adam menade att sanktioner och straff är mer applicerbart i större bolag som de själva med 25000 anställda men däremot är belöningar i mindre bolag mer lämpligt.
Björn i Företag 2 riktar sig mer in på belöningssystem. Han tycker att belöningssystem fungerar garanterat och att man inte tror på att straffa bort felaktigt beteende. Finns de inget tydligt uppsåt eller mönster i det felaktiga beteendet mot företagets policy så tänker man att problemet ligger mer i att regelverket och riktlinjerna är otydliga.
Calle från Företag 3 kom med intressanta insikter. Utöver att man i huvudsak tror på belöningssystem så kan man dessutom implementerat lite tävlingsanda i ISA vilket inte nämns i litteraturstudien. Genom att göra ett spel av att “hacka in sig” i kollegors öppna datorer där man kan ta och samla poäng så kan man på ett avslappnat och aktivt sätt öka personalens medvetande inom informationssäkerheten där anställda både kan belönas och “straffas” genom att hamna sist på poängtavlan.

5.4 Shadow security & företagskultur

I litteraturen nämner båda Bulgurcu (2010) & Alotaibi (2016) hur säkerhetskulturen inom ett företag kan påverka informationssäkerheten. De nämner specifikt riskerna med en avvikelsekultur och så kallad shadow security som i sig själv kan späda på avvikelsekulturen. Shadow security definieras av Alotaibi et al. (2016) som en situation där en anställd följer de givna information säkerhetsreglerna på papper men i praktiken så utgör de en säkerhetsrisk.
Det har tidigare varit ett problem för företag 1 men nu har man implementerat mjukvaruapplikation som övervakar exempelvis vilka molntjänster som används samt att alla anställda rekommenderas att logga in via smart card och VPN. Adam ansåg att shadow security är ett organisatorisk problem och inte bara begränsat inom IT. Många av deras incidenter sker på grund av misstag och oavsiktligt. Man måste hitta en balans i regelverket då komplexa regler kan öka risken för misstag.

Björn från företag 2 diskuterade att shadow security är för de allra flesta företagen oundvikligt. Med detta i åtanke kan det vara intressant att försöka göra personalen mer medvetna om shadow security och dess innebörd samt konsekvenser, snarare än blint implementera policyn som försöker avskära shadow security. Björn diskuterar två huvudområden och dessa är bristande förståelse samt mindre optimala alternativ som tar på effektiviteten. Viktigt är alltså att användaren också besitter kunskap inom informationssäkerhet för att policy ska fungera.

Calles (Företag 3) resonemang kring shadow security instämmer med litteraturen. Han betonade även vikten av balans samt att göra det enkelt för personalen att göra rätt. Har man för hårda krav vid säkerheten så kan det hindra personen från att jobba effektivt och när man har duktiga medarbetare så vill de jobba effektivt vilket leder till att man hittar egna lösningar på problem. Man väljer effektivitet före säkerhet. Sedan resonerar Calle kring att shadow security dels också handlar om okunskap. Det är därför viktigt att utbilda och göra personalen medvetna vilket tidigare nämndes hos företag 2.

Granskar vi på resultaten i avvikelsekultur är det genomgripande temat för de flesta bolag är att man i stort har svårt att väva in säkerhetstänk och en säkerhetskultur i den nuvarande arbetskulturen. Den nuvarande arbetskulturen domineras av stress, press och effektivitet. I både företag 1 och 2 har man försökt komma med

säkerhetspolicyn men i och med att det "kolliderar" med den nuvarande kulturen har den mötts av starka reaktioner som bl.a. lett till en mer påtaglig skugg-it. När tekniska lösningar dödar produktiviteten eller krav om komplexa lösenord uppstår så leder det till att användare letar efter genvägar för att effektivisera sitt arbete. Det verkar som att shadow security har blivit en oundviklig och oavsiktlig del av företagskulturen som man har svårt att bli av med.

Även om företag 3 t.ex. lever upp till litteraturens rekommendationer och arbetar med att införliva en säkerhetskultur ser de också allvaret i den rådande arbetskulturen och hur det påverkar säkerheten. Vad vi kan se i resultaten så måste företag göra avvägningar mellan shadow security och produktivitet. Det påtalas ofta om att det är svårt att hitta en balans. ISP ska alltså inte bara upprätthålla informationssäkerheten utan måste i en större utsträckning facilitera produktivitet och arbetsflöde. Utöver detta kan vi även se att företag 3 verkar leva upp till litteraturens rekommendationer med kontinuerligt lärande och uppföljning. Calle nämner dessutom att man arbetar proaktivt, i enlighet med “förutsägbarhet” delen i Shawns (2009) tre former av kunskap.

5.5 Övervakningsprogram och tekniska skydd

Alotaibi (2016) & D'Arcy (2006) framhäver båda att ett sätt att öka efterföljandet av informationssäkerhetspolicyn är att använda sig utav tekniska hjälpmedel såsom övervakningsprogram, och om anställda är medvetna om att de övervakas så minskar risken för avvikelser.
Företag 1 har implementerat olika tekniska hjälpmedel i enlighet med syftena som Alotaibi presenterat. Däremot resonerar företag 1 utöver litteraturen att tekniska skydd måste backas upp av kunskap och medvetenhet hos användaren. I slutändan är det individernas kunskap och medvetenhet som är den begränsande faktorn för säkerheten. Tekniska skydd är i sig värdelösa om användaren inte besitter kunskap och medvetenhet, resonerar företag 1
Företag 2 nämner att det är främst stora företag som arbetar med filter och brandväggar. En tämligen simpel lösning som inte kräver mycket hos slutanvändaren. Men man gör dock inte användarna medvetna om riskerna och hot som föreligger, vilket i sig är fortfarande en brist.
Calle menar att Företag 3 använder sig flitigt av teknologiska lösningar. Utöver dessa tekniska lösningar har de betonat vikten av att man måste lära ut, följa upp och vara konsekvent och beständig med sin

informationssäkerhet för att den ska vara effektivt. Detta i kombination med de tekniska lösningar lägger grunden för en god säkerhet menar företag 3.

5.6 Uppföljning och kunskapskontroll

I företag 1 fall så används simulerade phishing mail som en kontroll över hur många som klickar på mailet. På arbetsplatsen blev phishing mail en snackis och på så vis diskuterades säkerhetsfrågor bland anställda inom företaget. Med detta har företaget lyckats skapa diskussion och medvetande kring säkerhet.
Även resultaten hos företag 2 instämmer med litteraturen om att man måste arbeta med säkerheten kontinuerligt och se det som en viktig del för företagets verksamhet. Företaget arbetar väldigt intressant med detta då de har kontakt med externt bolag som utför penetrationstest samt sårbarhetsanalyser så att företag 2 vet vad som behöver förbättras. De får alltså lite mer konkreta underlag för vad som kan förbättras i deras säkerhetssystem.
Företag 3 har kontinuerlig uppföljning men en intressant fråga är hur kontinuerlig är kontinuerlig. Kan en gång om året räknas som kontinuerlig? Calle påpekade detta och menade att en av utmaningarna är ifall uppföljning en gång om året skulle räcka.

6 Slutsats

Forskningsfrågan med denna studie har varit att undersöka *Vilka säkerhetskriterier och förhållningssätt har säkerhetsansvariga i arbetet med IT säkerhet?*
För att förhindra obehörigt tillträde använder företag 1 och 2 sig av multifaktorautentisering där varje gång en anställd autentiserar sig mot sitt konto så måste hen bekräfta genom login och password och sedan plingar det på telefonen där hen måste godkänna på en app så att det är verkligen rätt person som loggar in i kontot. Det ger ett väldigt bra skydd. Företaget 3 använder sig också av multifaktorautentisering för alla medarbetare. Enligt Calle borde det vara standard. Man har även ett par andra skydd också där man tittar på avvikelser. Företaget har full disk kryptering på laptops. De kan dessutom spärra alla företagsmobiler och följa upp vilka applikationer man har vid behov.

Företag 1 ansåg att för två år sen så var det ett stort fokus på tekniska skydd hos bolag. Men fokuset har skiftat mer mot awareness and education och inte bara teknik. Adam förespråkar en kombination av teknik och utbildning men att anställda är medvetna om risker är viktigast i slutändan. Tekniska skydd spelar ingen roll om en användare är omedveten och utför saker som innebär en risk.

Efter att ha analysera och uppmärksamma hur organisationer arbetar med policys, utbildning och ansvarsbegränsningar ser vi att i arbetet kring informationssäkerhet hänger ansvaret främst på ledningen och att dessa är medvetna om riskerna och hoten som finns. Problemet är som Björn (Företag 2) påpekar är att de inte alltid finns tillgängliga kurser eller utbildningar för ledningen. Resultaten visar att fokus läggs på ISA och utbildning av anställda samt att dessa skall faciliteras av ansvariga på ett effektivt och bra sätt. De ansvariga för ett informationssystem har ett stort ansvar i att förmedla kunskap. Litteraturen redogör för att ISA och träningssessioner för anställda är viktiga verktyg för att motverka dataintrång. Dessa utbildningar skall vara meningsfulla och förmedla värdefull kunskap till slutanvändarna. Träningssessioner skall även anpassas till varje specifik situation och inte vara en generisk lösning för att lyckas. Alla anställda inom organisationen måste vara medvetna och ha samma tankesätt när det gäller informationssäkerhet. Om de inte gör det kommer organisationerna inte att nå de önskade målen i att bibehålla informationssäkerheten och de kommer potentiellt att utgöra risker, eftersom anställda som inte har liknande tankesätt som varandra vilket leder till att man arbetar i olika riktningar mot samma mål. Som det har påpekats tidigare blir informationssäkerheten därför endast lika stark som den svagaste länken.

