LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Hur utvärderas IT- och informationssäkerhetsinvesteringar?

Kandidatuppsats 15 hp, kurs SYSK02 i informationssystem

Författare: Omid Asali
Dennis Olsson

Handledare: Anders Svensson

Examinatorer: Miranda Kajtazi
Magnus Wärja

Hur utvärderas IT- och informationssäkerhetsinvesteringar?

Författare: Omid Asali och Dennis Olsson

Utgivare: Inst. för informatik, Ekonomihögskolan, Lund universitet

Dokumenttyp: Kandidatuppsats

Antal sidor: 64

Nyckelord: IT- och informationssäkerhet, Utvärderingsmodeller, Säkerhetsinvesteringar, Investeringsstrategier, Best practice

Sammanfattning (Max. 200 ord):
Internet har som verktyg kommit att spela en allt större roll för hur företag bedriver sina affärsprocesser. Med detta verktyg har även nya hot vuxit fram som kan resultera i ekonomiska förluster. För att mildra eller förhindra dessa ekonomiska förluster investerar organisationer i åtgärder för att skydda sig och sin information. Detta innebär att organisationer spenderar stora summor på IT- och informationssäkerhet. Den här typen av investeringar är dock svåra att utvärdera och rättfärdiga ekonomiskt. Vi ställde oss då frågan hur organisationer gör för att hantera detta problem, och om de tar användning av modeller för att göra detta. För att ge svar på frågan har akademisk litteratur på ämnet undersökts i syfte att jämföra med hur tre företag i olika branscher går tillväga i praktiken. Jämförelsen visar på att de ekonomiska utvärderingsmodeller som litteraturen talar för inte används bland de organisationer som deltagit i undersökningen. Varken innan, eller efter en investering har gjorts.

Innehåll

Figurförteckning

Tabellförteckning

1 Introduktion

I detta inledande kapitel introduceras uppsatsens bakgrund, problemdiskussion, forskningsfråga samt syfte och avgränsningar.

1.1 Bakgrund och problemdiskussion

Under de senaste tre årtionden har Informationsteknologi kommit påverka både hur organisationer fungerar, och bedriver sina affärsprocesser. I takt med Internets utveckling har dessa affärsprocesser genomgått stora förändringar (AO'Brien & Marakas, 2006). Den rent teknologiska utvecklingen, tillsammans med utvecklingen av Internet har gett organisationer nya möjligheter till att bedriva affärer över hela jordklotet (Business Roundtable, 2007).

Den ökande trend där fundamentalt viktiga affärsprocesser och transaktioner, som tidigare bedrevs över isolerade nätverk nu förlitar sig på Internet, skapar således ett tekniskt beroende. Med dessa nya möjligheter kommer även nya sårbarheter (Business Roundtable, 2007), och för dessa organisationer är säkerhetsrisker oundvikliga (Tsiakis & Stephanides, 2005).

Eftersom att affärsprocesserna nu är teknologiskt beroende, kan ett säkerhetsintrång således ha en ekonomisk påverkan hos en organisation. Tsiakis och Stephanides (2005) menar på att ett intrång kan resultera i olika typer av påverkan:

- *Direkt ekonomisk påverkan* - Kostnader som uppstår för att antingen reparera, eller byta ut system, samt kostnaden för avbrottet i verksamheten.
- *Kortsiktig ekonomisk påverkan* - Förlust av kontrakt och kunder, samt en negativ påverkan på organisationens rykte.
- *Långsiktig ekonomisk påverkan* - Minskat marknadsvärde samt aktiepriser.

För att mildra, eller förhindra att dessa ekonomiska förluster uppstår, investerar organisationer i åtgärder för att skydda sig. Givet att nästintill all företagsdata nu behandlas, sänds och lagras digitalt, krävs det att organisationer investerar i IT- och informationssäkerhet. Denna typ av säkerhet syftar till att skydda en organisations data från obehörig tillgång (Dutta, 2008).

Investeringar i IT- och informationssäkerhet genererar i förhållande till klassiska investeringar, inte i några intäkter. Vilket har lett till att just säkerhetsinvesteringar är ökänt svåra som organisation att rättfärdiga. Snarare än att generera intäkter skall resultatet av en säkerhetsinvestering vara ett undvikande, eller en minskning av den potentiella kostnaden om ett hot skulle komma att realiseras (Dutta, 2008). De beslutsfattare som faktiskt bestämmer om en investering skall göras eller inte, är främst inte intresserade av att veta huruvida en viss typ av virusskydd kan bidra till att skydda företags servrar. För att veta hur mycket pengar som skall spenderas vill de istället ha svar på frågor som de nedanför:

- Vilken påverkan har en brist på säkerhetsmekanismer på företagets produktivitet?
- Vilka lösningar är de mest kostnadseffektiva?
- Vilken påverkan skulle ett säkerhetsintrång ha?

En säkerhetsinvestering skiljer sig i beslutsfattarnas ögon inte på något sätt från traditionella investeringar. De vill veta om en investering kan rättfärdigas finansiellt, och det är således alltså inte lönt att spendera pengar på en lösning om kostnaden av denna överstiger den faktiska kostnaden om ett hot skulle komma att realiseras (Sonnenreich, Albanese & Stout, 2006).

Med detta som bakgrund vill vi därför undersöka hur organisationer går tillväga för att utvärdera och rättfärdiga en säkerhetsinvestering.

1.2 Forskningsfråga

- Hur utvärderas IT- och informationssäkerhetsinvesteringar, vilka modeller och metoder använder sig organisationer av för att göra detta?

1.3 Syfte

Syftet med denna uppsats är att undersöka hur olika organisationer går tillväga för att utvärdera investeringar de gör gällande informationssäkerhet. Genom att intervjua ansvariga gällande säkerhetsinvesteringar hos olika organisationer, ämnar vi till att utifrån dessa upptäckter identifiera och analysera likheter samt skillnader mellan den befintliga teorierna gällande ämnet kontra det faktiska genomförandet hos organisationer.

Uppsatsen är tänkt att läsas för de som är intresserade av att veta mer kring hur organisationer går till väga när de utvärderar investeringar gällande IT- och informationssäkerhet.

1.4 Avgränsningar

Uppsatsens fokus är att undersöka hur organisationer utvärderar sina IT- och informationssäkerhetsinvesteringar. Den kommer inte att behandla IT-investeringar som görs i syfte att skapa värde i form av processförbättringar och effektivisering av organisationen, utan investeringar som görs i syfte att skydda organisationens informationstillgångar. Uppsatsen kommer inte att ta upp hur organisationer skall göra för att uppnå maximal säkerhet. Specifika siffror eller milstolpar kommer vidare inte heller åläggas hänsyn. Uppsatsen kommer inte att undersöka hur organisationer gör att för kvalificera vilka organisatoriska områden, samt tillgångar som det skall investeras i, utan snarare vilka modeller och metoder som används för den ekonomiska kvalificeringen av investeringar i IT- och informationssäkerhet.

Vi kommer att fokusera på hur organisationer skall gå tillväga för att utvärdera den IT- och informationssäkerhetsinvestering som organisationer har gjort samt vilka modeller som kan användas vid en investering eller utvärdering. Orsaken till denna avgränsning är för att IT- och informationssäkerhet är ett brett ämne och vårt intresse ligger i att studera om dessa modeller och utvärderingsmetoder som finns i teorin faktiskt används i praktiken

2 Litteraturgenomgång

I detta kapitel kommer vi att presentera befintliga teorier samt modeller gällande utvärdering av säkerhetsinvesteringar

2.1 IT- och Informationssäkerhetens bakgrund

Idag har alla organisationer någon form av informationssystem, varav att det skapar ett behov av att fokusera på informationssäkerheten också för att inte vara sårbara då allting idag digitaliseras. Ciscos CIO, James Mcnab säger *”Det finns fortfarande stora verksamheter som inte har en säkerhetsstrategi, trots att dataintrång är lika allvarligt som finansiella risker. Förr var IT-säkerhet en fråga för experterna. Nu borde det vara högsta prioritet för varje bolagsledning”* (Lundström, 2016).

Detta tar oss till ett av de första historiska saboterande virusen mot organisationer vid namn Melissa. Vid den tidpunkten hade internet blivit en del av organisationernas affärsprocesser där Internet användes som kommunikationsmedel i form av e-post. Melissas tillvägagångssätt liknas väl vid spam-post, där viruset förökade sig genom att skicka vidare ett infekterat mail till de 50 första kontakterna i den redan infekterade adressboken. Stora företag, och även då inom IT-branschen, som Microsoft och Intel blev påverkade i den utsträckning att de valde att stänga ner sina e-posttjänster (Rosencrance, 2002).

Säkerhet är ord vars innebörd många skulle säga sig känna till, men vad är egentligen säkerhet? Man kan säga att ordet säkerhet syftar till *”Egenskapen, eller stadiet av vara säker – att vara fri från fara”* (Whitman & Mattord, 2011). Ordet syftar alltså till att vara skyddad från de som avsiktligt, eller oavsiktligt, vill göra skada.
För att en organisation skall anses lyckad ur ett säkerhetsperspektiv, och således skydda sin verksamhet, bör den ha implementerat följande lager av säkerhet:

- Fysisk säkerhet
- Personalsäkerhet
- Verksamhetssäkerhet
- Kommunikationssäkerhet
- Nätverkssäkerhet
- Informationssäkerhet

(Whitman & Mattord, 2011).

Detta är något som författaren Dhillon (2007) instämmer på och menar på att det finns tre olika delar som bör behandlas inom Informationssäkerhet, dessa delar är:

Technical Controls: Den tekniska delen. Hårdvara och datorer.
Formal Controls: Understöd och användarhjälp gällande informationssystemen.
Informal Controls: Utbildad medvetenhet gällande system samt risker.

Dhillon (2007) skriver att när frågan om informationssystem och dess säkerhet inom en organisation ställs, brukar användarna eller anställda enbart tala om Formal Controls. Anledning

till det tycket är för att anställda anser att det är kärnan för att få informationssystemets säkerhet att faktiskt fungera (Dhillon, 2006). Dessa tre delar är en helhet inom det som kallas informationssäkerhet. Enligt Lundström (2016) talar James Mcnab också om tre delar som kan liknas vid vad Dhillon (2007) menar på.

IT- och informationssäkerhet är alltså en vital del i att processen att uppnå en säker organisation. Grunden i den här typen av säkerhet syftar till att skydda informationstillgångars Konfidentialitet (Confidentiality), Integritet (Integrity) samt Tillgång (Availability), det som inom säkerhetsindustrin går under namnet ”C.I.A-triangeln”. Med hjälp av policys, utbildningar, medvetenhet samt teknologi kan en organisation applicera detta lager av säkerhet, och således säkra sina informationstillgångar (Whitman & Mattord, 2011).

Likväl som ordet säkerhet har en mer strikt definition har även informationssäkerhet en konkret definition. The International Organization for Standardiztion (ISO) och the International Electrotechnical Commission (IEC) definierar informationssäkerhet som ”beskyddandet av information från ett brett spektrum av hot för att säkerställa affärskontinuitet, minimera affärsrisker, samt maximera avkastning på investeringar och affärsmöjligheter” (ISO/IEC, 2005). Genom att implementera lämpliga kontroller i form av policys, processer, organisatoriska strukturer samt både hård- och mjukvara kan en organisation uppnå denna typ av säkerhet (ISO/IEC, 2005).

2.2 Utvärderingsmodeller

Modellerna kommer att presenteras utförligt och i sin helhet för att erbjuda full förståelse för hur de är uppbyggda. Förståelse på detaljnivå är dock inte nödvändig för att förstå uppsatsens resultat eller slutsats.

2.2.1 Return on Investment (ROI)

För att organisationer skall kunna estimera hur pass lönsamma deras investeringar är har en formell vid namn ”Return on Investment” förkortat ROI tagits fram som beräknar hur mycket en organisation får tillbaka av en gjord investering. En uträkning baserat på ROI kan inte göras helt punktligt då det är en approximativ uträkningsmetod (Investopedia, 2003).

$$\textbf{\textit{ROI}} = \frac{\text{(Gain from Investment - Cost of Investment)}}{\text{Cost of Investment}}$$

Figur 2.1 - Return on Investment (Investopedia, 2003)

Enligt Sonnenreich et al. (2006) är det en fråga om “Vilka av dessa alternativ ger mig mest värde för mina pengar jag ska investera”. Tanken bakom ROI är att svara på denna fråga, dock så är det ett rent estimat. Sonnenreich et al. (2006) menar på att även organisationer vet om att det är en hypotetisk uträkning, väljer de ändå att använda sig av detta ränkeexempel då det har fungerat i många år. Vidare menar författarna dessutom på att ROI kan användas för att organisationer skall ta ett beslut om det är lönsamt för dem att investera i en ny teknik eller att investera i att fortsätta bygga på deras nuvarande teknik (Sonnenreich et al., 2006). ROI

som uträkningsformell når ut till brett användarperspektiv. Inom olika verksamheter samt organisationer. ROI visar dock inte på specifikt kapital eller summor, utan presenteras i procent där det finns positivt respektive negativt ROI (Investopedia, 2003).

Uträkningsexemplet tar inte hänsyn till olika tidsperspektiv gällande uträkningar. Detta får användaren själv göra och i vissa fall är detta ett problem då många investerare naivt litar på uträkningsmetoden. Utfallet av att använda ROI som uträkningsmetod kan vara olika beroende på användare, detta kan dels bero på att olika perspektiv en användare har eller definitionen av meningen "Return on Investment" (Investopedia, 2003).

2.2.2 Return on Security Investment (ROSI)

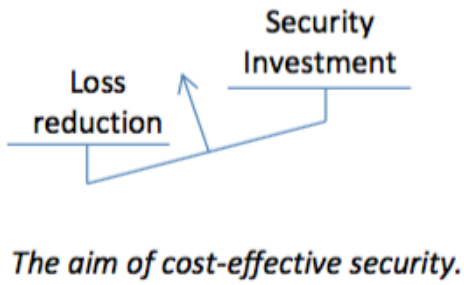
Enligt European Union Agency for Network and Information Security (Enisa, 2012) tillämpas ROI på alla former av investeringar och menar på att det är applicerbart på säkerhetsinvesteringar också. Dock så menar Enisa (2012) på att de som tar investeringsbeslut gällande säkerhet vill ha en vetskap om hur mycket pengar som faktiskt är rimligt att spendera på en säkerhetsinvestering, och vad som då kan ligga till grund för den investering som kan göras i framtiden. För att veta detta ställs frågor som hur mycket kostar säkerhetsinvesteringen organisationen, och vilken säkerhetsinvestering är den mest kostnadseffektiva lösningen (Enisa, 2012).

Hur utvecklades då ROI som är en allmän uträkningsmodell för investeringar till att bli anpassad för att räkna ut investeringar enbart för säkerhet? Det var Unversity of Idaho som tog fram "Return on Security Investment" som förkortas ROSI. En grupp på University of Idaho byggde år 2000 en säkerhetsmekanism i form av en intrångsdetektionslåda. Denna säkerhetsmekanism sattes i nätverket där gruppen kunde analysera användarnas beteende ifall det var misstänktsamt. Gruppen valde därefter att hacka säkerhetsmekanismen för att stärka sin studie. Studien menar på att när en risk väl inträffar, är det mer kostnadseffektivt att upptäcka risken sedan åtgärda den, än att försöka hindra den helt (Berinato, 2002).

$$\textbf{\textit{ROSI}} = \frac{\text{ALE x Mitigated Ratio - Cost of Solution}}{\text{Cost of Solution}}$$

Figur 2.2 - *Return on Security Investment (Enisa, 2012.)*

Det som skiljer mellan ROI och ROSI är det HuaQiang Wei och hans grupp kom fram till, detta är Annual Loss Exceptency, förkortat ALE. ALE innefattar hur frekvent en risk uppstår multiplicerat på riskens finansiella skada (Berinato, 2002). Dock så är denna uträkningsmetod likväl ROI ett approximativt sätt att försöka förmildra en skada som kan uppstå. Därför skall en mittpunkt hittas mellan det skadeförebyggande och säkerhetsinvesteringen. ROSI kan väldigt lätt manipuleras på grund av olika intressen och prioriteringar av användaren, det skiljer sig beroende kultur och den syn organisationen har på informationssäkerhet (Enisa, 2012).



Figur 2.3 - *The aim of cost-effective security (Enisa, 2012)*

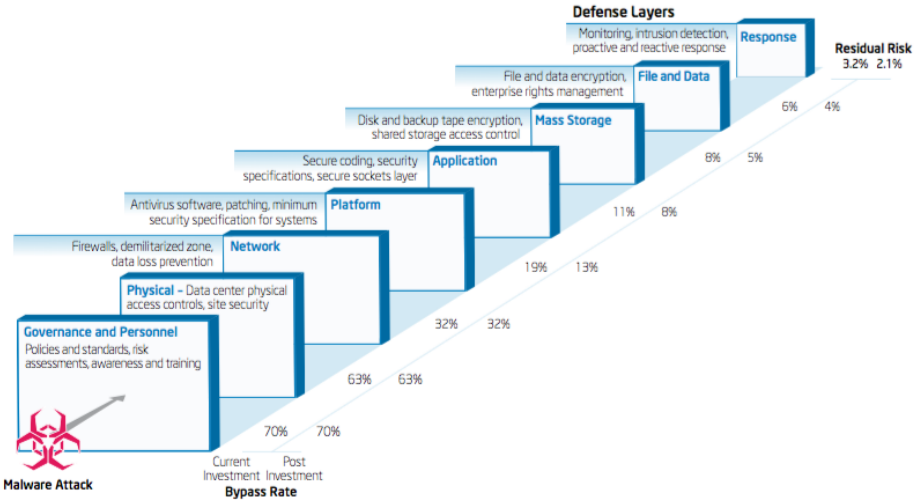
2.2.3 Intel IT Security Model (IISIM)

Alla organisationer går inte efter färdiga modeller för deras IT- och informationssäkerhetsinvesteringar. Intel har med delar av ROI tagit fram en egen uträkningsmodell för säkerhetinvesteringar för deras informationssystem och IT. Intel IT Security Investment Model togs fram 2012 och är anpassad efter Intels organisation då modellen följer best-practice för Intel (Carty, Pimont & Schmid, 2012).

Carty et al. (2012) skriver att modellens syfte är estimera värdet av det som finansieras i varje säkerhetsinvestering och hur investeringen minimerar IT-risker. Intel menar på att det som faktiskt är effektivt med deras uträkningsmodell är hur de kan analysera värdet för varje säkerhetsinvestering i en kontext inom deras IT-miljö. Modellen kan dessutom göras på varje del av IT-delen i organisationen, från hårdvara till medvetenhet bland anställda.

Anledningen till att de har tagit fram en specifik uträkningsmodell för deras organisation är för att de, som många andra inte alltid kan sätta säkerhetinvesteringar i förbindelse med ekonomi. Dessutom menar de på att detta kan bli problematiskt för organisationens olika delar som ekonomiavdelningen och IT-avdelningen. Meningen är att på ett tydligt sätt visa på hur säkerhetsinvesteringar påverkar så att en vanlig anställda skall förstå innebörden (Carty et al., 2012).

Vidare menar Carty et al. (2012) på att andra modeller utvärderar en investering i isolation, den tar alltså inte hänsyn till miljön den skall implementeras i, det vill säga att de redan befintliga säkerhetsåtgärderna. En investering kan när den utvärderas med dessa modeller visa på ett högt värde, och verkningsgrad, och då ge skenet av att vara en attraktiv investering. Det som glöms bort vid dessa typer av utvärderingar är faktumet att redan existerande säkerhetsåtgärder kan ha förmildrat stora delar av hoten. Därför bör en investering således utvärderas i den miljön den skall komma att implementeras i, och ta hänsyn till det ökade värdet den tillför de redan befintliga säkerhetsmekanismerna.



