Informationssäkerhet och ekonomi

Ett skannande projekt av aktuell forskning

JONAS HERMELIN, HENRIK KARLZÉN, PETER NILSSON

FOI-R--3927--SE
ISSN 1650-1942 Augusti 2014

Jonas Hermelin
Henrik Karlzén
Peter Nilsson

Informationssäkerhet och ekonomi

Ett skannande projekt av aktuell forskning

Titel	Informationssäkerhet och ekonomi – Ett skannande projekt av aktuell forskning
Title	Information security and economics – scanning the research frontier
Rapportnr/Report no	FOI-R--3927--SE
Månad/Month	Aug
Utgivningsår/Year	2014
Antal sidor/Pages	57 p
ISSN	1650-1942
Kund/Customer	Internt projekt / Internal project
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	I354151
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem (IAS)

Sammanfattning

Att investera i informationssäkerhet är idag mer självklart än tidigare inom många verksamheter. Samtidigt som brister i informationssäkerheten kan medföra stora negativa effekter, både monetära och ickemonetära, kan även bibehållandet av höga säkerhetsnivåer vara en mycket kostnadsdrivande faktor. Skyddsåtgärder kan både vara dyrt att införa och negativt påverka verksamheten genom att försvåra flexibla och produktiva arbetssätt. Ett sätt att hantera avvägningen för vad som är en lämplig nivå av informationssäkerhet är att nyttja ekonomiska modeller och metoder för riskhantering. Dessa modeller och metoder kan bidra med ramverk för hantering och jämförelse av risker och kostnader.

Syftet med denna rapport är att redovisa vad som är aktuell forskning inom gränslandet mellan informationssäkerhet och ekonomi. Litteraturöversikten visar på ett aktivt forskningsområde där det föreslagits en mångfald av metoder för beräkning av optimala investeringsnivåer. På grund av avsaknad av tillförlitlig indata till beräkningarna och att det saknas faktiska utvärderingar kvarstår dock många frågetecken gällande praktisk tillämpning av och nytta med dessa metoder, utöver att vara teoretiska ramverk. Förutom optimeringsberäkningar utforskar litteraturen även frågor rörande insamling och användning av mätdata och domänexperters bedömningar. Slutligen finns även en diskussion som rör hur och när beslut gällande investeringar tas och bör tas.

Exempel på intressanta uppslag för framtida forskning är vidare studier gällande hur beslut och inriktning av informationssäkerhet faktiskt sker inom olika typer av verksamheter. Vilken utgångspunkt har organisationer vid beslut och avvägning mellan risker och vad påverkar dem? Vilka metoder används idag och hur förhåller de sig till den aktuella forskningen?

Nyckelord: informationssäkerhet, ekonomi, säkerhetsinvestering, optimering, verksamhetsstyrning, riskhantering

Summary

To balance the risk and cost of potential security breaches with the benefit and total cost of a security investment is a considerable undertaking. Vulnerabilities in information security of organizations can induce major expenses, both monetary and non-monetary. Tight security requirements might on the other hand be a wildly cost-driving factor, both directly as an investment cost and indirectly if they hinder more flexible and efficient work processes. One approach to face this challenge is to make use of methods from economics.

The aim of this survey is to give an overview of current research topics bridging the domains of information security and economics. The crossover between information security and economics is an active research domain that covers several research topics. The research covers investment optimizing, investment strategies, the problems of collecting reliable data and how to handle low probability events. A common shortcoming shared by many of the optimizing methods described here is the presumption of precise data regarding threat frequencies, consequence costs and effectiveness of investments, data that is very scarce and perhaps impossible to fully obtain. These proposed methods are mainly theoretical constructs with uncertain practical use. This is underlined by the fact that no evaluations of the methods have been found.

Given the theoretical methods proposed in literature it would be valid to investigate in which ways organizations actually plan their information security investments today. How do organizations approach this issue, which methods are in use and how are they used? What are the differences between actual practice and literature?

Keywords:

Information security, economics, security investment, optimization, operations management, risk management

Innehållsförteckning

1 Inledning

Informationssäkerhet är ett begrepp som inkluderar ett flertal aspekter som rör hur information ska skyddas från otillbörlig spridning, ändring och användning, men samtidigt även vara tillgänglig för behöriga användare. Dessa egenskaper benämns ofta som krav på sekretess, riktighet och tillgänglighet. Vikten av informationssäkerhet har visats genom en lång rad intrång i IT-system resulterande i oönskad spridning av information – händelser som har skadat kommersiella företag men även offentliga organisationer och myndigheter. Antalet incidenter kopplade till informationssäkerhet är stort och kostnaderna som följer av dessa förväntas öka ytterligare (ISBS, 2012). En svår avvägning som måste göras i samband med systemutveckling är just hur stort fokus som behöver läggas på informationssäkerheten. En hög säkerhetsnivå kan vara en mycket kostnadsdrivande faktor, inte bara rent ekonomiskt utan även verksamhetsmässigt eftersom verksamheten kan påverkas negativt genom att arbetet försvåras (Anderson et al., 2012; Economides, 2010). Ett vardagligt exempel är komplicerade tillträdesskydd eller inloggningsfunktioner med krav på komplexa lösenord.

För låg informationssäkerhet innebär å andra sidan en ökad risk för intrång och om detta inte anses godtagbart innebär det att systemet inte kan användas. Det senare är relevant för Försvarsmakten som har mycket högt ställda krav på informationssäkerhet för att IT-system ska få börja användas. Försvarsmaktens *ackrediteringsprocess* innebär att alla IT-system granskas och godkänns utifrån dess informationssäkerhet innan de godkänns för införande och användning. Har inte informationssäkerheten i tidigare skeden beaktats kan det leda till merkostnader ifall problem upptäckts i samband med denna granskning. I extrema fall kan det även innebära att funktionalitet måste tas bort eller att systemet inte kan användas. Av dessa anledningar är det viktigt att tidigt analysera och uppskatta vilken nivå av informationssäkerhet som är nödvändig och lämplig utan att göra överdrivna investeringar.

Ett sätt att utvärdera om rätt satsningar görs på informationssäkerhet är att nyttja ekonomiska modeller och metoder för att beräkna vilken nivå av säkerhetsinvesteringar som är ekonomiskt lämplig samt att bedöma effekten av tidigare investeringar. Forskningsfrågorna som utforskas i denna rapport är därmed följande:

> *Vilka faktorer påverkar graden och typen av investeringar i informationssäkerhet?*
>
> *Vilka metoder finns det för att ta fram underlag för beslut rörande investeringar i informationssäkerhet?*

För att besvara dessa forskningsfrågor beskrivs i denna studie den aktuella vetenskapliga diskursen om kombinationen av ekonomi och informations-

säkerhet. Vad som inte omfattas är analys om indelning av olika typer av hot, varför riktlinjer följs eller inte följs, psykologiska faktorer i investeringsbeslut samt hur uppskattningar av säkerhet för specifika system eller teknik görs.

1.1 Terminologi

Huvuddelen av de artiklar som ligger till grund för studien är inte skrivna av informationssäkerhetsexperter utan av forskare från andra discipliner som exempelvis ekonomi, statistik och organisationsteori. Detta innebär att språkbruket kan skilja sig från litteratur författad av informationssäkerhetsexperter. För att förtydliga listas här de centrala begrepp som används i rapporten:

Hot är sådant som, om inte skyddsmekanismerna stoppar det, kan ge upphov till incidenter. Den eller det som står bakom hotet kallas hotaktör och kan vara antingen en *antagonist* (en medveten angripare) eller *icke-antagonist* (naturkatastrof eller misstag). I den här rapporten beskriver vi främst antagonistiska hot vilket är anledningen till att hot och *angrepp* används närmast synonymt.

Incidenter är händelser som har negativa konsekvenser för den som utsätts för händelsen. Eftersom enbart händelser med negativa konsekvenser är intressanta i rapporten, används händelse och incident i princip synonymt.

Sårbarhet är en brist (eller ibland flera brister) i skyddet och möjliggör därför att hot och angrepp ger upphov till incidenter. Hur allvarlig sårbarheten är mäts ofta i termer av sannolikhet för att ett givet angrepp lyckas ur angriparens perspektiv. Ibland diskuteras sannolikhet uppdelat på sannolikheten att ett angrepp sker och sannolikheten att, givet ett angrepp, att ett angrepp skulle lyckas. Det är det senare fallet som kallas sårbarhet.

Förväntad förlust är en funktion av kostnaden för en negativ händelse samt händelsens förväntade frekvens (eller sannolikhet). Funktionen beräknas ofta genom multiplikation av operanderna men även andra varianter förekommer.

Risk är förknippat med ovisshet och beskrivs ofta som kombinationen av sannolikheten för en negativ händelse samt händelsens konsekvens. Risk är därmed ungefär synonymt med förväntad förlust men är också beteckningen för det övergripande område där man analyserar och hanterar dessa händelser. Ibland används risk dock på ett sätt som fokuserar mer på sannolikheten än kombinationen av sannolikhet och konsekvens. Till exempel ”risk för regn” lyfter fram sannolikhetskomponenten i att ”regn utgör en risk”.

2 Bakgrund

Ett tidigt steg i att koppla samman informationssäkerhet med ekonomi var genom att börja använda metoder för riskhantering för att värdera behovet av informationssäkerhet. Detta skedde 1979 när National Bureau of Standards gav ut *Federal Information Processing Standard* (FIPS) 65 som utgjorde en standard för att bedöma risker associerade med stora datacenter. I denna standard introducerades en metod för att mäta datorrelaterade risker enligt metriken *Annual Loss Expectancy* (ALE) – ett mått på den förväntade årliga förlusten som följd av datorrelaterade risker (Soo Hoo, 2000). ALE bygger på att kostnaden för incidenter multipliceras med dess förväntade frekvens. Denna sammanslagning av kostnad och frekvens ansågs vara en stor fördel genom att förenkla beräkningarna, men innebär även att metriken inte kan skilja på högfrekventa incidenter med liten påverkan och lågfrekventa incidenter med stor påverkan – två olika fall som i verksamheten kan innebära stor skillnad. Genom att sedan summera konsekvenserna av alla tänkbara incidenter får man en total bedömd årskostnad (Soo Hoo, 2000).

$$\mathrm{ALE} = \sum_{i=1}^{n} I(O_i)F_i$$

$$O_i = \text{Incident}$$
$$I(O_i) = \text{konsekvens av Incident i}$$
$$F_i = \text{Frekvens för Incident i}$$

Figur 1. Den förväntade årliga förlusten utgörs av summan av alla tänkbara skadliga händelser multiplicerade med deras frekvens (Soo Hoo, 2000).

Under 1980-talet initierades forskningsprogram som resulterade i den första generationens riskhanteringsmodeller för informationssäkerhet vilka baserades på ALE. De olika metoder som uppstod utifrån detta kan enligt Soo Hoo (2000) gruppernas under benämningen *The Common Framework.* Detta ramverk la grunden för flera olika implementeringar i form av verktygsstöd och metoder under slutet av 1980-talet och en bit in på 1990-talet. Ramverket propagerade för en iterativ bedömning av en rad faktorer: tillgångar, säkerhetsaspekter (sekretess, riktighet och tillgänglighet), hot (t.ex. antagonister och naturliga), skydd och sårbarheter. Dessa faktorer kombinerades till en beräknad förlust med ALE. Den beräknade förslusten jämfördes sedan med fastställda krav på förlust, alltså vad som ansågs som en godtagbar förlust. Processen för att beräkna den förväntade försluten bestod av 7 steg, som itererades tills en godtagbar säkerhetsnivå var identifierad:

1. Identifiering av krav som anger vilken förväntade förslut som är godtagbar
2. Värdering av tillgångar
3. Identifiering av hot, sårbarheter och skydd
4. Analys av hot och sårbarheter samt generering och analys av scenarion
5. Riskberäkning
6. Acceptanstestning av förväntad förlust mot identifierade krav
7. Identifiering och analys av nödvändiga åtgärder för att minska gapet mellan krav och genomförda analyser

Ramverket fick dock aldrig någon större spridning och föll ur användning och standarden som introducerade ALE drogs tillbaka 1995. Trots det har ALE påverkat huvuddelen av efterkommande beräkningsmodeller och används även som metrik i nutida metoder som *Return of Security Investment* (ROSI). I senare modeller har händelsefrekvensen dock ersatts med sannolikhet. Detta mått har även förfinats genom en uppdelning av (1) sannolikheten att ett angrepp sker och (2) givet ett angrepp, sannolikheten för att det lyckas.

Att ansatserna under 1990-talet som låg inom ramen för *The Common Framework* inte blev framgångsriska förklaras av Soo Hoo (2000) utifrån tre orsaker. Den första (1) orsaken var att metoderna förespråkade en sådan detaljeringsgrad för scenarion som användes att det i praktiken blev orimligt att genomföra analyserna. Detta grundade sig i synen att system antingen var *säkra* eller *inte säkra* varför dessa tidiga modeller ville beskriva alla hot, tillgångar och sårbarheter – både hög- och lågfrekventa. Den andra (2) orsaken grundar sig i ett deterministiskt synsätt där alla variabler var tvungna att specificeras exakt snarare än som spann eller baserade på sannolikheter. Den tredje (3) orsaken var att metoden krävde tillgång till svårtillgänglig data för att beräkna de förväntade konsekvenserna och dessas frekvenser. Detta är information som även idag är mycket svår att ta reda på. Komplexitet, bristande hantering av ovisshet och avsaknad av data kan alltså ses som de orsaker vilka kraftigt begränsade ansatserna från 1990-talet.

Ur dessa erfarenheter går det enligt Soo Hoo (2000) att se utvecklingen till den andra generationens ansatser vilka går att dela in i fyra generella inriktningar: *Integrated Business Risk Management*, *Valuation-Driven Methodologies*, *Scenario Analysis Approches* och *Best Practices*.

Integrated Business Risk Management utgår från tanken att riskerna kopplade till IT-system är affärsrisker och ska därför hanteras som alla andra sådana. Modelleringen av risker rör sig här ifrån tekniska detaljer för att istället fokusera på inverkan på affärer och värdeökningen som följer av att man skyddar sig mot risker. Att analys sker på en högre konceptuell nivå innebär att en mer detaljerad

teknisk analys krävs som en uppföljande fas efter att en affärsinriktad plan för att skydda tillgångarna fastslagits.

Valuation-Driven Methodologies tar fasta på problemet att uppskatta sannoliketen för att incidenter sker genom att ta bort dem helt från ekvationen och enbart fokusera på värderingen av tillgångar. Att bortse från kostnader för skydd, effektivitet hos skydd och frekvensen av angrepp innebär dock risk för både över- och underdrivet skydd. Ansatsen ger stöd för att standardisera säkerhetsarbetet, men förenklingarna gör att det inte går att utvärdera investeringarna eller förfina de säkerhetskrav som ställts varför Soo Hoo (2000) menar att det inte är en långsiktig lösning. Problemet med värdering av tillgångar är flera och Jaquith (2007) menar att det saknas konsensus om hur värde ska definieras på en konceptuell nivå och ännu mer hur det ska mätas konsekvent och över tid. Däremot är det enklare att identifiera vad som benämns som kritiska tillångar (critical assets), vilket är de tillgångar där organisationen helt saknar risktolerans.

Scenario Analysis Approches fokuserar på att utveckla scenarion för hur säkerhetsincidenter kan ske och använder även penetrationsförsök som demonstration för bristande säkerhet. De scenariobaserade ansatserna används för att sprida kunskap hur allvarliga konsekvenser en aktuella risknivån kan innebära. Strategier för riskhantering baseras sedan på de scenarion som bedöms vara mest troliga och allvarligast. Medan ansatsen förenklar arbetet och skapar spårbara analyser begränsas analysen och skyddet till endast de scenarion som inkluderas. Soo Hoo (2000) menar även att ansatsen inte uppmuntrar en utökad insamling av data gällande säkerhet och riskerar att invagga organisationer i en känsla av falsk säkerhet, eftersom ansträngningar fokuseras på ett begränsat antal scenario.