Litteraturen pekar ut avsaknaden utav träningssessioner eller bristfälliga sådana som ett problem som leder till ökad mängd avvikelser från ISP och mer riskfyllt beteende bland användare. En annan effekt från denna studie visar att när en organisation ökar teknisk säkerhet och policyer, kan anställda tycka det är mer frustrerande eftersom produktiviteten kan drabbas. Vi kan se utifrån alla tre organisationer att komplexa regelverk kan öka risken av misstag samt avvikelser kan ske när anställda på grund av okunskap, tidspress m.fl. tar effektivitet före säkerhet. Ju mer man begränsar sig och säkrar desto mer svårarbetat kan det bli. Det gäller att sätta in information säkerhetsåtgärder som inte upplevs som störande eller begränsande.

Som allt annat i livet gäller det i grund och botten att hitta en balans mellan regelverket och anställdas kunskapsnivå kring informationssäkerhet. Att blint implementera policys räcker inte.
Slutsatsen i studien är att om en organisation ska öka informationssäkerheten måste dessa åtgärder vara mycket motiverade och i kontinuerlig dialog med de anställda. På detta sätt kan organisationerna se till att den ökade säkerheten får den önskade effekten. Tolkningsfrågor som sedan kan uppstå är hur kontinuerligt är kontinuerlig? Kan man räkna att uppföljning en gång om året är tillräckligt? I slutändan bör personalen inom företaget uppnå en viss grad av förståelse för innebörden och konsekvenserna inom informationssäkerhet för att kunna engagera sig och förhålla sig till det.

6.1 Förslag på vidare forskning

Genom denna studie har det identifierats ett antal säkerhets perspektiv som bör inkluderas vid arbetet med informationssäkerhet. Studien är dock avgränsad i form av att intervjuer som genomfördes för insamling av empiri riktade sig i huvudsak till respondenter med chefspositioner som har stor kunskap och förståelse för informationssäkerhet. En annan aspekt som hade varit intressant att undersöka är också hur detta säkerhetstänk ser ut på en lägre operativ nivå där man intervjuar fler anställda. Det kan finnas en brist på överensstämmelse mellan chefers säkerhetstänk och anställdas, där det sistnämnda eventuellt kan ge en mer verklig och bredare bild över medvetenhet kring informationssäkerhet. Ett förslag är därför att vidare forskning bör undersöka denna aspekt för att kunna ta fram mer empiri inom området.

7 Appendix

7.1 Figurförteckning

Tabell 1: Intervjuguide

Intervjufråga	Följdfråga	Motivering	Referens
1. Hur länge har du jobbat här, vad är din arbetsroll, dina dagliga arbetsuppgifter samt ansvarsområden?		Kort presentation om personen och hens arbete.	
2. Har du någon särskild utbildning/kunskap inom IT-säkerhet?		Avstämma kunskapsnivå och tidigare utbildning inom ämnet	
3. Hur väl insatt är du i dagens IT-hot och attacker?	Har du haft erfarenheter av IT-hot på din arbetsplats?	Avstämma kunskapsnivå och uppfattning (perception) kring IT-hot .	Shaw (2009)
4. Om vi åsidosätter vanligt förekommande teknologiska lösningar såsom antivirus och brandvägg, har du erfarenhet av att övervakningsprogram används för att övervaka att anställda följer informationssäkerhetspolicyn?		Tidigare forskning menade att om anställda är under övervakningsprogram så minskar risken för avvikelser. Det är ett sätt att öka efterföljandet av ISP.	Alotaibi (2016) D'Arcy (2006)
5. Hur uppfattar du den interna hoten av verksamheten? Kan ex. anställda utgöra hot mot verksamheten?	Vem anser du ska stå som ansvarig vid interna misstag och ovarsamhet? Vem ska förebygga detta?	Tidigare forskning tyder på att individen i företaget är ofta svagaste länken	Bulgurcu (2010) Safa (2016) Alotaibi (2016)

6.Vilka tankar och reflektioner har du kring ett s.k. sanktions- och belöningssystem? Det vill säga att avvikande beteende bestraffas medan korrekt beteende belönas.	Skulle ett sånt system öka säkerheten inom en organisation? Har du hört begreppet tidigare? Har du praktisk erfarenhet med begreppet?	Tidigare studier betonar vikten av att sanktionera beteenden som bryter mot informationssäkerhetspolicyn .	Al-Omari (2013) Alotaibi (2016) D'Arcy (2006)
7. Har du upplevt Shadow Security (SS) under din karriär inom informationssäkerhet? Kan man ha för mycket säkerhet, och att alltför strikta krav och regler leder till SS? När har man gått för långt med säkerhetspolicyn?		SS innebär att en användare följer säkerhetspolicyn på papper men utgör en säkerhetsrisk i verkligheten. Det kan vara till exempel att en anställd skriver ner sitt komplexa lösenord på en lapp och klistrar fast den på sitt tangentbord istället för att memorera den. Den anställde har således ett komplext lösenord men detta är självfallet en säkerhetsrisk med lappen.	Alotaibi (2016) Bulgurcu (2010)
8. Vilka utmaningar ser du i arbetet med ISA, kunskapsförmedling och utbildning?	Upplever du att utbildning, ISA och kunskapsförmedling får de resurser och den tid som krävs för att det skall genomföras på ett gediget sätt? Hur kan utbildningar och ISA-träning förbättras?	Tidigare forskning har visat att information security awareness (ISA), kunskap och utbildning av anställda är ytterst viktiga.	Al-Omari (2013) Alotaibi (2016) Bulgurcu (2010) D'Arcy (2006) Harold & Krause (2010) Safa (2016)

9. Vilka utmaningar ser du i återkoppling och att kolla upp att användarna tagit åt sig kunskapen från utbildningarna?	Hur undersöker ni säkerhetsmässiga kunskapsnivåer och/eller har du erfarenhet utav att ett företag undersöker det tidigare under din karriär?	Hur undersöker man och analyserar resultaten av organisationens utbildningar?	
10. Vilka andra brister kan du ofta se hos ledningen och hur kan man förbättra säkerhetsstrategin? Behöver ledningen ta mer ansvar?		Forskning nämner att styrelsen måste ta ansvar och spela en mer centraliserad roll när det gäller att bestämma organisations informationssäkerhetsstrategi.	Harold & Krause (2010) Johnston & Warkentin (2010)
11. Känner du att styrelseledamöter har tillräckligt med erfarenhet när det kommer till informationssäkerhet? Tycker du detta ska vara ett krav för alla eller alternativ för vissa?		Vilken kunskapsnivå och kompetens finns i organisationens ledning?	
12. Finns det någon träning/utbildning för befattningshavare angående företagsstyrning, har man rätt ledarskap och struktur i organisationens IT säkerhet?	Känner du att det finns tillräckligt med informationssäkerhets kompetens representerad i styrelsen?		Bulgurcu (2010) Safa (2016) Harold & Krause (2010)

7.2 Intervju 1

Min chef Robert rapporterar till CIO, vilket skulle kunna bli en intressekonflikt. För IT-chefen vill driva igenom sina grejer och bryr sig inte om säkerhet. MEn det fungerar ganska bra, men som sagt, om jag hade fått bestämma så hade jag sett till att IS hade legat utanför IT för det är mer än bara IT. Om man granskar på vår organisation så hade hela den här sockeln kunnat vara IT och dem här är tekniker och skulle kunna ligga under IT. Man kan ta bort denna delen och lägga den under legal. Och vi hade haft en koppling till IT, dem som sköter IT-säkerhet. Så hade jag gjort om jag hade fått börja från början.

Vi har så klart granskat tidigare forskning och ett fåtal nämner ett så kallat sanktions- och belöningssystem för att se till att folk följer den nuvarande policyn. Att avvikande beteende bestraffas och att korrekt beteende belönas. Har du stött på det här tidigare och har du praktiska erfarenheter med det här begreppet?

Hos oss kallas det stick and carrot approach. Ska man piska eller ska man ge morötter? När det gäller mina grejer med education och awareness så är det ganska intressant hur man ska hantera detta för det är ändå så att jag skickar ut ungefär en träningsmodul. Vi har en leverantör som sköter hela vår e-learning gällande all infosec. Så vi har 35 olika kurser i systemet som går runt i en cykel. Det är en continuous process så det är året om, varje år, ska alla anställda gå visst antal träningar. I och med att vi har den snabba intervallen som vi har, jag skickar ut en träning var sjätte vecka ungefär, till 20000. Ska man räkna det i tid, en modul tar 20 minuter, gånger 20000. Det tar ju ändå tid av organisationen för dem hade kunnat göra något annat. Då är frågan ska man tvinga dem att göra dessa träningar eller ska man försöka engagera dem? Företag 1 använder inte stick. Rent teoretiskt skulle jag kunna säga att om ni inte gör träningarna så stänger vi av eran e-post. Företag i bl.a. USA gör så och är väldigt hårda. Vi har inte gjort det utan vi går mer på att det är mandatory, vi skickar ut reminders, går via chefer och så vidare för att få dem att göra det. Vi ligger kanske på 75% completion på våra träningar. Jag tycker ändå det är okej för det är inte hela världen om de missar en modul eftersom det kommer nya hela tiden och det är till jul .Missar man den där så tar man den kanske sen. Jag skickar ut simulerade phishing-kampanjer. Så vi skickar ut phishing mail till 20000 anställda. Där känner jag nog att jag skulle vilja ha mer stick. Är du en användare som alltid klickar på mejlen så utgör du en risk för företag 1. Där är vår kultur att man är lite mesig. Tyvärr.

Skulle man alltså kunna säga att stick hade kunnat varit applicerbart och användbart i vissa situationer eller kan man applicera det...