Figur 2.4 - Grafiskt exempel på "Bypass rate" (Carty et al., 2012)

Modellen utgår från att IT-säkerhet kan appliceras i form av olika säkerhetslager, där det yttersta lagret, "Governance & Personnel", består av bland annat säkerhetspolicys och medvetenhet, med målet att förhindra att hot tar sig in i datamiljön. Vidare görs det i modellen antagandet att ett intrång sker vid det första lagret, för att sedan på ett linjärt sätt arbeta sig vidare till nästa lager tills dess att intrånget avstyrs. Vid varje lager där det sedan tidigare finns implementerade säkerhetsåtgärder förhindras en viss procent av antalet attacker, samtidigt som en de resterande attackerna kringgår dessa säkerhetsåtgärder och således tar sig till nästa säkerhetslager. Procentantalet attacker som kringgår ett säkerhetslager utgör vad Intel har valt att kalla "Bypass rate" (Carty et al., 2012).

Den andel attacker som kringgår tidigare lager och då tar sig vidare till det innersta säkerhetslagret utgör den kvarstående risken, "Residual risk", vilken även den representeras i procent Målet med de säkerhetsinvesteringar som görs i respektive lager, är att minimera den kvarstående risken.

Vid användande av modellen krävs det först en analys av den befintliga miljön för att räkna på det befintliga värdet på, samt kostnadseffektiviteten av de redan implementerade säkerhetsmekanismerna. Informationen som utvinns av detta används som grund mot vilka de nya säkerhetsinvesteringarnas värde kan mäta sig mot (Carty et al., 2012).

Analysen i helhet består av sju steg, varav de tre första relaterar till analysen av den befintliga miljön, och de resterande fyra används för att utvärdera värdet av nya tänkta investeringar.

1. Effektivitetsbedömning av befintliga säkerhetsmekanismer
Effektivitetsgraden definieras i modellen som den procentsats av attacker som förhindras av de redan befintliga säkerhetsmekanismerna för varje respektive lager. Information som krävs för att göra denna bedömning kan enligt Intel hämtas antingen från befintlig data gällande detta, alternativt genom expertutlåtanden. Från denna effektivitetsgrad kan då bypass rate för varje lager härledas, samt den kvarstående risken (Carty et al., 2012).
Exempel. Om det yttersta lagret har en bypass rate på 70 %, och nästkommande lager har en effektivitetsgrad på 10 % blir således bypass rate för lager två 70 % x 90 %= 0.63 %.

2. Bestämning av den finansiella risken samt värdet av befintliga säkerhetsmekanismer
Nästa steg enligt modellen är att fastställa ekonomiska värden för riskerna samt de befintliga mekanismerna. Första delsteget innefattar en uppfattning av den finansiella förlusten en lyckad attack på informationstillgångarna skulle innebära för organisationen. I rapporten ger Intel exemplet att en attack skulle komma att innebära en finansiell förlust på en miljard dollar. Denna förlust fördelas sedan över olika hotkategorier, som exempelvis malware och social engineering. Givet historisk data kan 13 % av attackerna härledas till malware, vilket resulterar i att den finansiella förlusten som kan tillskrivas denna kategori är 130 miljoner dollar. Ur denna information, i kombination med bypass, rate går det att beräkna den finansiella risken som kvarstår efter att ett lager blivit förbigått, samt den totala kvarstående risken. Vidare går det då även att se vilket värde respektive lager tillför i ekonomiska termer, genom att jämföra den finansiella risken innan, samt efter ett säkerhetslager har förbigåtts.

3. Bedömning av kostnadseffektiviteten av befintliga säkerhetsmekanismer
Genom att använda sig av ett mätetal som Intel valt att kalla för en "multiplier" går det att mäta förmildrandet av en risk i förhållande till den investerade summan. Värdet beräknas för varje lager individuellt, och tar således ingen hänsyn till övriga säkerhetslager. Detta görs för att ge en mer realistisk uppfattning, som inte annars skulle vara möjlig då de inre lagren skulle visa på en lägre kostnadseffektivitet på grund av färre antal förmildrade risker, då många attacker redan förhindrats vid tidigare lager.

Vid beräkningen används effektivitetsgraden för respektive lager multiplicerat med den totala finansiella risken. Detta värde för de olika hotkategorierna summeras sedan över hela säkerhetslagret för att ge en total riskförmildring per lager. Vidare måste även den allokerade budgeten för varje säkerhetslager tas med i beräkningen. Ur detta går det att få fram mätetalet multiplier genom att subtrahera budgeten från värdet av riskförmildringen, och sedan dividera detta på budgeten. Genom att jämföra multiplier över olika lager, går det att se vilka lager som utgör de mest kostnadseffektiva.

4. Effektivitetsbedömning av nya investeringar
En uppdaterad effektivitetsbedömning görs av de som tidigare givit expertutlåtanden, som nu tar hänsyn till de föreslagna investeringarna.

5. Värdeberäkning av varje ny investering
Det finansiella värdet av de nya investeringarna mäts i hur stor utsträckningen den kvarstående risken har minskat. Vilket beräknas genom att subtrahera den nyuträknade kvarstående risken från den tidigare, detta blir den gradvis förmildrade risken som investeringen tillför.

6. Bedömning av kostnadseffektivitet för varje ny investering
Den gradvis förmildrade risken, det vill säga, differensen mellan de kvarstående riskerna används som grund i bedömningen av kostnadseffektiviteten gällande ny investering. Samma metod som används i steg tre används nu återigen, där värdet av riskförmildringen nu ersatts med den framräknade gradvis förmildrade risken. Återigen subtraheras budgeten från detta värde för att sedan divideras med budgeten och således resultera i en multiplier. Detta mätetal används precis som vid tidigare steg för att jämföra kostnadseffektiviteten mellan olika investeringar som berör IT-säkerhet.

7. *Sammanslagen utvärdering av effektivitet samt kostnadseffektivitet för tänka investeringar*
I många fall både vill, och krävs det att mer än en investering görs för att förmildra en risk. Med hjälp av tillvägagångssättet modellen erbjuder går det även att vid sekventiella investeringar mäta det värde de tillför. Att hypotetiskt implementera en investering resulterar i att det försvinner en viss mängd risk att behandla. Övriga investeringar kan exempelvis bidra med ytterligare värde då en tidigare kan ligga till grund, alternativt krävas för att maximera värdet av den nya. Att då återigen räkna på hur nästkommande investering tillför värde går det således att räkna på ett sammanslaget värde av alla tänkta investeringar sett ur ett säkerhetsperspektiv, men även ur ett ekonomiskt perspektiv (Carty et al., 2012).

2.2.4 Gordon & Loeb Modell

Forskarna Lawrence A. Gordon och Martin P. Loeb vid University of Maryland presenterar i artikeln The Economics of Information Security Investment (2002) en ekonomisk modell för att beräkna den optimala kostnaden att investera i åtgärder med målet att skydda en given informationstillgång. För att beräkna denna kostnad har författarna tagit hänsyn till sårbarheten associerad till denna informationstillgång, samt den potentiella monetära förlusten om ett säkerhetsintrång skulle komma att inträffa (Gordon & Loeb, 2002).

Modellen är tänkt att appliceras för de investeringar som görs med målet att skydda en informationstillgångs konfidentialitet, tillgång samt integritet. Att upprätthålla en hög grad av respektive byggnadsblock i C.I.A-triangeln simultant tenderar till att resultera i en konflikt. Även om en avvägning till stor del behövs göras för en lämplig säkerhetskontroll då de olika delarna i triangeln inkräktar på varandra, är detta någonting som författarna valt att exkludera och modellen således inte tar hänsyn till (Gordon & Loeb, 2002). Den modell de presenterar visar istället hur den optimala investeringskostnaden påverkas av sårbarheten gällande informationstillgångens sårbarhet samt den potentiellt tillkommande förlusten (Gordon & Loeb, 2002).

Enligt författarna karaktäriseras en informationstillgång av tre parametrar, λ, t samt v. Den monetära förlusten som ett säkerhetsintrång kan åsamka representeras av parametern λ. Denna förlust kan vara resultatet av ett intrång relaterat till informationstillgångens konfidentialitet, integritet samt tillgänglighet. Denna kostnad bör rimligtvis återspeglas i hur påverkade information används, och således borde den därför förändras över tid. Författarna har för att förenkla modellen, dock valt att representera förlusten som ett av organisationen uppskattat fast värde (Gordon & Loeb, 2002).

Ett försök till ett säkerhetsintrång noteras $t \in [0,1]$, och således representerar parametern t hotets sannolikhet.

Sårbarheten för en informationstillgång representeras av parametern v, och syftar då till sannolikheten utan den tilltänkta säkerhetsinvesteringen. Då v även det är en sannolikhet blir alltså $v \in [0,1]$.

För både sannolikheten samt sårbarheten gäller att de typiskt faller inom värdet $0<t<1$ samt $0<v<1$. Författarna menar på att en informationstillgång är totalt osårbar när $v = 0$. Likvärdigt blir således en informationstillgång totalt sårbar när $v = 1$.

Produkten av dessa tre parametrar, $vt\lambda$ representerar då sannolikheten att av att en förlust inträffar för en given informationstillgång. Givet det faktum att $t > 0$ således leder till att den uppskattade förlusten ökar i takt med en ökning av sårbarheten.

Författarna gör i sin artikel antagandet att även om en organisation kan investera i informationssäkerhet, har dessa investeringar en större påverkan över sårbarheten än själva hotnivån mot en informationstillgång, och väljer därför att fixera hotets sannolikhet till $t > 0$. Eftersom att sannolikheten nu hålls konstant definieras $L = t\lambda$, där L representerar förlusten, eller den potentiella förlusten för en viss informationstillgång (Gordon & Loeb, 2002).

Vidare skall parametern z representera den finansiella investeringen i en säkerhetsåtgärd för en informationstillgång under förhållandet $z > 0$. För att vara korrekt skall z anges och mätas i samma enhet som den potentiella förlusten L. Funktionen $S(z, v)$, som författarna valt att namnge funktionen för säkerhetsintrångssannolikhet, visar sannolikhet att ett intrång sker med sårbarheten v, under förhållandet att en organisation har investerat z för att skydda den informationen.

Gordon & Loeb gör ur denna information tre antaganden gällande information säkerhet ur funktionen $S(z, v)$:

Antagande 1.
$S(z, 0) = 0$ för alla värden av z. Informationstillgången är totalt osårbar oavsett kostnadsinvesteringen z värde.

Antagande 2.
$S(0, v) = v$ för alla värden av v. Med andra ord är sårbarheten v oförändrad om det inte existerar någon investering, och således är säkerhetsintrångssannolikheten enbart beroende informationstillgångens parameter v.

Antagande 3.
För alla värden av $v \in (0,1)$ och alla z är $Sz(z,v) < 0$ samt $Szz(z,v) > 0$. Där Sz syftar till den partiella derivatan med avseende till z, Szz betecknar den partiella derivatan av Szz med avseende till z. Detta leder enligt Gordon och Loeb (2002) till att en ökning i investering leder till att säkerheten ökar, men i en sjunkande takt.

Även om det enkelt kan antas att den optimala kostnaden för en investering bör öka linjärt följande en ökad potentiell förlust, samt en given hotnivå visar författarnas modell på att så inte alltid är fallet. Resultatet av Gordon och Loebs studie menar på att de optimala kostnaderna när det kommer till att skydda en viss informationstillgång inte alltid ökar i takt med sårbarheten. Vidare visar resultatet på att den optimala investeringskostnaden inte bör överstiga 37 % av den uppskattade förlusten vid ett säkerhetsintrång (Gordon & Loeb, 2002).

Mer säkerhet är således enligt Gordon och Loeb (2002) inte alltid värt kostnaden, samtidigt som en investering under en viss kostnad kan anses som en väl genomförd investering.

2.3 Investeringsstrategier för IT- och informationssäkerhet

I detta stycke presenteras olika investeringsstrategier som kan användas vid en IT- och informationssäkerhetsinvestering.

2.3.1 Proaktiva och reaktiva säkerhetsinvesteringar

Författararna Gallaher, Rowe, Rogozhin och Link (2006) menar på att säkerhetsinvesteringar kan delas upp i två olika kategorier beroende på typen av implementationsstrategi. Dessa kategorier är proaktiva eller reaktiva säkerhetsinvesteringar. Beroende på vad det är för säkerhetsinvestering och vad det bakomliggande syftet till säkerhetsinvesteringen faktiskt är, så faller en investering in under den proaktiva eller reaktiva kategorin. Till proaktiva investeringar faller de åtgärder som tillsätts i ett förbyggande syfte medan en reaktiv investering syftar till åtgärda en redan identifierad, och inträffad risk. Detta innebär dock inte att det ena utesluter det andra, Gallaher et al. menar på att en åtgärd som implementeras i ett proaktivt syfte kan övergå till att definieras som en reaktiv, i takt med att tekniken blivit etablerad, samt hur den används. Han ger exemplet att en person som anställs för att övervaka ett intrångssystem är en investering som faller under kategorin proaktiva åtgärder, men om personen i fråga enbart letar efter redan identifierade trender, räknas åtgärden som reaktiv (Gallaher et. al, 2006).

Beroende på vilken typ av implementationsstrategi en investering faller in under, återspeglas i den ekonomiska investeringen. Gallaher et al. (2006) menar vidare på att en den proaktiva strategin tenderar till att färre intrång faktiskt inträffar, medan en reaktiv strategi i vissa fall kan vara mer kostnadseffektiv (Gallaher et al., 2006).

Även om de leder till färre antal intrång, menar Qian, Fang och Gonzalez (2012) på att proaktiva investeringar gällande IT- och informationssäkerhet är svåra att motivera, och att det existerar en paradox. En investering i ett proaktivt syfte sänker både incidentsfrekvensen och påverkan av eventuella incidenter, vilket leder till att organisationer får en lägre riskuppfattning. Resultatet av detta blir således ett försvårande i att rättfärdiga en investering, *"Nobody ever gets credit for fixing problems that never happened"* (Qian et al., 2012, s. 868).

2.3.2 Kostandsminimerande samt säkerhetsmaximerande investeringsstrategier

Gallaher et al. (2006), menar på att organisationer kan använda sig av två olika typer av investeringsstrategier när det kommer till IT- och informationssäkerhet. Den ena beskrivs som *säkerhetsmaximerande,* där organisationer avsätter en viss del av IT-budgeten för just IT-säkerhet. Målet är att utifrån denna allokerade del utnyttja budgeten på så sätt att högsta möjliga säkerhetsnivå nås. Den andra typen av investeringsstrategi benämns som *kostnadsminimerande*, och syftar till att organisationer istället väljer att granska verksamheten, och utifrån detta avgöra vilken typ, samt nivå av säkerhet som anses vara behövlig för verksamheten, för att sedan ta fram den mest kostnadseffektiva lösningen. På detta sätt försöker organisationer således minimera kostnader samtidigt som de uppnår den önskade nivån av IT-säkerhet.

2.4 Bakomliggande faktorer till en investering inom IT- och informationssäkerhet

Enligt Kwon och Johnsson (2011), är de två främsta faktorerna för investering inom IT -och informationssäkerhet kundernas förtroende och statliga lagar som tvingar organisationer att meddela informationsägaren eller kunden ifall ett intrång har inträffat där information kan ha läckt. Större press sätts på organisationer att uppnå de lagar som finns, samt att ta den kostnad som det innefattar för organisationer att uppfylla kraven. Författarna menar på att detta skapar nya organisatoriska arbetsprocesser då det blir ett fokusområde för att reducera olika risker.

Ett problem är att organisationer fokuserar på IT- och informationssäkerhet och en stor del av investeringen för att skydda sig mot externa hot. Författarna menar på den interna skadan är minst lika stor som den externa (Kwon & Johnson, 2011).

Vidare har enligt Chai, Kim och Rao (2010) lagar gällande integritet och IT-säkerhet som exempelvis. Sarbanes-Oxley Act of 2002 lett till att organisationer verksamma i USA inte längre kan se IT- och informationssäkerhet som någonting valfritt. Det sätts nu press på organisationer att förbättra sin säkerhet, så att de kan uppfylla de krav lagarna nu ställer. Genom att implementera policys, och en säker IT-infrastruktur kan detta uppnås. Tack vare dessa regleringar sker nu en förändring inom organisationer där ledningen tvingas se på IT- och informationssäkerhet och skyddandet av sina informationstillgångar med nya ögon. Det handlar nu om att följa lagar, vilket således påverkar hur beslut kring säkerhetsinvesteringar fattas.

En studie genomförd av Campbell, Gordon, Loeb och Zhou (2003, enligt Chai et al., 2010) undersöker den ekonomiska effekten säkerhetsintrång haft på börsnoterade företag i USA när dessa intrång blivit omskrivna i nyhetstidningar. Inte helt oväntat visar studien på en negativ marknadspåverkan för organisationerna när känslig data var inblandat. Ytterligare en liknande studie genomförd av Yayla och Hu (2005, enligt Chai et al., 2010) undersöker hur säkerhetsintrång påverkar organisationer ekonomiskt, mer specifikt hur påverkan återspeglas i aktiekursen. Deras undersökning visar på att internetbaserade företag drabbas mer frekvent än de företag som inte i samma utsträckning förlitar sig på Internet för sin verksamhet. De företag som inkluderas i undersökningen visar en genomsnittlig minskning på 2.1% av marknadsvärdet två dagar efter att intrången blivit publik kännedom.

Många organisationer har med IT som hjälpmedel kommit att bli tätare sammankopplade med sina kunder och leverantörer (Al-Humaigani & Dunn, 2003). Denna sammankoppling leder till att känslig information hos en organisation delas med andra aktörer tack vare internet och andra delade nätverk (Öğut, Raghunathan & Menon, 2011). Al-Humaigani och Dunn (2003) menar vidare på att organisationer behöver bygga en pålitlig och effektiv IT-infrastruktur som levererar både affärsnytta samtidigt som den skall leverera en positiv ROI. Utöver detta skall infrastrukturen kunna stå mot ett ökande antal IT relaterade hot, vilket kräver ytterligare investeringar i form av IT- och informationssäkerhetsåtgärder. Dessa står inför problematiken att de skall balansera säkerhet samtidigt som det krävs att de tar hänsyn till affärskrav. Bakgrunden till säkerhetsinvesteringar hos många organisationer kan då kopplas till en allmännytta, samtidigt som det till viss del kan härledas till affärs- samt klient krav, vilket stärks av Gallaher et al. (2006) som i sin rapport visar resultat från en undersökning där 16.2% av de tillfrågade organisationerna hävdar att investeringar drivs av krav från klienter.

2.4.1 Guidelines och best practice

Dynes och Freeman (2007) menar i sin rapport *Cyber Security: Are Economic Incentives Adequate?* precis som flertalet andra författare att bakomliggande orsaker när det gäller IT- och informationssäkerhetsinvesteringar grundar sig i kundkrav, regleringar samt varumärkesskydd. Det som han även tar upp är att motivationen även kommer ifrån att implementera best practice lösningar för att skaffa sig ett grundskydd. Detta menar Dynes och Freeman (2007) är lösningar som kan härledas ur branschtidningar, industrier samt regleringar. Även Christian Locher (2005) talar om grundskydd som ett tillvägagångssätt för att implementera säkerhetslösningar. Locher (2005) talar om *BSI baseline protection* som ett sätt att uppnå en säkerhetsnivå inom organisationen som anses vara tillräcklig.

Enligt LeVaque (2006) används ”baseline security practices” för att förhindra eventuell informationsförlust för en relevant kostnad för organisationens storlek. Dock så menar Putvinski (2009) att en säkerhetslösning aldrig kommer vara 100 % pålitlig oavsett hur mycket det investeras på säkerhet. Vidare anser Putvinski (2009) att det som idag är säkerhetspolicys och riktlinjer är ett förskrivande krav. Att ha dessa förskrivna krav gör så att organisationer kan behålla sina kunder samt marknadsandelar. Genom att använda sig av det tillvägagångssättet kan organisationer skydda sina system från hot med hjälp av standardiserade säkerhetsåtgärder. Problematiken enligt Locher (2005) ligger i att modeller med standardiserade lösningar inte ligger i linje med den teknologiska utvecklingen, samt att de alltid ligger ett steg bakom de aktuella hoten som finns mot en organisation. Samtidigt som de skapar värde för de organisationer som väljer att implementera dessa lösningar finns det ytterligare problematik då de inte hjälper till att prioritera planeringen gällande säkerhetsåtgärder och inte tar några ekonomiska aspekter i beaktning (Locher, 2005).