Best practices är den sista inriktningen och fokuserar på problemen med avsaknad av data samt avsaknaden av formella analysmetoder för att bedöma vad som är en lämplig säkerhetsnivå (Soo Hoo, 2000). Genom att definiera och följa vad som fastslagits som best practices kan analysfasen undvikas helt. En fara med en sådan ansats är att fokus hamnar på att uppfylla angivna standarder snarare än att hantera de faktiska riskerna för organisationen i fråga. I och med att ansatsen inte förlitar sig på kvantitativa analyser innebär det även att det saknas incitament för datainsamling gällande incidenter och kostnader för dessa. Detta riskerar att leda till en ökad okunskap om de faktiska förhållandena.

Soo Hoo (2000) ansåg att dessa typer av ansatser var alltför förenklade och kortsiktiga varför en återgång till mer kvantitativa modeller var att vänta. En sådan återgång går att skönja redan ett par år senare med publiceringen av ett arbete av Gordon och Loeb (2002) som sedermera har fått ett stort genomslag. De presenterar här en ny metod för att beräkna den optimala nivån av investeringar i informationssäkerhetsskydd och att denna nivå aldrig överstiger knappt 37 % av värdet som kan gå förlorat. Detta beskrivs närmare i avsnittet

4.2.1 om statistiska metoder. Gordon och Loeb (2002) argumenterade även för att investeringar endast är ekonomiskt försvarbara för ett mellanskikt av sårbarheter när det gäller vissa hot. Investeringar för att skydda sig mot extremt stora eller små sårbarheter är i deras modell inte ekonomiskt försvarbart.

Användningen av traditionella ekonomiska modeller för att beräkna optimal investeringsnivå verkar ha fått ett uppsving under 2000-talet. En sådan metod är *return-of-security-investment* (ROSI) som enligt Brotby (2009) introducerades omkring 2002. Metoden är lik den traditionella *return-of-investment* (ROI) som beräknar vilket värde en investering genererar minus investeringens storlek. Dessutom ges summan i förhållande till investeringens storlek för att beräkna hur stor nettovinsten blir per krona. Skillnaden med ROSI är att istället för att basera uträkningen på den förväntade vinsten används istället den förväntad minskning av förlust (Enisa, 2012). I sin enklaste form sker beräkningen som följande:

$$ROSI = \frac{Reduktion\ av\ monetär\ förlust - Årlig\ kostnad\ för\ säkerhetsinvestering}{Årlig\ kostnad\ för\ säkerhetsinvestering}$$

$$Reduktion\ av\ monetär\ förlust = ALE * Effektivitet\ hos\ investering$$

Användning av ALE som en del av ROSI kritiseras dock av Jaquith (2007) som lyfter fram tre brister hos ALE som metrik. Den första bristen är att ALE beräknas på uppskattade medelkostnader medan de faktiska kostnaderna tenderar att hålla sig närmre extremerna. Den andra bristen är avsaknaden av data vilket gör att det är nästintill omöjligt att göra uppskattningar om sannolikheter för att incidenter inträffar och eventuella kostnader om så sker. Detta leder till den tredje bristen som är att små förändringar hos de (grovt uppskattade) variablerna får mycket stor påverkan på resultatet, vilket alltså kan skapa en stor varians.

I vetenskaplig litteratur är begreppet ROSI inte särskilt spritt, men det förekommer i ett antal publikationer från 2005 och framåt med en topp vid 2007. Davis (2005) förklarar att ROSI inte fått ett större praktiskt genomslag då det är ett okänt begrepp för ekonomer, det är svårt att översätta säkerhetsinvesteringar till affärsnytta och att det finns flera olika, mer eller mindre komplicerade, modeller för hur ingångsvärden till ROSI-beräkningen ska tas fram. Ytterligare en utmaning är frågan om beräkningen ska göras för att motivera säkerhet på en allmän nivå eller för specifika åtgärder som brandväggar, virusskydd etc. De framgångsfaktorer som Davis framhåller är vikten av att genomföra beräkningarna på ett kontrollerat och dokumenterat sätt, så det blir tydligt vilka metoder som ska användas, i vilka fall beräkningar ska göras och hur de ska göras. Ytterligare framgångsfaktorer är att inte använda för komplexa beräkningar samt att nyttja ROSI som ett sätt att främja den interna kommunikationen. Genom att använda de beräkningar som ROSI innebär kan

personal kopplad till IT-säkerhet öka sin dialog med personal som är mer affärsinriktad.

3 Metod

I denna studie har en explorativ litteraturgenomgång används som metod, vilken genomförts genom ett antal sökningar i databaser med vetenskapliga publikationer samt med sökningar med generella söktjänster som Google och Google Scholar.

En del av litteraturgenomgången är baserad på en mer systematisk ansats där databasen Scopus användes för att identifiera vetenskapliga publikationer publicerade mellan 2011 och 2014. För den sökningen användes följande sökterm:

(information OR it OR ict OR cyber OR computer) /PRE2[1] security
AND
((investing OR investment OR economic* OR budget)
OR
cost /PRE2 (evaluation OR benefit OR assessment OR analysis))

Av ungefär 160 träffar bedömdes 55 artiklar vara av intresse och det är huvudsakligen dessa artiklar som denna litteraturöversikt baseras på. Utöver den primära sökningen inkluderades även artiklar omnämnda i referenslistor till inkludera artiklar. Litteraturen delades upp mellan tre personer där varje artikel sammanfattades kort. Utifrån sammanfattningarna kategoriserades artiklarna baserat på deras övergripande inriktning. De identifierade kategorierna var:

(1) investeringsstrategier för och styrning av informationssäkerhet – inkluderar litteratur som studerar på vilka olika sätt investeringar kan göras, samt vilka aktörer som leder säkerhetsarbetet och hur det utvärderas,

(2) optimering av säkerhetsinvesteringar – inkluderar litteraturen som inriktar sig på att beräkna optimal investeringsnivå för att balansera investeringskostnader mot konsekvenser av framgångsrika angrepp,

(3) mätdata och expertbedömningar – inkluderar litteraturen som diskuterar hur indata till investeringsanalysen ska samlas in och baseras på,

(4) hantering av osannolika händelser – inkluderar litteratur som specifikt tar upp problemen med att beräkna risker och kostnader för fall som har väldigt låg sannolikhet.

Litteraturen analyserades och beskrevs sedan utifrån dessa fyra kategorier. I ett par fall inkluderades även tidigare känd litteratur, i form av böcker och artiklar, om de matchade någon av de ovan presenterade kategorierna.

[1] Operatorn /PRE2 är en variant av AND, med tillägget att de sammankopplade fraserna dessutom ska finnas i samma ordning som i söktermen. Siffran 2 anger att det antal ord som får avskilja fraserna.

4 Litteraturöversikt

Utifrån de lästa artiklarna identifierades ett antal övergripande tematiska områden som används för att strukturera översikten. Dessa områden består av: investeringsstrategier för och styrning av informationssäkerhet, optimering av säkerhetsinvesteringar, mätdata och expertbedömningar samt hantering av osannolika händelser.

4.1 Investeringsstrategier för och styrning av informationssäkerheten

Investeringsstrategier gällande informationssäkerhet kan beskrivas utifrån två olika strategier (Gallaher et al., 2006). Den ena strategin benämns som *kostnadsminimerande* där organisationen analyserar sitt säkerhetsbehov och gällande prioriteringar för att därefter beräkna en optimal investeringsnivå. Investeringsnivån motiveras utifrån de faktiska behov organisationen har och minskar risken för att det varken överinvesteras eller underinvesteras i säkerhet. Den andra strategin kallas *säkerhetsmaximerande* och innebär att en viss andel av budgeten avsätts för informationssäkerhet. Målet är sedan att inom denna ram maximera nyttan och uppnå en så hög säkerhetsnivå som möjligt. Baserat på en intervjustudie menar Gallaher et al. (2006) att även om aspekter av båda dessa strategier är aktuella i de flesta organisationer är den säkerhetsmaximerande strategin mest framträdande. Det vanliga är nämligen att säkerhetsbudgeten sätts i enlighet med tidigare års budget. Det saknas dock enligt Stenbart et al. (2012) empirisk forskning avseende hur operativ styrning av informationssäkerhet går till.

4.1.1 Proaktiva och reaktiva investeringar

Enligt Gallaher et al. (2006) finns det en tendens hos organisationer att främst reagera på uppkomna incidenter och att investeringar fokuserar på att endast lösa aktuella problem, istället för att arbeta proaktivt och förekomma problem. Gällande investeringar krävs det en avvägning och balans av åtgärder som antingen är proaktiva eller reaktiva, eftersom detta har en påverkan på vilken effekt som uppnås av investeringen. I litteraturen finns det flera olika kategoriseringar och definitioner för vad som räknas som en proaktiv eller reaktiv investering. Till exempel kan investeringar ses som proaktiva:

- om de sker tidigast ett år efter senaste incidenten (Kwon och Johnsson, 2011),
- om investeringen är större än det aktuella behovet i situationer när ett ökat behov kan förväntas (Qian et al., 2012),

- baserat på syftet med investeringen (Gallaher et al., 2006).

Gallaher et al. (2006) menar att kategoriseringen av vad som anses vara proaktiva eller reaktiva åtgärder varierar efterhand som teknik blir mer etablerad och att samma åtgärd kan vara både proaktiv och reaktiv beroende på hur den implementeras. Det kan vara proaktivt att övervaka sina system med IDS (Intrusion Detection System), men om övervakningen endast letar efter kända trender kan åtgärden ses som reaktiv. Enligt den definitionen är proaktiva aktiviteter inriktade på att förutse nya typer av hot och fokuserar på åtgärder som ger generellt ökat skydd snarare än att skydda mot specifika hot. Åtgärder för att hantera specifika och tidigare kända hot kategoriseras som reaktiva aktiviteter.

En brist i att budgetera för informationssäkerhet baserat på föregående års budget är att det skapar en fördröjning i investeringar som kan förlänga tiden det tar för organisationen att hitta jämviktsläget. Ett fall där en ökning av antal säkerhetsincidenter kan förväntas är vid införande eller förändring av teknik i organisationen. Qian et al. (2012) modellerar detta med hjälp av *System dynamics* för att påvisa hur en proaktiv ansats (att öka investeringsnivån inför förändringen) är mer gynnsam än en reaktiv ansats (där nivån ökar efterhand som behov upptäcks). Modellen visar på interaktionen mellan en lång rad faktorer som den faktiska incidentfrekvensen, den *uppfattade* frekvensen, tid för att ändra uppfattning samt förmåga att hantera incidenternas konsekvenser. En viktig poäng i denna modell är faktorn med uppfattade frekvenser, skiljt mot den faktiska frekvensen som är okänd för organisationen. Att antalet uppfattade händelser är beroende av investeringsnivån är en orsak till att det skapas en stor fördröjning i att nå en önskvärd nivå för hantering av incidenter. Efterhand som investeringsnivån ökar upptäcks (och hanteras) fler incidenter, vilket ökar det uppfattade behovet och föranleder ytterligare ökning. På grund av att det totala antalet incidenter är okänt krävs det flera successiva höjningar innan en tillräcklig nivå nås. I modellen skulle en proaktiv ökning av säkerhetsinvesteringsnivån innebära att organisationen hamnar på en bättre avvägd investeringsnivå flera år tidigare än om de successivt ökar investeringsnivån efterhand som de upptäcker fler incidenter. De exakta resultat som Qian et al. (2012) redovisar i sin modell kan kanske kritiseras, men vad de tillför är en viktig diskussion om fördröjningar i komplexa system – där ovisshet och okunskap om faktiska hotnivåer kan dämpa investeringsgraden vilket bibehåller ovissheten. Soo Hoo (2000) hävdar att detta är något som tidigare har använts medvetet hos organisationer för att kunna förneka vetskap och därmed ansvar.

En proaktiv ansats innebär dock stora kostnader för att skydda sig mot hot som ännu inte gett upphov till incidenter (Gallaher et al., 2006). Detta innebär en risk för överinvestering, i den betydelsen att investeringar går till skydd som egentligen inte behövs. Även om en proaktiv strategi innebär färre incidenter, kan reaktiva ansatser i vissa fall vara mer kostnadseffektiva (Gallaher et al.,

2006). Det är dels mycket svårt (och därmed dyrt) att hitta och förutse alla brister i förväg, dels innebär det en risk att systemen blir alltför begränsade. Det är dessutom dyrt att implementera och underhålla skydd medan den som angriper ett IT-system kan göra det med betydligt mindre kostnader (Anderson et al., 2012). Anderson et al. (2012) föreslår därför ett skifte i fokus från att investera i tekniska skydd till att fokusera på att gripa och straffa angriparna, något som kräver utökade samarbeten mellan företag och myndigheter.

En tredjedel av de respondenter som Gallaher et al. (2006) intervjuade ansåg att smidighet för användare var lika viktigt eller viktigare än säkerhet, varför en mer reaktiv ansats förordades. Den reaktiva ansatsen innebär mer riktade insatser och investeringar för att hantera de problem som faktiskt uppstår. Genom att övervaka systemen samlas kunskap om incidenter och investeringar sätts in som punktinsatser. Fokus blir att investera så kostnadseffektivt som möjligt genom att acceptera en viss nivå av (för angriparen) lyckade angrepp snarare än att investera för att helt avvärja angrepp. Denna hållning kan enligt förespråkare vara fördelaktig genom att onödiga investeringar undviks (Ittner et al. 2001; Kwon och Johnson, 2011). Detta är dock mycket beroende på hur stora konsekvenser ett angrepp kan ha på verksamheten. Inom vissa verksamheter kan konsekvenserna vara så pass allvarliga att det inte ses som möjligt med en mer tillbakalutad hållning. Hantering av osannolika händelser med stora konsekvenser är något som diskuteras vidare i avsnitt 4.4.

4.1.2 Bakomliggande orsaker till investeringar

Enligt Gallaher et al. (2006) är externa regleringar och regler (se Tabell 1) en av de viktigaste faktorerna som driver säkerhetsinvesteringar, förutom för mindre företag där det främst är kundkrav som driver på säkerhetsinvesteringar. Extern reglering av informationssäkerhet är intressant då säkerhetsinvesteringar inte bara berör enskilda organisationer, utan samhället i stort då kostnader för incidenter sprids till flera aktörer. Virus eller trojaner hos en aktör kan leda till stora konsekvenser inte bara för kunder utan även för andra berörda aktörer. Informationssäkerhet har därför ett samhällsnyttigt värde som bör påverka vad som anses vara en optimal investeringsnivå ur samhällets perspektiv (Gallaher et al., 2006; Öğüt et al., 2011). Investerar organisationen optimalt utifrån sitt eget ekonomiska perspektiv och inte inkluderar kostnader utanför den egna organisationen innebär det vanligen en underinvestering utifrån ett samhällsnyttigt perspektiv. En investering i säkerhet höjer i många fall inte bara säkerheten hos den enskilda organisationen utan bidrar även till en allmän ökning av säkerheten som alla drar nytta av. Det kan innebära att organisationer har incitament att inte investera mer än nödvändigt för att undvika att stödja konkurrenter. På liknande sätt är den totala kostnaden för en incident normalt inte begränsad till den drabbade organisationen. Av den anledningen är det angeläget att diskutera hur myndigheter kan eller bör reglera krav beträffande

informationssäkerhet. Gallaher et al. (2006) menar att myndigheterna borde stödja innovativa strategier för informationssäkerhet för att öka incitamentet för proaktiva aktiviteter och en mer samhällsoptimal nivå. Extern reglering, i form av lagar och förordningar kan stimulera organisatoriskt lärande och förändring mot att uppnå bättre säkerhet, men har även en baksida. Kwon och Johnson (2011) menar att statistik från sjukvårdsorganisationer i USA visar att organisationer som oberoende av reglering investerar proaktivt har färre incidenter än andra organisationer. Men att detsamma inte gäller organisationer som investerar som följd av regleringar, trots att investeringen kan ses som proaktiv. De menar att regleringar riskerar att leda till ett ensidigt fokus på specifika kända problemområden och att mer övergripande åtgärder prioriteras bort. Anderson (2001) instämmer i att ökade externa säkerhetskrav på ett specifikt område kan ge bieffekter i form av minskad säkerhet på ett annat. Kwon och Johnson (2011) nämner vidare att detta innebär att lärande och upptäckande av nya problem uteblir. Mer utforskande proaktiva aktiviteter blir en möjlighet för organisationen att lära sig baserat på egna incitament och inte bara som reaktion på incidenter. Studien begränsas dock kraftigt genom att ingen hänsyn tas till storleken på investeringar, utan bara antalet investeringar samt att kostnaden för bekräftade incidenter inte beaktas. Anderson et al., (2012) ger dock visst stöd genom sitt resonemang om att ökade restriktioner, till följd av exempelvis extern reglering, försvårar innovation.