Jag tänker att det handlar om storlek på bolag. I och med att vi är 20000 anställda och finns i hela världen så mycket att ta in i det med kultur. Det är helt annan kultur i kina än i Europa och massa olika lokala lagar i olika länder man måste ta hänsyn till . Jag tänker att hade man kanske 1000 anställda så hade jag kanske inte valt stick utan carrot. Man engage alla använda i något belöningssystem eller poäng. Varje gång du tar en träning så får du x poäng som du kanske kan använda det i en webbshop eller någonting. Jag har undersökt såna lösningar också. det är alltid ett problem när man är så många och det är kultur. Så har vi då blue collars. Alla människor som jobbar i fabriker. det är en annan målgrupp och de utgör 7 tusen. De har inte en egen dator och jobbar i produktion och dem ska vara där för annars förlorar vi produktionstid vilket är förlust av pengar i slutändan. Det är också svårt. Alla såna målgrupper måste man väga in hela tiden. Det är alltid svårt när vi är 25 tusen som vi är att hitta något globalt som fungerar för alla. Nu har jag fokuserat mycket på white collars. dem är lättare.

Finns det en one size fits all lösning när det kommer till informationssäkerhet? Ett system som kan appliceras på hela organisationen globalt.

Den leverantören vi använder är en amerikansk leverantör. Deras plattform är bara för infosec. Det dem gör handlar bara om infosec. Alla deras träningar och phishing. Phishing kommer från samma leverantör. Så det är integrerat. Om du är en användare som klickar på 3 mail som jag skickar ut 3 månader i rad så kommer du automatiskt bli tilldelad en träning om phishing. Så det hänger ihopa. Det är lite behavior-anpassad.

Det låter lite mjukare, inte fullt ut en piska. Är det ett mellanting?

Det är ändå så att om du klickar 3 gånger när du blir “assigned” för phishing träningen så blir din chef notified vilket kanske inte är så roligt. Skulle du trycka på 4 mail i fyra månade i rad så blir det en manager conversation, alltså ett fysiskt möte med din chef om det. Sen tar min process slut. Sen blir det ett HR-ärende.

Jag kan bara driva det till en viss gräns i min roll som informationssäkerhets människa. Sen blir det en chefsfråga och ett HR-ärende. Så man kan inte dra det hur långt som helst som användare.

Har du upplevt shadow security under din karriär inom informationssäkerhet? Kan man ha för mycket säkerhet, och att alltför strikta krav och regler leder till falsk känsla av säkerhet? När har man gått för långt med säkerhetspolicyn?

Det här med shadow IT är ett problem. Så är det. Just nu tror jag vi har kommit en liten bit. För ett år sen var det ett problem. Jag tänker framförallt på whatsapp och olika chattappar som business använde i arbetet som inte var godkända. Det var inte godkända applikationer från Företag 1 sida. Eftersom vi inte hade något att erbjuda till våra användare så är det rätt naturligt att om jag har en arbetsuppgift att lösa men inget systemstöd för detta så laddar jag ju ner whatsapp så jag kan prata med den leverantören där för att lösa mitt problem. Jag förstod exakt hur användaren tänker men det är ju ändå en risk utifrån oss. Nu har vi fått på plats olika applikationer som löser de problemen som vi hade. Vi har OneDrive, OneNote, nya microsoft-appar som är godkända och säkrade. Även om det är molntjänster så är det uppstyrt. Men så klart finns andra system som folk använder som vi inte har koll på. Sen har vi också en lösning som vi har heter CrowdStrike som håller koll på vilka molntjänster som Företag 1 använder. Där kan vi se, helt plötsligt dyker det upp saker som vi inte godkänt och då kan vi ta tag i det. Så vi har ändå någon typ av koll på vilka, framförallt molntjänster, som används. Vi har smartcard. Vi har ett 15-tecken password för att komma in i datorn. Till vårt Windows Konto. Vilket är ganska hårda krav i den och så måste vi byta den varje 90 dagar. Det är ett krav vi har från vårt moderbolag. Vissa krav kommer uppifrån moderbolaget och då måste bolagen i gruppen följa det. Det där med lösenord är ett sånt. Vi från informationssäkerhet vill inte till exempel byta det regelbundet för det spelar ingen roll. Det är längden som är viktig för att minimera risk och då ska man byta det här med 15 tecken varje 90:e dag då finns en risk att man börjar glömma och då blir det nästan en större risk än de här 15 tecken från början. Vi måste införa vissa andra grejer för att kunna ta bort 90-dagars kravet. Vi har inte gjort det än men vi kommer ta bort det. Smartcard använder vi till exempel loggar in hemifrån med VPN. Det är tvåfaktorsautentisering. Det är kortet och en pin kod. Jag loggar alltid in med det när jag sitter på kontoret. Då är pin koden inte 15 tecken utan 6. Det blir inte så jobbigt att komma ihåg. Vi rekommenderar alla att alltid logga in med smartcard för då finns det mindre risk för lappar.

Skulle man kunna säga att det här med shadow IT och shadow security är ett organisatoriskt problem och inte bara begränsat till IT-säkerhet och IT-security?

Ja, det tror jag nog. Vi har så otroligt många policy, procedure och guidelines globalt inom alla område. Om man tittar utifrån användarens perspektiv; om du ska hålla koll på 250 procedures om miljö, kvalitet, hälsa,informationssäkerhet, det är typ omöjligt att hålla koll på alla regler du ska följa. Såklart blir det att folk ibland missar. De kanske gör saker oavsiktligt. Som kan leda till en.. .det är samma inom informationssäkerhet. Jag skulle nog säga att i alla fall 7 av 10 incidenter är oavsiktligt. Användaren gör saker av misstag eller för att de inte vet och det leder till en incident.

Skulle man då kunna säga att om man då har väldigt stora och komplexa regelverk så ökar risken för att man av misstag missar en regel eller så?

Ja, det skulle jag nog hålla med om. Det måste ju vara en balans. Men samtidigt måste man ha det dokumenterat för när det väl händer någonting, så är en procedure mandatory för alla anställda. Så du kan aldrig säga att jag visste inte. Sorry, policy och procedure är mandatory hos Företag 1 så det måste alla anställda följa. Guideline är mer av en riktlinje och är lite otydligt men policy och procedure måste alla anställda följa.

I annan forskning så har vi sett att företagskultur, säkerhetskultur eller brist på den , har visat sig påverka infosec inom en organisation. Så frågan är vilka utmaningar stöter du på i din roll som driftansvarig med organisationskultur? Hur kan man motarbeta om det finns en så kallad avvikelsekultur inom företaget? Vad finns för utmaningar med att motarbeta en avvikelsekultur?

Kultur och beteende är ju det jag försöker jobba med mest. För att det är ju olika i olika länder. När det gäller education and awareness så är det ändå så att vi försöker anpassa... nu är min roll global så då ska jag ju dra ut grejer till alla. Men sen med hjälp av infosec-officers så kanske vi måste göra något lokalt i brasilien säger vi. Då tar jag ju hjälp av den officeren som är i det klustret för han känner till hur kulturen är, vad som

fungerar och inte fungerar. Men det är alltid så att man måste anpassa vissa grejer beroende på var man ska leverera saker och ting. Hela mitt awareness-program handlar om att förändra beteende så vi får en kultur där säkerhet är inbyggt i det dagliga. Det är hela målet med mitt awareness-program. Allt från när dem får in ett mail som ser konstigt ut i min inbox så tänker man direkt att man ska kolla det här och det här innan man trycker på länken . Det är sånna småbeteenden som vi försöker få in i organisationen. Mitt awareness program började 2017 så det är ganska nytt awareness program. Det finns bolag som kört i typ 7 till 8 år så vi är fortfarande i början så att säga. Vi är inte riktigt mogna än. men vi har absolut förändrat lite beteende och kultur. Men det är en lång resa kvar.

Skulle man kunna säga att om anställda anser att ett väldigt komplext regelverk hindrar deras produktivitet så kan avvikelsekultur växa fram ur den situationen. Som accepteras av till exempel skiftledare och mellanchefer som granskar mellan fingrarna så att produktiviteten förblir som den är.

Vi har haft lite problem med tekniska lösningar. Granskar man utifrån användarperspektiv så finns inget värre än när det trycks ut tekniska säkerhetslösningar som dödar lite produktivitet eller gör datorn lite långsammare. Som jag sa tidigare om moderbolagets password så fanns ett antal andra krav som vi måste implementera och det gynnar inte min roll när vi måste installera en agent på datorn som slöar ner hela maskinen, 15 tecken lösenord, klassificering på alla dokument, e-post, allt. Såna grejer kan få en användare att bli negativ mot security och det är egentligen inte vår organisation som kommer med dem förslagen, även om vissa av sakerna håller vi med om. Såsom klassificering som är grunden. Den här med 15 tecken var inget positivt för oss. Det kan jag säga. Sånna grejer kan leda till att användare tar genvägar för de blir arga på oss från säkerheten fast att det inte var oss från säkerheten... allt kommer inte från oss utan vi blir också tvingande att leverera vissa saker.

Vi var lite inne på det här innan en fråga handlar om övervakningsprogram för att se till att folk håller sig till policyn. Du nämnde det här med övervakningsprogram så det inte kommer in någon konstig cloudtjänst.

Dels har vi Data Loss Prevention på alla klienter, den granskar så att du inte råkar skicka ut någon konfidentiell information. Den är rätt tung som slöar ner saker och ting men det är också ett krav som vi hade på oss. Sen har vi cloud strikes som granskar sårbarhet.

Skulle man kunna säga att företag fokuserar allt för mycket på de tekniska lösningar för säkerhet?

Ja fram tills för två år sedan. Det är bara att kolla här till exempel, innan när vi bara var fyra för tre år sedan då jobbade jag här som information security-specialist i Sverige. Då jobbade jag för ISA i sverige och sen fanns det här globala teamet men de jobbade inget med ISA så jag hoppade över för tre år sedan för att jobba med education and awareness men sen har det exploderat, förr var det mycket teknik men inte nu. Som Igor, data privacy, det är inte heller bara teknik det är legal, HR och så granskar man på oss som är där uppe så är Grant inte teknisk, igor, jag inte, richard inte, bernard. Så det är ändå ett antal i ledningen som inte jobbar med teknik utan mer med organisation.