Dirk Henze (2000) vid Federal Agency for Security in Information Technology, vilka är ansvariga för framtagandet och utgivandet av BSI menar å andra sidan att koncepten som återfinns i manualen för BSI baseline approach går att implementera både enkelt och ekonomiskt. De kostnader associerade med att implementera åtgärder för att uppnå säkerhetsgrunden anses vara en ”cost of doing business” just för att de grundar sig i branschstandarder samt regleringar, och således inte kräver några djupare konversationer med ledningen innan eventuell implementation (Dynes & Freeman, 2007).

3 Metod

Denna del skall representera det tillväga gångsätt som har tillämpats för förarbete, insamling och analys för vårt empiriska material. Jacobsens - Vad, hur och varför? – Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen (2002) har använts som utgångspunkt för vårt val av datainsamling. Anledning till att vi har valt denna bok är för att vi anser att den tillför god vägledning för hur empiriskt material skall se ut.

3.1 Metodval

Valet av metod kom att falla på en kvalitativ ansats, vilket stärks av Jacobsen (2002) som menar på att denna metod är lämpligast när forskaren ämnar att skapa mer klarhet gällande ett fenomen. Vidare anser vi att vår problemställning, som är explorativ, har styrt metodvalet mot just det kvalitativa då vi varit intresserade av att gå in på djupet samt få fram nyanserad data gällande ett fenomen. Jacobsen (2002) menar på att problemställningar av en undersökande karaktär kräver att metodvalet skall resultera i att många nyanser lyfts fram, vilket vanligtvis kräver ett fåtal enheter. Detta stärker ytterligare valet av metod då en kvantitativ ansats ämnar till att förstå omfattningen av ett visst fenomen (Jacobsen, 2002). Genom det kvalitativa metodvalet fick vi möjligheten att ställa öppnare frågor vilket kunnat främja diskussioner med intervjuobjekten, något som inte varit möjligt om en kvantitativ ansats hade tagits.

Eftersom att vi velat undersöka hur organisationer i praktiken arbetar med att utvärdera IT- och informationssäkerhetsinvesteringar var målet med våra intervjuer att samla in relevant data som ett underlag för vidare analys. För att minimera risken att den insamlade data blev svåranalyserad semi-strukturerades intervjuerna med hjälp av en intervjuhandledning hållande öppna frågor på de ämnen som skulle tas upp. Genom att strukturera intervjun på detta sätt tilläts vi hålla en öppen dialog där intervjuobjektets svar styrde frågornas ordningsföljd och samtalet föll sig mer naturligt.

3.2 Urval

Att intervjuer sker med rätt personer så att den insamlade data blir relevant, och tillgodoser god och riklig information, är av stor vikt för att undersökningen ska bli rättvis. Valet av personer speglar huruvida syftet med en empirisk undersökning faktiskt uppnås. Eftersom att syftet är att visa hur verkligheten faktiskt ser ut (Jacobsen, 2002) är valet av intervjuobjekt avgörande för att bidra med god forskning.

Urvalet begränsades till tre intervjuobjekt tillhörande tre olika organisationer. Samtliga organisationer har sitt huvudkontor i Skåne, men tillhör olika branscher. Vidare anses att en spridning av branschtillhörighet bidragit till en bredare tolkning av problemet, och ett resultat som inte begränsats till enbart en viss typ av bransch. Intervjuobjektens befattningar har varit av varierande grad, men samtliga har stor insikt i, och ansvar för just IT- och informationssäkerhet inom sin respektive organisation.

De tre organisationer som inkluderades i urvalet har bestått av följande: Candy People, Lunds Universitet Datacentral (LDC), samt en organisation som valt att förbli anonym.

Candy People är en organisation som utsätts för kraftig konkurrens från andra stora godisleverantörer. Med en aggressiv marknadsstrategi expanderar de fort på den globala marknaden. Organisationen besitter en mängd känslig information gällande avtal och expansionsstrategier som behöver skyddas. Carl Tennberg är IT-chef, men även ansvarig för många andra delar av organisationen, och delaktig i de flesta beslut som tas.

Lunds Universitets Datacentral (LDC) är IT-tjänsteleverantör som i huvudsak arbetar med Lunds Universitet. På begäran från kunder tillhandahåller LDC varierande tjänster, men ett av dess huvudområden är IT-säkerhet där Magnus Persson är IT-säkerhetskoordinator och arkitekt.

Den tredje organisationen arbetar med digital kommunikation, och utvecklar samt erbjuder kommunikationslösningar åt företag. De hanterar en stor mängd känslig information, och har av säkerhetsskäl valt att förbli anonyma. Den respondent som deltagit i undersökningen åt organisationens vägnar valde även denne att förbli anonym. Respondenten valde däremot att dela med sig av sin titel, Group Security Manager. Vidare är personen även Certified Information Systems Security Specialist.

Tabell 3.1 Sammanställning av urval

Företag	Bransch	Antal anställda	Omsättning	Roll
Candy People	Grossist- och detaljhandel	17 (2015)	170 miljoner (2015)	IT-chef Operativ chef
Lunds Universitet Datacentral	IT-tjänster	123 (2015)	157 miljoner (2014)	IT-säkerhetskoordinator
Anonym	Tillverkning & Industri	636 (2015)	1,6 miljarder (2015)	Group Security Manager/CISSP

3.3 Genomförande av intervju

Själva genomförandet av intervjuer har varierat mellan att bestå av fysiska intervjuer samt telefonintervjuer. Jacobsen (2002) menar på att det tycks vara enklare att få ett givet och öppet samtal vid en besöksintervju än vid en telefonintervju, vilket är något vi tagit hänsyn till när vi valde intervjuform med Lunds Universitet. Vidare anser Jacobsen (2002) att telefonintervjuer är något mer opersonliga än fysiska intervjuer, och att intervjuer av den senare sorten bidrar till att lättare skapa en öppenhjärtig stämning. Att vi trots detta valde att genomföra två intervjuer per telefon grundade sig i att respondenterna haft svårigheter att hitta tid för en fysisk intervju, och motiveras vidare med det faktum att det mellan oss och intervjuobjekten funnits en relation sedan tidigare, vilket minskade risken att intervjuer över telefon faktiskt skulle bli opersonliga. Den fysiska intervjun samt telefonintervjun med Candy People kom att spelas in för att senare transkriberas, och därefter skickas till intervjuobjekten. Den tredje intervjun, även den per telefon, kom inte att spelas in av hänsyn till dennes rätt till anonymitet. Däremot kom de anteckningar som fördes under samtalets gång att skickas till respondenten.

3.4 Intervjuguide

Den intervjuguide som användes vid den empiriska insamlingen utformades för att ta upp frågor som belyst vår frågeställning. Valet att använda sig av en intervjuguide för att tillföra en viss grad av struktur stärks av Jacobsen (2002), som menar på att en intervju utan struktur kan resultera i att viktiga ämnen glöms bort under intervjun. Vidare så kan däremot en intervju med för hög grad av struktur, med en i förväg serie frågor med fasta svarsalternativ, tendera till att röra sig bort från den kvalitativa ansatsens syfte. Med denna intervjuguide tilläts vi hålla en öppen intervju samtidigt som vi säkerställde att de ämnen vi velat belysa kommit att tas upp (Jacobsen, 2002).

Vid utformning av intervjuguiden försökte vi att ställa öppna frågor för att tillåta intervjuobjekten få fram vad denne anser vara av vikt, samt dennes beskrivningar av det fenomen vi undersökt, vilket ligger i linje med hur Jacobsen (2002) ser på hur en öppen intervju bör utformas. Jacobsen (2002) belyser vikten av tillit vid en intervju, därför valde vi att inleda den fysiska intervjun genom att ställa frågor som bidrog till en avslappnad stämning för att bygga upp en grad av tillit. De objekt som intervjuades per telefon fanns det en relation till sedan tidigare, och tilliten fanns således även den där sen tidigare. Detta gjorde att de intervjuer gick aningen mer direkt på de frågor som vi planerade att ta upp. Vidare har dessa frågor inte haft någon fast följdordning, utan togs upp i den ordning som föll sig naturligt för samtalet och objektet.

Fokus under intervjuerna var att undersöka hur organisationer utvärderar sina IT- och informationssäkerhetsinvesteringar, om det används modeller för att göra detta, samt vad det är som motiverar organisationer att göra den här typen av investering. De frågor användes som grund vid intervjun kom därför att kretsa kring den tidigare presenterade litteraturen:

- Utvärderingsmodeller och modellanvändning
- Bakomliggande orsaker och investeringsstrategier

Den kompletta intervjuguiden återfinns i sin helhet under Bilaga 1.

3.5 Analys av intervjuer

Analysprocessen av den empiriska insamlingen består enligt Jacobsen (2002) av tre delar; *beskrivning, systematisering och kategorisering* samt *kombination.*

Beskrivning av den insamlade data från de två intervjuer som spelats in har skett i form av transkribering. På detta sätt säkerställdes att informationen kunnat återges i sin helhet på ett ofärgat sätt. Gällande den intervju vars respondent valt att förbli anonym har beskrivningen återgetts i form av anteckningar som togs direkt under intervjutillfället då denne föredragit att inte spelas in. Det antecknade materialet har sedan mailats till respondenten på dennes begäran.

Under *systematiserings- och kategoriseringsfasen* har vi behandlat de olika transkriberingarna samt det antecknade materialet för att strukturera upp detta. Detta resulterade i tre kategorier, *Modeller och modellmedvetenhet, Drivande anledningar och incitament till investeringar* samt *Utvärdering av investeringar*. Med hjälp av dessa kategorier har vi kunnat samla, jämföra och presentera den insamlade informationen på ett tydligt sätt, samtidigt som oväsentlig information har sållats bort.

Vi har under *kombinationsfasen* valt att använda oss av citat för att försöka belysa skillnader och likheter mellan olika de olika respondenterna. Vid de intervjuer som transkriberats har vi kunnat använda oss av direkt citat. När det gäller den intervju som inte transkriberats har vi valt att istället ta oss en viss frihet att referera till innehållet eftersom dessa anteckningar inte är ordagranna.

3.6 Undersökningskvalitet

3.6.1 Validitet

En undersöknings validitet kan enligt Jacobsen (2002) delas upp i två kategorier; *intern-* och *extern* validitet. Den *interna* validiteten syftar till att en beskrivning som flera personer kan enas över att den är korrekt, är det närmsta vi kan komma sanningen. För att pröva undersökningens interna validitet har vi låtit intervju objekten ta del av de slutsatser som dragits ur undersökningarna. Detta har låtit oss undersöka huruvida de känt igen sig i resultaten som presenterats. Den här typen av validering, vilket enligt Jacobsen (2002) är ett vanligt tillvägagångssätt, låter de enskilda intervjuobjekten ge sin syn på innehållet oberoende av varandra.

Den externa validiteten syftar till huruvida undersökningens resultat från ett område även kan komma att sträcka sig till att gälla vid andra. Det är svårt att utifrån undersökningen generalisera resultatet eftersom att den enbart tar tre organisationer, och intervjuobjekts åsikter i beaktning. Samtidigt tycker vi oss, trots det begränsade urvalet, kunnat se likheter mellan dessa organisationer.

3.6.2 Reliabilitet

Jacobsen (2002) menar på att i stort sett alla undersökningar utsätter respondenten för diverse signaler och stimuli som skapar en reaktion hos den som blir undersökt, och således även ger en effekt på utfallet. Det blir därför viktigt att kritiskt granska resultaten för att säkerställa reliabiliteten.

För att minska den eventuella effekt vårt klädval samt sätt att tala skulle kunnat ha på respondenten, valde vi att under intervjun klä oss relativt avslappat för att inte komma överklädda i förhållande till personalen på arbetsplatsen. Vidare kände vi av den rådande stämningen och anpassade både tempo och ordval efter respondenten för att ytterligare minimera risken för vad Jacobsen (2002) benämner som undersökareffekt.

Vidare behöver kontexten intervjun skall genomföras i tas i beaktning. Jacobsen (2002) menar på att människor tenderar till att anpassa sitt beteende efter de rådande omgivningarna. Med det i åtanke valde vi att genomföra den fysiska intervjun i ett konferensrum på intervjuobjektets arbetsplats. Detta för att hålla intervjun på en plats som respondenten besöker dagligen, det vill säga i ett naturligt sammanhang för att således minska risken att omgivningen skulle komma att ha en effekt på intervjuns resultat.

För att inte låta uppmärksamhet hos intervjuaren påverka datainsamlingen, och således sänka trovärdigheten krävs det att informationen registreras på ett korrekt sätt. För att kunna få ut all relevant information valde vi att spela in två av tre intervjuer för att vid senare tillfälle både kunna gå tillbaka, men även återge intervjuerna i sin helhet. Däremot var vi under den tredje intervjun, med hänsyn till respondenten, tvungna att avstå från att spela in och då istället anteckna informationen. Detta ger svårigheter för intressenter att i efterhand kontrollera den nedtecknade informationen. För att på bästa sätt gardera oss mot att den antecknade informationen skulle komma att uppfattas som mindre tillförlitlig skickades en kopia på dessa anteckningar direkt till respondenten via e-post.

3.7 Etiska aspekter

För att en undvika att det vid en undersökning uppstår etiska dilemman, understryker Jacobsen (2002) att tre grundkrav; *informerat samtycke, krav på privatliv* och *krav att bli korrekt återgiven* skall uppfyllas.

Samtliga respondenter informerades om huvudsyftet med undersökningen samt hur resultatet skulle komma att användas. Vidare har samtliga respondenter kontaktats personligen för att diskutera hur deras organisation ser på problemet i fråga, detta har tillåtit respondenterna att själva ta beslutet över huruvida de har velat delta eller inte. Påtryckningar från exempelvis chefer har alltså inte varit aktuellt. Att samtliga respondenter deltagit av egen vilja när syftet med undersökningen varit känt, bidrar till att höja undersökningskvaliteten.

Vidare har våra intervjuobjekt deltagit i undersökningen och svarat utifrån organisationen denne jobbar på, vilket har minimerat andelen privat information som har samlats in under intervjun. Med detta i åtanke har då istället rätten till privatliv kretsat kring organisationens rätt att behålla information privat. Det kan vid den här typen av insamling samlas in information

som antingen organisationen, eller intervjuobjektet, kunnat tänkas vela hålla utanför datainsamlingen. Samtliga respondenter har blivit tillfrågade huruvida de velat vara anonyma i både undersökning och presentation av resultat för att påvisa att vi respekterar denna rätt. Enbart en respondent har som tidigare nänts valt att hålla både sin identitet, och organisation anonym.

Samtliga intervjuer har antingen transkriberats, eller antecknats för att sedan placeras som bilagor i denna uppsats. Denna dokumentation har förmedlats till respektive respondent för att stärka att den information som återges är korrekt, och inte tagen ur sitt sammanhang. Givet detta så tillåts inspelade intervjuer att återfinnas i sin helhet, samt att antecknat material återfinns efter godkännande av respondent.

Givet ovanstående information har alltså hänsyn tagits till intervjuobjekten för att uppfylla Jacobsens (2002) grundkrav för undersökningar i syfte undvika att etiska dilemman uppstår.

4 Resultat

I denna del av uppsatsen kommer resultatet av den empiriska undersökningen att presenteras. Resultatet kommer att redovisas under följande rubriker: Drivande anledningar och incitament till investeringar, Modeller och modellmedvetenhet samt Utvärdering av investeringar.

4.1 Drivande anledningar och incitament till investeringar

Hos Candy People så görs investeringarna inom IT- och informationssäkerhet främst av anledningen att de vill skydda sig från alla andra, och således skydda den information som verksamheten innehar. Företaget besitter i sin ägo många avtal med kunder och tillverkare vilket enligt Carl skulle vara *”bära eller brista om de försvinner eller kommer ut”* (Bilaga 3, Rad 143). Detta gör att IT- och informationssäkerhet är någonting som Carl värdesätter väldigt högt, och därför prioriterar. *”Jag ser att det är viktigt. Men jag ser att det är en kostnad också”* (Bilaga 3, Rad 117-118). Samtidigt understryker Carl att vad det är man vill skydda för något spelar in *“[...] då kan man skydda och lägga hur mycket som helst på för att man inte vill att det ska komma ut”* (Bilaga 3, rad 146-147).

Vidare anser Carl att Candy People i den mån det går försöker ha ett proaktivt tänk gällande investeringar i IT- och informationssäkerhet, men att det är en kostnad som är svår att motivera.

> *”Oftast är det såhär att du inte vet att det lönar sig förrän det är någon som tar sig in, det är då du vet att det lönar sig. Till dess är det en kostnad inget företag vill ta. Den enda gången de förstår det är när de får ett virus.”*
>
> (Bilaga 3, rad 53-55)

Som exempel på detta så berättar Carl att Candy People blev offer för ett så kallat ransomware. Ett intrång som ledde till att organisationen var tvungen att stänga ner i nästan 12 timmar vilket i sin tur resulterar i höga kostnader. Efter den incidenten var det inte längre någon tvekan kring en tänkt investering, *”[...] och när viruset kom sa dem kör”* (Bilaga 3, rad 199). Carl menar vidare på att det var en dyr kostnad som fick dem faktiskt aktualisera en investering, *”Det är då folk förstår att man måste lägga pengar på det”* (Bilaga 3, Rad 85-86).

Precis som att det hos Candy People till stora delar är ett reaktivt förhållningssätt till risker, gäller detta även hos LDC. *”Men vi försöker vara proaktiva där vi kan”* (Bilaga 2, rad 343-344). *”Så där vi vet att det åtminstone finns lågt hängande frukost som de är ute efter så försöker vi ta det innan det händer någonting”* (Bilaga 2, Rad 336-337). Problematiken gällande ett proaktivt tänkande kring investeringar för IT- och informationssäkerhet är enligt Magnus kostnaden för åtgärderna. *”[...] Vi skulle kunna lösa det här på ett par sätt. Men det skulle bli alldeles för dyrt”* (Bilaga 2, Rad 515).

Däremot menar Magnus att den främsta anledningen till att det investeras i säkerhet hos LDC är när Myndigheten för samhällsskydd och beredskap *”kommer och slår oss på fingrarna och*

säger att vi måste göra något" (Bilaga 2, Rad 693). Det är således alltså krav från myndigheter som till stor del avgör i vilken utsträckning, och i vilka säkerhetsåtgärder det skall investeras i. *"MSB [Myndigheten för samhällsskydd och beredskap] kom ju och sa att ni måste arbeta enligt ISO 27000. All right, då måste vi göra det."*(Bilaga 2, Rad 695-696). Att arbeta enligt ISO 27000 som LDC tvingas göra, resulterar i att investeringar sker för att följa den best practice som MSB talat om för dem att göra. I och med att den befintliga personuppgiftslagen inom kort kommer att ersättas av en ny EU-förordning om dataskydd menar Magnus på att den drivande anledningen till att ytterligare investeringar i IT- och informationssäkerhet blir rent ekonomiska. "*Och i och med det så är det ju inte längre bara en smäll på fingrarna vi får, utan då är det ju böter."* (Bilaga 2, rad 720-721). Det är alltså inte längre enbart en säkerhetsfråga för LDC, utan även en ledningsfråga. Det är först när det en ledningsfråga som det enligt Magnus får börja kosta pengar att göra investeringar gällande IT- och informationssäkerhet.

Vår anonyma respondent menar på att investeringar i IT- och informationssäkerhet görs när det identifierats ett behov från kunder eller marknaden. Att inte tillhandahålla en viss typ av säkerhetsåtgärd kan resultera att de kraven som kunder ställer inte uppfylls. De tillfällen när det är ett fåtal kunder som ställer krav kan enligt respondenten räddas genom att se det hela ur ett affärsmässigt perspektiv. Denne menar på att om man är duktig och affärsorienterad kan man köpa något inte många kunder har som krav, och sedan erbjuda det som en tjänst. Respondenten menar på att erbjuda någonting som en förlust till början kan med tid, och i ett ökat antal kunder, generera vinst i framtiden. Därför kanske de inte alltid väljer den lösning som är bäst, men tar den med bra funktionalitet och licensmodell så att de kan signa den till kunder.