Tabell 1 Olika faktorers påverkan på investeringsbeslut. Värdet anger i vilket utsträckning faktorer har bidragit till investeringar (anpassat från Gallaher et al., 2006).

Faktor	**Påverkan på investeringar (Genomsnitt över organisationer)**
Extern reglering	30,1 %
Erfarenhet hos personal och historik av det egna nätverket	18,9 %
Kunder	16,2 %
Reaktion på intern eller extern revision	12,4 %
Reaktion på aktuella händelser (t.ex. mediabevakning)	8,2 %
Reaktion på interna säkerhetsincidenter	7,3 %
Externt beslutat	5,0 %
Annat	1,7 %

Regleringar kan emellertid användas för att motivera en mer lärande ansats om de formuleras på rätt sätt. Kwon och Johnson (2011) föreslår därför att regleringen inte ska kräva specifika tekniker eller åtgärder utan istället ange vilken budgetandel som ska användas för informationssäkerhet, vilket ger

organisationerna makt att bestämma hur och vad investeringarna ska gå till. Organisationen kan därmed inte ignorera problemet med informationssäkerhet, samtidigt som de har möjlighet att arbeta förbyggande snarare än reaktivt. Förslaget är alltså väldigt nära det som Gallaher et al. (2006) benämner som den säkerhetsmaximerande ansatsen och som de menar redan är en vanlig form av strategi, om än med en internt satt nivå.

4.1.3 Involverade aktörer

Via ett ekonomiskt perspektiv på informationssäkerhet möts två områden med olika bakgrund och perspektiv. Å ena sidan är det tekniker med fokus på den tekniska sidan av informationssäkerhet och å andra sidan är det ekonomer och organisationsledare som ser informationssäkerhet utifrån dess effekt på verksamheten. Gallaher et al. (2006) visade att det varierar mellan olika organisationen var ansvaret för investeringsstrategin ligger (Tabell 2). I samma studie visade det sig även att de organisationer där ledningen är ansvarig i högre grad övervakade olika metriker för incidenter, som hur mycket tid som gick åt för att hantera incidenter samt antalet användare som påverkades.

Tabell 2 Ansvarig avdelning för investeringsstrategi för informationssäkerhet (Tabell anpassad från Gallaher et al., 2006).

Domän	IT-avdelning	Ledningsavdelning*
Finansiella sektorn	33,3 %	66,7 %
Hälsovårdsorganisationer	33,3 %	66,7 %
Tillverkningsindustri	83,3 %	16,7 %
Universitet	60,0 %	40,0 %
Övriga	85,7 %	14,3 %
Totalt	60 %	40 %

* eng. management department

Gallaher et al. (2006) skriver att flera organisationer som de intervjuade hade pågående arbete för att omvärdera hur informationssäkerhet ska hanteras. Detta skedde dels genom att informationssäkerhet började hanteras som annan riskhantering och att säkerhet i högre grad sågs som ett affärsproblem där ledningen har ett större ansvar. Från att informationssäkerhet helt hanteras av IT-ansvariga börjar fler delar av organisationen engageras för att bidra med information och data, samt att externa källor användes i högre grad för att få underlag till investeringsbeslut (Gallaher et al., 2006). Denna svängning kan ses höra samman med den förnyade satsningen på formella, ekonomiska modeller för att kvantifiera informationssäkerhet som beskrivs i samtida vetenskaplig litteratur. Att organisationsledningen har ett större intresse för investeringsbeslut

rörande säkerhet sammanfaller väl med Davis (2005) som menade att användandet av mått som ROSI gör säkerhetsinvesteringar mer transparanta för mer affärs- och ekonomiinriktade aktörer. Att skapa förutsättningar för mer kommunikation och förståelse om säkerhetsfrågor inom fler delar av organisationen lyfts fram som framgångsfaktorer av både Davis (2005) och Steinbart et al. (2012). Att nyttja perspektiv och metoder grundande i ekonomisk teori kan användas som metod i syfte att föra samma delar av organisationen som annars inte interagerar i hög utsträckning. Davis (2005) har som exempel att användandet av ROSI innebär att IT-avdelningen måste ta stöd av andra avdelningar för att ta fram korrekta mått och siffor vilket kräver ökad internkommunikation med kunskapsspridning inom organisationen som följd. Därför kan själva processen att göra beräkningen ge mervärden, även om måtten i sig inte är exakta (Davis, 2005).

Styrningen av informationssäkerhet delas av Gallaher et al. (2006) upp i två delar: (1) investeringsstrategi, vilket handlar om den övergripande styrningen och (2) implementeringsstrategi, där beslut tas om vilka typer av tekniker och skydd som ska användas, samt om proaktiva eller reaktiva åtgärder ska genomföras. Implementeringsstrategin är något som tas fram av IT-ansvariga. Steinbart et al. (2012) menar att det saknas empiri för hur denna mer operativa styrning av informationssäkerhet går till. Detta trots att vedertagna standarder för styrning av IT inom verksamheter som COBIT[2] poängterar vikten koordinering, kommunikation och samarbete mellan IT-avdelningar och interna kontrollorgan, som internrevisorer. Steinbart et al. (2012) menar att det saknas empirisk forskning som utforskat hur sådant samarbete påverkar säkerhetsarbetet, men menar att det finns exempel som tyder på att förhållandet mellan IT-avdelningar och internrevisorer ofta kan vara ansträngt. Detta kan förklaras delvis med att det finns kommunikationssvårigheter mellan funktionerna på grund av skillnader i bakgrund och kunskap. Baserat på en explorativ intervjustudie föreslår Steinbart et al. (2012) fem faktorer som är viktiga för att samarbetet mellan revisorer och IT-ansvariga ska ge positiva effekter. Den första (1) faktorn är vilken kunskap och kompetens om informationssäkerhet som revisorn har. Saknas kunskap om området informationssäkerhet blir samarbetet med IT-ansvariga lidande och revisonen blir alltför inriktad på att kontrollera processefterföljande. Vikten av revisorns generella kunskap om informationssäkerhet påpekas även av Wallace et al. (2011). Den andra (2) faktorn är revisorns förmåga att kommunicera omfånget och syftet med revision. En god förmåga ökar förtroendet och acceptansen av kontroll vilket gynnar samarbetet. Den tredje (3) faktorn är attityden hos revisorerna. Fokuserar revisorn på samarbete och processförbättring uppnås bättre effekt än när revisorn har en mer avståndstagande ”polisiär” funktion att kontrollera efterlevnad och straffa avsteg. Den fjärde (4) faktorn är vilken attityd ansvariga har till samarbetet mellan funktionerna. Har de ansvariga

[2] Se http://www.isaca.org/COBIT/

för revision och säkerhetsansvariga en samarbetande attityd kommer samarbetet öka även på lägre nivåer. En femte (5) faktor är kopplad till organisationens karaktär där externa regleringar kan påverka samarbetet. Utifrån sina intervjuer menar Steinbart et al. (2012) att internrevision kan påverka informationssäkerheten positivt. En god relation mellan revisorer och ansvariga för informationssäkerhet ökar efterlevnaden av säkerhetsregler och innebär även att revisionen kan inriktas mot prioriterade områden. Ett ökat samarbete kan dock innebära oklarheter med revisorernas opartiska ställning och självständighet, men Steinbart et al. (2012) menar att det i dagsläget vore mer gynnsamt för båda funktionerna att fostra en mer samarbetande relation.

4.2 Optimering av säkerhetsinvestering

Litteraturen inom området informationssäkerhetsekonomi (eng. *information security economics*) handlar om att ha ett ekonomiskt perspektiv på informationssäkerhet. Området domineras av försök att hitta metoder för att beräkna vilken investeringsnivå som är optimal. Det är här av vikt att balansera risken för överinvestering som leder till ekonomiskt slöseri, med risken för underinvestering som leder till lyckade angrepp som följd (Bojanc et al, 2012). För att uppnå detta används både etablerade ekonomiska termer som *Net Present Value* (NPV) och *Return of Investment* (ROI), samt anpassade begrepp som *Return of Security Investment* (ROSI). NPV är ett mått på ackumulerad kostnad och nytta över tiden vilket exempelvis innebär att man kan beräkna när nyttan överstiger investeringskostnaden vilket är användbart vid investeringar i säkerhet eftersom dessa ofta är långsiktiga till sin natur (Davis 2005). ROI är ett mått på förhållandet mellan investeringskostnader och nyttan av en investering. Ett positivt ROI-värde innebär att nyttan eller intäkterna som genereras av en investering är större än investeringskostnaden (Davis 2005). Att investera i säkerhet innebär dock, till skillnad från andra affärsinvesteringar, normalt inte ökade intäkter som sådana, men däremot minskade potentiella kostnader. Detta faktum hanteras av ROSI som istället för förväntade intäkter använder förväntande uteblivna förluster. Det innebär att ROSI delvis är ett mått på förhållandet mellan en säkerhetsinvestering och de förväntande uteblivna förluster som investeringen innebär (Davis 2005). Ett positivt ROSI-värde innebär alltså att de uteblivna förlusterna är större än kostnaden för investeringen. ROSI utgår således från synen att investeringar i säkerhet är något nödvändigt ont snarare än en möjliggörare. Denna syn är vanlig enligt både Gallaher (2006) och ISBS (2012). Organisationer ser inte investeringar i informationssäkerhet på samma sätt andra typer av investeringar utan snarare som något som inte bidrar till generering av intäkter och därför ska hållas nere.

De metoder som föreslås i litteraturen går att dela in utifrån vilket sätt de närmar sig optimeringsproblematiken och de redovisas gruppvis nedan. Den första och mest omfångsrika gruppen är metoder baserade på statistiska modeller. Därefter

beskrivs gruppen av metoder baserade på *heltalsprogrammering*[3], vilka försöker lösa problemet med tillgången på tillförlitligt underlag. En tredje typ av metoder grundar sig i riskhantering. Slutligen finns det metoder med sin grund i spelteori som syftar till att fånga den interaktion som sker mellan angripare och försvarare, faktorer som andra metoder har svårt att hantera.

4.2.1 Statistiska metoder

Ett centralt arbete inom domänen för att beräkna den optimala nivån för säkerhetsinvesteringar är en artikel av Gordon och Loeb (2002) som presenterar en statistisk metod för att beräkna den optimala nivån för IT-säkerhetsinvesteringar. Artikeln fokuserar på beräkningsprinciper snarare än praktisk tillämpning vilket innebär att metoden som beskrivs är av principiell natur och bygger på en rad förenklingar och antaganden. I stället för händelsefrekvens (som utgör basen i ALE) används sannolikheten för olika säkerhetshändelser och den förväntade förlusten beräknas som en funktion av hot, sårbarhet samt förlust vid ett för angriparen lyckat angrepp. Sårbarhet definieras här som sannolikheten för att ett givet angrepp ska lyckas, det vill säga hur bra (eller dåligt) skyddet är mot en viss typ av hot.

$$Förväntad\ förlust = Sannolikhet\ för\ angrepp * Sårbarhet * Potentiell\ förlust$$

I Gordon och Loebs modell är sannolikheten för att angrepp inträffar en extern variabel som inte går att påverka, däremot kan sårbarheten – och därmed sannolikheten att angreppet leder till en incident – reduceras genom investeringar i IT-säkerhet. En följd av detta är att sambandet mellan förväntade kostnader och sårbarhet blir väldigt starkt.

Ett exempel kan vara att den förväntade förlusten utifrån det aktuella läget, utan ytterligare skyddsmekanism, för hot x är:

$$Förväntad\ förlust_{utan\ skydd} = 0{,}5 * 0{,}8 * 100\ 000 = 40\ 000$$

En investering i en skyddsmekanism kan minska sårbarheten och därmed den förväntade förlusten:

$$Förväntad\ förlust_{med\ skydd} = 0{,}5 * 0{,}2 * 100\ 000 = 10\ 000$$

Skyddet innebär alltså att den förväntade förlusten minskar med 30 000 och därmed bör inte investeringskostnaden överstiga 30 000. Om kostnaden för denna investering hålls så låg som möjligt, nås den optimala investeringsnivån.

[3] Heltalsprogrammering (eng. *Integer Programming*) är en metod för att lösa optimeringsproblem. Metoden bygger på att variabler och utfall endast kan ta formen av heltal vilket gör även komplexa problem lösbara med datorstöd.

Gordon och Loeb (2002) bygger sitt resonemang på tre fundamentala antaganden:

A1. Om en informationsmängd är helt osårbar är den helt skyddad vid alla olika investeringar i säkerhet. (Detta innebär att det inte behövs något skydd eftersom det inte finns någon sårbarhet, sårbarheten är 0).

A2. Om ingen investering görs i säkerhet är sannolikheten för en incident identisk med informationsmängdens sårbarhet. (Detta innebär att det fullständigt saknas skydd, angreppssannolikheten är 1).

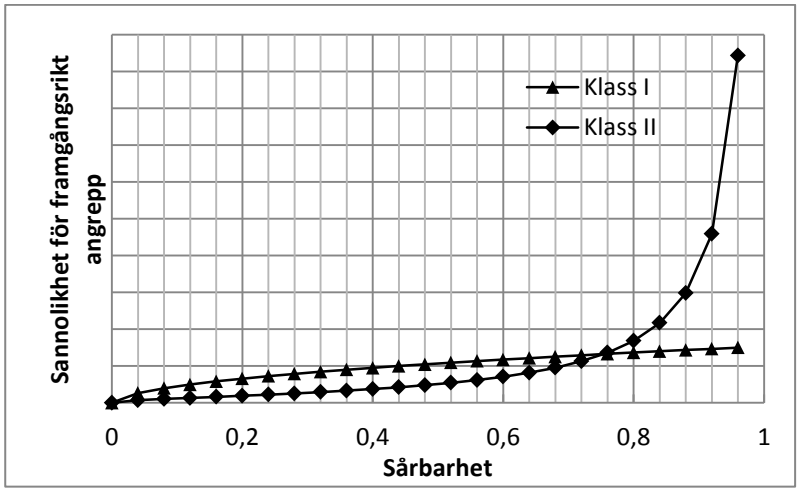
A3. Investeringar i säkerhet minskar informationsmängdens sårbarhet men i avtagande takt.

Författarna definierar och formulerar sedan två klasser av matematiska funktioner för incidentsannolikheter som satisfierar A1-A3 (det finns många funktioner som satisfierar antagandena men Gordon och Loeb väljer två som är enkla men samtidigt tillräckligt olika för att vara intressanta). Dessa klasser beskriver på varsitt sätt förhållandet mellan skyddsinvesteringars kostnader och effekt på säkerheten.