Om vi kallar de hårda metoderna för det tekniska och de mjuka metoder för utbildning och awareness, väger någon av dessa tyngre eller lika mycket och likvärdiga i arbetet för informationssäkerhet.

Nej det måste vara en kombination, man måste ha både och. men i slutändan så måste vi se till att alla anställda är aware och medvetna om alla risker där de vet hur de ska reagera i olika scenarier. Ja teknik måste vi ha men ibland så spelar det ingen roll när en användare är omedveten och utför saker som innebär en risk för oss.

Forskning har visat att ISA, kunskap och utbildning av anställda är av ytterst vikt. Och vad ser du för utmaningar i arbetet med ISA, kunskapsförmedlingen och utbildningen av anställda? Upplever du att det får de resurser och tid som det krävs för att genomföras?

Just nu är vi för få resurser. För jag är själv men jag kommer inte vara det. För jag kommer behöva hjälp. Mitt problem är: nu har jag implementerat alla de här cyklarna, phishing mail varje månad, träning var sjätte

månad och dessa ska underhållas. Det ska vara som ett hjul som snurrar samtidigt ska jag vara den som ska titta fem år framåt, och titta på strategi, hur ska vi förbättra, vad behöver vi lägga till för utbildningar? Just nu är jag både visionären och den som ska förvalta så jag kommer behöva någon som sköter den här förvaltningen. Mitt största problem är tid, jag skulle säga att min egen tid räcker inte till. De jag skickar ut per år tar 1,5h per anställd per år, så det är svårt för en anställd och skylla på att de inte hinner. Vi har fått det godkänt att allt jag skickar ut är mandatory, du ska liksom göra det. Räknar man då 1,5h per år så räcker det med att en anställd tar lunch en halv timme två gånger per år så hinner hen med modulerna.

Vi har tittat på tidigare forskning och de kom fram till att implementering graden av de är organisatoriska och utbildnings metoderna är den lägsta när det kommer till informationssäkerhet. Skulle man kunna säga att man missar det är med ISA och utbildning och istället fokuserar allt för mycket på antivirus och brandväggar.

Det stämde för 3 år sedan, men här hos oss stämmer det inte riktigt nu.

Man kan säga att det har skiftat lite nu?

Jag tror att det är generellt, jag var på en utbildning i London i höstat just om hur man bygger upp och förvaltar informationssäkerhetsprogram. det var 15 andra bolag i olika storlekar. Allt från 1000 till 100 000 anställda men alla dem jobbar kontinuerligt med awareness program. För fem år sedan var det mindre vanligt men nu har alla större bolag någon typ av awareness program igång, sen är man på olika platser på vägen mot samma mål.

Så man kan säga att många företag har förstått vikten av den här mjuka biten så att säga. Vilka utmaningar ser du i återkopplingen med användarna att dem har tagit åt sig kunskapen som förmedlas, undersöker ni om man faktiskt har lärt sig från detta som t.ex phishing mailen?

Det ser vi i, där följer jag upp och ser hur många procent som klickar på detta och sen kan jag följa detta under året. Så där kan jag absolut se. Sen när det gäller det andra e learning ochd e olika dem modulerna som

vi skickar ut kan handla om travel security, phishing, social media det är olika områden inom infosec och när jag började awareness program så körde jag ut en assessment som en baseline så då fick alla anställda 22 frågor om de här olika topics inom infosec. Så jag hade ett resultat innan jag började hela resan så nu efter två år körde jag ut dem 22 frågorna igen så kunde jag jämföra men nu har jag inte fått resultatet ännu så jag hoppas att det blir bra. Om allting står rätt till då så kommer jag se områden har sjunkit och då kan man så att det vi gjort har gett någonting. Sen märker man också för 3 år sedan så prata ingen i korridorerna om infosec träningar och phishing och sådant. Så jag märker att det, speciellt om phishing mailen, blir en diskussion varje månad. Även när det går bra för oss phishing kampanj så blir det ändå en snackis exempelvis att "åh det var alldeles för lätt" och det uppstår diskussioner vilket är lika mycket värt som om vi skickade ut något jättesvårt som alla faller för.

Är det viktigt att skapa sådant enormt engagemang för att se till att säkerhet genomsyrar det dagliga arbetet?

De här diskussionerna som uppstår tror jag är väldigt viktiga, bara att folk pratar om det. Det är så att de här negativa grejerna om vi tar exempelvis det här med password, så måste det komma bra diskussioner som kommer upp i kafferummet och inte bara " åh de här lösenorden måste vara 15 tecken, vilket skit" osv.. Så jag tror de här phishing mailen har hjälpt till så att de blir något roligt även om de ibland åker dit.

Du nämnde innan att du kände resurserna inte var tillgängliga, vi vill gärna veta om du tycker att styrelsen tar sitt ansvar eller behöver man spela en mer aktiv roll när det gäller bestämmandet av infosec strategi.

Vår ledningsgrupp är helt med på tåget när det gäller infosec, annars hade vi inte varit 5 stycken. Vi har inte haft problem med att tillsätta fler resurser i vårt team, de här med att jag behöver mer handlar om att jag ska säga till Robert min chef att jag göra det här, det här och jag hinner inte med. Det är mer upp till mig. När det gäller vår global leadership team så är de helt med på tåget. Vet ni vad en jammer är? Microsoft har ju de här OneDrive, word excel powerpoint, jammer är liksom facebook fast för företag så den är perfekt för mig att använda eftersom kommunikation är en stor del i min roll, att kommunicera ut vad som sker och allt som vi

håller på med inom infosec. Jammer har blivit en jättebra grej för där får alla skriva vad som helst om intern information och där når man ut till alla i företaget, där delar jag ut information om ex. phishing kampanjerna där jag säger “nu skickade vi ut de och de, så här många klickade, tänk på det här” osv, bara för att koppla tillbaka till vår ledningsgrupp, där har vi ansvarig för business finance and transformation som är inne där och han “like’ar” och skriver om saker som vi postar, de är med i allting vi gör och så fort han skriver någonting så ser ju anställda de och då blir det mycket mer intressant för alla då det är ändå en typ av hierarki. Så det är jättebra att även de högst upp är engagerade.

Om vi tänker bolag generellt, är det vanligare nu att topp ledningen engagerar sig mer i infosec än det var tidigare.

Ja det är klart. Med tanke på allt som har hänt och hur det uppmärksammas i media om cyber security.- Attacker sker hela tiden attacker ungefär varje vecka som fallet med Maersk, de här stora container företaget som räddades med nöd och näppe för att de hade en AD server som var offline någonstans random i världen, just när de blev attackerade, allt annat blev ju smittade av ransomware. Hade de inte haft den servern som var offline så hade inte kunnat bygga upp sitt nätverk igen och då hade det varit över för de bolaget. Så när det sker sådana händelser så är det naturligt att andra bolag runt om ser och hör, och då blir det väldigt aktuellt med cyber security. Så det är klart att företag blir oroliga och fokuserar över sin cyber security.

Finns det någon träning eller utbildning för befattningshavare angående företagsstyrning och har man rätt kunskap om struktur och IT säkerhet? Har man tillräckligt med kompetens i ledningsgruppen?

De får targeted training från mig, det finns ca 1000 seniora cheferna, de får speciella moduler som vi skickar ut till dem. Nu när vi inför ny klassificering till exempel, hur man ska skicka krypterade mejl och filer, hur man ska samarbeta med externa parter osv. De får ju speciell träning och är liksom en VIP grupp som får lite mer än alla andra. De jobbar med highly confidential information. Min roll är väldigt rolig eftersom i alla projekt så finns det alltid education och awareness någonstans där och jag är nästan med i allting som sker.

7.3 Intervju 2

Vad har du för tankar och erfarenhet med sanktions och belöningssystem. Har du hört det tidigare, skulle ett sådant system öka informationssäkerheten inom ett företag?

Belöningssystemet kommer garanterat att fungera. Att straffa bort felaktigt beteende, det tror jag inte på. Inte i denna typen av organisation. Organisationen består av högutbildade ingenjörer, systemvetare och civilingenjörer m fl. Det är smarta och intelligenta människor man kan ju alltid se ett mönster när det sker ett brott mot våra policyn och det inget ont uppsåt bakom utan då är det otydligt regelverk eller riktlinjer, eller pressad situation där man kanske gör avsteg gällande policyn för att rädda en kund, affär eller annan relation. Därför tror vi aldrig på att straffa men däremot så kan vi belöna, den delen funkar bra.

Företag 2 tycker att belöningssystem fungerar garanterat. Man tror inte på att straffa bort felaktigt beteende. Organisationen består av högutbildade ingenjörer, systemvetare och civilingenjörer m fl. Det är smarta och intelligenta människor, finns det inget tydligt mönster vid brott mot organisationens policyn och det inget ont uppsåt bakom utan då är det otydligt regelverk eller riktlinjer, eller pressad situation där man kanske gör avsteg gällande policyn för att rädda en kund, affär eller annan relation.

Hade man kunnat använda straff i andra industrier som använder sig mycket av IT men som kanske inte har så mycket högskoleutbildade anställda? Jag tänker mer produktionsföretag och sådant.

Straff funkar ju nästan aldrig i det här sammanhanget är det nästan alltid kontraproduktivt utan det bygger på förtroende på båda sidor och förståelse om varför det är viktigt med informationssäkerhet. Det är klart att i vissa sammanhang är det extremt viktigt, till exempel jobbar vi en del med försvarsmakten och försvarets materielverk och där är det ultra viktigt att man inte bryter mot någon policy för där är det ju direkt hot mot rikets säkerhet. Där är det lite skillnad, där kanske man kan jobba med straff men sen beror det på vad det är för straff, man kanske inte ska få jobba med de frågorna eller man blir av med jobbet.