Däremot anser respondenten att det bör vara ett reaktivt tänk gällande IT- och informationssäkerhet hos verksamheter överlag, och att en säkerhetschef inte kan eller ska säga vad som behövs. Utan understryker att det snarare kommer som ett incidentkrav på grund av att någonting har hänt, och menar vidare på att det är krav från marknaden eller regleringskrav som ställs på branschen. Det är alltså kund- och branschkrav som löser säkerhets- och affärsrisker som avgör när vår anonyma respondents organisation väljer att investera i IT- och informationssäkerhet. Samtidigt talar respondenten om att mognadsgraden hos ett företag spelar in på huruvida en proaktivt eller reaktiv angreppsätt skall finnas inom organisationen. Denne menar på att det många gånger gå att få en bra lösning till ett bra pris med låg implementeringstid, men att företaget inte är redo för det med hänsyn till infrastruktur, kunskap och annat, att de nödvändiga processer som krävs inte finns inom verksamheten.

En viss typ av investeringar i IT- och informationssäkerhet kan vara funktionalitet och kontroller som alla förväntas att ha, och menar att de är ett basbehov. När det gäller exempelvis en brandvägg, så ses det inte längre som en säkerhetskontroll, och menar att detta nu är grundfunktionalitet. Vidare understryker respondenten att en del investeringar som görs gällande säkerhet har blivit en de facto-standard.

4.2 Modeller och modellmedvetenhet

Den befintliga litteraturen på ämnet visar på att det för investeringar inom IT- och informationssäkerhet finns välarbetade modeller gällande den ekonomiska uträkningen, men även gällande den optimala kostnadsnivån för en investering av just den här typen.

Carl på Candy People var medveten, eller kände i alla fall till Intels modell för hur man i förväg kan räkna på hur en säkerhetsinvestering kan bidra till en organisation i ett värdeskapande syfte. En modell som binder samman delar av ROI för att sedan sätta tänkta åtgärder i en rätt kontext. Även om medvetenheten kring modellen finns hos organisationen är det fortfarande ingenting som används eller räknas på. Candy People har gått från att tidigare hantera all sin egen IT inom organisationen, men efter ett säkerhetsintrång 2010 gått över till att outsourca IT-driften till en partner. Det tidigare valet av lösning involverade kostnader för underhåll av denna infrastruktur. Den typen av kostnader som en verksamhet dras med på när det kommer till egen IT-drift fanns tillgängliga inom verksamheten. Så enligt Carl var valet enkelt när de med hjälp av en partner kunde få en högre säkerhetsnivå till en kostnad som var ungefär densamma.

När det kommer till deras nuvarande lösning görs antagandet att kostnadsuträkningar från görs hos den partner Candy People valt att använda sig av.

> *”Så här fungerar det, jag säger till våra outsource partners. Ja vi behöver det här, eller så säger jag vi har problem med det här, hur kan ni lösa det? Vad är lösningen. Och sen presenterar de vilka lösningar och vilka, vad de lösningarna er oss sen tar vi ett beslut efter och implementerar dem”*
>
> (Bilaga 3, Rad 40-43).

Tidigare har Candy People gått enligt strategin att alltid implementera det som varit den lösning som varit billigast. Problematiken kring att göra investeringar av den här karaktären ligger i svårigheten att mäta lönsamheten i en säkerhetsinvestering. Att kostnader av den här typen är ingenting organisationer vill spendera pengar på då den ses som en onödig kostnad.

För LDC ser situationen gällande modellanvändandet annorlunda ut. LDC är en statlig myndighet vilket innebär att inköp sker med hjälp av offentliga upphandlingar. Resultatet av detta, när det kommer till användning av modeller, innebär att det som skall inhandlas är det vars pris är det lägsta. Det enda som i förväg kan gå att påverka gällande investeringen är kraven på vad som skall upphandlas. *”Förutsatt att det är uppfyller de kraven vi har, och är det flera som uppfyller kraven måste vi ta det billigaste”* (Bilaga 2, Rad 121-122). Enligt Magnus ligger svårigheter kring användande av modeller hos LDC i problematiken att de inte vet vad de kommer att få för någonting, och då till skillnad från privata företag och organisationer inte kan räkna hem investeringar i förväg.

Hos vår anonyma respondent finns medvetenhet kring modellen ROSI för beräkning av IT- och informationssäkerhetsinvesteringar. Detta är däremot ingenting organisationen använder sig av. De försöker räkna på vad kostnaden kommer att bli för en investering, och hur den kan fördelas över tid. Enligt respondenten använder de sig av intäktsformen när de räknar på en investering, och menar på att försöker att investera i sådant som de sedan kan sälja vidare. Denne menar på att om de köper något som kostar en viss summa räknas det på kostnader. Vad kostar det, vad kan de sälja det för? Vad är mellanskillnaden - d.v.s. vad kan de tjäna. Enligt respondenten skall IT- och informationssäkerhet ses som en IT-fråga, något som bidrar till svårigheter med analyser, då säkerhetschefer och de som kan tekniken inte är några affärs-

människor och då inte innehar den kunskap som krävs. Vidare uttryckte respondenten missnöje med modeller som ROSI för att räkna på investeringar gällande säkerhet, och gick själv i tankar om att definiera en metodik som är mer affärsorienterad, och menar på att stor del av de som sysslar med säkerhet inte har någon affärsbakgrund, och istället fastnar i ett tekniskt tänk.

4.3 Utvärdering av investeringar

Hos Candy People har de inte sedan de 2010 gick över till sin outsource partner inte haft ett enda intrång, eller problem. Carl berättar att *”oavsett vilken IT-lösning vi har valt inom säkerhet eller inte, så har det lönat sig”* (Bilaga 3, Rad 124-125)

Vid frågan gällande huruvida det är ren funktionalitet, d.v.s. säkerhet som ska utvärderas för att en investering skall klassas som bra eller lyckad svarar Carl *”Exakt, det är ju framför allt säkerheten, den är högst prioriterad”* (Bilaga 3, Rad 135). Samtidigt understryks det hur organisationens arbete påverkas vid en investering bidrar till vad som är viktigt, och en investeringsåtgärd som skulle ta tid av någon aldrig skulle bli realitet, *”Det är dubbla kostnader”* (Bilaga 3, Rad 161).

När det kommer till rapportering gällande IT- och informationssäkerhet hos LDC sker rapportering upp till högre instanser enligt Magnus lite i den omfattning som de vill ha. Men menar på att hur det faktiska arbetet sköts *”Det är lite upp till oss”* (Bilaga 2, Rad 627). Mycket understryker Magnus handlar om *”[...]best effort, och vad vi kan göra med de resurser vi har”* (Bilaga 2, Rad 630). Han ger exempel på när nättrafiken varit överbelastad och av säkerhetsskäl krävde någon form av åtgärd. De kunde ha spenderat 100 000 kr för att behandla problemet, eller istället göra det själva. Det faktum att Magnus har ganska fri styrning över sin arbetstid resulterade i att han istället för att lägga pengar på problemet kunde hantera det själv med hjälp av sin egen kunskap. *”[...]med en halv veckas jobb kanske, och begagnad hårdvara - kostade oss inte ett skit, att med lite arbete ta bort två tredjedelar av trafiken på nätet. Det är lyckat”* (Bilaga 2, Rad 603-605). Devisen tycks således vara att investeringar klassas som lyckade när de uppfyller någonting till minsta möjliga kostnad.

Hos det anonyma företaget menar respondenten att investeringar som sagt sker på grund av krav från kunder, från branschen i sig, eller som ett resultat av regler. Att investeringar kan tillskrivas som lyckade anser respondenten är när dessa krav faktiskt uppfylls. Men att de kan tillskrivas som lyckade ur ett ekonomiskt perspektiv menar respondenten är svårt, och understryker att när organisationer köpt sådana lösningar är de dåliga på att göra en efteranalys. Utifrån egen erfarenhet talar respondenten om att det är svårt, och att företag alltså inte gör det. Samtidigt understryks det att man genom deras tillvägagångssätt, att erbjuda lösningar som tjänster för sina kunder, kan gardera sig mot detta. Genom att välja en licensmodell där man inte köper för mycket utan exakt vad man behöver så att man går +/- 0 kan de ta en kostnad ut mot kund som gör att de har ett system som lönar sig. Vidare menar respondenten att denne är intresserad av att årligen göra återkopplingar på investeringar för att se arbetsnyttan de bidrar till, och anser att om faktum skulle vara så att de inte bidrar till lönsamhet bör avvecklas.

5 Diskussion

Under detta kapitel kommer det tidigare presenterade empiriska resultatet att diskuteras vidare och knytas an till den teori som lyfts fram tidigare i uppsatsen.

5.1 Incitament och bakomliggande faktorer

De drivande anledningarna till IT- och informationssäkerhetsinvesteringar hos de undersökta företagen ligger i linje med vad Kwon och Johnson (2011), Gallaher et al. (2006) samt Al-Humanigani och Dunn (2003) beskriver som de främsta incitamenten. Att organisationer investerar i dessa åtgärder i syfte att upprätthålla lagar samt kund-, affärs- och branschkrav. Dessa anledningar tycks ligga som argument för att en investering i slutändan skall komma att genomföras.

Det är dock enbart hos ett av de undersökta företagen som det tycks finnas krav om att en investering av den här kategorin skall resultera i ett finansiellt värde. Det är alltså enbart hos den organisationen som det i förväg räknas på huruvida det går att ekonomiskt rättfärdiga investeringen. Däremot tycks inte de modeller som presenterats tidigare i uppsatsen användas som grund för hur lönsamheten på en ~~ en~~ investering kan beräknas, utan istället räknar de på den initiala kostnaden för åtgärden, och hur ett pris skall sättas när denna åtgärd sedan kan säljas som en tjänst till organisationens kunder.

Samtidigt är det hos de övriga organisationerna ekonomiska faktorer som spelar in till att investeringen görs, att ett undvikande av investeringen istället kan komma att resultera i ekonomiska förluster. Ett misslyckande att uppfylla lagkrav kan sluta i att organisationer blir bötesskyldiga, och att ignorera en investering kan resultera i organisationer går miste om sina kunder.

Det gemensamma för samtliga undersökta organisationer kan alltså ses vara att investeringarna till skillnad från litteraturen, där syftet anses vara att skydda sina informationstillgångar och således undvika en ekonomisk förlust, istället görs för att undvika ekonomiska förluster i form av böter eller förlorade kunder då krav inte uppnås. Den sorts lönsamhet som litteratur och modeller talar om tycks alltså inte mätas hos de undersökta organisationerna.

5.2 Investeringsstrategier

Precis som Gallaher et al. (2006) nämner så visar vår empiriska undersökning på att de olika organisationerna förhåller sig till olika typer av investeringsstrategier. Dessa val av investeringsstrategier kan tyckas grunda sig i de olika incitament som faktiskt driver investeringarna, men även i vilka byggnadsblock av C.I.A-triangeln organisationer tenderar att prioritera (Dhillon, 2006).

I LDCs fall så är det regleringar som sätter press på IT- och informationssäkerheten, då i form av guidelines och best practice enligt MSB. Resultaten pekar på att LDC följer Gallaher et al.

(2006) linje genom att försöka maximera säkerheten i förhållande till en begränsad budget. Att investeringar som följer best practice och guidelines tycks vara en cost of doing business (Dynes & Freeman, 2007) kan motivera en bristande utvärdering gällande investeringens tänkta lönsamhet.

Hos Candy People är det andra krafter som driver investeringar för IT- och informationssäkerhet, att en förlust av information kan avgöra huruvida det bär eller brister för organisationen. Denna typ av incitament tycks leda just Candy People närmare kostnadsminimerande strategi, där organisationen granskas, och en lämplig säkerhetsnivå bestäms som det sedan investeras i för att uppnå. Att anta en investeringsstrategi som drar åt det kostnadsminimerande hållet tycks stärka viljan att anta ett proaktivt förhållningssätt gentemot IT- och informationssäkerhet. Men precis som Qian et al. (2012) nämner, så tycks det även i praktiken råda en paradox, då investeringar av proaktiv karaktär blir svårmotiverade på grund av svårigheter att i förväg påvisa investeringens lönsamhet.

Oavsett vilka incitament som organisationerna har för en investering, och vilken typ av investeringsstrategi som antas, tordes det finnas ett behov av att utvärdera sina investeringar. Att göra detta kan ge organisationerna en fingervisning över vad en investering returnerar, och hjälpa dem avgöra om de kanske antingen över- eller underinvesterat när det kommer till IT- och informationssäkerhet.

5.3 Utvärdering av investeringsstrategier

Den empiriska undersökningen visar på att uppföljning av gjorda investeringar hos de undersökta företagen är bristande. Varken kostnader för den gjorda investeringen eller lönsamheten utvärderas i efterhand. Modeller som presenterats tidigare används alltså varken att i förväg räkna på huruvida en investering kan bli en lönsam sådan, och inte heller i efterhand för att följa upp.

Att den här typen av utvärdering med hjälp av tidigare presenterade modeller faktiskt inte används hos de undersökta organisationerna är vid eftertanke inte särskilt märkvärdigt. Det finns alltså hos våra respondenter en viss modellmedvetenhet. Men att dessa teoretiska modeller inte används i praktiken kan bero på den överdrivenhet och komplexitet som de innefattar. Däremot kan det tyckas att dessa organisationer bör intressera sig av att tillämpa de modeller som presenterats för att ge något form av värde på om en investering kan komma att bli lönsam. Även om det kan tyckas att de bakomliggande faktorerna som driver investeringar hos organisationerna inte riktigt går hand i hand när de sätts i relation till hur litteraturen utvärderar lönsamheten av en säkerhetsinvestering, kan detta ge en fingervisning. Investeringar görs hos de undersökta organisationerna för att undvika ekonomiska förluster i form av böter och förlorade kunder. Att använda sig av de modeller som litteraturen förespråkar riktar sig således inte mot samma sak. En beräkning av lönsamhet enligt ROSI talar för huruvida en investering kommer att bli lönsam i förhållande till att en risk inte realiseras.

Att utvärdera investeringar enligt dessa modeller när det hos samtliga företag tycks råda koncensus att investeringar utvärderas som lyckade när de bakomliggande drivande kraven uppfylls, nämligen kundkrav och regleringar, kan då anses vara motsägelsefullt.

Vår uppfattning är att utvärdering hos de undersökta organisationerna alltså verkas göra i form av funktionalitetseffektivitet. Om de bakomliggande kraven som driver investeringarna uppfylls, och att en eventuell informationsförlust förhindras så tycks investeringarna utvärderas som positiva. De teoretiska modeller att antingen utvärdera, eller avgöra den optimala investeringskostnaden, som litteraturen presenterar tycks alltså inte att användas.

När det gäller en investerings lönsamhet kan Gordon och Loebs modell anpassad för den optimala investeringsnivån användas som ett hjälpmedel för att i den mån som det går att försöka garantera att en investering kan anses bli lönsam. Problematiken kan tänkas ligga i svårigheten att kvantifiera informationstillgångarnas värde, men modellen ger en fingervisning om vad som kan sägas vara en rimlig kostnad att investera för att skydda en viss informationstillgång snarare än att mäta i vilken utsträckning en investering är lönsam.

6 Slutsats

Forskningsfrågan som presenterades i början av uppsatsen var:

- *Hur utvärderas IT-säkerhetsinvesteringar, vilka modeller och metoder använder sig organisationer av för att göra detta?*

Vår empiriska undersökning visar på att utvärdering av IT- och informationssäkerhetsinvesteringar hos de undersökta organisationerna är bristande. Detta gäller speciellt när det kommer till utvärdering ur ett ekonomiskt perspektiv. Ingen av de undersökta organisationerna tycktes vara intresserade av att räkna ut lönsamheten av gjorda investeringar.

De teoretiska modeller som presenterats för utvärdering av IT- och säkerhetsinvesteringar användes inte av de undersökta företagen. Det tycks alltså inte göras några utvärderingar gällande huruvida en investering av den här typen kommer att bli, eller har varit lönsam. Den utvärdering som verkas göra tycks baseras på huruvida de bakomliggande orsakerna till investeringen uppfylls. Detta tycks alltså avgöra huruvida investeringen anses vara lyckad eller ej.

Modeller som presenterats skulle även kunna komma att användas i efterhand då en investering redan är gjord för att undersöka dess lönsamhet. Men att detta inte görs kan komma att bero på de olika drivande anledningarna som finns gällande investeringarna. Då en del säkerhetsåtgärder tillhör best practice och andra anses vara baskrav, så tycks organisationerna vara beredda att ta den kostnaden utan någon egentlig ekonomisk uppföljning. Om de drivande åtgärderna grundar sig i ett undvikande av en ekonomisk förlust, borde det rimligtvis krävas en ekonomisk analys i efterhand för att se om det varit en investering väl gjord.

Att en uppföljning inte görs, eller tycks krävas av organisationen kan anses vara något märkligt eftersom att de då inte får ett kvitto på den ekonomiska effekten investeringen bidragit till. Organisationerna får som ett resultat av detta aldrig reda på om dem faktiskt över- eller underinvesterar i IT- och informationssäkerhet.

6.1 Förslag till vidare forskning

Med ovanstående som slutsats ser vi ett antal frågor som kan komma att användas som underlag för framtida forskning inom området. Den bristande ekonomiska utvärderingen tordes återspeglas i organisationernas ekonomi, och då att de spenderar ekonomiska tillgångar på något de inte vet huruvida det kommer att löna sig, eller om det i efterhand varit en lönsam investering. 1. Vad får då den bristande utvärderingen och uppföljningen för konsekvenser på organisationerna? 2. Hur kommer det sig att organisationer väljer att inte göra ekonomiska efteranalyser på investeringar av den här typen?

7 Bilagor

7.1 Bilaga 1 – Intervjuguide

1. Roll i företaget
2. Känner du till något av ROI, ROSI, Intel IT Security Model eller Gordon & Loeb?
3. Hur tänker ni angående IT- och informationssäkerhet i er organisation?
4. När var det senast ni investerade i IT- och informationssäkerhet? Och vad gjorde ni då? Använde ni er av någon modell?
5. Hur ser processen ut från att behovet uppstår tills det genomförs?
6. Hur stor del av er budget estimerar du till säkerhet?
7. Utvärderar ni er investering i efterhand? Har ni någonsin gjort det? Hur kan en sån utvärdering då se ut? Och varför just den metoden isåfall?
8. Hur värderar ni vad som är en lyckad investering inom IT- och informationssäkerhet?
9. Kräver ni en processförbättring - ska arbetsbördan bli smidigare medhjälp av investeringen.
10. Väntar ni tills att ett hot har realiserats för att sedan åtgärda det, eller är ni mer proaktiva?
11. Vad driver eller motiverar IT- och informationssäkerhetsinvesteringar? (kundkrav, regleringar osv)
12. Hur försöker ni uppskatta avkastning på er IT- och informationssäkerhetsinvesteringar?

7.2 Bilaga 2 – Transkribering Lunds universitet LDC

Företag: Lunds universitet, LDC

Titel: IT-säkerhetskoordinator

Plats och datum: Lund. Tisdag 26 april 2016, 15.30–17.00.

Längd: 90 minuter.