Klass I beskriver ett nästan linjärt samband mellan den initiala sårbarheten och förväntad förlust. För klass I är den optimala investeringsnivån noll tills sårbarheten når ett tröskelvärde. För sårbarheter över detta tröskelvärde ökar den optimala investeringsnivån nästan linjärt med sårbarheten.

Klass II är av exponentiell karaktär vilket innebär att förväntad förlust ökar exponentiellt med sårbarheten vilket i sin tur medför att den optimala graden av säkerhetsinvestering kommer att nå ett maximum för att sedan sjunka eftersom kostnaden för säkerheten blir för hög. Även för denna klass finns det ett tröskelvärde för sårbarheten. Under tröskelvärdet är den optimala investeringsnivån noll.

Författarnas avsikt med dessa två klasser är att visa att den ekonomiska nyttan av säkerhetsinvesteringar inte alltid ökar med investeringens storlek, utan att den optimala investeringen i informationssäkerhet är betydligt lägre än den maximala potentiella förlusten som följer av sårbarheten. Enligt Huang, Hu och Behara (2008) kan klass I användas för att representera riktade attacker och klass II för distribuerade attacker eller massattacker (se Figur 2).



Figur 2 Principiella egenskaper för klass I respektive II. Bild anpassad från Huang et al., (2008, s.797)

Gordon & Loeb drar slutsatsen att det finns en kritisk punkt där kostnaden för att skydda sig faktiskt överstiger den förväntade förlusten vid ett givet angrepp. Genom att kombinera Klass I och Klass II visar de att den optimala investeringen i IT-säkerhet aldrig överstiger 1/e (ungefär 36,79%) av den maximala förlusten. Modellen är ganska avgränsad och tar till exempel inte hänsyn till förändring över tiden eller en angripares anpassning till nya säkerhetsinvesteringar. Gordon och Loeb utgår dessutom från antagandet att organisationen är riskneutral, det vill säga att den inte gör någon skillnad på vinst och utebliven förlust.

Flera författare har utgått från Gordon och Loebs modell och gjort olika modifieringar och tillägg. Huang, Hu och Behara (2008) har exempelvis infört en variabel som beskriver en organisations riskaversion, alltså hur ovillig en organisation är att ta risker. En riskavert organisation är en organisation som accepterar en fast kostnad för att undvika en potentiell förlust. Graden av riskaversion kan dessutom beräknas genom att undersöka hur hög fast kostnad som accepteras innan den kostnaden inte anses vara värd den minskade risken, alltså hur mycket extra man är beredd att investera för att skydda sig mot förluster. Hua och Bapna (2012) har med utgångspunkt i Gordon och Loebs modell studerat de ekonomiska konsekvenserna av cyberterrorism. Genom att utgå från Gordon och Loebs klass I och lägga till en avskräckningsfaktor (terrorister är svårare att avskräcka än andra angripare) visar de att kostnaderna för skydd mot en högmotiverad cyberterrorist vida överstiger kostnaderna för skydd mot vanliga angripare.

Även Lelarge (2012) har utgått från Gordon och Loebs modell då han studerat hur motivationen att investera i IT-säkerhet påverkas av IT-säkerhetsmiljön i

stora nätverk (exempelvis internet). Lelarge utgår från att säkerhetsinvesteringar hos en aktör bidrar till säkerheten i nätverket som helhet. Detta medför att ju säkrare nätverket blir, det vill säga ju fler som investerar i säkerhet, desto lägre blir motivationen för de som ännu inte investerat eftersom hotet minskar. IT-säkerhetsmiljön är ofta komplex (Bojanc et al, 2012) med ett stort antal hot och intressenter. Aissa et al. (2011) har utvecklat en metod för att bryta ned komplexiteten i mindre beståndsdelar som kan bedömas var för sig. Metoden är baserad på matriser, som medger såväl multipla intressenter som säkerhetskrav, komponenter och hot. PT-vektorn (*Threat Vector*) anger för varje möjligt angrepp sannolikheten att det inträffar. IM-matrisen (*Impact Matrix*) beskriver för varje komponent sannolikheten att komponenten skadas av respektive givet angrepp. DP-matrisen (*Dependency Matrix*) beskriver sannolikheten att var och ett av säkerhetskraven inte uppnås ifall någon komponent i skyddet skadas. I ST-matrisen (*Stakes Matrix*) anges för varje säkerhetskrav hur viktig det är för respektive intressent. Utifrån de fyra matriserna kan sedan MFC (*Mean Failure Cost*) beräknas enligt den sammansatta funktionen:

$$MFC = ST \circ DP \circ IM \circ PT$$

En nackdel med flertalet statistiska metoder är att de utgår från att sannolikheterna för incidenter är kända samt att kostnaderna för konsekvenserna av ett angrepp går att beräkna. Att fastställa dessa värden med rimlig precision har dock visat sig vara svårt. Ett sätt att hantera detta är att öka mängden indata och samtidigt ställa lägre krav på precisionen. Med denna utgångspunkt har Garvey, Moynihan och Servi (2013) utvecklat en praktisk och handgriplig metod som de kallar The Table Top Approach. I stället för att försöka fastställa exakta sannolikheter för olika typer av hot och sårbarheter låter de en panel med verksamhetsrepresentanter grovt ange (med 5-20% noggrannhet) hur allvarliga olika typer av hots potentiella konsekvenser bedöms vara för olika delar av en organisations verksamhet samt ungefär hur sannolika de olika incidenterna bedöms vara. Genom att sedan bedöma kostnaden för skydd mot de olika typerna av hot kan verksamhetsnyttan av olika säkerhetsinvesteringar beräknas. Denna kostnad-nytta-analys kan presenteras genom ett så kallat Pareto-diagram som visar de mest kostnadseffektiva kombinationerna av IT-säkerhetsinvesteringar för olika ambitionsnivåer genom att representera de olika kombinationerna av säkerhetsinvesteringar och vilken grad av verksamhetsnytta de förväntas ge. Genom att binda ihop de högsta punkterna för varje x-värde bildas en så kallad Pareto-front som representerar optimala kombinationer. Punkter som ligger innanför Pareto-fronten är per definition suboptimala. Olika kombinationer av investeringar och hur de påverkar de olika verksamheterna i CSE-matrisen kan sedan jämföras. Även om metoden ger ganska grova resultat ger den en överblick över ett komplext optimeringsproblem.

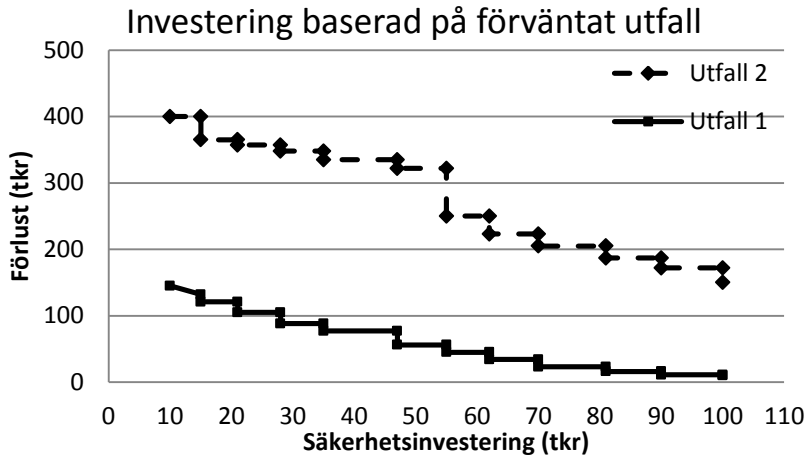
4.2.2 Heltalsprogrammering

Att använda statistiska metoder som underlag för planering är inte helt oproblematiskt. Detta gäller särskilt händelser som har mycket låg sannolikhet att inträffa, men samtidigt skulle innebära stora konsekvenser (se avsnitt 4.4). Dessa händelser kan vara besvärliga eftersom det oftast saknas underlag för att beräkna sannolikheten med någon högre precision. Även om det i det långa loppet inte är någon egentlig skillnad på osannolika förluster av stora värden och mer sannolika förluster av små värden kan en stor momentan förlust innebära katastrof för en verksamhet. Detta har Rakes, Deane och Rees (2012) tagit fasta på med en metod för IT-säkerhetsplanering som hanterar osäkra förhållanden. Metoden bygger på *Mixed Integer Programming* som är en matematisk optimeringsmetod där vissa variabler begränsas till att endast vara heltal. Metoden föreslagen av Rakes et al. (2012) hanterar både förväntad förlust (sannolikheten att ett hot realiseras multiplicerat med den potentiella förlusten vid händelsen) och värsta tänkbara förlust (den potentiella förlusten). Metoden generera diagram som presenterar förluster (både förväntade och värsta tankbara) som funktioner av olika kombinationer av säkerhetsinvesteringar. I diagrammen kan man enkelt identifiera stora potentiella förluster som man eventuellt vill undvika. Den bakomliggande tanken är att det ibland kan vara viktigare att hantera händelser med stora konsekvenser än att reducera den förväntade förlusten. I grunden presenterar metoden fyra olika utfall (Tabell 3) beroende på vad som planerades för och vad som faktiskt sker.

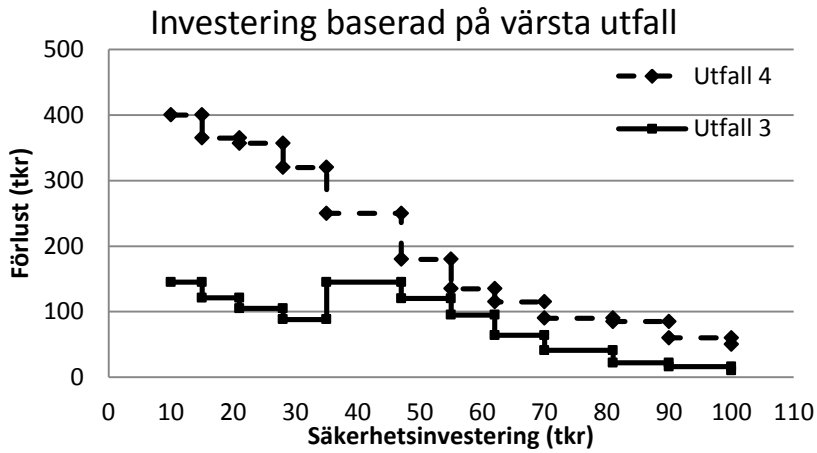
Tabell 3 Fyra olika utfall som en investering kan utvärderas utifrån (Rakes et al., 2012)

	Förväntat utfall realiseras	**Värsta tänkbara utfall realiseras**
Plan enligt förväntat utfall	Utfall 1	Utfall 2
Plan enligt värsta tänkbara utfall	Utfall 3	Utfall 4

Metoden ger ett strukturerat stöd att analysera om det är positivt att investera för ett värsta tänkbart utfall. Eftersom investering utifrån det perspektivet innebär en fokusering på mer allvarliga hot kan det innebära en sämre förmåga att skydda sig mot vanligare hot. Genom att illustrera detta dilemma från olika perspektiv är tanken att identifiera vilken nivå av investeringar som sådana effekter uppstår.



Figur 3 Illustration över uppskattad förlust vid olika nivåer av säkerhetsinvesteringar om investeringarna görs baserat på ett förväntat utfall. De två utfallen visar på skillnaden mellan om det förväntade utfallet eller om det värsta utfallet realiseras. Bild anpassad från Rakes et al. (2012, s. 85).

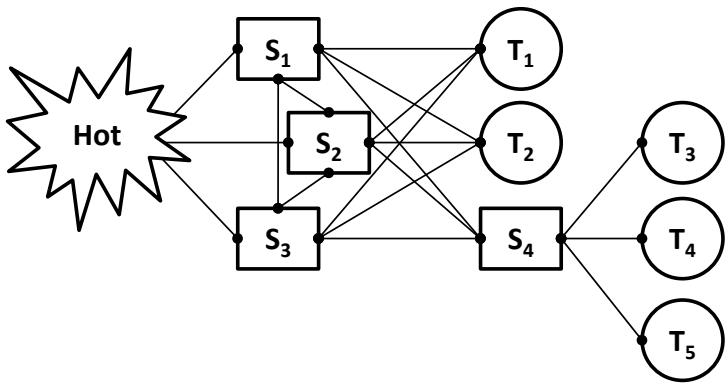


Figur 4. Illustration över uppskattad förlust vid olika nivåer av säkerhetsinvesteringar om investeringarna görs baserat på ett värsta tänkbara utfall. De två utfallen visar på skillnaden mellan om det förväntade utfallet eller det värsta utfallet realiseras. Bild anpassad från Rakes et al. (2012, s. 85).

Att investera baserat på värsta tänkbara utfall kan innebära att förlusterna blir större om det förväntade utfall sker (jämför Utfall 3 i Figur 4 med utfall 1 i Figur 3) men å andra sidan innebär det även att den potentiella förlusten om det värsta

tänkbara utfallet realiserars minskar dramatiskt vid en säkerhetsbudget större än 35 000 (se Figur 4). Anledningen till detta är att om fokus läggs på att hantera värsta tänkbara utfall tas resurser från skydd som förhindrar mer frekventa händelser. Genom att presentera de olika utfallen kan analysen om vad olika investeringsstrategier innebär fördjupas och belysas från flera perspektiv.

Sawik (2013) har använt sig av *Mixed Integer Programming* men har fokuserat på riskneutralitet respektive riskaversion. Han menar att det finns en poäng i att använda etablerade finansiella begrepp och har därför utgått från de ekonomiska riskmåtten VaR[4] (*Value at Risk*) och CVaR[5] (*Conditional* Value *at Risk*). Baserat på dessa begrepp har Sawik skapat en riskneutral modell som minimerar förväntade förluster samt en riskavert modell som optimerar hanteringen av värsta tänkbara utfall.



Figur 5 Hot, skydd och tillgångar modellerat i ett kombinatoriskt nätverk. Bild anpassad från Wang et al. (2009).

I IT-miljöer som består av sammankopplade datorer uppstår kombinatoriska sårbarheter och antalet attackvägar ökar dramatiskt. Detta innebär att man inte kan hantera sårbarheter oberoende av varandra utan att de måste hanteras som en helhet. Wang, Chen, Stripe och Hong (2009) adresserar detta genom att beskriva skydd (S_n) och tillgångar (T_n) som noder i ett nät (Figur 5). Med utgångspunkt i detta nät med noder beräknas sedan alla olika kombinationer av sårbarheter och

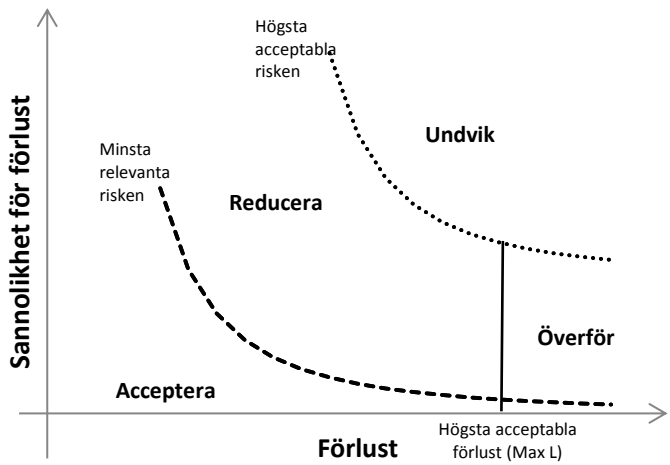
[4] *Value at Risk* är ett finansiellt begrepp som anger ett tröskelvärde för risknivån hos en investering. Begreppet anger det riskerade beloppet, konfidensnivån och över vilken tidsrymd det gäller. Ofta är tidsrymden en dag vilket innebär att man vid ett belopp om 1000kr med konfidensnivån 99% förväntar sig att förlora 1000kr eller mer var hundrade dag.