Det finns så klart olika men låt säga att det finns hårdare straff, att bli av med jobbet. Men vi har haft andra intervjuer och någon annan har sagt att straff kan vara ett samtal med chefen.

Ja så skulle man kunna göra men sen beror det på vad man menar med straff, för mig låter straff som väldigt hård mot åtgärd, de med att man måste gå på en informationssäkerhetskurs, eller gå på möte med chefen, det är heller inget straff, inte så som jag värderar och lägger inte i det ordet straff i alla fall.

Har du stött på det här med shadow security och när kan man ha gått för långt med säkerhetspolicyn att det skadar en själv?

Ja det där är en intressant fråga, när det gäller då lösenord som exempel så finns det två olika skolor. Den ena säger att man ska ha så långa och komplexa lösenord och sedan byta de så ofta som möjligt. Och alla som jobbar med människor vet ju att så funkar det inte. Vi är inte konstruerade att komma ihåg den typen av lösenord och hela tiden byta. Och sen finns det den andra skolan som menar att det är bättre att ha ett långt komplext lösenord men som du kanske inte byter hela tiden. Du har det kanske i ett år. Jag står kanske nånstans mittemellan med lite mer vikt på det senare för det här med komplexa lösenord och tvinga anställda att kontinuerligt byta var 90 e dag som ofta är standard i branschen, det får ofta till följd att folk skriver det på post it lappar och lägger det under tangentbordet, klassiskt.

Om man tänker organisation och generellt då, är det vanligt förekommande med shadow security ifall policyn är så enormt komplex.

Det största problemet med skugg-IT som jag brukar kalla det för är man använder molntjänster som ligger utanför företaget kontroll. Det vill säga att företaget har exempelvis sagt att vi ska använda oneDrive, Sharepoint eller annat och ändå finns det enheter ute i linjen som köper en Dropbox och gör på egen hand eftersom man tycker den är enklare, bättre, smidigare, snyggare. Och företaget har ingen kontroll över den information eller datan som ligger på den Dropboxen och det är ju skugg-IT och jag skulle säga det är mer regel än undantag att det finns skugg-IT. Finns vissa företag som har informationssäkerhet så djupt förankrat i kulturen, i väggarna så där förekommer det inte. Men i de allra flesta företag så finns skugg IT enligt min bedömning.

Det är stor utmaning att jobba emot skugg-IT?

Ja det är nog den större utmaningen man har.

Företagskultur, säkerhetskultur eller bristen av en sådan kultur har visats påverkat informationssäkerheten inom ett företag. Frågan är då vilka utmaningar stöter du på som driftansvarig med olika organisationers kulturer, hur kan man motverka en avvikelse kultur om sådan existerar? Vilka utmaningar finns när man ska införliva säkerhetstänk i organisationskulturen som helhet.

Det finns två huvudområden här det första är bristande förståelse, de förstår inte hotbilden och varför är det viktigt med säkerhetstänk. De andra är att alternativen kanske inte är helt optimala, då skapar vi företaget skugg-IT och dåligt säkerhetskultur, ska man ställa krav, ha ordning och reda, peka på regelverk, säkerhetspolicyn och så vidare, så ska det man pekar på först och främst fungera. Ofta är det så att man pekar på någonting som inte funkar så jättebra och då är människan så kreativ och tänker på andra utomstående lösningar: “ja men här är ju dropbox/Slack” eller vad det nu kan vara som man tycker fungerar bättre och man använder då det. Så det är en kombination av bristande insikt och att alternativen som man har pekat på oftast inte är så bra.

Skulle man då kunna säga att om anställda anser att de tekniska hjälpmedel som använd är otillräckliga, det är då avvikelsekulturen uppstår. Kan man säga att mellancheferna hänger med på det bara för att inte hindra produktiviteten, ser mellan fingrarna lite.

Ja precis. Därför är det himla viktigt att när man inför en säkerhetskultur så måste man ha alla linjecheferna med sig. Sen finns det alltid en liten svans, det finns alltid early adopters som förstår grejen och vill gå ute i fronten för informationssäkerhetskulturen sen finns det ju dem i den andra ändan som vill nästan motarbeta det.

Om vi åsidosätter vanligt förekommande tekniska lösningar som antivirus och brandväggar. Har du erfarenhet av att övervakningsprogram används för att se över anställda så att de följer säkerhetspolicyn?

Det förekommer mest på de stora företagen, man granskar brandväggsloggar, surf loggar var folk har surfat lite så sporadiskt, att övervaka personalen minutiöst det kostar enorma pengar och det är inget företag som gör det, utan vad man gör är att man har lite intelligenta filters och om någon går in i vapen sidor, porrsidor eller drog sidor på internet så finns det logik i brandväggarna som klipper till och säger att det är en otillåten sajt. Sen finns det IDS, intrusion detection system och IPS, intrusion prevention system men de är mer logik i nätverken som detekterar externa intrång och kanske inte så mycket internt, om var man surfar och så vidare.

I tidigare intervju så nämnde de att de övervakade vilka cloudtjänster som anställda använder och frågan är då kan vetskapen av att ett sådant här system finns, avskräcka? Vetskapen av att man blir upptäckt om man t.ex. använder dropbox när det inte är tillåtet.

Det kan det göra absolut, det viktigaste med informationssäkerhet är att det är ett återkommande arbete där företag måste komma in i ett årshjul där man jobbar hela tiden med att definiera informationssäkerhetsmål och man måste prata om säkerheten hela tiden i företaget. Det kan inte bara vara en fråga som lever sitt eget liv vid sidan om. Det ska upp på agendan och man måste lyfta upp det under viktiga möten.

Kan man då säga att informationssäkerheten ska genomsyra det mesta som sker inom organisationen?

Ja så är det ju, men sen beror det på vad det är för företag också. Vi har valt att certifiera vårt ledningssystem mot ISO 27000-standarden och därför blir det naturligt för oss att informationssäkerheten genomsyrar företaget men sen finns det andra företag där det kanske inte är lika viktigt. När det gäller informationssäkerheten så måste det ta en avstamp i riskbedömning, man måste göra en riskanalys och utifrån den definiera sina infosec mål och var man ska lägga ribban.

Tidigare forskning har visat att infosec awareness kunskap, utbildning av anställda är ytterst viktiga. Vilka utmaningar ser du i arbetet med ISA, kunskapsförmedling och utbildning. Upplever du att infosec utbildning och ISA får de resurser som behöver för att de ska kunna genomföras på ett korrekt vis?

Det finns alltid konfliktlinjer med att skicka folk på infosec utbildning och de står alltid i konflikt med att produktiviteten minskar. Tar du exempelvis 100 anställda ut från deras dagliga verksamhet och säger nu ska ni gå en halv dag på utbildning, ja då minskar produktiviteten. Här inom Företag 2 ska vi ta och lyfta bort debiterande konsulter som sitter ute hos Volvo, Eriksson, eller Ikea för att göra en informationssäkerhetsutbildning så är det en prislapp på den. Det kostar pengar någonstans. Och då får man göra en värdering och bedömning och vi inom Företag 2 har valt att satsa på informationssäkerhet så vi avsätter pengar för att göra detta men det är inte alla företag som tycker det är värt det.

Vilka utmaningar ser du i återkoppling av att användarna har tagit åt sig kunskap från dessa utbildningar? Undersöker ni säkerhetsmässiga kunskapsnivåer hos anställda och har du någon erfarenhet av att företag undersöker anställda.

Ja vi håller på med ett projekt just nu som går ut på att mäta mognadsgraden när det gäller informationssäkerhet, det är ett projekt vi drog igång för en månad sen. Det är fortfarande i planeringsstadiet och vi har avsikt att börja mäta under hösten. Och då får man låta det gå några månader eller ett år och sedan göra en ny mätning där man jämför utvecklingen och ser ifall det skiljer sig. Det är ett svårt område med att mäta kunskapsnivå, man kan klart ha regelrätta prov men det är också svårt att göra såna prov.

Vad anser du om simulerade intrång tex. phishing mail, eller på något sätt simulera vanligt förekommande intrång för att se om en anställd nappar?

Det kan man säkert göra, men här gör vi så kallade sårbarhetsanalyser där vi kontakter ett externt bolag så får de ett IP range eller adress till våra nätverk och så säger vi ni har en dag på er att hacka oss. Det ena är penetrationstest och det andra är sårbarhetsanalyser där de säger till oss om våra sårbarheter och vad vi måste

förbättra. Om vi går tillbaka till den frågan där om att skicka fiktiva phishingmejl enbart i syfte för att se hur många som eventuellt klickar på länkar skulle kunna vara ett sätt att få en lite grov uppfattning om hur mognadsgraden är i bolaget.

Tidigare litteratur nämner att styrelsen måste ett mer aktivt ansvar och ta en mer aktiv roll för att bestämma ett bolags informationsstrategi. Kan det vara så att styrelser generellt då i olika bolag måste ta mer ansvar och vilka andra brister ser du där man kan förbättra säkerhetsstrategin hos ett bolag?

Ledningens stöd kallar jag det för men det är samma sak som ledningens ansvar. Stödet är A och O för att informationssäkerhet ska fungera i ett bolag oavsett om det är ett tremanna företag eller om man har tusen anställda. Högsta ledningens stöd och support är helt avgörande utan den så kommer man inte lyckas. Det är så pass viktigt. Informationssäkerhet kostar både i pengar och lite engagemang och har man inte högsta VDn eller styrelseledamöter som stöttar detta till 100 procent så kommer det inte bli bra. Ofta handlar det om att dessa personer kanske inte alltid förstår risker och vilka hot som finns ute på internet. Man tänker amen de har funkat bra hittills och bolag i Företag 2 storlek på ungefär 3000 anställda, får runt 50 000 phishing mejl om dagen. Det mesta klipps ju och stoppas av filter men 98 procent är automatgenererat där det är bots som bara trycker ut mejlen genom internet hela tiden. Vi har kanske tusentals hackings försök på vår yttre brandvägg där de flesta är automatgenererade men sen finns det vissa kriminella nätverk som sitter och letar efter sårbarheter i brandväggarna kanske från uzbekistan, ukraina, nordkorea, kina, iran, usa och mexiko. Whatever. Vi har fått hackningsförsök från Holland också så det kan komma varsomhelst ifrån. Och den här hotbilden tror jag inte VD och ledningar i bolag är så medvetna om alltid om vilket tryckt det är på våra bolag utifrån. Det är sanslöst tryckt.