D & O = Dennis och Omid, intervjuare

M = Magnus, respondent

- Här inleds intervjun

M - Det är väldigt olika, alltså det är både högt och lågt. Från institutioner som är små och kanske har forskare som jobbar halvtid, och lite IT-support. Till dem som har mer personal per anställd, eller där vi kan ge då.
D - Mm.
M - En del som gått samman är ju, liksom, grupperingar som HRT till exempel, data [OHÖRBART] gruppen på LTH, så här som, täcker allt av institutionen.
D - Okej.
M - Så att det är en massa mindre där vi har samma behov. Där är det bättre att vi lägger där. Mer centraliserat. Så LDC har ju bara, är ju bara en av de här.
O - Mm.
M - Och vi sköter ett antal maskiner, alltså klient maskiner, för olika institutioner. Så att, ja väljer någon att använda LDCs lösning, vi har väl två och ett halvt tusen klienter som vi sköter här.
D – Okej.
M – Men, vad kan vi ha på universitetet, 15 000 datorer.
O – Mm.
D – Det är ju ganska mycket såklart.
M – Det är bara en gissning. Så att, de flesta sköts ju på annat sätt. Och hur? Det vet inte jag.
D – Det är upp till dem, tills det går åt helvete liksom.
M – Ja, tills det går åt skogen. Då kan v säga att nu, nu har ni gjort fel. Ni måste göra rätt.
D – Ja.
M – Och, varpå vid enstaka tillfällen, har vi faktiskt, i princip satt hårt mot hårt. Ni måste det här, alltså. Det var en institution som är löst knuten till universitetet. De har ju egentligen inte universitetet som huvudman [ohörbart 1:49], som huvudman De hackades gång på gång, på gång, så till slut sa vi att vi kommer att sätta er bakom brandväggen, varken ni vill eller ej.
D & O – Mm.
M – Ni sköter det inte. Så sa de, okej, så vi gjorde det, och sen var det ju lugnt. Vi gav dem, att ni måste göra såhär, och sen måste ni sitta bakom brandväggen.
D – Då löste det sig till slut.
M – Så ett fåtal gånger kan vi ju gå in och… lite hårt mot hårt, men det är mycket sällan.
O – Mm, okej.
M – Så att det är så det ligger till. Det kanske är en bra bakgrund.
D – Jo men absolut. Vi kan försöka ta det lite ur, vad ska man säga LDCs perspektiv på det hela.
M – Ja.
D – Vi kan ju ta till exempel, scenariot med en brandvägg egentligen. Hårdvara, som ni köper och förvaltar. För att göra det enkelt och få din syn på det hela.
M – Det är ju en ganska enkel bit.
D & O - Mm.
M – Ett fåtal saker kostar en jävla massa pengar, och får vi ut nyttan av detta.
D – Det är det där som är lite intressant tycker vi. Hur mäter man att man får ut nyttan av det?
M – Alltså.
D – Eller ja, med en brandvägg, eller vad det nu må vara. Det känns som att det är ganska svårt att [avbruten av M].
M – Det är extremt svårt att mäta nyttan.
D – Mm.
M – Vi gjorde så den här gången, förra gången vi handlade upp ny nätinfrastruktur, vilket var 20… Ja vi hade flyttat hit, så att någon gång mitten på 2000-talet, 2005 – 2006 någonting, skulle jag tippa.

D – Mm.
M – Då inhandlade vi från Xtreme, då var det jättestora routrar. Såhär från golvet [Visar med händerna] stora saker, med åtta fläktar där bak.
D – Åh fan.
M – Vi köpte antal sådana, åtta stycken tror jag. Sen blev de end of life. Så att vi var tvungna att göra någonting 2014.
D – Mm.
M – I april 2014 så var det slut. Då var det, då fanns det ingen servicesupport kvar. Så att, vi hade lite servicesupport efter. Men då var det liksom finito. Under den här tiden så började vi bygga upp, eller då hade vi börjat bygga upp lite brandväggar redan innan. Men då körde vi vanliga hårdvara, både servrar, rackmonterande med [ohörbart] och packet-filter.
D – Okej.
M – Det fungerade alldeles utmärkt med de prestandabehov vi hade och den trafikmängd vi hade. Sen valde vi så att vi körde ett X antal WLAN i varje. Sen så när det blev fullt så köpte vi till en ny server, de kostar ju då 15 000 – 20 000. Så stakade vi ihop dem. Till slut hade vi ju tjugo par, och vissa WLAN var väldigt belastade. Så att vi kände också att vi hade lite grand nått end-of-life där också. Vi hade svårt att hänga med på vissa WLAN som då det då var väldigt mycket trafik på. Så vi märkte att vi hade nått ungefär så långt vi kunde skala på den där lösningen.
D & O – Mm.
M – Och samtidigt skulle vi byta switchar, switchar mot routrar. Då valde vi att slå ihop allti-hopa, och köpte alltså Fortinets brandväggar, som också har routingfunktion i sig.
D & O – Mhm.
M – Så istället för åtta stycken routrar i den här storleken [Visar med händerna], dem har vi i källaren. Så om ni vill ha liksom tre ton skrot så varsågoda.
D & O – Haha.
M – Plus tjugo brandväggar som också står i källaren. Så nu sitter det två [visar med händerna] hög i rack här nere, och en på Sölvegatan, som både är brandvägg och router.
O – Hur lång var tidsperspektivet från att ni köpte in de stora giganterna till att ni faktiskt gick över. [Avbruten]
M – 10 år.
O – Okej, 10 år.
M – Ungefär, körde vi med dem. Så att storleksmässigt så blev det ju extremt mycket mindre. Så att nu är det väldigt tomt i hallen. Just för att vi kastat ut så mycket. Men dyrt var det.
D – Mm, det kan jag tänka mig. Hur, när man ska göra en sån investering då.
M – Mm.
D – Det rör ju sig om extremt mycket pengar. Hur, hur kan man räkna på det till en början. Hur kan man rättfärdiga den kostanden?
M – Vad man kan göra är ju att ställa, i det här fallet, ja vi måste ha med routrar. Ja vad kostar routrar? Det är bara att slänga ut en offert så folk kan svara. Vi visste ju ungefär vad det kostar från Cisco, vad det kostar det från Xtreme, vad kostar det från Fortinet.
D & O – Mm.
M – Man hade ju ett någorlunda humm. De brukar inte ligga allt för långt ifrån varandra. Sen behövde vi ju brandväggar också.
D – Mm.
M – Så de som kunde leverera en vettigt lösning, med de prestandakrav vi hade så var det ju billigare än att köpa brandvägg och router för sig. I det här fallet så en av de saker som var uppe på agendan, som kanske inte sådär var en deal breaker, men som låg ganska bra till var att licensmodellen hos Fortinet är ganska bra.

D – Okej.
M – Man köper liksom en licens så kan man använda den hos hur många som helst. Så visar det sig att det gällde ju inte i alla [ohörbart 07:58]. Men i det stora hela så stämmer det
D – Mm.
M – När vi köper in en licens och vi ska göra det här också. Ja då kan vi köra det liksom för hur många instanser som helst. Så den är inte stackad liksom. Som vissa så köper de till, så behöver de 10, så köper de till och hålla på hela tiden, och leka med licens. Här var det bara köpa licens – ok. Så att kör man efter det. Jag satt ju inte med i utfallet av det här, men jag satt ju inte med i liksom i upphandlingen. Så jag vet inte exakt vad det kostade, men att det var dyrt, det hade det varit oavsett vad vi hade köpt.
D – Ja.
O – Använde ni er av någon sorts modell när ni liksom kom fram till att ni faktiskt behövde någonting, räknade ni ut någonting, som typ return on investment eller return on security investment, eller någon Gordon & Loeb modell, eller något? Eller har ni någon egen uträkningsmetod liksom? Använde ni er av någon modell eller någon slags metod?
M – Som sagt, jag satt ju inte med i upphandlingsgruppen
O – Men vid utvärderingen?
M – Ja, alltså.. Vi var ju tvungna att köpa någonting, och vi är en statlig myndighet.
O –Mm.
M – När vi lägger ut det här till upphandling, när vi lägger ut en offertförfrågan så måste vi ta det billigaste.
D – Förutsatt att det uppfyller de kraven?
M – Förutsatt att det uppfyller de kraven vi har. Och är det flera som uppfyller kraven så måste vi ta det billigaste.
O – Så det är pengarna som stryper en?
M – Det är det. Så är det med all statlig upphandling.
D & O – Mm.
M – Det är viktigt att skriva exakt de kraven man vill ha.
D & O – Mm.
M – Är det då så att man verkligen vill ha låt oss säga nu, Fortinet. Så skriver man ju krav som passar det man vill köpa va. Annars kan man ju få något på halsen som man faktiskt inte vill ha.
D – Mm. Så det går ändå att forma det lite?
M – Ja, man kan forma det lite. Det finns, om man är väldigt duktig på upphandling, så finns det ju ett antal sådana här saker som man kan ta till för att styra sin upphandling lite grand åt något håll, eller bort från något som man inte önskar.
D & O – Mm.
M – Sen när man väl har bestämt vad man ska ha så allting annat är ju följd upphandlingar på det va. Så det är kompletteringsköp och sånt. Då behöver man ju inte göra det, för har vi Fortinet så måste vi ju köpa något som passar.
D – Ja exakt.
M – Då är det kompletterande upphandlingar. Så vet man vad man får för någonting. Låt oss säga jag ska ha den här saken, så är det bara priset.
D – Så det är med alla era investeringar?
M – Alla statliga investeringar.
D – Även om det skulle vara att ni måste få en lite bredare [Avbruten]
M – Köp ett kärnkraftverk, det är samma sak.
D – Ja.
M – Eftersom att det är staten som betalar så är det staten som betalar.

D – Men en liten workshop för säkerhetsmedvetenhet t.ex? Också det billigaste bara?
M – Japp. Om du inte skriver till någonting. Sen finns det ju också så att vi har ju ramavtal på vissa saker va, och då är det ju redan upphandlat. Så då har man ju gjort en sån här upphandling och så skrivs ett ramavtal med en viss leverantör. Så upp till en viss summa kan man handla direkt där. Så att det är inte för varje papper och penna som vi köper.
D & O – Nej nej.
M – Utan då finns det ramaval som säger att vi köper på de thär avtalet till de här priserna, så är det redan upphandlat en gång för alla. Så får man ju skriva om den med jämna mellanrum. Så att vi har inte riktigt samma möjligheter att räkna hem en investering innan så att säga. För vi vet inte riktigt vad vi kommer att få.
D – Nej det är klart.
M – I ett privat företag så är det väl ofta så att man gör sin utvärdering först.
D & O – Mm.
M – Sen är man ganska klar med vad mans ka ha. Sen går man ut till ett antal återförsäljare av den utrustningen och frågar vad får vi för pris på den. Vi kan inte göra riktigt på sammas ätt, vi kan inte peka ut att vi ska ha den här. Utan vi ska de här funktionerna, och sen skickar man ut den, och säger hur kan ni lösa det här problemet? Och det kan ju lösas med Cisco, det kan lösas med Fortinet, det kan lösas med [ohörbart], det kan lösas med vilken annan som helst.
D – Jaja.
M – Sen är det priset.
D & O – Mm.
D – Det är ju faktiskt rätt intressant, det tänkte inte jag på ens en gång. Att det är offentlig upphandlingar på det här. Men det är ju ja, då kan man ändå tänka sig att mycket av, alltså, det som verkar vara mycket av ett problem när vi suttit och läst, är ju egentligen att hitta kraven på vad det ska vara. Att det kan vara en svårighet i sig också.
M – Ja.
D – Vad, om vi tänker den här brandväggen nu, som vi pratade om. När ni skulle lista upp specifikationerna för det, hur ser hela den processen ut?
M – Alltså, vissa saker ger sig ju ganska enkelt. För vi har ju vår nätinfrastruktur så det togs bort det, och kommer det till ett nytt hus så får vi ju gräva en bit, och sen så får vi ju dra nätet där. Att vi expanderar i flera hus samtidigt och sånt där, ja det händer ju med jämna mellanrum. Men det finns ju en viss plan för det, för ett par år fram kanske. Trafikmängden i nätet, den ökar och den är ganska linjär så här alltså. Så där kan vi ju ganska hyffsat se så att händer det ingenting radikalt, och att det kommer något nytt som är väldigt krävande… När fildelningen startade en gång i världen så gick ju trafiken såhär va [visar med händerna] helt plötsligt. Så var det ju ett teknikskifte som gjorde att vi fick det väldigt hårt. När vi sen gick i taket och stängde av fildelning vilket var med Nutella och Kazaa och lite andra av de här enklare protokollen. Då hade vi två stycken, två 100 Mbits linor till SUNET, och de var fulla med streck, 200 Mbit, dygnet runt. Det finns ju ingen möjlgihet, vi kan ju inte jobba.
D – Nej nej.
M – Då hade vi också studentområdena kopplade till vårt nät, och vi kunde inte jobba på dagtid, och folk som satt och spelade spel hade så hög latency i nätet så att de blev ju dödade hela tiden. Så de var ju förbannade på det också. Vi kunde inte hålla en SSH session uppe för det var så hög latency. Mycket paketförluster, och dem som tankade film sket ju fullsätndigt i det va.
D & O – Ja ja.
M – De startar, sen går de på föreläsning, så står den och tankar.
D – Så den står och tuggar dygnet runt.

M – Ja ja. Så att då satte jag mig ner och jobbade en vecka ungefär, och identifierade hur ser de här protokollen ut. Sen använde vi Snort, som är egentligen ett IDS verktyg. Som också kan användas för att skjuta ner sessioner.
D & O – Mm.
M – Men som också kan identifiera hur protokollen ser ut, så drog jag igång den här snorten på fredag, Så såg vi på SUNETs statistik hur det gick från 200 ner till 70 Mbit. Alltså två tredjedelar var trafik var fildelningstrafik. Det var inte bittorrent då, men det var fildelnignstrafik. Så försvann det två tredjedelar Folk blev ju förbannade.
D – Men det är ju inte det som det är till för.
M – Men alltså dem, radio var här och intervjuade, och i tidningen och alla var förbannade. Det är ju på sätt och vis statligt, vi är ju en statlig myndighet. Vi kan inte med skattepengar finansiera ett nät som två tredjedelar kör bittorrent. Vi kan inte jobba.
D – Nej nej nej.
O – Det är klart.
M – Men de lugnade sig snabbt. Som sagt kom de här lundahubbarna, då var det mycket DC++ trafik.
O – Juste!
D – Det var längesen det.
M – Så satte de upp ett par hubbar här. Då var den ju den största, den satt på Sparta. Då var det så jävla mycket trafik till Sparta, så att även om vi utåt inte berättade, liksom alla trodde ”Nu lurar vi LDC, de fattar ingenting”, så sa vi till de här killarna som drev hubben att ni får inte, ni måste ha fler hubbar på nätet.
O – Mm.
D – Ja.
M – Vi kan inte ta all trafik på ett ställe. Sen kom ju Delphi, och sen kom några hubbar till. Så var ju nätet ganska jämnt belastat. Då var det ju inte något som drabbade oss speciellt hårt. Utan inne i nätet så var vi mycket högre prestanda än ut mot SUNET. Sen körde de i många år på det sättet, och vi brydde oss inte för det störde oss inte.
O – Nä.
M – Vi fick inga klagomål utifrån, utan det var ju helt internt va. Ville man ha in någon ny film så fick man ju bära in det på något annat sätt, och lyfta in det i det interna nätet. Så är det. Sen flyttade ju alla studentnätet ut och det blev någon annans problem.
D & O – Haha.
D – Ja det måste ha varit skönt för dig, och slippa det.
M – Det var jätteskönt att slippa det, och studenterna tyker det är jätteskönt att slippa oss.
D & O – Haha.
M – Det är inte bra, liksom att ha privatpersoner som kör inne på en myndighets nät. Det fungerar inte.
O – Nä.
D – Nä det känns lite sådär.
M – Från början så var det väldigt god reklam för Lunds Universitet, för vi var väldigt tidiga med att ha nätverket i studentområdet. Då var det ju jättetrevligt att läsa i Lund, för vi fick ju en egen fast lina.
O – Mm.
M – Inkluderat, så du betalade bara för AF Bostäders uttag, och själva nättrafiken var gratis.
D – Mhm.
M – Så då var det ju en fördel för oss. Sen blev det ju kvarnstenar att gå och dra på. Det var lite långt från ämnet kanske…
D – Intressant ändå. Lite roligt såhär.

M – Men i alla fall, vi vet nättrafiken, vet vi ganska väl. Så sker det är inte något paradigmskifte någonstans så kommer vår nättrafik, vi ligger ungefär på 3 – 3.5 Mbit, eller Gigabit ut för tillfället. Och vi ser på statistiken att det går ganska linjärt.
D – Ja det går ju att ganska bra förutspå behovet så att säga.
M – Ja kanske, en gigabit per år som vi kan se, hur kurvan sticker upp. Man kan ju gå in på SUNETs sida och se på statistik.
D – Okej.
O – Mm.
M – Det är öppet för alla, så kan man se precis Lunds Universitets trafikkurva.
D – Det får vi kolla upp sen. Kan vara roligt att spana lite.
M – Och ibland så ser vi ju att om vi gör saker i nätet, som vi har gjort då under året, för att t.ex. begränsa bittorrent från det trådlösa nätet.
D – Mm.
M – Så ser vi att [visar med händerna] i kurvan. Det är samma sak där, men även om vi har stängt av bittorrent i wireless nätet, så stör ju bittorrent trafiken. Även om man inte kan hämta någonting. Ja vi får lite klagomål, varannan vecka kanske. Om vi öppnar upp det så får kanske 10 om dagen. Så vet ju att det fungerar.
D & O – Mm, jaja.
M – Men ändå ibland så smiter det ut något litet paket som gör en announce på en tracker eller sådär. Då kan vi få ett klagomål, men det är liksom inget stort. Men ändå så ligger varje torrentklient och försöker hela tiden, även fast de inte kommer ut.
D & O – Mm.
M – Väldigt mycket på den här UDP trafiken som ligger. Den kan ju ha flera tusen peers som den ligger och skickar till hela tiden och försöker, och försöker, och försöker. Varje gång så skickas ett paket såhär. ”Request to send” och alla maskiner ligger såhär ”Request to sen”, ”Request to send”, ”Request to send”.
D & O – Mm.
M – Och så måste ju accesspunkten säga såhär, nu är det du, och nu är det du, och nu är det du. Eftersom de är så små de här, alltså de skickar bara några byte. Så får de ofta sådana här klient to send signaler. Så att hade den försvunnit från trådlösa nätet hade det fungerat skitbra.
D & O – Haha.
M – Faktiskt!
D – Ja för det är rätt så svajigt till och från.
M – För det mesta så är det inga problem där vi inte har studenter.
D & O – Mm.
M – Och där vi har studenter som slår upp sina datorer när det är rast eller när det är middag eller sådär. Då vroom. Och det är väldigt mycket torrentklienter som ligger på.
D – Mm.
M – Hade alla stängt av sina torrentklienter så hade det trådlösa nätverket fugnerat jättemycket bättre.
O – Det är sjukt för att man fick väl skriva under en sån här grej innan man började använda internet, Eduroam, att man inte skulle använda sig av torrentklienter och liknande.
M – Jo.
O – Man fick skriva under någonting.
D – Haha, det kommer inte jag ihåg.
O – Jag har för mig det.
M – Det är möjligt.
D – Det känns ju rimligt i och för sig.
O – Mm.

M – Sen så ligger den där hela tiden, och det är klart man stänger inte av det. Slår upp, och så vroom så går den igång. Det är ingen som ser den, det är ju en liten ikon till höger.
D – Ja folk glömmer väl bort att det ligger där då.
O – Ja, haha.
M – Ja och det vet vi ju om. Det är liksom inte någon möjlighet att jaga folk. För då har vi inget annat att göra.
D – Nej det förstår vi.
M – Då är det bästa att försöka blockera det, och det gör vi i de här Fortinet-brandväggarna. De har ju sådana regler. Så för det här, för VPN- nätet, och för det trådlösa så har vi stängt av bittorrent, eller ja peer-to-peer över huvudtaget.
D & O – Okej.
O – Försöker ni… [Avbruten]
M – Resten av nätet spelar ingen roll.
D – Så om man kör på kabel.
M – Då är det helt okej.
O – Hmm, de fungerar dock aldrig. Kabeluttagen som ni har.
D – Har inte provat, har inget uttag på min dator heller.
O – Men brukar ni försöka hindra saker från att hända, eller brukar ni… Brukar ni låta en risk eller någonting hända, och sen bearbeta den. Eller brukar ni [Avbruten].
M – Vi försöker mitigera de risker som vi ser. Men med tanke på att vi är en och en halv person, och vi har liksom tio tusentals datorer, och bara vi har nästan 400 servrar i hallen.
O – Mm.
M – Runt om på universitet så, alltså, vi har ju, nu gissar jag, vi har ju mer än några tusen servrar.
D & O – Mm.
M – Säg att vi har 1000-2000 servrar, jag vet inte. Eftersom jag inte ens vet var de finns så hur fan ska jag kunna hitta risker?
O – Ja precis.
D – Det blir svårt såklart.
M – Men vi gör sånt där ibland, när vi vet att… Wordpress är ju en sån här typisk grej som hackas.
D – Mm.
M – Av alla de hackade webbsidor som de här trojanerna sprids ifrån och sådana här [ohörbart] brev och sånt där som har en länk, är ju till en hackad sida. Jag skulle säga att mer än hälften av dem är Wordpress. Man ser det ju ganska enkelt, ser man på länken så står det väldigt ofta WP och så någonting annat.
O – Mm.
M – I URLen. Då är det något Wordpress plugin som inte uppdaterats som man utnyttjar. Där vi kan ju gå ut och scanna hela nätet efter Wordpress, och plocka ner… Det finns en som heter WP-Scanner som går in och så plockar den all information den kan, vilken version, vilka add-ons och plugins ligger addade i den här.
D & O – Jaha okej.
M – Sen så kan vi ju skicka klagomål. Så där vi vet att det åtminstone finns lågt hängande frukt som de är ute efter så försöker vi ta det innan det händer någonting.
O – Mm ja okej.
M – Men vi har väldigt dålig kontroll på vad körs var.
D – Mm.
M – Och ja…
D – Så det är lite mer ett reaktivt agerande överlag.