[5] *Conditional Value at Risk* är medelvärdet av alla de utfall som överstiger VaR.

potentiella förluster. Exempelvis kan en attack mot T_1 gå via S_1 men den kan även gå via S_2. På detta sätt kan de potentiella förluster som kan uppstå som följd av ett lyckat angrepp matchas mot säkerhetsinvesteringar.

4.2.3 Hantering och reducering av risker

Risker kan delas upp i externa och interna faktorer. Ett grundantagande i Gordon och Loebs modell (2002) är att det inte går att påverka de externa faktorerna. Interna faktorer är sådant som går att påverka, till exempel sårbarhet och potentiell förlust. Bojanc, Jerman-Blažič och Tekavčič (2012) har utvecklat en modell för optimering av riskhanteringsstrategin som beskriver fyra olika sätt att hantera risker: undvika, reducera, överföra och acceptera (se Figur 6). Undvika-strategin innebär att man helt enkelt tar bort den potentiella förlusten, kanske genom att förändra sin verksamhet eller genom att dela upp värdefulla data så att man inte riskerar att förlora samtliga data vid ett och samma tillfälle. Reducera-strategin innebär att man minskar sårbarheten genom att investera i säkerhetslösningar på traditionellt vis.



Figur 6 Rekommenderade riskhanteringsstrategier i relation till sannolikhet och potentiell förlust. Risken syftar på kombinationen av sannolikhet och förlust. Bild anpassad från Bojanc et al. (2012)

Acceptera-strategin rekommenderas endast för små risker med så små potentiella förluster att det inte motiverar investeringar i säkerhetslösningar eftersom investeringen i säkerhet riskerar att överstiga de förväntade förlusterna. Om de förväntade förlusterna är låga blir en motsvarande säkerhetsbudget helt enkelt så liten att det inte går att göra några meningsfulla säkerhetsinvesteringar. Överföra-strategin innebär att man överför risken på någon annan genom exempelvis outsourcing eller försäkring. Denna strategi rekommenderas av Bojanc et al.

(2012) för de potentiella förluster som överstiger den största tänkbara engångsförlusten (Max L) som organisationen kan hantera.

Försäkring mot förluster genom dataintrång kan ses som komplement till investeringar i IT-säkerhet men Öğüt, Raghunathan och Menon (2011) påpekar att IT-säkerhetsförsäkringar kräver större transparens än vad som är vanligt i dag. För att försäkringar mot förluster orsakade av IT-attacker ska fungera måste förlusterna gå att påvisa och fastställa på ett tydligt sätt. Vidare måste försäkringstagaren kunna visa att den vidtagit rimliga skyddsåtgärder. Författarna hävdar att en samhällsnyttig optimal balans mellan skyddsåtgärder och försäkringar bara kan uppnås genom full transparens eftersom det annars finns risk att försäkringen helt ersätter investeringar i IT-skydd vilket skapar obalans och ökar den totala sårbarheten i systemet. I praktiken innebär detta att om några organisationer väljer försäkringsstrategin i stället för att investera i säkerhet ökar det sårbarheten för övriga organisationer i nätverket. För att uppnå fullständig samhällsnyttig optimering hävdar författarna att investering i skydd bör subventioneras samt att försäkringar bör beläggas med skatt.

4.2.4 Spelteoretiska metoder

En brist med statistiska beräkningarna som lyfts fram av vissa författare är att de inte förmår ta hänsyn till den interaktion och växelverkan som uppstår mellan angripare och skyddsåtgärder. Ett alternativ till statistiska beräkningar för att hantera detta är spelteorestiska metoder där ett antal villkor och regler definieras för olika aktörer och sedan simuleras i en serie omgångar där aktörerna gör val baserat på de definierade reglerna samt utfallen i de tidigare omgångarna. Detta är en metod som exempelvis Paté-Cornell och Guikema (2002) förespråkar i riskanalysarbetet. Gao, Zhong och Mei (2013) har med hjälp av spelteoretiska metoder studerat hur investeringar i informationssäkerhet påverkar konkurrens mellan företag. Författarnas resonemang bygger på att investeringar i informationssäkerhet inte bara gynnar den som investerar utan även konkurrenterna eftersom branschen som helhet framstår som säkrare vilket skapar förtroende hos kunderna. Slutsatserna av studien är att det ur konkurrensperspektiv är effektivt att investera i informationssäkerhet upp till en punkt där konkurrenterna gynnas lika mycket som det investerande företaget samt att vad som är optimal investeringsnivå beror på den specifika konkurrenssituationen.

4.3 Mätdata och expertbedömningar

Denna rapport redovisar ett antal beräkningsmodeller för kostnadseffektiv säkerhet. Gemensamt för dessa modeller är att det krävs en uppfattning om hur sannolik förekomsten för olika angrepp är, hur sannolikt det är att skydden inte lyckas stå emot angreppen, samt storleken av angreppens eventuella

konsekvenser. Uppfattningen kan baseras dels på historisk mätdata, dels på expertbedömningar. Mätdata kan komma både från externa källor, till exempel leverantörer eller databaser över kända sårbarheter samt angreppsmetoder, och interna mätdata, som till exempel hur uppdaterat systemet är, säkerhetspolicyn samt penetrationstester. Då det i flera fall är svårt eller omöjligt att få tillgång till mätdata används expertbedömningar för att uppskatta exempelvis säkerhetsnivån, angriparens förmåga eller sannolikheten för att nya angrepp inträffar.

En del av kostnad-nytta-analysen där det ofta saknas kunskap är minskad produktivitet, i egenskap av kostnad. NRC (2010) noterar att det saknas teorier och data för säkerhetsmekanismers påverkan på produktiviteten, speciellt då studier om användbarhet (eng. usability) i regel har universitetsstudenter som studiedeltagare vilket kan förvränga resultaten. Det finns emellertid väletablerade tekniker för att testa användbarheten hos färdiga system (Economides, 2010). I sin kartläggning av IT-säkerhetskostnader inkluderar Anderson et al. (2012) faktorn minskad nytta som bieffekt av ökad säkerhet. Kartläggningen bygger på begränsad data samt expertbedömningar. Fler exempel på studier som ställer kraven på sekretess och riktighet mot behovet av tillgänglighet är Albrechtsen(2007) samt Post och Kagan (2007).

4.3.1 Expertbedömningar

En fördel med att använda expertbedömningar är att det går att uppskatta säkerhetsnivån även för sådant som man saknar mätdata för – såsom motståndarens förmåga och intention samt till viss del framtida skeenden (Boyer och McQueen, 2007; Schechter, 2004). Bedömningen av motståndarens intention kan till exempel basera sig på en beräkning av angriparens return-on-attack (ROA), som fungerar på ett liknande sätt som försvararens ROI (Cremonini och Martini, 2005).

När det gäller beslutsfattande är det viktigt att säkerhetsexperterna kan kommunicera sina resultat samt ovissheten i sina bedömningar till beslutsfattare (Frewer et al., 2003). Camp et al. (2007) visade att lekmän och informationssäkerhetsexperter har olika mentala modeller – tankesätt – för informationssäkerhet. Till exempel är lekmän mer benägna att använda en modell av IT-säkerhet med tänkta fysiska lås och reglar medan experter är mer benägna att tänka i termer av angrepp och försvar eller biologi (virus, maskar och liknande). Värt att notera är dessutom att ingen av grupperna utmärkte sig för att använda ett ekonomiskt tankesätt.

Hur lekmäns och experters sätt att bedöma skiljer sig åt är dock inte helt klarlagt. Experter bedömer vanligen förväntade förluster inom sitt ansvarsområde som betydligt lägre än vad lekmän gör. Sjöberg et al. (2004) tror trots allt att samma faktorer, som till exempel rädsla och känsla av kontroll, påverkar både experter

och lekmän. En potentiell skillnad mellan experter och lekmän är att lekmän generellt har dålig förståelse för låga sannolikheter. Starr (1969) och Schmidt (2004) indikerar att experter ofta gör en mer pessimistisk kostnad-nytta-analys än lekmän. Detta verkar förknippat med upplevd kontroll över situationen som faktor i riskbedömningar. Fischhoff (1978) har dock ifrågasatt de data som ingick i Starrs studie.

I vissa situationer är det nyttigt att anlita flera experter. Att ta medelvärdet av flera experters bedömningar har visat sig ge minst lika exakt resultat som den bästa av experterna. Det innebär att det är troligt att olika experter bedömer på ungefär samma sätt bortsett från en individuell felfaktor (Wallsten et al., 1997). Som nämndes i avsnittet om involverade aktörer, kan samarbete mellan experter från olika delar av organisationen dessutom leda till positiva bieffekter som ökad kunskapsspridning i organisationen (Davis, 2005).

Ett fall då flera experter är av särskild nytta är vid sannolikhets- och konsekvensbedömningen för mycket osannolika men mycket allvarliga potentiella händelser, eftersom mätdata är mycket knapphändig för sådana situationer. (detta utvecklas i avsnitt 4.4).

Det finns dock en möjlighet att experterna uppvisar grupptänkande genom att förstärka varandras (gemensamma) åsikter trots att mängden erfarenhet är begränsad (Paté-Cornell och Fischbeck, 1995). En annan nackdel med experter kan annars vara att deras bedömningar varierar alltför mycket från expert till expert samt till och med från gång till gång (Jaquith, 2007). Dessutom kan experterbedömningar påverkas av så kallad kognitiv bias som känslor. Exempelvis bedöms risker generellt som lägre för en själv än andra (Sjöberg, 2004) medan risker förknippade med händelser som finns färska i minnet bedöms högre än andra risker (Kahneman, 2011).

4.3.2 Mätdata

Mätdata kan antingen komma inifrån organisationen eller utifrån. I den välanvända standarden Common Vulnerability Scoring System (CVSS) (Mell et al., 2014) som nyttjas för att jämföra olika typer av sårbarheter i mjukvara, delas metriker in i tre kategorier. Den första kategorin är generell för en sårbarhet och berör bland annat allmän attackvektor, attackkomplexitet och direkt konsekvens. Den andra kategorin rör tidsberoende egenskaper som exempelvis hur välutvecklat det specifika angreppsverktyget och motsvarande skydd är. I båda kategorierna är främst data från tillverkare av mjukvara och säkerhetsprodukter av intresse eftersom det inte finns någon koppling till det faktiska system som angrips (Mell et al., 2014). Schechter (2004) noterar dock att det ofta är svårt att kontrollera hur korrekt tillhandahållen information en produkts säkerhetsnivå faktiskt är. Det är överhuvudtaget besvärligt att mäta skyddseffekten hos exempelvis antivirusverktyg och intrångsdetekteringssystem (McQueen et al.,

2006). I den tredje kategorin inkluderas kontextberoende faktorer såsom specifika och indirekta (affärsmässiga) konsekvenser samt antal svaga komponenter i systemet. Här behövs således interna bedömningar eller data (Mell et al., 2014).

Jaquith (2007) understryker att externa data inte säger mycket om den enskilda kontextlösa mjukvarans påverkan på den specifika organisationens verksamhet. Vidare menar Jaquith (2007) samt Anderson et al. (2012) att medelvärden som fås från exempelvis amerikanska FBI:s årliga dataintrångsstatistik visar på trender, men är meningslösa att använda som metrikdata på mer specifik nivå för den enskilda organisationen. Det är därför viktigt att på ett vettigt sätt kombinera data från externa mätdatakällor med interna sådana.

4.3.2.1 Externa mätdatakällor

Tillgången till externa data beror på andras villighet eller tvång att dela med sig. Medan organisationer som banker ofta är ovilliga att dela med sig av IT-incidentdata är samarbetsviljan och transparensen betydligt högre när det gäller medicinsk informationsdelning. Samordnande myndigheter för sjukdomar finns och man har som tradition att dela med sig av information. Inblandade är förutom sjukhuspersonal och myndigheter även läkemedelsindustrin och försäkringsbolag samt, genom transparensen, politiker och journalister (Oram och Viega, 2009). Anderson et al. (2012) ger en översikt över incidenters kostnader på främst samhällsövergripande nivå, vilket kan reglera bland andra myndigheters incitament att agera på området. Friedman et al. (2013) introducerar en förenklad modell som uppdelat på industrisektor beskriver hur dataintrång påverkar organisationer på lång sikt.

Det finns flera potentiella anledningar till att inte vilja dela med sig av data. Icke-anonymiserade data kan leda till att organisationens rykte skadas eller att den råkar illa ut om oegentligheter avslöjas. Vidare kan viss information vara affärskritiskt och organisationen kan vara ovilliga att dela säkerhetsrelaterade data med myndigheter om det innebär att informationen blir offentlig. Datadelning kan också hindras av att det skulle innebära alltför mycket jobb att skapa den infrastruktur som krävs eller att översätta mellan olika organisationers definitioner av relevanta begrepp. Ytterligare möjligheter är att samarbete organisationer emellan hindras av konkurrenslagar (Jaquith, 2007) samt att företag tror sig kunna få en fördel genom att inte dela med sig av sina mätdata. En organisation kan anse att dess mätdata är mer värdefulla än andras eller försöka få ta del av andras mätdata utan att själva bidra med några eller bidra med falska sådana (Gordon et al., 2003). Även NRC (2010) nämner svårigheten att kontrollera externa mätdatas autenticitet.

För att hantera de problem som är förknippade med att dela med sig av data sponsrar USA:s departement för inrikes säkerhet (DHS) Predict-projektet (RTI, 2014) som ger legitima forskare tillgång till stora mängder internetdatatrafik

inklusive loggar från angripna datorer. Data som ska ge insikt i säkerhetsläget på internet delas in i kategorier beroende på hur känslig den är från exempelvis personlig integritetssynvinkel. Viss data anonymiseras innan den lämnas ut till forskare som även måste skriva på avtal som reglerar hanteringen. I vissa fall behöver särskilt tillstånd ansökas direkt till de som har tillhandahållit viss data.

Det finns ytterligare exempel på databaser i USA som kan öka möjligheterna för andra organisationer att få tillgång till incidentdata. För IT- och telekomleverantörer finns ett system där information om hot, sårbarheter samt faktiska incidenter kan rapporteras på frivillig basis. Vidare finns en databas som internetleverantörer måste rapportera till om det uppstår omfattande nätverksproblem som till exempel kan påverka allmänhetens möjlighet att nå nödnummer (GAO, 2013). Amerikanska företag är dessutom enligt lag tvungna att rapportera incidenter där information relaterad till personlig integritet läckt ut. Dessa inrapporterade fall redovisas i en öppen databas[6] och är därmed tillgängliga för analys (Oram och Viega, 2009). Den än så länge största incidenten rapporterades i oktober 2013 och rörde läckta kreditkortsuppgifter från mjukvaruföretaget Adobe.

Två av de främsta externa källorna för säkerhetsrelaterade mjukvarusårbarheter är Bugtraq[7] och Carnegie Mellons CERT[8]. Dessa listar kända mjukvarusårbarheter och kan därför underlätta bedömningar av potentiella incidenters sannolikheter och konsekvenser. Det kan ifrågasättas om offentlig listning av sårbarheter verkligen leder till högre säkerhet eller om angripare gynnas lika mycket av externa data som försvararna. Anderson och Moore (2006) nämner forskning som indikerar att sårbarheter som hittats av en part men inte offentliggjorts, så småningom hittas även av andra i alla fall. Att istället publicera sårbarheterna leder till att de snabbare åtgärdas och därmed fås, på sikt, en minskad mängd sårbarheter.

Giroux och Burgherr (2012) beskriver en öppen icke-kommersiell databas med data om icke-statliga aktörers angrepp mot energiinfrastruktur sedan 1980. Datakällor som används är nyhetsartiklar, vetenskapliga journaler, myndighetsrapporter, böcker, online-material och annan öppen information. Ett problem är dock hur angrepp via datornätverk ska kategoriseras eftersom det är besvärligt att avgöra vem angriparen är och information om sådana incidenter är svårare att få tag på.