Vi vill gå in mer på det här om du känner att styrelseledamöter har tillräckligt med erfarenhet och kunskap när det kommer till IT säkerhet och kanske det ska vara ett krav eller alternativ för vissa styrelseledamöter att utbilda sig mer inom säkerheten.

Ja jag tycker det. Vissa fattar ju att det här är en viktig fråga men det finns dem som inte inser hur mycket skit som finns ute på internet och hur mycket det är som vi blockar. Vi blockar 99.9 procent av allting och det är ju en bra siffra men omfattningen är så himla stor att det trillar alltid igenom någonting.

De som inte är kanske så insatta bland styrelsen, tycker du det är en stor utmaning att förmedla kunskapen och se till att de tar åt sig och inser att detta är ett problem som kräver mycket resurser och tid.

Ja det är ju en utmaning och det är dem själva som är ansvariga ytterst för bolag och för infosec, det är VD:n som är ansvarig och han har i sin tur sitt ansvar att informera styrelsen om han behöver mer pengar för IT säkerhet.

Vi gick in lite på detta men träning och utbildning för befattningshavare eller VD. Finns det någon slags träning eller utbildning som kan appliceras där så de får mer kunskap. Känner du att de finns tillräckligt med kompetens i styrelsen generellt?

Nej det gör det inte och det finns inga bra kurser eller utbildningar heller. Styrelseledamöter och ordförande har inte all tid i världen till att ägna sig åt detta, därför skulle det behövas ta fram små intensiva kurser på kanske 3 timmar, det räcker där. Bara så man får lite insikt om hur hotbilden ser ut och vad som händer ute på internet, men de typen av utbildning finns det inte mycket om. Finns ju långa tekniska men de riktar sig inte till dem personerna. Informationssäkerhet kommer bara tas upp mer och mer med tiden. Det finns sårbarheter överallt och till och med en hiss har programvara som kan bli manipulerat hur enkelt som helst. Det kanske inte finns mycket att hämta där men det finns liksom överallt sårbarheter och det finns de ute på internet som är beredda på att störa och förstöra för skojs skull men det kommer ju mer och mer nu att det finns ekonomiska incitament för att hålla på med denna typen av brottslighet. Om man drabbas av det är det väldigt svårt att ställa dem tills vars, ofta går den genom proxyservrar i länder som inte har något fungerande rättssystem eller som kanske inte sparar loggar.

Kan man säga att folk generellt tar för lättsamt på det här med infosec? Att man inte inser allvaret i det?

Ja det skulle jag säga. Men informationssäkerhet är väldigt komplext, det utvecklas ständigt och man måste anpassa skyddet efter hotbilden och kraven och man kan ju också skydda sig till tänderna men då blir det väldigt svårt för det är som ett dragspel. Ju mer man begränsar sig och säkrar desto mer svårarbetat kan det bli. Det gäller att sätta in information säkerhetsåtgärder som inte upplevs som störande eller begränsande. Ett exempel på de är att vi håller på att införa multifaktorautentisering här inom Företag 2, där varje gång du autentiserar dig mot ditt konto så måste du bekräfta genom login och password och sedan plingar det på telefonen där du måste godkänna på en app så att det är verkligen du som loggar in i kontot. Det ger ett väldigt bra skydd, då vet man ju att om man autentiserat sig genom telefonen så är det du som är du. Då minskar kravet på de här långa komplexa lösenord. Detta är exempel på sådan grej som inte är speciellt störande för användarna jämför med att få byta komplexa lösenord var 90 e dag.

Det ska alltså hela tiden en balans då, lagom som vi säger på svenska.

Precis lagom är ju bäst samt att man ska ha en medvetenhet hos användarna, en insikt om hur mycket skit och vilket tryck det är utifrån där vi hela tiden blir bombarderade i brandväggs attacker, phishingmail och ransomware, allt det dära och det är andra typer av attacker också, social engineering till exempel där man fejkar avsändare adressen och ger sig ut för att vara VD som skickar mejl till finanschefen eller ekonomichefen i bolaget: “Hej jag är ute på resa jag skulle behöva 25 000 euro för att göra en affär, kan du föra över pengarna?” och så är det ett fejkat mejl och den typen av social engineering är ganska vanliga. Vi då som jobbar med informationssäkerhet vi fattar ju direkt när det är något lurt men skickar man såna attacker till ett bolag som Företag 2 på 3000 anställda så är det alltid någon som inte tänker sig för och utgör en säkerhetsrisk.

7.4 Intervju 3

Skulle sanktions- och belöningssystem kunna öka informationssäkerheten inom ett bolag. Har du stött på detta fenomenet tidigare i din karriär inom informationssäkerhet?

Det låter lite som barnuppfostran. Carrot eller stick. Det är en modell jag tror mycket på för det är nog det bästa sättet att få ett mer positive reinforcement, att man uppmanar folk att göra rätt och det ska vara enkelt att göra rätt istället för att man tar genvägar och gör fel helt enkelt. Där fel kan vara lite subjektivt ibland. Ett exempel som jag inte gjort men läst om och som jag tycker var väldigt bra är det här med att låsa sin dator när man lämnar skrivbordet vilket inte alla är så jättebra på. Istället för att kollegan kanske går in och skriver något tråkigt på din facebooksida eller någonting annat som får dig att förstå att det är en bra grej att göra. Vi använder ett chattsystem. Det finns många olika men vi använder Microsoft Teams i företaget. Så för gruppdiskussioner. Det var någon någonstans som gjort en bot där man kan gå in i en olåst dator, öppna Teams-klienten och ge sig själv poäng. Det vill säga att man snor poäng från den vars dator man tar över. Sen trackar man och har en leaderboard där man ser vem har tjänat mest poäng på att jaga öppna datorer den här månaden till exempel. Och sen om man vill koppla ett pris till det eller vad man vill göra. Men det tycker jag är ett jättebra exempel. Det är ett ganska konkret och ganska billigt sätt att öka medvetenheten och få med lite gamification.

Har rena straff en plats i arbetet med informationssäkerhet? Det behöver inte vara att man blir sparkad, men något kännbart såsom ett möte med chefen eller att bli avstängd från konton. Har det en plats i arbetet eller är det för mycket så att säga?

Menar du rent praktiskt eller vad jag anser vara rätt eller fel?

Bara vad du utifrån din erfarenhet inom området tycker om detta och om det har en plats i informationssäkerhetsarbetet inom en organisation.

Det är ju ganska... Om man tittar på amerikanska företag så är det väldigt vanligt förekommande om man läser runt lite grann. Gör man fel får man sparken. I Sverige fungerar det inte så. Det krävs väldigt mycket för att avskeda någon om man misskött sitt arbete. Det ska vara väldigt gravt och med uppsåt. Jag känner

personligen att vi har väldigt få... Det är klart, gör man något brottsligt, gör man någonting med uppsåt, ja, såklart måste man ha ett system där man kanske tar ett samtal med medarbetaren eller att det får några konsekvenser. Absolut. Vi har inte varit där och hoppas att vi inte kommer dit heller utan det är väldigt mycket individens ansvar och vi litar väldigt mycket på våra medarbetare. Vi är väldigt noga när vi rekryterar. Vi försöker jobba preventivt. Men alla kommer göra misstag och där gäller att pränta in att det är okej att göra misstag och vi ska ha dem skydd som krävs för att man ska kunna göra misstag också utan att det får alltför kännbara konsekvenser för företaget eller för våra kunder. Så svaret på frågan är väl nja. Det är klart att det måste finnas för grova förseelser så måste det finnas kännbara konsekvenser men i praktiken händer det här, för oss i alla fall, så pass sällan så det är inget vi behöver ta ställning till i dagsläget.

Har du upplevt shadow security under din karriär inom informationssäkerhet? Kan man ha för mycket säkerhet, och att alltför strikta krav och regler? När har man gått för långt med säkerhetspolicyn?

Det tror jag absolut. Det är ju ett faktum att så är fallet. Det är samma sak där. Där tror jag väldigt mycket på att göra det enkelt att göra rätt. Ofta är en anledning till att det blir shadow-IT eller att användaren hittar egna lösningar på problem. Det är ju för att man antingen har för tajt säkerhet så att folk inte kan jobba eller att det inte finns tillräckligt bra tekniska lösningar eller lösningar överlag för att man ska kunna jobba effektivt. Har man duktiga medarbetare så är de här för att jobba effektivt. Dem kommer hitta vägar runt allting för att kunna jobba effektivt. Det handlar mycket om att jobba med användarna för att bygga lösningar som är säkra att använda och som användarna vill använda. Sen kommer det där aldrig vara 100% utan man måste ibland säga nej för det blir för kostsamt att bygga enkelt och bra alla gånger. Men det måste vara en balans. Det måste vara tillräckligt enkelt att göra rätt. Men där har vi exempel, till exempel man använt... kanske inte för att det är smidigare men kanske ren okunskap. Man använder sin google docs och privata mail och cloud lagring... Man kanske säger det är så här jag brukar göra men det är inte vad vi använder i företaget. Trots att vi har fullgoda andra ställen att lagra informationen. Där handlar det också om utbildning och se till att medarbetarna vet att det är detta som gäller och jag måste använda dem här lagringsställen och man vet att det är minst lika bra. Det vill säga att man inte använder andra system av ren vana för man kan det utan man

använder det som företaget säger man ska använda och att man vet hur det fungerar och vilka fördelar som finns med det.