M – Ja, med tanke på att vi är så få så blir det ganska reaktivt. Men vi försöker vara proaktiv där vi kan.
D & O – Mm.
M – Men det är långt ifrån det.
D – Det är som du säger, det är svårt med en och en halv tjänst.
O – Det är också en budget fråga. Ska vi ha fler som är på den tjänsten eller inte.
D – Ja, exakt.
M – Det är ju så att pengarna kommer ifrån IT-kontoret, och det är ju pengar som ska taxeras ut från alla institutionerna och det är ju inte speciellt populärt att betala till det centrala administrationen.
D & O – Mm nej nej.
M – Oavsett, det går ju i en klump. Då tar man ju en viss procent av alla pengar som delas ut till alla institutioner. Även om man får forskningsbidrag från externa, så tar vi administrativt en viss procent, och lägger på det centrala. Det är lika stort för varje gång vi plockar ut pengar.
D & O – Haha.
M – Det är ju bara en klump så att säga. IT-säkerhet, vi hade säkert fått mer pengar om det stått ”Vad vill ni betala till?” Vill ni betala till ekonomiavdelningen, eller vill ni betala till IT-säkerhet.
D – Ja.
M – Ja IT-säkerheten. Men så är det, allting kommer ju bara i en klump, och sen fördelas ju den av förvaltningen.
D – Mm.
M – Och sen till IT-kontoret, och sen fördelar dom ut, så får vi en och en halv tjänst.
D & O – Mm.
D – Vad skulle du uppskatta det till, hur mycket av IT-budgeten läggs på säkerhetsfrågor då?
M – Det är inte mycket.
D – Det är inte mycket?
M – Nä. På LDC jobbar ungefär 120 personer, om vi tittar på hela universitet och här har vii service desk, och vi har telefonväxel och lite sådana här saker också. Som inte är direkt IT. Men alltså, vi hade någon genomräkning någon gång. Jag skulle gissa att det kanske rör sig om 250 personer som jobbar med IT på ett eller annat sätt någorlunda dagligen.
D & O – Okej.
M – Då kan vi räkna en och en halv tjänst av 250 va.
D – Ja.
M – Det är väl någon halv procent.
O – Det är jättelite ju.
D – Det är väldigt väldigt lite.
O – Mm.
M – Om du tittar på vad som investeras i hårdvara, ja nu har vi ju fått nya fräcka brandväggar. Det kostar en hel del, men det var ju routrar i dem också så att. Och hur mycket vi ska lägga på brandvägg, hur mycket vi ska lägga på att det är en router det kan vi ju diskutera va. Men förutom det så körs i princip allting som är IT-säkerhet och hårdvara, körs på begagnade prylar och free och open software.
D – Jaha, okej.
M – Väldigt sällan vi går in och ber om att få köpa någonting. Då är det t.ex. nya diskar och sånt här, det får vi inte köpa begagnat. Annars, det blir en jävla massa brandväggar över va, och en del av dem är ganska nya. Så där har vi ju [ohörbart] maskiner vi kan ta i drift.
D – Okej.

M – Men jag kan säga så, ge mig mycket, mycket hellre ett par personer som har rätt inställning till jobbet än en jävla massa hårdvara och fräcka säljare med glansiga kostymer och fyrfärgstryck. Jag gör det mycket hellre själv, för om vi använder open-software så förstår vi hur det fungerar på ett helt annat sätt än t.ex. Fortigate. Fortigate brandväggen har en väldig massa funktionalitet, men det är bara av och på.
D & O – Jahaja.
D – Så inte mycket till konfigurering?
M – Vill du använda det där filtret – ja. Då får du allting som finns i den. Så kan man fråga vad är det i filtret? ”Nja det vet vi ju inte, det har vi en avdelning som sitter och fixar.” Så säger du att vi ska skjuta ner all peer-to-peer. Jaja, klick så är det bara på. Sen vad det är man skjuter ner, det vet vi ju inte riktigt.
D – Åh fan.
M – Det får vi ju lite. Peer to peer är ganska simpelt, men om vi säger ett porrfilter.
D & O – Mm.
M – Vad är det som räknas som porr. Vi tittade på det där en gång för vi hade ju ett fall uppe på UB. Där var ju en snubbe som satt och surfade på porr hela dagarna, någon jävla gubbe. De blev ju rätt sura på honom, och de var väl lite för timida för att säga till och kasta ut honom. Men då sa vi, okej. Vi kan sätta ett porrfilter framför UB, så tröttnar han väl.
D & O – Mm.
M – Då tittade vi på hmm vad kostar det att köpa? Ja det kostar rätt mycket när vi pratar den trafikmängd som vi har. Kan vi göra det själva? Ja vi kan göra det sjäva. Vi löste det med relativt enkla medel eftersom att de flesta som porrsurfar väljer Google. Så gjorde alla Googlesökningar, vi satte en proxy, en squidproxy framför. Alla URL som gick till google sökningar hade vi lagt om till en Google safe search.
D & O – Mm.
M – Så lät vi Google filtrera bort all porr.
D & O – Jaha.
M – Sen så la vi ett filter på också. När vi tittade på det här filtret, alltså vad är det för URLer, så hittade vi liksom, det var väl damernasvärld.se liksom. Hänt i veckan, alltså.
D & O – Haha.
M – Svenska veckotidning, ja svensk damtidning. Visst du kan se nakna bröst och hud och sånt. Någon som triggat igång på detta, vi vet ju inte hur de har skapat de här filtren.
O – Nä.
M – Och det är samma problem med allting man köper. Du vet inte hur, och du kan inte se filtret för du har inte tillåtelse att läsa filtret. Då vill du inte ha det heller.
D – Nej nej, det är klart.
M – En del använder ju, de köper så här IPS, Alltså intrång, Intrusion Prevention System. Ja den triggar på en regel, så skjuter den ner sessionen så är den väck. Så har de då blivit av med det här hotet. Vi skulle aldrig våga köra någonting sånt i IPS, utan vi skulle köra det i IDS läge, bara detektera och rapportera. Och låta oss [ohörbart ut det], okej det kan vara det som har hänt.
D – Ja.
M – För man vet aldrig vad är det i de här reglerna. Kan jag inte läsa reglerna så vet jag inte vad jag skjuter ner för någonting.
O – Mm.
D – Nej nej.
M – Vad händer när någon inte kan få någonting att fungera? Jo de ringer till vår servicedesk och säger det här fungerar inte. Var ska vi felsöka. Jo det är någon låda som sitter i hallen och

skjuter ner just den sessionen. Så det blir väldigt svårt att felsöka. Man måste vara väldigt säker innan man skjuter ner trafik.
D & O – Mm.
M – Speciellt på ett sånt här bygge, som alltid ska vara öppet och fritt och vi ska inte blockera någonting. Det är den allmänna tanken på ett universitet. Vi blockerar ingen trafik, och det är inte meningen att vi ska blockera någon trafik. Så finns det ju ett barnporrsfilter men det är ju Polisens barnporrsfilter, det sköts ju av SUNET, så det är inte vi utan det är för alla, alltså ett steg högre upp.
O – Mm.
M – Men det är alla filter vi har. Sen är det vissa protokoll höll jag på att säga, vissa portar som vi har stängt av eftersom att det finns ingen legitim användning att köra dem utanför LU-NET, och vi vet att det är säkerhetsbrister och hackning. T.ex. på Windows BIOS protokoll, folk som valt att dela ut sin C-drive till hela världen, och det finns dem som hela tiden sniffar efter det här va. Vi hade väldigt stora problem på våra studentbostadsområden på den tiden där vi hade då va. Det var jättekul att liksom sniffa efter tja, tjejer som inte fattat och delat ut hela sin C-drive.
D & O – Haha.
M – Så att man då såg deras datorer. Så de höll de ju på med hela tiden.
D – Ja.
M – Men det är ju ett lokalt protokoll. Hela Net bios protokollet är alltid lokalt, det ska köras lokalt på ett kontor, det ska ju aldrig lämna liksom ett WLAN.
D & O – Nä.
M – Men du kan köra det över hela världen för att det är helt okej att köra det icke lokalt också. Men då har vi ju stoppat det, det finns ju ingen vettig orsak till varför man ska montera diskar på det sättet, över internet. Så det är ett antal sådana som vi har blockerat. Vill man göra det utifrån så får man köra via vår VPN så kommer du in så kan du.
D – Okej, så att då går det.
M – De ligger också ute på vår webbsida. De här protokollen och portarna är blockerade, så det är helt öppet. Sen förutom det så är det som sagt väldigt lite blockerat.
O – Rätt kul när du går tillbaka i historien, man märker liksom att ni får svårare och svårare utmaningar hela tiden med tanke på att tekniken går framåt också.
M – Ja.
O – Det där med Kazaa och DC ++, till bittorrent till när man sniffade runt och sånt.
M – Ja alltså, skjuta ner Nutella var ju jätteenkelt för att den frågade alltd, eller den skickade en fråga så svarade alltid Nutella ”okej” i klartext.
D – Mhm.
M – Bittorrent är ju binärt, så det är mycket svårare att hitta. Men den gör alltid en announce, och den kommer i klartext.
D – Nä jag har lite dålig koll på hela, hur det fungerar rent tekniskt.
M – Nä men den pratar ju alltid med en tracker för att ta reda på vem är det fler som har delar av den här filen som jag är intresserad av. För den är ju uppdelad i småbitar. Så får man reda på att den här IPn den har den här biten. Trackern håller reda på vilka som just nu här upp-kopplade som har den här biten.
D – Ja okej.
M – Så, då måste man ju ha lite trafik förutom själva datatrafiken till filen. Så är det ätt mycket overhead trafik. Det är ett ganska pratigt protokoll.
O – Mhm.
D – Jahaja.
M – De gör ju allting för att inte skjutas ner.

D – Ja det är klart. De vill ju finnas där.
M – Ja visst, och vi måste skjuta ner det på vissa ställen. Men annars så används det ju väldigt ofta för att dra ner Linux distributioner och sådana här saker. Så vi vill ju inte ha det blockerat där vi inte behöver.
D – Nej nej, det är klart. Det finns ju bra användningsområden med det också.
M – Så att, ja vi får ibland klagomål på anställda forskare som bär med sig sin laptop, så tankar de hemma, så pluppar de in den här och så ser vi att ”jaha, ni laddar South park” Då får vi klagomål direkt. För det är en av dem som man inte ska ladda ner, det är den som får mest klagomål. Alla nyaste filmerna, och så South park.
O – Är det så?
M – Japp. De är väldigt aktiva på att leta.
D – Jaha.
O – Mhm.
D – Jag tänkte lite på det här med, om vi bara går tillbaka lite till kostnader för saker och ting. Finns det, händer det ibland att du ser att t.ex. då ni måste mitigera någon risk, eller behandla en risk här. Men att kostnaden för att göra det här, nu bara den blev alldeles för hög, så att det här, det går inte att genomföra. Det går inte att motivera den höga kostnaden.
M – Det finns egentligen två saker, eller tre saker som gör att man inte kan mitigera en risk som man vill. Den ena är ju pengarna.
D – Mm.
M – Att ja, vi skulle kunna lösa det här på ett par sätt. Men det skulle bli alldeles för dyrt. Så det är helt klart. Eller nej vi har inte, vi har inte mantid.
O – Mm.
M – Vi kan inte göra det här för att det skulle ta oss alldeles för lång tid. Vi skulle gärna vilja sitta och sniffa nätet hela tiden. Sitta och titta vad är det för typ av risker det finns med [ohörbart]-installationer, med Drupal-installationer, med Wordpress-installationer, allmänt webb, SQL-injektions, vi skulle kunna sitta fyra-fem man liksom och hålla på med det där full tid, om vi nu säger att vi ska säkra upp alla våra webbtjänster.
D & O – Mm.
M – Det hade vart, jag skulle säga minst två man skulle kunna sitta och hålla på med det hela tiden.
D – Det är så mycket jobb alltså?
M – Det är så mycket jobb. Vi tog ju lite penetrationstestning, alltså du får bara att här är en potentiell risk. Sen måste du verifiera att det faktiskt är en risk. Så det tar extremt mycket tid. Så att vad vi ska göra, nu, vi har haft tidigare, men det gick i stål när vi bytte, bytte miljö här för ett tag sen. Att vi ska sätta upp en ny scannerdator, alltså en dator som innehåller alla de här scannerverktygen. Ska börja med det, så att vi faktiskt har alla dem på ett ställe. Det finns extremt mycket bra verktyg för att scanna nät på olika sätt. Då får vi åtminstone en bild av hur det ser ut, och var saker och ting finns, vilka tjänster som är öppna på vilka datorer. Och ha det som en base line. Sen skulle vi också i nästa steg, ha en automatiserad scanning över vissa saker och se vad är det som skiljer sig. ”När ändrade det här sig?”. Vad är det som kommer till vad är det som försvinner. Så att vi inte bara har att det är en nulägesbild, utan att vi har [ohörbart].
D – Okej.
M – När vi har tid. Och plus att vi ska kunna använda den ad-hoc, när vi vet att här är någonting som har hänt på det här nätet. Då kan vi gå till det WLANet och scanna av det, och se eter vad, hur ser det ut. När vi tittar på det här utifrån, vad svarar de för tjänst och vad säger tjänsterna att de gör för svar. Sen kan vi titta på trafiken, trafikloggar. Se vad är det för trafik som går in och ut ur det här nätet. För att försöka hitta det som är abnormiteter. Då har ju en

praktikant, en praktikant i 10 veckor. Han började i förra veckan, så att han har gjort en vecka. Det är väl hans nästa uppgift, han har fått lite trevliga script. Mycket av våra varningar kommer ifrån script och sånt vi skriver själv.
D – Ja okej.
M – Eftersom det är väldigt svårt att hitta färdiggjorda saker. För att vår miljö ser annorlunda ut, vi tankar in vår trafik på olika sätt som inte är standard. Det är ofta väldigt svårt att återanvända saker. Man kan ta idén från andra, men sen får man ofta alltså fibbla till det själv. Men vi har ju massa script och, som varna t.ex. har vi ju ett som tittar på all trafik på det trådlösa nätet. Då är vi bara intresserade av vilken user-id som har loggat in. Sen jämför vi det med VPN-loggarna och ser efter har samma user-id, samma dag loggat in från VPN, dvs. utanför Sverige. Inte hemifrån utan utanför Sverige. Men samma dag varit i Lund och kört på vårt trådlösa nät. Då kan det ibland vara fel. Ibland ser vi att en person, vi kan se den har vart på det trådlösa nätet, nästa inloggning var VPN från Köpenhamns flygplats, och sen två timmar senare så kommer en VPN ifrån Tyskland Jaja då kan vi se att det är en person som varit ute och rest. Men vi kan se ibland, här är en person den är i Lund ansluten till en av våra accesspunkter, som finns här i Lund. Inte en platta, iPad som ligger på laddning, och är ute och gör en push pull för att hämta lite data. Utan en person som har rört sig här och finns i Lund, och samtidigt loggar på ifrån Kina.
O – Mm.
M – Kineserna är ju väldigt mycket ute efter våra VPN-inloggningar. För att de är ute efter våra litteraturdatabaser.
D – Jaha.
M – Vi abonnerar ju på litteraturdatabaser som är extremt dyra.
O – Mhm.
D – Ja dem har vi ju utnyttjat här.
M – Kineserna vill ju inte betala för, eller kan inte ens betala. Så det är mycket billigare att stjäla VPN-access.
D – Jaha.
M – Så använder dem det för att komma åt våra databaser. Så upptäcker den här databasägarna det, så blir dem förbanna så får vi in en not att vi stänger av er om inte ni fixar. Så att kineserna inte kommer in och stjäler data. Och då kan vi vara lite proaktiva, och lite då och då hittar vi. Ja det väl en vecka sen, två veckor sen så var det en dam ”Nä jag har ingen aning varför den har loggat på både ifrån Kina och Kanada.” Så sa jag ändra lösenord, och då var problemet ur världen.
D – Haha mm.
M – Så att det är ett sånt script som vi skriver. Det tittar på vilka maskiner har flest sessioner förra dygnet, och vem har skickat mest data för dygnet. Där är alltid samma som ligger i topp 10, och praktikanten har nu lagt till lite som jag tyckte var väldigt bra. Innan stod det IP-nummer bara, nu har han lagt till namnet på maskinen också, så att vi vet det. Så la vi till hur många gånger under de sista 30 dagarna har det här IP-numret varit med på listan. Vad var förra rankingen, har den gått ifrån att vara 20 till att vara två, eller har den… Så hur den rör sig. Har den varit med mycket, har den gått upp. Det ger oss en liten sådan här blick över vem är det som kör mycket, vilka serverar är det, dem som är belastade. För helt plötsligt kommer det som en raket upp, så kan vi sep å namnet att det här är ju, en vanlig klientdator. Då är det ju skumt.
D – Ja.
O – Mm.
M – Så att det är väldigt mycket sådana här script. Väldigt sällan vi kan göra script som säger bing, här har vi fel.

D – Mm.
O – När brukar ni se något som lyckat? Alltså, när är det ”gött, nu löste detta sig, alltså..”
[Avbruten]
M – När jag sköt ner två tredjedelar av trafiken på nätet.
O – Då ja, när någonting ni har , och använder till ett helt annat syfte faktiskt börjar fungera i rätt syfte. Typ som nätet där?
M – Det var typiskt en sådan här sak, då var det en experimentell grej just för nedskjutningen av data som de hade lagt till då, Snort, precis. Eftersom jag hade, vi körde Snort som IDS-system, jag hade läst att det här hade kommit, då tänkte jag då kanske vi kan använda det till det här syftet också. Och då, då lyckades det så bra, alltså från att hela nätet gått trögt, och vi var överbelastade, med en halv veckas jobb kanske, och begagnad hårdvara kostade oss inte ett skit, att med lite arbete ta bort två tredjedelar av trafiken på nätet. Det är lyckat.
O – Det är lyckat, ja men det är det. Det är klart.
M – För att vad var alternativet, skulle vi investera i ett större nät.
O – Mm, dyrare såklart.
M – Eller skulle vi köra ett nät som man inte kan jobba i?
O – Mm. Man skjuter ned dem istället.
M – Det var det ju liksom inte, eller då var det en no brainer alltså.
O – Ja.
M – Det var bara, då kunde man ju säkert gått ut och köpt en grej för 100 000 som hade gjort det. Eller så kan man tänka efter, okej, kan vi göra det själv? Och då föaktiskt också förstå vad det är som händer.
D – Ja men förstå bakgrunden, och inte bara läsa utan att förstå någonting.
M – Så det är därför jag säger att jag tar hellre folk som förstår vad dem gör, och har rätt inställning till jobbet. 10 gånger hellre än att köpa massa hårdvara.
D – Men då har du, eller det verkar som att du har ganska så fria tyglar ändå, över hur du kan göra på din arbetstid så att säga.
M – Jaja. Det har jag. Vi har rätt fria tyglar, vi rapporterar upp till den mån de vill ha rapporter så att säga, då rapporterar vi upp. Vi har ju vårt eget request, vårt ärendehanteringssystem. Så att alla våra ärenden finns ju där va. Man kan titta [ohörbart] tillkommit.
D – Mm.
M – Men det rapporterar vi ju upp. Lite grand i den omfattning dom vill ha. Men sen hur vi löser vårt arbete, det är ganska mycket upp till oss. Det är ju generellt på Universitetet.
D – Så det är lite, om jag säger säkerhetsmaximerande tänk då egentligen? Att gör så mycket du kan.
M – Ja. Alltså väldigt mycket är best effort, och vad kan vi göra med de resurser vi har.
D & O – ja.
M – Då, alltså, det är väldigt lite så att vi kom kusiner från landet, när man kommer till USA och pratar säkerhet med andra amerikanska universitet t.ex. Nu visar det sig att de har precis samma problem. De är precis lika underbemannande, de har precis lika lite pengar, och de löser problem på exakt samma sätt. Så att så här ser det ut på alla svenska universitet. Så ser det antagligen ut på alla universitet i världen.
D & O – Mm ja.
M – Jag tror inte skillnaden är så jättestor. Och det var ganska skönt första gången man, för man trodde ju att alla andra har det så mycket bättre liksom. Pengar, mer personal. En del har säkert mer pengar och personal, men ändå så filosofin om hur man löser problemet är ganska lika.
D – Det är ganska intressant faktiskt.
M – Jag träffade en säkerhetskonsult, vi var på en kurs i San Diego.