4.3.2.2 Interna mätdatakällor

I sammanhang som regelefterlevnad och ansvarsutkrävande är externa mätdata och expertbedömningar av begränsad användning. Här finns alltså en fördel med

[6] DatalossDb - http://datalossdb.org/
[7] Bugtraq, Security Focus – http://www.securityfocus.com/archive/1
[8] CERT – http://www.cert.org/

interna mätdata (NIST, 2008). Dessutom är interna mätdata mer specifika för organisationen än externa. En nackdel är dock att det bara går att mäta aktuellt läge i systemet medan externa mätdata och expertbedömningar kan användas för att undersöka potentiella skyddsmöjligheter.

Till skillnad från expertbedömningar är mätdata normalt mer detaljerade. Det kan innebära ökad exakthet men medför också att det måste tydliggöras vilka mått som ska användas för varje del av säkerheten som bryts ner i metriker. Ett stort antal metriker har föreslagits och vilka som bör väljas är – i viss likhet med expertbedömningar – i dagsläget en subjektiv fråga (Boyer och McQueen, 2007). NIST (2008) rekommenderar att enbart etablerade och konsistenta processer mäts och en organisations val av metriker beror därför på dess mognad. Exempel som föreslås är bland annat följande metriker:

- andel informationssystem med säkerhetsplaner och lösenordspolicyer
- andel incidenter som inträffat på grund av undermålig åtkomstkontroll
- andel servrar med standardkonfiguration
- andel buggfixar som införts
- andel komponenter som underhålls enligt schema
- andel av informationssystemsbudgeten som går till informationssäkerheten
- antal säkerhetsinvesteringar som rapporterats till högre chef.

Boyer och McQueen (2007) anser dock att det finns en fara med generella metriker som ignorerar aspekter som att vissa systemkomponenter är viktigare än andra. De föreslår istället följande (för kontrollsystem):

- försvararens kunskap om systemet inklusive antal testade komponenter
- antal administratörer
- antal åtkomstpunkter till internet
- antal sårbarheter
- lösenordsstyrka
- detekteringsnivå
- djupet i försvaret (ungefär antal skydd)
- värsta möjliga konsekvensen av ett angrepp
- tid för återhämtning efter angrepp.

Som kan ses finns ett övergripande systemperspektiv, snarare än ett på komponentnivå, även för deras metriker.

De potentiella konsekvenserna för ett angrepp baseras bland annat på tillgångarnas värde. Camp och Wolfram (2000) föreslår att systemkomponenters värde uppskattas genom att mäta deras processorkraft. Detta täcker dock inte informationstillgångarna i systemet.

De interna datakällor som kommer ifråga är alla de system som organisationen använder. Jaquith (2007) nämner några exempel på dessa:

- nätverkshanteringssystem
- sårbarhets- och händelsehanteringssystem
- kodanalysverktyg
- identitetshanteringssystem (eng. Identity and Access Management)
- incidenthanteringssystem
- infrastruktur (exempelvis routrar, brandväggar, databaser, webbservrar och antivirusskydd)
- system för förvaltning av organisationens tillgångar
- policy-, revisions- och regelefterlevnadssystem
- personalsystem (eng. HR-system).

Vidare exempel på datakällor är penetrationstester och övningsdatabaser (NIST, 2008). Det är dock svårt att jämföra penetrationstester med verkliga angripare eftersom det vid iscensatta övningar finns regler som den spelande angriparen förhåller sig till, exempelvis att inte angripa loggningsfunktioner. Sådana skillnader gör det svårt att skapa helt realistiska övningar (Schudel och Wood, 2000).

Ytterligare en potentiell datakälla är så kallade honungsburkar (eng. honeypots). Dessa nätverksenheter ser för angripare ut som riktiga system, men deras egentliga syfte är att locka till sig angripare för att kunna samla in data om deras tillvägagångssätt vid angrepp. Detta utan att organisationen kan drabbas av faktiska förluster. Än så länge finns dock främst honungsburkar som kan lura osofistikerade angripare som använder oriktad skadlig kod. Honungsburkar för att lura även mer komplexa angripare är dock under utveckling (Kaaniche et al., 2006).

Ett sätt att bedöma om angriparen gör en nettovinst vid ett angrepp är att utfästa belöningar för sårbarheter, vilket föreslås av Schechter (2002). Är de potentiella konsekvenserna av ett angrepp större för försvaren än nettoangreppsvinsten för angriparen kan det vara mer gynnsamt att utfästa en belöning för att rapportera

upptäckta sårbarheter. Denna typ av belöningar är kända från kryptovärlden och används av ett antal både icke-statliga och statliga organisationer rörande informationssäkerhet (Panton et al., 2013). En nackdel med metoden är att antagonister som tidigare inte tjänade något på ett angrepp plötsligt kan få monitärt incitament att identifiera sårbarheter. Anderson och Moore (2006) noterar dock att dessa sårbarheter ändå skulle hittas av någon annan förr eller senare. Organisationen bör dock se till att belöningen som erbjuds håller sig inom vissa ramar såsom att inte överstiga konsekvenserna för sårbarhetens utnyttjande vid ett angrepp (Schechter, 2002).

4.3.2.3 Mätdatainsamling och analysförberedelse

Eftersom data från olika datakällor finns i stora mängder, bör automatisk inhämtning och hantering av dessa data användas i så stor utsträckning som möjligt. Att inhämta och integrera olika data- och metadatakällor inklusive externa sådana, samt att sammanställa, visualisera, rapportera och publicera resultat från dataanalyser kan automatiseras med befintliga verktyg. Däremot krävs manuellt val av datakällor samt manuell metrikdefiniering, modellering och dataanalys (Jaquith, 2007).

Automatiserad datainsamling har ett antal fördelar som exempelvis att det ökar möjligheten till upprepningsbara och centraliserade – och därigenom tillgängliga – resultat (NIST, 2008). Centraliseringen möjliggör vidare att data kan aggregeras vilket är en fördel då angripare ibland sprider ut sina angrepp i ett system för att undgå upptäckt (Anderson, 2001). För att automatiserad datainsamling ska fungera tillfredställande, krävs dock att den har vissa egenskaper. För att uppnå tillräcklig noggrannhet och funktionssäkerhet (eng. reliability) samt kunna garantera att likvärdig mätdata alltid leder till samma resultat, måste metoden bygga på en exakt översättning av den underliggande modellen. Det måste också vara tydligt vilken underliggande modell som metoden nyttjar. Även spårbarhet genom exempelvis loggning krävs (Jaquith, 2007).

För att det ska vara möjligt att göra kontinuerliga mätningar från så många relevanta datakällor som möjligt behöver metoden vara tillräckligt snabb, kostnadseffektiv och skalbar. För att undvika höga kostnader för insamling och analys är det viktigt att fokusera på intressant och tillgängliga data. Exempelvis kan det vara mer kostnadseffektivt att viss analys görs redan nära datakällorna och resultaten av den analysen – istället för rådata – inhämtas till den centrala databasen. Eftersom insamlad data kan vara känslig och behöva skyddas är en ytterligare fördel med detta tillvägagångssätt att minimera mängden känslig metrikdata som behöver skickas i nätverket (NIST, 2008).

För att inte få en skev bild av säkerhetsläget måste data samlas konsekvent från hela systemet. Det verktyg som används måste därför kunna kommunicera med, samt normalisera data från, heterogena datakällor (NIST, 2008).

Kommunikationsdelen finns väl utbyggd i insamlingsverktygen (Jaquith, 2007). Normaliseringen gör det möjligt att beskriva data på ett gemensamt sätt. NIST (2008) rekommenderar att man förutom värde, värdeenhet och datakälla uttrycker sådant som frekvens för, och mål med, varje datainsamling samt ansvarig person eller roll. Eftersom det kan vara nyttigt att kunna dela data med andra organisationer kan det vara lämpligt att nyttja ett standardiserat format som till exempel det som är knutet till NIST:s rekommendationer.

För att underlätta datainsamlingen kan det vara lockande att för det övergripande arbetet nyttja verktyg som redan används i organisationen. Jaquith (2007) varnar dock för detta och förespråkar istället användning av ett verktyg som tagits fram just för riskanalysändamål. Security Incident and Event Management-verktyg (SIEM) är ett exempel på verktyg som är närliggande de som krävs för datainsamling och -analys för riskanalysmetriker. Jaquith (2007) menar dock att SIEM har ett realtidsfokus som inte riktigt passar för de mer strategiska skeenden som riskanalysmetriker är ute efter. Vidare finns frågetecken om hur väl utvecklade normaliserings- och aggregeringsfunktionerna är. Dessutom har SIEM fokus på att hitta avvikelser från normala säkerhetsförhållanden vilket gör det svårare att få siffror som säger något om just de normala förhållandena och avvägningen mellan säkerhet och nytta. Alla säkerhetshändelser täcks heller inte nödvändigtvis in, och koppling till andra system såsom identitetshanteringssystem som kan ge kontext saknas delvis. Jaquith (2007) menar vidare att SIEM inte har tillräckligt hög transparens vad gäller underliggande modell. Därtill är rapporteringsverktyget inriktat på att rapportera till andra typer av aktörer – främst IT-avdelningen – än vad som krävs inom riskanalysområdet. I riskanalyssammanhang är det normalt olika personer eller roller som designar metriker, samlar data, sammanställer data, analyserar resultat, och tar beslut.

4.4 Osannolika händelser med stora konsekvenser

En svårighet vid riskbedömningar är hanteringen av mycket osannolika händelser med potentiellt mycket stora konsekvenser. Eftersom händelserna är ovanliga är det svårare att bedöma dess sannolikhet eftersom bedömningen inte kan baseras på tidigare frekvenser. Små skillnader i uppskattad sannolikhet har dessutom stor påverkan på den förväntade förlusten förknippad med en viss potentiell händelse med hög konsekvens (Sjöberg, 1999; Taleb, 2007b). Dessutom kan konsekvenserna vara så stora att en organisation inte överlever dem, vilket gör att konsekvenserna kan ses som oändligt stora ur organisationens perspektiv.

Taleb (2007) hävdar vidare att när en sådan händelse skett, trots en låg sannolikhet, finns det en psykologisk tendens att i efterhand försöka konstruera förklaringar till varför sannolikheten för händelsen felbedömdes. Exempel på en

sådan efterhandskonstruktion menar han är åsikten att händelsen borde ha förutsetts om det inte hade varit för att viss data hade missats. Sjöberg (1999) och Taleb (2007) menar istället att anledningen till att händelsen inte förutsågs istället beror på antagandet av en felaktig statistisk fördelning. Det är dock inte klarlagt om det överhuvudtaget är möjligt att gissa rätt fördelning.

Denna typ av händelse förknippad med låg sannolikhet, hög konsekvens och efterhandskonstruktioner benämns som en *svart svan* – ett begrepp myntat av Taleb (2007). Det finns olika åsikter i litteraturen om hur vanliga och viktiga dessa typer av händelser är. Ett exempel som beskriver svarta svanar – både positiva och negativa sådana – är teknisk skyddsutveckling där det är svårt att förutsäga hur morgondagens skydd kommer att se ut (Sjöberg, 1999; Schechter, 2004). Vidare kan de flesta informationssäkerhetsincidenter definieras som svarta svanar enligt Jaquith (2007) samt Kaaniche et al. (2006). Taleb (2008) har fokuserat på svarta svanar på finansmarknaden och presenterar data som pekar på deras existens där, men Hubbard (2009) understryker att detta inte säger något om de svarta svanarnas existens på andra områden såsom intern affärsverksamhet eller teknikutveckling.

Paté-Cornell (2012) menar tvärtemot Taleb att verkliga svart svanar är mycket ovanliga och att det ändå oftast finns tillräckliga modeller för, och möjlig data att inhämta även före, ovanliga katastrofala händelser. Dessa data, eller varningssignaler, kan bland annat utgöras av händelser som nästan var katastrofala men där skyddsmekanismerna precis klarade av att hantera det hela. Dessa signaler ignoreras dock ofta eftersom systemet lyckades hantera händelserna tillfredsställande trots att detta kan ha berott på tur snarare än tillfredsställande skydd. En annan typ av varningssignal utgörs av latenta fel och Anderson (2001) ger två exempel på sådana. Det första exemplet rör *diversifiering* och *röstande kontrollmekanismer*. För att minska sannolikheten för felimplementeringar och därmed att fel beslut tas, kan samma funktion implementeras på olika sätt och ett kvalificerat majoritetsbeslut bland de olika implementationerna får vara styrande. Ett latent fel skulle då kunna vara att en av implementationerna är felaktig och att upptäcka detta vore önskvärt. Ett ytterligare exempel kan vara att en bank av misstag utfärdat samma kod till samtliga kunders kort. Eftersom kunderna inte diskuterar sina koder med varandra och bankens säkerhetssystem hindrar de bankanställda från att ta del av koderna, upptäckts inte det latenta felet (sårbarheten) och varningssignalen för en mycket ovanlig händelse missas. Anderson nämner dock inte huruvida generella svarta svanars varningssignaler kommer tillräckligt tidigt för att vara till någon större nytta.

Anderson (2001) konstatera att lågfrekventa händelsers exakta sannolikhet är svårbedömd. Det kan vara svårt att ens upptäcka att dessa händelser inträffat eftersom det krävs säkerhetsmekanismer som är extremt känsliga för att inte missa dessa ovanliga händelser. Vid exempelvis övervakning av nätverk måste

ovanliga, sofistikerade angrepp identifieras bland enorma mängder legitim data vilket kräver larm med hög känslighet (Anderson, 2001). En försvårande aspekt gällande svarta svanar kan dessutom vara att åtminstone lekmän saknar intuitiv förståelse för vad små sannolikheter är (Sjöberg 1999; Desaulnieres 1991).

Existensen av svarta svanar innebär inte nödvändigtvis att en viss riskmetod är undermålig. Först och främst måste man veta om riskmetoden användes för att försöka förutsäga skeendet ifråga och även om så var fallet innebär inte det automatiskt att någon annan existerande metod är bättre (Hubbard, 2009). Att undersöka alternativa metoder är dock av vikt. Den framstående amerikanska strategen Viktor Utgoff har i en intervju med Burns och Miller (2014) föreslagit att dessa osannolika händelser ska inkluderas i USA:s försvarshögskolestudier för att därmed utveckla kreativa strategier för att hantera händelserna. Paté-Cornell (2012) instämmer i att kreativitet är av vikt för att förbereda sig för svarta svanar. Hon ger Columbia-katastrofen som exempel på vikten av fritt och explorativt tänkande, där det faktiska händelseförloppet beskrivits i riskanalysen, även om de exakta siffrorna var fel. En närliggande metod är att analysera även kombinationer av risker eftersom en del svarta svanar består av flera osannolika händelser. Därför kan svarta svanar grovt förutsägas genom analys av kombinationen av andra händelser. Vidare anser amerikanska Institute for defense analyses, som arbetar med amerikansk nationell säkerhet, att osannolika scenarier – som svarta svanar utgör – bör inkluderas vid inventering och bedömning av risker (Thomason, 2009).

Huvudfrågorna i detta avsnitt är hur svarta svanar ska bedömas och hanteras i en riskhanteringsprocess. Det bör för övrigt noterats att den omvända typen av händelser – med hög sannolikhet och låg konsekvens – inte studerats i någon större utsträckning, åtminstone inom riskperceptionsområdet (Sjöberg, 1999). Å andra sidan är det i högsannolikhetssammanhang knappast tal om risk.