Förutom att det ska vara enkelt, vad är avgörande för att shadow-IT eller shadow security blir så minimalt som möjligt inom en organisation?

Utöver utbildningen är det tekniska åtgärder också. Man tar exemplet med lösenordspolicyn till exempel. Att man skriver det på en lapp är svårt att komma undan men det är... jag faller tillbaka på utbildning igen. Vi har en obligatorisk informationssäkerhetsutbildning för alla anställda tidigt i anställningen och där går vi igenom varför vi har den här lösenordspolicyn och du har möjlighet att välja antingen ett kort men komplext lösenord med små och stora bokstäver, siffror och konstiga tecken. Eller så kan du välja en längre mening, en lösenfras, och då tillåter vi mindre komplexitet, men i gengäld att du skriver en lite längre mening men som också är lättare att komma ihåg. Så det är väl... jag faller nog tillbaka på utbildning och varför det är viktigt att upprätthålla en god informationssäkerhet. Motivera användarna att tänka varför måste jag göra det här som är lite krångligare. Jo, det är för att skydda företagets data och det är för att skydda kundernas data. Det är bland det viktigaste vi kan göra; se till att våra kunders data inte kommer på avvägar. Men i förlängningen är det något som ger oss nöjda kunder och bra business. Att verkligen motivera medarbetarna att veta varför gör vi det här? Det är inte för att jävlas med er eftersom vi krånglar till det utan det är av en bra anledning. Sen kan det vara svårt för oss ibland för vi har gått från att vara ett litet bolag med några få kunder till att växa och bli större och större med fler medarbetare. Tidigare har vi haft få kontroller och åtgärder och nu i och med att vi växer så kan inte alla ha åtkomst till allt. Det finns GDPR, kunder som ställer krav så vi måste hela tiden tajta till säkerheten. Det är också en balansgång. Det är en utmaning att gå från något helt öppet där alla är admins på sina datorer och alla kan installera saker på sina datorer, fritt blås överallt. Till att sakta men säkert plocka bort lite av dina behörigheter och begränsa din frihet lite. Det är en balansgång.

Skulle man då kunna säga att just för det här med Shadow-IT att utbildning är ganska centralt bit av det?

Utbildning och att tillhandahålla bra alternativ. Och att vara lyhörd för organisationens krav och hänga med i utvecklingen skulle jag säga.

Företagskultur, säkerhetskultur, eller bristen på säkerhetskultur, har visat sig påverka informationssäkerheten inom en organisation. Vilka utmaningar stöter du på i din roll som driftansvarig med olika organisationers kultur? Hur kan du som driftansvarig motarbeta avvikelsekultur om en sådan finns, och vilka utmaningar finns i arbetet mot det? Vilka utmaningar ser du i att införliva ett säkerhetstänk och säkerhetskultur i ett företags rådande organisationskultur?

Det är ju dels det jag nämnde tidigare om att anställer man duktiga medarbetare så kommer dem vilja jobba så effektivt som möjligt och ibland kan det vara så att under tidspress. När man kämpar mot klockan så blir det mycket enklare att ta genvägar. Att göra saker på fel sätt snarare än att göra det på rätt sätt. Det är ju en utmaning och det är ju i vår leveransorganisation där vi dels måste vara väldigt noga för vi hanterar våra kunders data. Samtidigt så finns en tidspress på våra medarbetare att leverera och prestera inom en viss tidsram och vi jobbar med ett ganska stort antal individer som är... rätt många kommer direkt från skolan och har bara några få års erfarenhet. Det vill säga man vet inte riktigt vad är okej vad är inte okej. Ska jag göra på det här sättet eller är det bättre att göra på det här sättet som tar längre tid? Någon sa att det var säkrare men hur viktigt var det? Så det skulle jag nog säga är en av våra större utmaningar. Stress och tidspress.

Om vi tänker organisationer generellt, världen runt och i Sverige, är avvikelsekultur ett stort problem?

Vad var din definition på avvikelsekultur?

Det är det här att om anställda anser att någon lösning eller policy hindrar deras produktivitet så ser dem och till exempel driftchefer mellan fingrarna på det och att man frångår för att upprätthålla en viss produktivitet.

Frågan var då om jag upplever det som ett problem?

Ja, utifrån din erfarenhet och organisationer generellt och inte bara här hos företag 3.

Det är klart det är ett problem. Antingen får man följa reglerna reglerna som man godkänt och satt upp och gör man inte det så gör man fel. Eller så är det fel på regeln för den är för hårt tillskruvad eller annat. Det gäller att... Det är den svarta eller vita historien. Man måste anpassa reglerna så att de går att efterleva. Går inte regeln att efterleva så kommer den inte efterlevas. Det är ett problem om mellancheferna ser mellan fingrarna om deras medarbetare inte följer reglerna.

Att införliva säkerhetskultur har också visat sig ha en påverkan på informationssäkerheten. Vad ser du för utmaningar i att införliva en säkerhetskultur i en organisations vanliga kultur ?

Enligt Calle (Företag 3) är en utmaning att införliva säkerhetskultur eftersom folk glömmer väldigt snabbt. Man måste påminna hela tiden, utbilda och göra folk medvetna om säkerhetstänk kontinuerligt. Det är ett lärande man måste ha hela tiden. Företag 3 arbetar proaktivt istället för att vänta på att en incident sker. Till exempel så har vi kört phishing tester internt där vår IT-avdelning skickar ut test med jämna mellanrum till alla medarbetare och följer upp resultatet. Vilka öppnade det, vilka rapporterade det, vilka ignorera det bara? Vi försöker tracka hur det går för oss. Det är faktiskt någonting som har blivit en kul grej, en liten snackis. Är det här ett test? Det har lett till att man är mycket mer medveten vad gäller just phishing. Det är definitivt en stor utmaning. Det är en sak också att lära ut säkerhet i teorin under en utbildning men sen när du väl sitter i din kontorsstol, du ska jobba praktiskt med det du har lärt dig, under tidspress, du har många bollar i luften, många som skriker på dig. Det är klart det är en utmaning. Tidsbrist och att man glömmer bort. Stora utmaningar.

Om vi åsidosätter vanligt förekommande teknologiska lösningar såsom antivirus och brandvägg, har du erfarenhet av att övervakningsprogram används för att övervaka att anställda följer informationssäkerhetspolicyn?

Vi har väl lite mer av en detekterings mjukvara på våra laptops och så vidare. Det beror på lite vad man anser vara standard nu för tiden. Det varierar ganska mycket. Men du tänker fortfarande tekniska åtgärder?

Rent tekniska, mjukvara och hårdvara men inte de vanligaste. Vi kan förmodligen anta att dem flesta har någon slags antivirus och brandvägg åtminstone.

Vi har ju mjukvara som loggar varifrån man loggar in och jämför. Här har vi Nisse och han brukar sitta i stockholm men ibland är han nere i skåne. Men nu försöker han logga in från ryssland här och det är ju antagligen lite fuffens och det triggar ett larm. Det typen av detektering har vi. Vi har också multifaktorautentisering för alla våra medarbetare vilket är en väldigt bra grej. Borde vara standard. Det är väl två konkreta exempel. Vi har ett par andra grejer också där vi tittar på avvikelser. Vi har full disk kryptering på laptops. Vi kan spärra alla företagsmobiler och följa upp vilka applikationer man har vid behov. Den typen av saker.

Skulle man kunna säga att någon bit väger tyngre, det här mjuka med utbildning eller det här tekniska eller måste man ha någon slags balans?

Man måste definitivt ha en balans och det är väldigt lätt att implementera de här konkreta åtgärderna. Är man lite teknisk lagd är det lätt att trilla dit på att man installerar verktyg efter verktyg, tänker verktyg, drömmer system och tjänster och det kommer nya grejer hela tiden. Häftiga grejer som ska spara in en massa tid. Och tittar man återigen på amerikanska bolag så handlar det mycket om data loss protection, du ska låsa ner allt så mycket det bara går så du kan se till att inte en sur anställd snor med sig kundregistret när de slutar. I praktiken är det extremt svårt att skydda sig mot det. Det är väldigt lätt att plocka med sig data ut om man skulle vilja och vet vad man håller på med. Det är i princip omöjligt att spärra det. I alla fall på ett sätt som fungerar i arbetslivet. Så jag tror mycket mer på utbildning, jag tror på att göra folk medvetna, jag tror på att berätta för medarbetarna varför gör vi det här och varför vill vi att du ska göra så här? Så att man själv känner ja men jag måste göra det här även om det är jobbigare. Ett väldigt tydligt exempel är vi hade inbrott här för några veckor sen. Någon snodde tio laptops på två minuter. Nu har vi köpt laptopskåp så man kan låsa in sin dator. Där blir det väldigt tydligt ... det finns en tydlig anledning med varför du ska lägga in din laptop i

skåpet. Det är för att du inte ska bli av med den. Vi ska inte bli av med den. Det är lite after the fact. Hade vi haft dem innan så hade det varit en bra grej naturligtvis. Men det blir mer tydligt varför behöver jag göra detta extra momentet varje dag innan jag går hem om jag inte tar med mig datorn hem. Jo, det är för vi inte ska bli av med den.

Om vi tänker organisationer generellt, utifrån din erfarenhet, upplever du att dem förlitar sig alltför mycket på rent tekniska lösningar och glömmer bort biten med awareness och utbildning?