D – Mhm.
M – Han heter Eric Conrad, väldigt duktig kille. Han sa det att han hade jobbat på ett universitet ett par år, och han rekommenderade alla som skulle börja i säkerhetsbranschen att jobba på ett universitet ett par år, för då kommer ni se allt som finns.
D & O – Haha.
M – Eftersom här är var man sin egen IT-administratör i princip. Det finns ju inte en standardiserad plattform [ohörbart] låsta miljöer liksom. Du kan inte nå nätet om du inte kör VPN, och så startar du VPN på din laptop så måste det vara jobbets laptop, och då låser alla andra kommunikationer sig, och du måste köra det och detta. Så ser det ju ut om man går till vissa företag, så är de ju extremt nedlåsta. Du kan inte hemma med din egen dator, utan det måste vara jobbets dator, och du måste ha kort i och sådana här saker. Ubikey eller något annat. Annars kan du inte köra på… Och det är klart, Ericsson har mycket hemligtheter som dom inte vill bli av med, för att det är dyrt. Här har vi ju inte så hemskt mycket hemligheter, utan det är precis tvärtom, det här är forskning det är till för alla. Vi är en statlig myndighet, vi har väldigt få sekretessbelagda saker, resten är en allmän handling.
D & O – Mm.
M – Så att vi har inte så mycket att skydda.
O – Mm nä.
D – Nej nej.
M – Nu tycker jag att det är fel approach. Allting, allting är skyddsvärt enda tills någon begär ut det. Vi ska behandla all information som den är skyddsvärd.
D & O – Mm.
M – Alltså, det finns ingen orsak att lämna ut information till folk som inte vill ha den.
D – Nej nej nej, absolut inte.
M – Och sen har vi ju en tredje uppgifter som det heter, som alla universitet. Det är forskning och utbildning sen är det information till allmänheten och omvärlden. Det är den tredje uppgiften. Det är klart att vi ska väldigt öppna med vad som händer, och vad som, och all forskning ska vara öppen för alla. Men det betyder ju inte att alla uppgifter, och allting liksom, ska behandlas som om det redan var läckt.
O – Nej precis.
M – Men väldigt många ser det på det sättet.
O – Man värdesätter ju ändå information rätt högt, allmänt.
D – Det finns ju alltid ett värde i det.
O – Men precis.
M – Därför är det lite grand så att, de förra IT-säkerhetsreglerna, även de nya som kommer vara ännu mer trycka på det. Att detta är informationssäkerhet det handlar om, det är inte IT-säkerhet, det är inte datasäkerhet, utan det är informationssäkerhet. Sen vilket media på, om det ligger på din laptop eller på ditt USB-minne eller transit i nätet spelar ingen roll. Utan du ska skydda din data din information på ett säkert sätt. Sen att du sen måste skydda din dator för att inte din data ska komma på drift det är en följdeffekt av det. Men det är informationens säkerhet som är det viktiga. Det är ju så att skyddar man den, så är ju allting annat runt omkring. Då har du brandväggar, du har säker lagring, du har kryptering, och du har det och detta.
O – Mm.
M – För att annars är inte din data säker. Så att det är informationssäkerhet som gäller, och jag trodde att rektorns, universitetsstyrelsen skulle ta det den 15e. Men det var tydligen rektorns beslut istället, så nu ligger det på den juridiska enheten, den juridiska avdelningen heter det. Ledningen har ibland en förmåga att ta tid på sig. Så vi vet inte riktigt när det kommer, men det kommer nya riktlinjer.

D – Skulle du säga att det ofta är, de här regleringarna och reglerna som driver nya säkerhets-åtgärder?
M – Nej. Inte på ett sånt här ställe. Här använder vi reglerna för att slå folk på fingrarna.
D & O – Haha.
O – Men när vet ni att ni har ett behov då?
M – Förlåt?
O – När vet ni att det finns ett nytt behov då, för en säkerhetsinvestering?
M – Vi vet att det är ett nytt behov när MSB, Myndigheten för samhällsskydd och beredskap, och internrevisionen kommer och slår oss på fingrarna och säger att vi måste göra något.
O – Jaja okej.
M – Lite grand är det på det sättet tyvärr. MSB kom ju och sa att ni måste arbeta enligt iso 27000. All right då måste vi göra det. Internrevisionen kommer och säger att ”Hur behandlar ni PUL” alltså personuppgifter i era servrar och på nätet. Jaha då måste vi göra någonting åt det. Så att vi upprätthåller de krav som kommer utifrån. För att vi som universitet skulle ha nog ha lägre krav kanske än vissa de krav som kommer ovanifrån.
O – Mm.
M – Mycket på grund av att universitetsfilosofin, alltså miljön är sån att allting ska vara öppet och fritt. Så då skyddar vi det som vi måste skydda, så får resten vara så öppet det går.
D – Okej.
M – Men, kommer ISO 27000 då måste vi liksom köra efter det. Då blir det ju som en best practice som kommer från MSB till exempel.
O – Intressant. För då kan det vara så att någon faktiskt kommer till er och ber att ”ja detta ska ni göra” och så gör ni det, fast sen så är inte utfallet så bra som ni, ni som jobbar så nära det, faktiskt vill ha det.
M – Ja ja. Nä alltså vi försöker ju först och främst att liksom nå upp till de krav som vi måste.
D & O – Mm.
M – Och kan vi göra det bättre, utan att serveravdelningen, eller juridiska avledningen, eller någon annan här slår bakut, så är det klart att vi kanske då om vi… Låt oss säga kryptering t.ex. så finns det ju väldigt få uttalade krav på kryptering. Det är på kvalificerat hemliga, och hemliga uppgifter som faktiskt inte är en allmän handling, utan då är hemlighetsstämplat från början. Då ska det vara krypterat. Enligt då en viss standard. Medan allting annat, även om vi pratar personuppgifter så behöver de inte krypterade på något sätt. Men det kanske vore bra om de var krypterade. För att vi sover lugnare på nätterna. För att det kommer ju med det här. PUL kommer ju dö nu, om ett år. Oh det kommer nya persondatadirektivet från EU.
D & O – Jaha okej.
M – Som tar plats istället. Och i och med det så är det ju inte längre bara en smäll på fingrarna vi får, utan då är det ju böter.
D – Mm.
M – Och det är ju upp till, fyra procent av globala omsättningen, eller upp till 20 miljoner euro. Nej två miljoner är det, 20 miljoner kronor. För böter.
D – Det är helt sjukt.
M – Om man blir av med personuppgifter, och inte sköter det. Alltså har man verkligen [ohörbart] alltså sköter sig riktigt riktigt illa. Under lång tid och borde ha vetat bättre, och blir av med väldigt skyddsvärda uppgifter så kan man råka på väldigt dryga böter. Så helt plötsligt är inte bara detta en IT-säkerhetsfråga, nu är det helt plötsligt en ledningsfråga.
O – Ja.
M – För vi kan bli skadeståndsskyldiga, och bötersskyldiga. Få böter på det här. Så det är en sån här lite game-changer. Som gör att det här kommer nu inte att ligga på IT-säkerhet, utan på rektorn. För att det här kan bli kostsamt.

D – Jaja.
M – Så hur mycket pengar ska vi lägga för att skydda det här? Då börjar vi prata, liksom, vi ska ha försäkringar, vi ska köpa en försäkring. Vi måste se till oss att skydda det här, för annars kan det bli dyrt, och då kanske de är beredda att lägga en del pengar. I och med att nya reglerna från MSB så måste vi också börja utbilda vår personal. Så att ni håller vi på med en utbildningsinsats, som jag precis fick från säkerhetschefen, ska precis läsa igenom den. För att i början på maj ska vi börja skicka ut det här på prov till några fakulteter, oh det är alltså utbildningar av alla anställda. För staten måste utbilda alla anställda i IT-säkerhet.
D – Då får det kosta också.
M – Då får det börja kosta.
O – Så fort det blir en ledningsfråga.
M – Sådana saker lägger vi på säkerhetschefens bord. För säkerhetschefen är ansvarig för all säkerhet. Han är ytterst ansvarig för all säkerhet. Så även om jag får mina pengar från IT-kontoret så är jag underställd säkerhetschefen.
D – Mm.
M – När det gäller ansvar för IT-säkerhet, eller informationssäkerhet. Så att jag har egentligen två huvudmän. Så det beror på vad jag gör eller [ohörbart] pengarna. Det kan också ställa till lite problem.
D – Ja, det kan jag tänka mig.
M – Men hittills har det fungerat. Men som sagt sådana här andra grejer som kostar pengar som är stora, och gemensamma för universitetet, det är sånt som vi får skicka till säkerhetschefen.
D – Mm.
M – Det tar på hans budget. För jag har ju ingen budget.
D – Nähä okej.
M – Det enda som jag egentligen avsätter i budget, som kostar pengar, är utbildning.
D – Personlig utbildning för dig då?
M – Personlig utbildning för mig, och mina två kollegor.
D – Okej.
M - De ska, åtminstone en gång om året, få ha kvalificerad utbildning. Så det är mycket mycket viktigt.
D & O – Mm.
D – Så att resten av din budget så att säga, är det lite fria tyglar över eller?
M – Ja eller det är lite utrustning och sånt. Men det är inte.. Det är några hundratusen kanske. Men utbildningen, alltså en bra kurs någonstans i Europa eller USA, där kostar kursen 35-40 000.
D – Per näsa då? Per person.
M – Mm. Så är det ju resor och boende till det så att. En kurs går ju på uppåt 60 000 kr kanske. Så jag avsätter i alla fall 150 000 kr till kurs. Det tycker jag att vi behöver.
D – Ja ja, det är viktigt att få den kompetensen.
M – Inte bara kompetensen, utan det är en liten kick. Man får en liten sån inspirationskick, man får träffa folk som är jävligt jävligt duktiga.
O – Mm.
M – Man får ofta en massa bra tips. Och på de här större konferenserna så är det ofta en massa gratis utbildning också på sidan om. Så jag lägger mycket hellre pengarna där än köper pryler.
D – Ja det är klart, det är ju en investering i sig.
M – Sen gäller det att de inte slutar.
D – Jaja. Men så är det alltid, så att det…

M – Det var ju den här tekniska, eller finans, vad heter han.. Ekonomichefen som sa till tekniska chefen att ”tänk om vi nu lägger en massa pengar på personal, i utbildning, och de slutar?” Ja, sa tekniska chefen, tänk om vi skulle göra tvärtom. Och inte utbildar dem, och de stannar kvar. Det är mycket värre.
D – Ja oja. Det är världens förlust.
O – Är det någonting vi har missat?
D – Nej vi har ju egentligen haft lite mer, det är här motiverande och ekonomiska approachen på vår uppsats. Så jag tycker väl att det vi har kunnat få ut, har vi väl ändå nästan fått ut.
O – Ja jag tycker det är bra.
M – Ja, för som jag sa, jag har inga pengar.
D & O – Haha.
D – Nej precis.
M – Så att det är liksom inte ett så stort issue för mig.
D – Nej.
M – Och mäta, för vi gör inte så mycket investeringar. De investeringar vi gör, är i mantid och personer. Så när det gäller grejer vi har så är det begagnade grejer, i princip allting har vi bara plockat hos skroten. Då har vi en jävla massa gamla brandväggar, så att det har vi gott om. Vi har just fått ett lite [ohörbart] kluster som vi ska köra en wmware instans, ett litet lagringskabinett också. Som blev över när vi uppdaterade vår egen andra miljöer, så den ska vi ta och köra och lite små wmware instanser.
D – Ja, men..
O – Jag känner väl nästan att vi är klara. Om inte du har något själv som du vill tillägga?
M – Nej, jag ska iväg och dricka öl med pojkarna

7.3 Bilaga 3 – Transkribering Candy People

Företag: Candy People

Titel: IT-chef och operativchef

Plats och datum: Lund, Tisdagen 26 april 2016, 19.30-20.20.

Längd: 50 minuter.

D & O = Dennis och Omid, intervjuare

C = Carl, respondent

- Här inleds intervjun

O - Första punkten är, vad är din roll i företaget?
C - Jag sitter på rätt mycket men, de som gäller dessa punkterna är. System och IT.
O - Typ IT-ansvarig eller.
C - Jaja i högsta grad, men utöver har jag hand om verksamheten.
O – Okej.
C - Allting faller på mig oavsett vad det är.
O - Okej, ja.
O - Känner du till något om Return of Investment, Return of Security Investment, Intel IT Securtiy Model eller Gordon & Loeb. Det är olika modeller och uträkningssätt.
C - Nä, inte någon av dem. Intel IT Security Model har jag hört talas om.
O - Okej, den har du hört talats om. Snyggt. Det är den bästa, haha. Gillar att du känner till den bästa.
O - Tredje frågan är: Hur tänker ni angående IT och Informationssäkerhet i er organisation? Tänker endå att ni håller på med, ni omsätter, ett bolag som omsätter en hel del och om man tänker typ att. Hur värderar ni er information för annat folk liksom. Hur viktig är information, att den inte läcker?
C - Att den inte kommer ut menar du?
O - Gällande konkurrenter och annat folk, alltså hur värdesätter ni information ni har i bolaget till att faktiskt skydda den i form av IT och informationssäkerhet liksom
C - Den är ju jätteviktig. Den är ju viktig, det är ju inte dödsviktig i heller, på något sätt egentligen. Men informationen vi sitter på är ju konfidentiell såklart men den finns ju att få tag på annat håll.
O – Exakt.
C - Det finns ju alltid, det går ju alltid att komma runt också om du vill ha informationen. Så att det, vi är ju varken i första eller sist i ledet. Därför är det svårt att skydda sig 100 % och vi gör ju så gott vi kan. Eh, vi säkrar upp vår leverantör så gott det går. Vi är faktiskt, när vi kommer till IT så är våra leverantörer så långt bak i IT att de inte kan dela med sig av någon information.
O - Okej
C - De använder fax idag. Telefonfax.
O - Det är sjukt
C - Eh, där är någon som använder mejl, någon som plockar upp order, alltså typ lägga in det i sina system. Sen finns det dem som inte har någonting.
O – Okej.
C - Sen finns det de som är jättejätteavancerade, det är så stor kontrast. Så det finns inte ett riktigt sätt att jobba på.06.00.
O - När ni investerar i någon form av säkerhet, IT-lösning eller informationssäkerhetslösning. Använder ni er av någon modell då när ni gör det eller ni vet vad ni har för behov och sen kör ni på det och sen får ni se om det funkar eller inte
C - Det vi gör är att vi, jag, såhär funkar det, jag säger såhär till våra outsource partners. Ja vi behöver det här eller så säger jag vi har problem med det här hur kan vi lösa det? Vad är lösningen. Och sen presenterar dem vilka lösningar och vilka, vad de lösningarna ger oss sen tar vi ett beslut efter och sen implementerar vi dem.
O - Okej, så ni har liksom en annan partner ni gör detta med.
C – Ja vi outsourcar det ju.
O - Ja, precis.
C – 100 %
O - Okej

D - Då är det lite intressant, hur stor roll spelar kostanden liksom vad väger tyngst? Är det bästa lösningen eller är det den mest kostnadseffektiva lösningen, eller vad man ska säga.
C - Asså vi brukar ju, vi har ändrat vår modell, innan gick vi alltid efter det som var billigast. Så vi brukar gå efter just när det kommer till IT-säkerhet så är det väldigt svårt att säga vad är det som lönar sig. Oftast är det såhär att du inte vet att det lönar sig förrän det är någon som tar sig in det är då du vet att det lönar sig till dess är det en kostnad inget företag vill ta. För att det känns som en onödig kostnad. Ni får tänka såhär 95 % procent av alla företag idag de förstår inte säkerhet. Den enda gången de förstår det är när de får ett virus. De förstår annars inte vad är IT-säkerhet. Vad är det vi ska skydda, vem vill åt vår information, varför? De förstår inte det. Eh, och jag har precis fått igenom att vi ska höja säkerheten och bygga ut vårt system och sätta ut nya serverar och höja säkerheten med typ 300 % det ska vi göra i helgen. Just för att vi fick in det här ”Locky viruset”.
O - Mhmmm
C - Vet ni vilket det är?
O & D – Nej.
C - Det är ett virus som kommer via mejl och har man en användare i nätverket som öppnar detta mejlet och öppna filen så går viruset in och krypterar allting som finns i nätverket.
O & D - Mhm, oh fan.
C – Asså vi snackar om att den krypterar ALLT. Krypterar allt som är delat, allt, den krypterar allt.
O – Vadå har ni råkat ut för detta?
C: Vi råka ut för det för vi hade en av våra inköpare han är ju tvungen att ta emot filer.
O – Mm.
C - Eh, och då hade han öppnat en ZIP fil som han inte skulle öppna. Och den satte igång och krypterade saker i hela nätverket.
D - Oh fan.
C - Så tur så har han inte tillgång till allting men tillexempel om det hade varit jag, tillexempel. Så hade den ju, vi hade ju. Vi stängde ju ner Candy People ifrån klockan 16.00 till 03.00 på morgonen vi höll på i nästan 12 timmar med att få bort viruset. Och då hitta jag viruset på 8 minuter att det kom in i närverket.
D – Herregud.
O – Sjukt.
C - På 8 minuter 10:10.
O - Så sjukt.
C - Då har man bara spindlar som sitter och kollar du vet. Men det räcker inte. Just därför, folk förstår inte såna här saker händer om man inte lägger pengar. Du säger O, att vi omsätter mycket pengar. Men en dyrkostand fick oss att investera. Det då folk förstår att man måste lägga pengar på det.
O - Men hur gör Candy People, i sig då. Är ni proaktiva eller reaktiva? Väntar ni att något ska hända, sen löser ni problemet. Eller försöker ni skydda er från det innan det har hänt?
C - Vi har försökt skydda oss hela tiden, detta viruset är helt nytt vi är skyddade idag. Men just detta viruset. Asså, om du tänker. Jag pratade med vår outsource partner som har fördjupat sig i detta jättemycket och han säger att alla antivirus tillverkare, alla dem försöker jobba med det. Alla jobbar med Locky viruset. Ingen som har en lösning mot det, ingen som kan skydda sig.
O – Så sjukt.
D – Det är riktigt sjukt asså.
C – Ja, det sjukaste är at de vill ha pengar också.
D – Aah det är sånhär ransomware?