4.4.1 Expertbedömning av svarta svanar

Det finns ett vanligt problem att riskanalytiker kan förlita sig i för grad på tillgänglig statistik när det är just i de fall då statistik saknas som avvägningar med riskanalys främst är av intresse (Sjöberg, 1999; Hubbard, 2009). Paté-Cornell (2012) påstår också att det är viktigt är att ha en helhetssyn för systemet och inkluderar även den mänskliga faktorn (som felkälla) i modellen. En sådan faktor är att människor är mer benägna att göra fel när det gäller sådant de gör sällan – som i oförutsedda eller oväntade situationer (Anderson, 2001). Sjöberg (1999) hävdar dock att den mänskliga faktorn liksom motståndare är mycket svårmodellerade. I sin forskning ger Paté-Cornell (1996) exempel på helhetstänk vid bedömningar. Jordbävningsrelaterade risker är ofta svårbedömda, men genom att ha expertstöd från ett brett antal områden kan bättre bedömningar göras. Ett problem kan då vara att man får en uppsjö olika bedömningar – en per expert – och även om ett snittvärde kan vara bättre än varje enskild bedömning

(Page, 2007), tror Paté-Cornell att experternas olika modeller, synsätt och information gör detta alltför trubbigt. För att ensa dessa experters bedömningar förespråkas en fri debatt där varje expert får propagera för sin åsikt och diskutera de andras. Viktigt är då att experterna antar olika roller där de kan både försvara och angripa en viss modell för att de inte ska låsa sig fast i att försvara "sin" modell. Annars finns en möjlighet att en expert undanhåller viktig information om den modell som experten föreslår. Paté-Cornell hävdar att denna riskbedömningsmetod kan appliceras även på andra områden. För att en sådan metod ska vara användbar och att experter ska ha möjlighet att påverka utformningen av system måste säkerheten inkorporeras i ett tidigt skede av systemutvecklingen (Anderson, 2001).

Hansson (2005) menar att nya typer av agerande – där befintlig kunskap är mer knapphändig – innebär större sannolikhet för oväntade händelser och på så vis kan uppkomsten av svarta svanar, som grupp, förutsägas för olika typer av potentiella ageranden. Införs en helt ny typ av teknik bör större förberedelser göras för oväntade händelse än om existerande teknik endast varieras i mindre grad. Utifrån detta går det dock inte säga något om eventuella konsekvenser – vare sig positiva eller negativa. Taleb (2009) menar även att förutom sådant som är nytt, gör all typ av komplexitet att det blir svårare att göra riskbedömningar. Därmed kan problemet med svarta svanar minskas genom att minska systemkomplexiteten. Sådana åtgärder kan ha nackdelar som till exempel sänkt produktivitet och automatisering. Taleb (2009) argumentrar dock att det inom vissa områden är mer värt att sänka komplexiteten än de nackdelar det innebär.

Paté-Cornell (1996) samt Paté-Cornell och Guikema (2002) förespråkar i viss likhet med Hansson (2005) en generell metod för att bedöma sannolikheter för klasser av incidenter när det gäller svarta svanar. Metoden bygger vidare på att flera olika källor och/eller experter används för indata och man fokuserar inte enbart på vad som hänt tidigare utan kombinerar det med vad som kan hända i framtiden. Vidare inkluderas viss spelteori för att hantera angriparnas anpassning till vald försvarsstrategi och istället för att försöka komma fram till exakta siffror är fokus på prioritering av risker. I en närliggande artikel föreslår Paté-Cornell och Fischbeck (1995) att bayesianska sannolikhetsmodeller används för att uttrycka måttet av tillförlitlighet till sina underliggande hypoteser. På detta sätt kan tidigare förväntningar justeras utifrån ny information – det vill säga varningssignalerna (Paté-Cornell, 2012).

Då svarta svanar är lågfrekventa händelser men med stora konsekvenser, kan det vara olämpligt för en organisation att tänka i termer av medelförlust per år. Om konsekvensen är koncentrerad till en kortare tidsperiod kan den nämligen vara tillräckligt stor för att organisationen inte ska klara av den och exempelvis gå i konkurs (Jaquith, 2007; Rakes et al., 2012). Det finns alltså ett visst riskavert resonemang kopplat till de svarta svanarna (Paté-Cornell, 2012). Ett exempel är oljeindustrins strategi att konstant och avsiktliga undervärdera sina

oljefyndigheter för att vara bättre förberedd på möjligheten att oljan plötsligt tar slut (Hubbard, 2009). Givet att det finns en gräns för vad en organisation kan klara av för momentana konsekvenser kan alla konsekvenser över denna nivå betraktas som likvärdiga, vilket i sin tur ger stöd för att behandla svarta svanar i grupper.

4.4.2 Hantering av de svarta svanarnas konsekvenser genom flexibilitet

Jenkin (2006) och Taleb (2007) nämner att riskhantering för svarta svanar kan vara otacksamt. En anti-terrorismenhet får kritik om de missar en svart svan (läs: terroristattack) men eftersom deras arbete ofta är hemligt får de normalt inget beröm om de stoppar en. Detta är möjligen generellt för all riskhantering, men blir tydligast just för svarta svanar och kan påverka riskanalytikerns incitament att stoppa svarta svanar i den övriga organisationen. Taleb (2009) nämner ett liknande förhållande inom finansvärlden där stora organisationer tar alltför stora risker samtidigt som de inte förbereder sig för oväntade händelser. När det sedan går dåligt så kan stater gå in med räddningspaket som enligt Taleb (2009) skapar incitament att fortsätta med samma typ av risktagande beteende.

Eftersom det är svårt att bedöma svarta svanars sannolikhet kan det vara viktigare att istället fokusera på att förbereda sig på och hantera själva konsekvenserna (Taleb, 2007; Thomason, 2009). Detta är nära de ansatser som beskrivs av Soo Hoo (2000) samt Hole och Netland (2010) där fokus ligger på att beräkna värdet av det som skyddas eller andra relaterade finansiella kostnader snarare än en sannolikhetsbedömning.

Eftersom karaktären av svarta svanar är okänd behöver de hanteras som grupper av händelser snarare än specifika händelser. Händelserna bör alltså ses på en mer generell nivå som exempelvis ”terroristattack” istället för ”terroristattack med bilbomb mot marknad X på tisdag”. För att hantera en grupp konsekvenser menar Burns och Miller (2014) att man bör fokusera på att vara adaptiv för att kunna reagera flexibelt när något väl händer. Att specialisera sig kan alltså vara kontraproduktivt när det gäller svarta svanar. Anderson (2001) håller med om att det är viktigt att bemöta de svarta svanarna med flexibilitet och reaktivitet. Exempelvis bör man ha personal redo att agera när incidenter inträffar och ha förberett en PR-strategi. Dessutom är det lämpligt att hålla sig informerad om sina sårbarheter, exempelvis genom att betala utomstående som rapporterar sårbarheter i ens produkter (Panton, et al., 2013). Anderson nämner dock även att ovissheten som de svarta svanarna är förknippade med gör det svårt att formulera precisa säkerhetskrav. Schudel och Wood (2000) rapporterar dessutom att det verkar vara svårt att ta fram ett skydd som klarar flera typer av angrepp.

Ett vanligt generellt sätt att hantera stora konsekvenser är att försäkra sig. Vissa typer av händelser kan dock vara svårförsäkrade, enligt Böhme och Kataria

(2006). Eftersom världens datorer i hög grad är sammankopplade och likartade sprids till exempel maskar och virus globalt. En incident som drabbar en försäkringstagare drabbar därmed också många andra vilket ställer krav på alltför stora kapitalresurser hos försäkringsbolagen. Av samma skäl sprids dock även organisationsspecifika händelser snabbt, fast enbart inom organisationen, vilket ger ökat incitament för att försäkra sig. Detta innebär att försäkringar är mer lämpade som lösning för vissa typer av IT-säkerhetsproblem – exempelvis insiderrelaterade sådana – än andra. Något annat som talar mot försäkringsstrategin är att IT-säkerhetsvärlden kan ändras för snabbt för att försäkringsbolagen ska hinna uppdatera sina modeller (Goodman och Lin, 2007).

5 Diskussion

Det finns historiskt flera försök att kvantifiera behovet av informationssäkerhet, vilket Soo Hoo (2000) beskriver. Det verkar dock som att det under 2000-talet skett ett skifte från en riskhantering primärt fokuserad på teknik till att se skyddet av IT-resurser som en integrerad del av verksamheten. Vikten av att betrakta informationssäkerhet utifrån ekonomiska aspekter lyfts av Anderson (2001b) där han argumenterar att tekniska lösningar inte är tillräckliga för att hantera säkerhetsproblemen med IT. Dessa problem består i lika stor del i de incitament som angriparna har – incitament som går att beskriva med hjälp av ekonomiska ramverk. Likaså går det att förklara varför system utvecklas som dem gör – säkra eller inte säkra – med hjälp av ekonomiska resonemang. Litteraturöversikten har visat att det finns ett stort intresse inom den vetenskapliga litteraturen att diskutera och studera aspekter av informationssäkerhet utifrån och med hjälp av ekonomiska frågeställningar och metoder.

Det har publicerats en stor mängd litteratur som belyser området informationssäkerhet och ekonomi från en rad olika vinklar. Fokus i det här arbetet har varit främst utifrån forskningsfrågorna:

> *Vilka faktorer påverkar graden och typen av investeringar i informationssäkerhet?*
>
> *Vilka metoder finns det för att ta fram underlag för beslut rörande investeringar i informationssäkerhet?*

Dessa frågor diskuteras var för sig under de kommande två rubrikerna. Ett tredje avsnitt beskriver därefter förslag till framtida forskning.

5.1 Faktorer som påverkar investeringar i informationssäkerhet

Den första forskningsfrågan om vilka faktorer som påverkar investeringar av informationssäkerhet belyses i denna rapport utifrån två områden. Det (1) första området handlar om de strategier som organisationer använder för investeringar, samt hur samarbete och kontroll inom organisationen påverkar arbetet med informationssäkerhet. Det (2) andra området handlar om föreslagna metoder för att beräkna vilken investeringsnivå som är optimal och ekonomiskt rationell samt metoder för att stödja beslutsfattande rörande informationssäkerhetsinvesteringar.

5.1.1 Strategier för styrning av investeringar i informationssäkerhet

Under 2000-talet skedde en förskjutning av informationssäkerheten från att ha varit ett specialområde till att i högre grad ingå i organisationers normala funktioner och alltmer hanteras på samma sätt som andra verksamhetsrisker. Detta är en tendens som bland annat noterats av Gallaher et al. (2006) och går hand i hand med uppsvinget av olika metoder för att kvantitativt bedöma risker gällande informationssäkerhet. I litteraturöversikten som presenteras i denna rapport identifieras en begränsad mängd litteratur med fokus på styrning och kontroll samt en mer omfattande mängd artiklar rörande beräkning av eller bedömning av lämplig investeringsnivå. Detta överensstämmer med Steinbart et al. (2012) som menar att det finns en brist på empirisk forskning rörande styrning och kontroll inom detta område. Både Steinbart et al. (2012) och Davis (2005) påtalar vikten av samarbete mellan olika organisatoriska funktioner och att kommunikationen mellan experter på informationssäkerhet och affärsverksamhetsområdena måste underlättas. Expertsamverkan kan förutom kunskapsspridning i organisationen även minska subjektiviteten kontra enskilda experter (Wallsten et al., 1997). Vidare behövs en större förståelse mellan beslutsfattare och experterna, något som försvåras av att grupperna tenderar att använda sig av olika mentala modeller och riskbedömningar. Mer återkoppling från beslutsfattare ökar dock säkerhetsexperter möjlighet att förstå åtgärder ur ett verksamhetens perspektiv och kanske även bättre argumentera för åtgärder. I ISBS (2008) menas det att organisationer som alltid gör formella business case tenderar att spendera en större andel av IT-budgeten på skyddsåtgärder än andra organisationer. Detta skulle kunna vara ett exempel på att hur verksamhetens krav används för att motivera investeringar i informationssäkerhet.

Gallaher et al. (2006) menar att den vanligaste strategin för att sätta nivån för säkerhetsinvesteringar är att informationssäkerhetsbudgeten baseras på föregående års budget, istället för ett beräknat behov för kommande år. Detta kan eventuellt förklaras med att det är för omfattande och svårt att göra en uppskatting av behovet, vilket återspeglas i ISBS (2014) där endast 51 % av större organisationer och 30 % av de mindre anger att de mäter trender i kostnader för säkerhetsincidenter. Vidare gör 29 % av de stora respektive 45 % av de mindre organisationerna ingen formell utvärdering av effekten av investeringar.

Det är fortfarande en utmaning att avgöra hur hot, sårbarheter samt skyddseffekter ska mätas eller bedömas – det vill säga vilka mått eller metriker som ska väljas. Svårigheterna leder ofta till att metrikerna blir subjektiva snarare än objektiva, samt att de är svåra att validera (Jaquith, 2007). Vad som är enklare att mäta hur mått som hur välplanerat säkerhetsarbete utförs, men detta kan innebär ett byte av fokus från innovativa säkerhetslösningar till reglering och

regelefterlevnad. Här finns alltså en fråga om vilken nivå av delegering av beslut för säkerhet som är lämplig.

5.1.2 Optimal nivå av investeringar i informationssäkerhet

En ansenlig del av litteraturen som identifierats i denna litteraturöversikt har fokuserat på att lösa optimeringsproblemet att balansera kostnaden av IT-intrång mot kostnaden för att investera i skydd. De metoder som presenteras i litteraturen är dock till största del på en teoretisk nivå inom en ofta kraftigt avgränsad och förenklad domän. Exempelvis görs ingen skillnad på initiala och löpande kostnader. I den genomgångna litteraturen finns heller inga fallstudier eller utvärderingar som undersöker användningen eller effekten av denna typ av beräkningar i verkliga situationer, varför det är oklart vilken praktisk tillämpning de har i dagsläget. Varför verkar denna typ av optimeringsberäkningar då inte ha fått något genomslag? Delvis kan detta troligen förklaras med den komplexitet som kännetecknar moderna IT-miljöer och IT-hot. Flertalet av metoderna verkar dessutom kräva ett alltför omfattande kartläggningsarbete av sårbarheter och hot för att kunna nyttjas. Detta verkar vara en återgång till det som Soo Hoo (2000) benämner som den första generationens riskhanteringsmetoder som togs ur bruk på grund av deras omfattning. Denna problematik förvärras även av att det finns mycket oklarheter gällande vilka sannolikheter som gäller för hot och vilka konsekvenser de kan medföra. Denna avsaknad av indata är enligt Gallaher et al. (2006) ett av de primära skälen till att denna typ av metoder inte används i större utsträckning. Tillgången till denna typ av data verkar fortfarande inte vara tillräcklig.

Problematiken att sätta siffror på sannolikheten för hot, utnyttjandet av sårbarheter samt kostnader för incidenter innebär att uppskattningarna är behäftade med stora ovissheter. Eftersom huvuddelen av metoderna som redovisats i rapporten bygger på kedjor av sannolikheter blir det slutliga resultatet förknippat med stor felmarginal. I enstaka fall, exempelvis Table Top Model (Garvey et al, 2012), presenteras metoder som explicit hanterar faktumet att bedömningar är subjektiva med en stor inneboende felmarginal. De modeller som behandlats i studien avgränsar bort befintliga investeringar i informationssäkerhet och beräknar bara den totala optimala investeringen utan att värdera eller ta hänsyn till tidigare investeringar och befintliga skyddsmekanismer.

För att omformulera problemet att balansera kostnader för investeringar och kostnaden för angrepp görs en hel del antaganden och förenklingar i de föreslagna metoderna. Ett vanligt antagande är att det för varje sårbarhet finns en säkerhetslösning med ett fixt pris samt att säkerhetslösningens effektivitet (sannolikheten för att den stoppar angrepp) är känd. Att en säkerhetslösning skulle kunna påverka flera sårbarheter eller att det skulle kunna krävas flera olika säkerhetslösningar för att reducera en sårbarhet är det få metoder som hanterar.