Det tror jag definitivt. Det är väldigt lätt att göra. Det är mycket enklare att sitta vid sitt skrivbord, konfigurera ett system som man skjuter ut än att förbereda ett bra utbildningsmaterial och genomföra en utbildning. Det är tidskrävande, det är inte alla som gillar den typen av jobb. Jag kan tänka i många organisationer så är informationssäkerhetsarbetet är lagt på IT-avdelningen och särskilt med mindre organisationer så är det nog utbildnings insatserna som får lida på grund av det. Sen finns det många bra och mindre bra onlineutbildningar som man kan köpa in med övningar och så vidare. Dem är fortfarande relativt dyra också. Det kan vara svårt att motivera den kostnaden innan det har hänt något som vanligt. Vi kör som obligatorisk utbildningsinsats för samtliga har vi en två timmars introduktion som antingen genomförs live eller att man sitter och tittar på en film med samma innehåll. Sen har vi en uppföljningsutbildning en gång om året för samtliga anställda som vi ska ta fram innan sommaren som är tanken. Vi körde igång med det här programmet förra året så det kommer bli 15-30 minuter som en refresher för samtliga.

Bara en snabb återgång till det här med övervakningsprogram. Skulle man kunna säga att dem har en avskräckande effekt; att bara vetskapen att man blir övervakad av ett sånt program minskar risken för policy brott och dylikt?

Ja det tror jag nog, i de fall att man faktiskt är medveten om... det är inte av den anledningen vi har mjukvarorna men det kan det nog absolut vara så. Särskilt om man hör av sig till användaren efter att det kommit ett larm. Då blir reaktionen ofta oj har ni koll på det här? När man återkopplar 5 minuter senare efter att någon råkat installera något på sin dator så skriker antivirusprogrammet till, så ringer vi efter 5 minuter

och frågar vad som hände. Ja oj, såg ni det såhär direkt? Jag hade nog tänkt till en extra gång, nästa gång, om jag varit i den sitsen. Man kan alltid spela på folks skamkänslor.

Vilka utmaningar ser du i arbetet med kunskapsförmedling och utbildning av informationssäkerheten? Upplever du att utbildning och kunskapsförmedling får de resurser och den tid som krävs för att det skall genomföras på ett gediget sätt? Hur kan utbildningar och ISA-träning förbättras?

I och med att vi är ju 240 anställda ungefär och vi har en IT-avdelning på 3 personer här. Vi sätter ju våra egna prioriteringar i väldigt hög utsträckning. Johan bestämmer hur mycket utbildning ska vi köra, när ska vi göra det, hur mycket tid kan vi lägga på det? Det är dem resurserna vi har och där handlar det om att bara få det gjort. Så det handlar om att vara proaktiv. Nu har vi satt det här programmet att vi alla kör obligatoriskt 2 timmar introduktion och sen följer vi upp 15-30 minuter per år. Så utmaningen där är mest att se till att alla vet och hjälper alla att se det som obligatoriska moment och vi följer upp det i vårt karriärsystem och man får bocka av att man gjort den här utbildningen. En utmaning är... räcker det en gång om året? Är det tillräckligt? Vi har phishing testerna som komplement, borde vi göra något annat också? Man kan göra hur mycket som helst. Man hade kunnat lägga ut veckans säkerhetstips fem minuter en liten film. Fem minuter tar en ganska lång tid att producera, så är det. Så en utmaning är väl någonstans var drar man gränsen? Hur mycket är lagom? Hur mäter vi att det här är framgångsrikt? Phishing Testerna kan man mäta på lite grann. Samtidigt skickar vi inte ut samma test mail varje gång. Man kan vara olika lättlurad beroende på innehållet. Det är jättesvårt att dra några slutsatser om det. Ska vi titta på hur många säkerhetsincidenter vi har? Det beror lite på vilken typ av folk vi anställer. Det beror lite på är deras datorer mer nedlåsta från början? Vissa kategorier av medarbetare är kanske mer nedlåsta än andra. Kan vi dra slutsatser av det? Det är väl två utmaningar i all fall, att veta hur mycket är lagom och vad får vi tillbaka för det? Jag tror samtidigt inte att ett företag i vår storlek, med den personalen vi har som ändå är relativt teknisk... vi har nog lagt det på en ganska så rimlig nivå. Jag känner att jag inte behöver veta exakt hur mycket vi får ut av det. Jag vet att utbildningen är viktig och att den tjänar sitt syfte och att den gör per automatik att vi får färre incidenter för vi får en ökad medvetenhet hos våra medarbetare. Skulle man mäta på detta så skulle man behöva en kontrollgrupp där man inte kör någon utbildning och nej, det behöver vi inte göra. Så utmaningarna är väl lägga ribban lagom högt

och se till att det händer och se till att ha bra innehåll. Nu har vi valt att producera vårt innehåll själva istället för att köpa in någonting och det är väl också någonting som vi gjort... även om det tagit ganska lång tid att producera det materialet så är jag ganska nöjd att vi gjort det för det blir anpassad precis efter vår verksamhet.

Om vi tänker organisationer generellt, känner du att styrelser i olika organisationer ger tillräckligt med resurser till dem som är ansvariga för ISA och utbildning och så vidare? Eller är det ett problem att lösgöra resurser för detta generellt?

Jag kan bara tala för min organisation här. Där har det ju... jag kan inte säga att någon motarbetat oss utan tvärtom, vi har fått väldigt mycket positiv feedback ända uppifrån styrelsen som är medvetna om det här programmet så nej, där känner jag fullt stöd.

Vilka utmaningar ser du i återkoppling och att kolla upp att användarna tagit åt sig kunskapen från utbildningarna? Undersöker ni de anställdas säkerhetsmässiga kunskapsnivåer och/eller har du erfarenhet utav att ett företag undersöker det tidigare under din karriär?

Jag tror det är mindre vanligt utanför företag som har ett medvetet säkerhetsarbete och om man ser till antalet små och medelstora bolag i Sverige så kan jag tänka mig att det är ganska få som faktiskt har ett security awareness-program. Vi kommer göra en internrevision till hösten där vi kommer intervjua medarbetare men mer än så gör vi inte just nu. MEn det är klart att det hade varit kul att skicka ut en liten quiz ibland. Det hade varit en bra grej men det är ytterligare en grej som måste göras.

Skulle man kunna säga att detta är viktigt för informationssäkerheten inom ett bolag, att återkoppla och kolla hur mycket anställda har tagit till sig?

Det borde ju vara så. Det är ju viktigt annars vet man inte hur lyckat programmet är. Det är samtidigt svårt att mäta utan att lägga mycket tid på det och frågan är väl kanske om vi kanske får bättre resultat om vi istället lägger den tiden på att faktiskt utbilda?

Tidigare litteratur nämner att styrelsen måste ta ansvar och spela en mer aktiv roll när det gäller att bestämma organisations informationssäkerhetsstrategi. Kan det vara så att styrelser behöver ta mer ansvar. Vilka andra brister ser du och hur kan man förbättra säkerhetsstrategin?

Vår informationssäkerhetspolicy är godkänd av vår styrelse och dem är informerade om vad som står i den och dem har fått en briefing förra året gällande det säkerhetsarbetet vi gör. Sen tror jag generellt sätt kanske att man inte riktigt är medveten om hur viktigt arbetet är och jag man underskattar det lite grann innan det har hänt en incident som påverkar verksamheten ordentligt. Tyvärr. Det ligger lite i människans natur.

Skulle man kunna säga att styrelser är lite hands off när det gäller informationssäkerhet om man tänker organisationer generellt i världen.

Jag kan bara tala för min egen styrelse men där skulle jag kanske säga så är nog fallet. Man tycker det är viktigt men det är bra om någon som kan det tar hand om det.

Känner du att styrelseledamöter har tillräckligt med erfarenhet när det kommer till informationssäkerhet? Tycker du detta ska vara ett krav eller alternativ för vissa eller alla styrelseledamöter?

Ja det skulle jag nog säga. Vi har en styrelse som är... jag skulle inte säga att dem är väldigt tekniska, men dem är i alla fall tekniska i att jobba med ett mjukvarubolag och informationssäkerhet är en väldigt viktig detalj. Så nej, det är jag väldigt nöjd med.

Om vi tänker bolag generellt, finns det kunskapsbrist bland styrelseledamöter och hade behövt ha någon specialutbildning för styrelser så att dem kommer in i det här med informationssäkerhet.

Det hade inte skadat. Jag har nog lite svårt att uttala mig i den frågan men varför inte? Det skadar ju inte med utbildning. Ju mer insatt man är som styrelseledamot desto bättre jobb kan man göra. Sen har dem mycket andra saker dem ska kunna göra också.

Referenser

Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. ISBN: 9780128008126

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. *2013 46th Hawaii International Conference on System Sciences*. Wailea, Maui, HI, USA 7 - 10 january 2013. pp 3018 - 3027. DOI: 10.1109/HICSS.2013.272

Alotaibi, M.,Furnell, S., Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*. Barcelona, Spain 5-7 december 2016. pp 352 - 358. DOI: 10.1109/ICITST.2016.7856729

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, 13(4), ss. 195 - 201. DOI: 10.1016/j.istr.2008.10.006

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34(3), pp 523–548

Chang, S. E. & Lin, C-S (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems*, 107(3), ss. 438 - 458. DOI: 10.1108/02635570710734316

Chen, Y., Wen, K.-W., Ramamurthy, K. (2014). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29(3), pp. 157-188. DOI: 10.2753/MIS0742-1222290305

Cohen, Manion & Morrison (2007) *Research Methods in Education*. Sixth edition.

D'Arcy, J., Hovav, A., Galletta, D. (2006). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20(1), pp. 79-98. DOI: 10.1287/isre.1070.0160

Jacobsen, D. I., 2002. *Var, hur och varför?* Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Lund: Studentlitteratur.

Johnston, A. C. & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3), ss. 549 - 566. DOI: 10.2307/25750691

Katsikas S, Backes, Gritzalis & Preneel. (2006). *Information Security: 9th International Conference*; ISC

Safa, N. S., Von Solms, R., Furnell, S. (2016). Information security compliance model in organizations, *Computers & Security*, 56, pp 70-82

Von Solms, B. & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), ss 371-376. DOI: 10.1016/j.cose.2004.05.002

Whitman, M.E. & Mattord, H.J. *Principles of Information Security 4th edition*(2012) Course Technology, Boston