C – Jaja de låser upp dina grejer om du betalar.
O & D – Hahaha.
D – Så fräcka asså.
C – Jaja det är riktigt sjukt. De vill ju ha stora summor. Därför försöker vi skydda oss så mycket som vi kan ju.
D - Det händer ju alltid nytt liksom, det går inte alltid att vara hur proaktiv som helst heller.
C - Nä så klart, det är därför vi har en outsource partner gällande IT och informationssäkerhet för de är bra. De har koll. Riktigt bra koll.
O - När ni har gjort en investering, har ni någonsin blickat tillbaka och kollat hur mycket har vi fått i avkastning typ?
D – Det är i för sig också svårt. För det är ju lyckat, tills någon bryter sig igenom.
C – Ja såklart, vi har ju varit nöjda. Vi har haft ett säkerhetsintrång 2010. Och då gick vi över till en outsource partner helt och hållet sen dess har vi inte haft ett enda intrång eller ett ett enda problem under denna tiden.
O & D – Okej.
O - Och en anledning till att ni har en IT-säkerhetsinvestering, är det för det är ett kundkrav eller reglering eller för att er information är så värd att ni vill skydda er från alla andra?
C – Nummer 1 är att vi vill skydda oss från alla andra. Nummer 2 är ju att jag värdesätter det väldigt högt. Och därför har jag prioriterat det. Jag ser att det är viktigt. Men jag ser att det är en kostnad också. Vi hostade allting själva innan, nu har vi gått ifrån det och kör en hostad lösning, Exchange lösning. Och vi har väldigt väldigt hög säkerhet. Och om man jämför vad den kostade oss att hosta den själv. Med då att vi fick ha underhåll på servrar och såna här grejer. Så blev det ungefär samma kostnad, det blev ju lite dyrare men säkerheten blev högre och därför såklart, det är väldigt enkelt att välja.
O - Jaja det är bra.
C – Fast nä, än så länge vad jag kan säga så alla våra investeringar oavsett vilken IT-lösning vi har valt inom säkerhet eller inte så har det lönat sig. För annars hade vi inte gjort det. Sen är det den stora investeringen som kommer nu så får vi se, det är ju den vi får följa upp
D – Hur planerar du att följa upp den då liksom?
C – Ja jag hade ju tänkt tvinga in ett virus.
O & D – Haha.
O – Det är ju ett bra sätt att kolla det på.
C – Ja, jag hade tänkt göra det för att se om det verkligen har lönat sig att ha den.
D – så det är ren funktionalitet? Som ska utvärderas håller den vad den lovar eller är en säker så är det en bra investering liksom.
C – Exakt, det är ju framför allt säkerheten, den är högst prioriterad.
D – Men okej om man tänker, hur ehm, hur värderar ni eran information liksom? När bli en kostnad för en investering för hög för att vara en faktiskt vad den bidrar med?
O – Lite oklar fråga.
D – Ja, lite oklart men,
C – Jag förstår vad du menar. Jag hade nog sagt såhär att, beroende på vilka avtal man har så kan den kostanden öka hur mycket som helst. Om man tänker såhär, om man bara kolla af-färssystem ut och in priser avtal som står skrivna. Riktiga avtal med stora kedjor och liknande det är bära eller brista om de försvinner eller kommer ut. Det beror på vart man pekar, var man pekar hur vilka delar i området. Hade du frågat någon om inköpspris och så hade de sagt ”det är inte så noga det är okej” kollar man på rena avtal som är skrivna så pratar vi om något helt annat då kan man skydda och lägga hur mycket som helst för att man inte vill att det ska komma ut. Det är olika delar i området.
D – Det måste vara svårt att kvantifiera värdet på er information när den är så diffus.

C – Ja, och det är därför vi har valt att köra domän nätverk där vi delar upp säkerheten på olika delar på området. Olika delar i hela verksamheten vissa delar i området bryr man sig inte om, de kan vara helt öppna i princip. De andra är säkra så inget kan hända. Där finns liksom ingen kontakt med omvärlden i princip. Känns frågan besvarad?
D – Ja det tycker jag ändå. Det är ju ett bra svar på en klurig och oklar fråga.
C- Ja
O – Vad har vi mer D?
Deniis – Ska vi se. Ja men det är ju lite typ en investering. Är det ett krav att det ska kunna underlätta processer osv eller bara full fokus på säkerheten eller ska det ha någon arbetsnytta?
C - Ja asså. Vi har inte gjort en enda investering som vi inte har skrivit själva.
D – Så tiden är viktig också liksom?
C - Den är jätteviktig. Det finns, jag hade aldrig fått för mig att göra en investering i bolaget idag som skulle ta tid av någon. Det är dubbla kostnader.
D – Om man tänker på att om vi sänker tillgängligheten, så kanske det är otroligt mycket säkrare men det kommer ta längre tid för folk att arbeta. För de som ska hantera information en osv. Det kan vara en svår.
C - Ah du menar så. Jojo det är ju asså, man får ge och ta men där finns alltid sätt att lösa det på. Vi ser bara tillexempel våra dokument. Man ska kunna dela dokument med alla andra. Ja okej, då får man sätta upp en delningspunkt och vissa personer får då ha tillgång till den och vissa personer som kan få se vissa saker osv osv. Bara kan göra vissa saker, bara läsa kanske bara skriva osv osv. Jovisst det ställer till det men, det är ett systematiskt sätt att arbeta på och inom rimliga gränser kan man göra det men inte för mycket. För blir det för mycket bli det plötsligt mycket tid och då kommer folk börja hitta genvägar för att lösa, eller för att inte göra det på rätt sätt så att säga.
D & O – Mmm.
C – Förstår ni hur jag menar?
D – Ja absolut.
O – Ehm, vad har vi mer vi kan fråga.
D - Hur ser ni på det här med nya risker och hot. Gör ni kontinuerliga riskanalyser?
O – Eller är det er outsource partner som tar hand om det? De som kollar upp det och fixar det åt er och säger C nu har det kommit ett nytt hot och vi måste skydda oss mot för att det kan skada er såhär liksom.
C – Jag kan ju säga såhär, vår outsource partner är ju kopplad till företaget 24/7. Han har ju full kontroll på allt. Han sitter och uppdaterar våra brandväggar och sånt hela tiden. De uppdaterar allt hela tiden så, så fort något händer så uppdaterar han dem. Men skulle det vara något specifikt som vi måste åtgärda så är det vår outsource partner som tar kontakt med mig. Jag är absolut inte insatt som han är, inte ens hälften av den kollen han har. Inte ens 70 %.
O – Så ni har en person som tar hand om hela verksamheten gällande IT-säkerhet.
C – Ja, vi outsourcar hela vår IT-lösning till vår partner och de sköter allting liksom.
O – Najs.
C – Det är egentligen så vi jobbar.
O – Och det är för de har spetskompetensen eller? Och för att de har tid att göra det för det är deras grej?
C – Jaja de är grymt duktiga. Anledningen till att jag vet det är för att har jobbat med dem. Det är framförallt spetskompetensen de är grymt duktiga.
O – Men om er partner kommer med en lösning till er, detta måste ni göra. Förklarar han hur er avkastning på investering kommer vara inom 5 år och om ni inte gör det så tar ni denna smällen liksom? Eller er partner pratar inte siffror eller modeller alls?

C – Jo ungefär så. Vi har ju haft denna dialogen nu när vi ska uppgradera våra serverar och hela paketet. Den har vi haft i ungefär 1 år, jag har sagt vi kör vilken dag du vill. Men det har varit en budget fråga. Jag har sagt okej, och när viruset kom så sa dem kör. Det är dumt. Och det är också så att alla företagare har en ledning och det är de som tar beslutet. jag kan tycka givetvis, jag kan tycka, men jag har inte sista ordet.
O – Ja.
C – Så att, ja. Det är alltid högsta hönset som har sista ordet. Är han med?
O – Ja precis.
C – Det är tråkigt.
O – Jag är skitnöjd
D – Jag med, bra svar.
O – Ja. Jag vet inte om vi har något mer att säga, har vi det D?
D – Nä inte vad jag kommer på nu.
O – är det okej om vi återkommer till dig C om det är någonting någon dag?
C – Absolut, gör de.
O – Tack så mycket så hörs vi.
C – Tack själv

7.4 Bilaga 4 – Anteckning anonym respondent

Då respondenten ville var anonym är det anteckningar från samtalet. Omid höll intervjun och Dennis antecknade respondentens svar.

Företag: Anonymt

Titel: Group Security Manager

Plats och datum: Lund. Tisdag 27 april 2016, 10.10–11.00.

Längd: 50 minuter

- Här inleds anteckningarna

Roll - Group Security Manager

Känner till ROSI

Säkerhet värderas högt. Kärnaffären core business - marknaden och kunderna. I vissa fall ägarstrukturen som avgör hur man ska positionera sig gällande säkerhetsskalan gällande IT.

Delar man information i fysisk och informationssäkerhet, dvs information i alla former. Går man in och delar på dessa skapas det förvirring. Brukar säga säkerhet - ett enhetligt ord. Många kan inte skilja på IT-säkerhet. Infosäkerhet är en IT fråga. ROSI kan implementeras på kameror osv och olika säkerhetskontroller.

Nej. Använder oss av intäktsformen. Köper vi något som kostar så mycket, räknas på kostnader och gör ett business case. Vad kostar det, vad kan vi sälja det för. Vad är mellanskillnaden - dvs. vad kan vi tjäna? Identifierar ett behov från kunder eller marknaden. Om några kunder kommer med behovet är det inte värd investeringen. Kommer fler kunder med behovet om lösningen kostar en miljon om året. Är det inte värt det då.

Kan vara ett kundkrav - dvs. uppfyller man inte kravet kan man inte vinna upphandlingen. Det kan påverka business case - kollar i koppling till affären. Kan tänka sig en kostnadsförlust.

Man ser det ofta som ett IT-projekt även fast det inte är det. Den lösningen, XXX drev business case tillsambas med ansvariga. Måste vi köpa in det, och på vilket sätt? Kalkylera på hur kostnaden ska spridas över tid.

Kunder kommer med ett krav, för att sedan bli ett baskrav. Är man duktig och affärsorienterad kan man köpa något inte många kunder har som krav och sedan erbjuda det som en tjänst. Gör det som en tjänst till förlust i början för att sedan göra vinst på det.

I framtiden kommer fler kunder 5- 10 osv, det ökar. Om det ökar gör vi investeringen. Har affärsmässig approach - göra business case och sedan proof of concept. Det vill säga passar det företaget som ska ha tjänsten. Gäller även för licensmodeller.

Lägger inte för mycket pengar - man kan signa lösningen beroende på hur många kunder. När vi tittade på funktionaliteten - vi kan välja topp 10 lösningar från Gartner. Vi kanske inte väljer den bästa, men tar den med bra funktionalitet och licensmodell så vi kan signa den till kunder.

Behovet uppstår via marknaden eller kunder - för att sedan initieras.

Tror inte att säkerhetschef ska säga vad som behövs. Det kommer som ett incidentkrav på grund av att något har hänt. (Reaktivt) Man löser säkerhets och affärsrisker. Det är krav från marknaden eller compliance krav som ställs på branschen.

Hur stor del av it budgeten går till säkerhet? – Brukar säga att cirka 5-7% av företagets totala omsättning går till IT-budgeten. Säkerhetssidan handlar oftast om IT. Av 5-7% går 5 % till säkerhet. Om företaget har produktionsanläggningar och fysiska locations finns det en overhead, och pengar går till fysisk säkerhet. Säkra dörrar, väggar, kameror är också säkerhet, Vilket kan leda till att det blir dubbla.

Beroende på vilket företag - renodlade IT-företag t.ex. Swish och Klarna kanske lägger cirka 10 %. IT företag har större benägenhet att skydda sin IT och lägga pengar på säkerhet på IT-sidan.

Fysiska företag kanske 3 % på it och 7 % på fysisk säkerhet. 10 % av 5 % är XXX uppskattning för företag som har fysisk produktion. 50 % IT 50 % produktion lägger man kanske 0.5% av totala omsättningen. Beror på vinst och hur mycket säkerheten kan bidra till vinsten. Gör den ingenting blir det mindre, gör den mycket får den större delen.

Säkerheten dras ofta till IT, och felkalkyleras ofta. Det är fel. Man förbiser bevakning och fysiska säkerheten och investeringar. Den totala omsättningen skall säkerheten relateras till.

Utvärdering i efterhand. Det finns inte. Om det t.ex. gäller brandvägg ses inte längre som en säkerhetskontroll. Brandväggen dirigerar om trafik vilket är grund funktionalitet. Brandvägg antivirus osv har blivit de facto IT. Basbehov förändras. Basbehoven har förändras gällande företag och brandväggar t.ex. Alla förväntas ha dessa kontroller.

En renodlad säkerhetskontroll som IPS eller IDS som inte är standard. Vilket går att göra en kalkyl på. När de köpts sådana lösningar är företag dåliga på att göra en efteranalys. De flesta företag har varit dåliga. Därför att de säkerhetschefer och de tekniska är inga affärsmänniskor och kan inte detta. Kan inte ompröva sina finansiella beslut. Få som kan göra det - jobbar man inom IT kan man inte. Jobbar man på c-level kanske man kan men 70-80% av dessa kan inte. Det görs alltså inte. XXX kan från egen erfarenhet - har försökt.

Man kan skydda sig mot detta och väljer en licensmodell där man inte köper för mycket utan vad man behöver så att man går +/-0. Man skyddar sig. Man vet kostnaden. Ex. Om lösningen per enhet kostar 300kr/år + 100 administrativt. Mot kunden säljs det för 700 per år. Gör man på detta sätt så har man ett system som lönar sig. Vi har system som klarar av våra behov om det inte går att sälja tjänsten. Om kunder är intresserade går det att sälja och tjäna pengar. XXX vill göra återkopplingar per år för att se arbetsnyttan. Lönar det sig inte så bör det avvecklas.

När kraven inte uppfylls anses investeringen inte lyckad. Staten, regler, compliance och så vidare kräver. Interna och externa krav. Kunder har sina krav, branschen och lagar har sina egna krav. Lösningen är inte lyckad när kraven inte kan uppfyllas.

Business case ska inkludera tiden för anställda som påverkas. En bra säkerhetskontroll ska inte kännas vid, men det ska finnas där. Processtiden skall inkluderas i business case. Ex. Vi byter passagesystem, och inte längre använda kort utan också kod. Det är förlängning på 10 sekunder. Om det handlar om timmar och halvtimmar, 30 min på 1000 människor blir 500 timmar. Hur många inloggningar per dag? Det är något som måste ta hänsyn till. Detta ska läggas in business case.

Man kan köpa in något som behöver övervakning vilket kräver personer som engagerar sig i detta. Vilket kräver en förbättring av process vilket blir svårt för ingen vill göra mer. Eller anställa fler personer. Måste finnas i business case. Om det inte inkluderas så har man inte gjort en bra business case.

Proaktivt/Reaktivt - Allting beror på. Beror på kostnad och mognadsgrad för företaget. Implementering. Efter en riskanalys görs bedömning. Om det ska köpas en lösning - vad kostar det,

implementeringstid, fördelar? Det går att få en bra lösning till bra pris, med längre implementeringstid. Men företaget är inte redo för det när det kommer till infrastruktur, kunskap osv. Kan även saknas processer för det. För att implementera en kontroll krävs det vissa input, om dessa inte är redo så går det inte att köpa dem. Ex, om du inte vet vad som finns i förrådet är det onödigt att köpa en databas eftersom du inte vet vad som ska läggas in. Riskanalysen är A/O. Riskanalys bygger business case. Krav. Interna krav kommer från en riskanalys. 3 flöden för krav som resulterar i business case. Interna efter en risk har uppstått eller på väg att uppstå. Kundkrav samt compliance.

Det saknas styrning hos universitet menar XXX. Strategisk, taktiskt operativa. De jobbar operativt men inte strategiskt och taktiskt.

Var missnöjd med t.ex. ROSI och andra modeller. Gick i tankarna om att själv definiera eller skapa en metodik som är mer affärsorienterad. Få människor har en affärsbakgrund vilket gör många fastnar i det tekniska men ser inte annat. Det tekniska ser inte påverkan hos företagets business. De tänker inte ur ett affärssätt och kan då inte heller prata på det sättet, och hamnar då hos tekniken

Referenser

Al-Humaigani, M. and Dunn, D., 2003. A model of return on investment for information systems security. *Circuits and Systems*, *1*, pp. 483-485.

AO'Brien, J., Marakas, G.M., 2006. Management information systems. *DIAS Techonolgy Review*, 4(2), pp. 102-103.

Berinato, S., 2002. *Finally, a real return on security spending*. [Online] Från: http://www.cio.com/article/2440999/metrics/finally--a-real-return-on-security-spending.html. [Besökt: 2016-04-11]

Bodin, L.D., Gordon, L.A. and Loeb, M.P., 2005. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, *48*(2), pp.78-83.

Business Roundtable 2007. *Growing Business Dependence on the Internet*. [pdf] Business Roundtable. Från: http://businessroundtable.org/sites/default/files/200709_Growing_Business_Dependence_on_the_Internet.pdf [Besökt 2016-04-04]

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L., 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), pp.431-448.

Carty, M., Pimont, V. och Schmid, D.W., 2012. *Measuring the Value of Information Security Investments*. [pdf] Intel. Från: http://www.intel.fr/content/dam/www/public/us/en/documents/best-practices/information-security-investments-paper.pdf. [Besökt 2016-04-04].

Chai, S., Kim, M. and Rao, H.R., 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), pp.651-661.

Dhillon, G., 2006. *Principles of Information Systems Security: text and cases* New York, NY: Wiley.

Dutta, A. och Roy, R., 2008. Dynamics of organizational information security. *System Dynamics Review*, *24*(3), pp.349-375.

Dynes, S. and Freeman, M., 2007. Cyber security: Are economic incentives adequate?. In: E. Goetz och S. Shenoi, ed. 2008. *Critical infrastructure protection.* New York, NY: Springer. pp. 15-27.

European Network and Information Security Agency (ENISA), 2012. *Introduction to Return on Security Investment*. Heraklion: ENISA.

Gallaher, M.P., Rowe, B.R., Rogozhin, A.V. and Link, A.N., 2006. *Economic Analysis of Cyber Security*. Research Triangle Park: Research Triangle Institute.

Gordon, L.A. and Loeb, M.P., 2002. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), pp.438-457.

Henze, D., 2002. *IT baseline protection manual*. Bonn: Federal Agency for Security in Information Technology.

Investopedia.com, 2003. *Return on investment – ROI*. [Online] Från: http://www.investopedia.com/terms/r/returnoninvestment.asp [Besökt 2016-04-06].

International Organization for Standardization and International Electrotechnical Commission, 2005. ISO 27002 - *Information Technology: Security Techniques: Code of Practice for Information Security Management*. Genève: ISO/IEC.

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

Kwon, J. and Johnson, M.E., 2011. An Organizational Learning Perspective on Proactive vs. Reactive investment in Information Security. In*: 10th Annual Workshop on the Economics of Information Security (WEIS).*

Locher, C., 2005*. Methodologies for evaluating information security investments-What Basel II can change in the financial industry*. [pdf] Association of Information Systems*.* Från: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1136&context=ecis2005 [Besökt 2016-05-02].

Lundström, M., 2016. *Kundens tillit är CIO:s ansvar*. [Online] Från: https://www.atea.se/sidor/artikel/trendspaning-james-mcnab-cisco/. [Besökt 2016-04-11]

Putvinski, M. 2009*. IT Security Series Part 1: Information Security Best Practices*. [Online] Från: http://corporatecomplianceinsights.com/information-security-best-practices/. [Besökt 2016-05-03].

Qian, Y., Fang, Y. och Gonzalez, J.J., 2012. Managing information security risks during new technology adoption. C*omputers & Security*, *31*(8), pp.859-869.

Rosencrance, L., 2002. . Melissa virus creator sentenced to 20 months in prison. *Computerworld*, [Online] 1 maj. Från: http://www.computerworld.com/article/2575637/security0/melissa-virus-creator-sentenced-to-20-months-in-prison.html [Besökt 2016-04-04].

Sonnenreich, W., Albanese, J. and Stout, B., 2006. Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and practice in Information Technology*, *38*(1), pp.45-56.

Symantec Security Response, 2006. *Timeline of Major Events in Internet Security*. Symantec. Från: https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Timeline.pdf [Besökt 2016-04-04].

Tsiakis, T. and Stephanides, G., 2005. The economic approach of information security. *Computers & Security*, *24*(2), pp.105-108.

Whitman, M. and Mattord, H., 2011. *Principles of information security*. Boston: Cengage Learning.

Yayla, A. and Hu, Q., 2005. The impact of security breaches on the value of stocks: a short-term vs. long-term perspective. In *Proceedings of the Annual Conference of IS in Asia-Pacific (ISAP 2005), December* (Vol. 10).

Öğüt, H., Raghunathan, S. and Menon, N., 2011. Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), pp.497-512.