En del metoder hanterar inte alls att reducering av sårbarheter kan innebär olika typer av investeringar utan anger endast vilken nivå i pengar som investeringen totalt får betinga, oavsett hur investeringen realiseras i lösningar. Detta gör att de passar in i metodgruppen Integrated Business Risk Management definierad av Soo Hoo (2000) där IT-risker likställt andra verksamhetsrisker genom att inte fokusera på lösningen eller tekniken. Ytterligare ett vanligt antagande är att samtidigt som ett system blir säkrare minskar skyddseffekten per ytterligare investerad krona exponentiellt (Gordon & Loeb, 2002; Anderson & Choobineh, 2008).

De kvantitativa säkerhetsmetoderna bygger ofta på antaganden rörande angriparen. Exempelvis antas att olika steg i angreppssekvenser är oberoende av varandra trots att det kan tänkas att intelligenta angripare inte beter sig så. Samtidigt kan metodernas modell av angripare som rationella, där angriparen maximerar sin vinst och minimerar sina förluster, ifrågasättas mot bakgrund av beslutsforskning (Verendel, 2009). Exempelvis Schechter (2004) ställer sig skeptisk till rationaliteten medan Schudel och Wood (2000) tror på angriparens rationalitet. Ett flertal metoder väljer att utgå från de angriparmodeller som Gordon & Loeb (2002) presenterat i form av fallen klass I och II. Detta trots att det verkar saknas empirisk grund för detta och artiklarna innehåller heller ingen motivering till antagandet. Vidare utgår så gott som samtliga författare från att relevanta sannolikheter är normalfördelade vilket kan ifrågasättas, särskilt när det gäller högmotiverade angripare som motsvarar klass I (Hua & Bapna, 2013).

Vid beräkningen av vad som är en optimal investering baserat på riskerna antas även att organisationerna i de flesta fallen är riskneutrala samt att de är vinstdrivande företag där kostnader för incidenter, förutom att lösa tekniska problem efter intrång, även kan bestå av minskat antal kunder, försämrat rykte, stämningar etc. Gordon & Loeb (2002) skriver uttryckligen att deras modell inte är avsedd att hantera skydd av publika/nationella tillgångar eller andra omständigheter där en förlust skulle kunna få katastrofala följder. Hua och Bapna (2013) hävdar att organisationer som ansvarar för nationellt viktig infrastruktur behöver investera mer i informationssäkerhet än andra. Hur dessa olika typer av utgångspunker påverkar hur investeringar bör ske verkar i mångt och mycket vara oklart.

Metoderna antar vanligen att en händelses sannolikhet och konsekvens är oberoende. För icke-antagonistiska hot som naturkatastrofer är det rimligt men när angripare är involverade är det rimligare att det finns en koppling. Angripare blir förmodligen mer motiverade att utföra ett angrepp om den potentiella vinsten ökar samtidigt som ökad vinst för angriparen kan antas innebära större konsekvens för den angripne (Schechter, 2004). I Gordon och Loebs (2002) arbete gjordes antagandet att det inte går att påverka sannolikheten för ett angrepp, utan bara sannolikheten för att angreppet lyckas. Detta är ett antagande som i många fall hänger med i senare modeller, men det finns ett par exempel där

detta antagande ifrågasätts. Anderson et al. (2012) menar till exempel att det är just på sannolikheten för angrepp som fokus borde ligga snarare än att investera i skydd. Eftersom det är alltför svårt och dyrt att skydda sig mot den ökade mängden av hot skulle det vara mer effektiv att minska antalet angrepp (genom till exempel polisära åtgärder), istället för att skydda sig mot dem.

Vidare är det inte klarlagt om sårbarheter i systemkomponenter är oberoende av varandra eller hur ett eventuellt beroende ser ut. Samtidigt antas i många modeller att systemen är statiska istället för att de uppdateras i snabb takt. Antagandena kommer ofta från andra forskningsfält och de stöds in med empiri. När validering av dessa antaganden väl görs sker den normalt knapphändigt under kort tid, i enstaka system eller med resultat som sekretessbeläggs och som därmed inte kan kontrolleras av andra forskare. Det primära undantaget är modeller för upptäckt av tekniska mjukvarusårbarheter där viss validering gjorts (Verendel, 2009).

Hur man förhåller sig till tidsaspekten varierar mellan olika författare. I ALE-modellen utgår man från förväntade förluster under en ettårsperiod vilket innebär att investeringsbehovet enkelt går att koppla till en budget. Många av de senare modellerna är dock av så kallad *one period model*, vilket innebär att de sannolikheter man räknar med representerar en ögonblicksbild och att tidsfaktorn inte ingår i kalkylerna. Skyddseffekten som olika typer av säkerhetsmekanismer erbjuder är föränderlig. Sårbarheter av olika dignitet upptäcks hela tiden vilket innebär att sannolikheten för intrång (incident) snabbt kan förändras eller visa sig vara felaktig, vilket i sin tur medför att många säkerhetslösningar enbart ger ett tillfälligt skydd (Anderson & Choobineh, 2008).

5.2 Metoder för att ta fram beslutsunderlag för investeringar i informationssäkerhet

Att kartlägga sårbarheter och hot är kanske den största utmaningen vid optimeringsberäkningar. Sannolikheten för att en viss typ av skyddsmekanism stoppar en attack skulle kunna vara relativt enkelt att uppskatta om det fanns tillgång till statistiska underlag, men det är ytterst få organisationer som öppet redovisar attackerna de utsätts för, både stoppade samt för angriparen framgångsrika attacker. Dessutom är det ovanligt att det sker någon uppföljning av stoppade attacker överhuvudtaget. Om man dessutom beaktar målinriktade angripare, klass I enligt Gordon och Loeb (2002), är statistiskt underlag av begränsad nytta eftersom angriparens motivation är svår att fastställa. Gordon och Loeb (2002) hanterar detta genom antagandet att sannolikheten för angrepp är normalfördelad och att den optimala investeringsnivån är en i det närmaste linjär funktion av sårbarheten. Dessutom antar man att angriparen inte anpassar sin strategi efter de investeringar som görs i informationssäkerhet. Frågan blir då vilka angripare man behöver skydda sig mot och hur motiverade de är.

När det gäller händelser med mycket låg sannolikhet och stora konsekvenser är statistiska metoder av begränsat värde eftersom det per definition saknas historik och empiri. Då är expertbedömningar av särskild nytta. Händelser förknippade med låg sannolikhet och höga konsekvenser där upptäckta felbedömningar av sannolikhet bortförklaras med efterhandskonstruktioner kallas ofta svarta svanar (Taleb, 2007). Svarta svanar är ett problem på grund av den stora ovissheten som är förknippade med dem samt att en organisation kan ha svårt att överleva de stora negativa konsekvenserna som följer av svarta svanar. Detta innebär att exakt konsekvensbedömning är mindre viktigt, givet att konsekvensen är större än organisationen kan hantera, men gör sannolikhetsbedömningen desto viktigare. Ett sätt att förenkla bedömningen av sannolikheter är att låta experter bedöma grupper av risker istället enskilda och detaljerade risker (Thomason, 2009). Alternativt kan svarta svanar ses som kombinationer av – någorlunda mer lättbedömda – risker. Kreativa scenarier kan nyttjas för att kartlägga och öva på det okända (Anderson, 2001; Burns och Miller, 2014). Dessutom gäller det att vara observant på varningssignaler som nära katastrofer och latenta fel (Paté-Cornell, 2012), vilket ställer krav på larm med hög känslighet (Anderson, 2001). Flexibilitet är av vikt för att reagera trots ovissheten, vilket gör försäkringar attraktiva. Men även försäkringsbolagen kan se riskerna som alltför ovissa om de är förknippade med IT som global och snabbföränderlig företeelse. Dock kan försäkringsbolag rikta in sig på mer organisationsspecifika, kontextuella, problem såsom insiderproblematiken (Böhme och Kataria, 2006; Goodman och Lin, 2007). Slutligen kan minskad systemkomplexitet möjligen minska mängden svarta svanar, men då kan även den positiva utvecklingstakten påverkas negativt (Taleb, 2009).

Att analysera vilka konsekvenser och kostnader (både direkta och indirekta) som varje framgångsrik attack skulle kunna innebära är även det ett svårt och omfattande arbete som dessutom skiljer sig mellan olika typer av organisationer och IT-system. Det finns i dagsläget inga enkla eller etablerade metoder för att värdera olika former av tillgångar och hur dessa tillgångar påverkas vid olika former av incidenter och attacker. Sannolikt behöver värderingsmetoder anpassas till olika branscher eller sektorer eftersom den underliggande verksamhetslogiken skiljer sig åt mellan exempelvis offentlig förvaltning och kommersiell affärsverksamhet.

Externa mätdata är särskilt lämpligt för sådant som är generellt för ett hot eller en sårbarhet och som därmed inte påverkas av den specifika organisationens kontext. Frågan är dock vad som påverkar organisationers vilja och möjlighet att dela med sig. Data kan vara förknippade med sekretess, myndigheter kan reglera i vilken mån samarbete får och måste ske, och en gemensam infrastruktur och terminologi är essentiellt.

Vid uppskattningar av sannolikheter för angrepp är det viktigt att inte bara utgå från den egna organisationen, utan även ta hänsyn till vilka beroenden som finns

till andra aktörer. Den mesta litteraturen avhandlar riskhantering utifrån vad som är en teoretiskt optimal investeringsnivå i en enskild organisations perspektiv. Liu et al. (2011) påvisar dock hur organisationer påverkas av vilken information som de delar med andra organisationer. Beroende på om organisationer har överlappande information eller kompletterande information jämfört med andra påverkas incitamentet hos en angripare att genomföra angrepp. Det innebär att kunskap inte bara om den egna organisationen behövs utan även om andra aktörer. Om den information angriparen söker är (disjunkt) utspridd på flera organisationer kommer angriparen bara vara intresserad av att angripa en organisation om den tror att även angrepp mot varje annan organisation kommer att lyckas. Därför finns ett naturligt incitament hos organisationerna att utbyta information om sin informationssäkerhet. Men i andra fall kan externa påtryckningar i form av lagstiftning eller subventioneringar behövas för att uppnå ett kunskapsutbyte syftande till att skapa bättre underlag för beslut. Påtryckningar kan även behövas för att uppnå en mer samhällsnyttigt optimal investeringsnivå, då organisationer i vissa fall har incitament att underinvestera utifrån ett samhällsnyttigt perspektiv.

5.3 Förslag till fortsatt forskning

En stor del av litteraturen rörande optimeringsberäkningar är av teoretisk karaktär och det finns en märkbar avsaknad av utvärderingar av deras praktiska tillämpbarhet. Det vore därmed angeläget att vidare empiriskt undersöka hur beslut rörande investeringar i informationssäkerhet görs i praktiken idag, vilka faktorer som inkluderas i bedömningar och var vilka metoder som används. Det vore även relevant att undersöka vilka organisatoriska faktorer som kan spela in gällande syn på investeringar i informationssäkerhet och hur arbete på området praktiskt går till. Tidigare studier genomförda i USA har pekat på vikten av samarbete och kommunikation mellan olika delar av organisationer för ökad effektivitet hos investeringar inom informationssäkerhet. Även här kunde det vara aktuellt att se till den svenska situationen för att se om liknande mönster går att identifiera, samt se hur organisationer kan leda och koordinera arbetet rörande informationssäkerhet på mest gynnsamt sätt.

Teorier som den av Gordon och Loeb (2002) utgår från riskneutrala organisationer och menar explicit att samhällskritiska verksamheter inte lyder under samma antaganden som dessa. Det vore därmed relevant att undersöka skillnaderna mellan samhällskritiska verksamheter och andra organisationer gällande beslutsprocesser och avväganden kopplat till investeringar i informationssäkerhet, både vad gäller dagsläget och framtida metoder. Kopplat till en empirisk undersökning om hur dessa avvägningar görs idag kan det vara intressant att undersöka vilken nytta formella metoder kan ge.

I Storbritannien genomförs regelbundet en enkätundersökning gällande informationssäkerhet där bland annat kostnader för intrång och skydd, metoder för investeringar samt kontroll tas upp. Genom denna enkät (ISBS, 2012) uppskattades den genomsnittliga kostnaden för skydd mot intrång vara runt 8 % av organisationers IT-budget (11 % i de fall där säkerhet är prioriterat). Hur situationen är i Sverige och vilka nivåer som är rådande verkar inte vara lika väl kartlagt varför en liknande undersökning skulle vara intressant.

Tidigare har vissa länder (ex. USA) infört obligatorisk rapportering av incidenter för statliga och privata aktörer gällande vissa typer av händelser. I Sverige har MSB föreslagit en form av obligatorisk rapportering för statliga myndigheter (MSB, 2012). Med anledning av detta vore det relevant att djupare studera hur sådan rapportering kan gå till och hur insamlad data kan användas.

Metoderna för att beräkna lämplig investeringsnivå är sällan särskilt detaljerade beträffande vilka kostnader som bör ingå i beräkningarna eller hur man bör mäta detta. En relaterad frågeställning är hur verksamheten och dess effektivitet påverkas av högt ställda krav på sekretess- och riktighetsaspekterna av informationssäkerhet. NRC (2010) efterfrågar ökat samarbete mellan forskare från relaterade discipliner och saknar metoder för kvantifiering och jämförelse mellan användbarhet och säkerhet för olika intressenter. Forskningen om svarta svanar indikerar att ökad systemkomplexitet ökar risken samtidigt som godartad teknisk utveckling normalt medför mer komplexa system (Anderson och Moore, 2006). Hur kan denna potentiella motsättning neutraliseras? Ett vanligt antagande är att ju säkrare ett informationssystem är, desto jobbigare är det att använda. Stämmer verkligen detta antagande och vad kostar i så fall säkerhet i form av förlorad tid för inloggning, återställning av lösenord, utbildning, väntetider och liknande? I de studerade artiklarna behandlas initialkostnader för teknik och i viss mån kostnader för utbildning och drift, men ingen artikel nämner de löpande kostnader som ligger utanför informationssäkerhetsbudgeten.

En avslutande och övergripande fråga är hur informationssäkerhet ska hanteras utifrån ett samhällsnyttigt perspektiv. En följd av interaktionen mellan flera organisationer på en gemensam marknad är att en för enskilda organisationers optimala investering blir suboptimal för samhället i stort (Anderson, 2001; Liu et al., 2011). Det finnas därför argument för att reglera hur organisationer investerar i säkerhet då det kan få vidare konsekvenser. Kwon och Johnson (2011) samt Anderson et al. (2012) pekar dock på en rad problem som lagstiftning och reglering gällande informationssäkerhet kan innebär och det finns därför ett behov av att studera hur myndigheter kan påverka för att samhället ska uppnå en gynnsam nivå av säkerhet. Vilka typer av regleringar är effektiva och vilka riskerar att hämma innovation och felrikta säkerhetsinvesteringar?

Referenser

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computer & Security* 26, 276-289.

Anderson, R., Bartin, C., Böhme, R., Clayton, R., van Eeten, M.J.G, Levi, M., … Savage, S. (2012). Measuring the Cost of Cybercrime. Workshop on the Economics of Information Security. Berlin, Tyskland, 25-26 Juni.

Anderson, R. & Moore, T. (2006). The Economics of Information Security: A Survey and Open Questions. *Science* 314, 610-613.

Anderson, E. E. & Chioobineh, J. (2008) Enterprise information security strategies, *Computers & Security* 27, 22-29.

Anderson, R. (2001b). Why Information Security is Hard – An Economic Perspective. *Proceedings 17th Annual Computer Security Applications Conference.*

Anderson, R. J. (2001). *Security Engineering* (1:ed). Wiley Computer Publishing.

Aissa, B. A., Abercrombie, R.K, Sheldon, F.T. & Mili, A. (2010). Quantifying security threats and their potential impacts: a case study. Innovations in Systems and Software Engineering 6, 260-281.

Böhme, R. & Kataria, G. (2006). *Models and Measures for Correlation in Cyber-Insurance*, Workshop on the Economics of Information Security. Cambridge, Storbritannien, 26-28 Juni.

Bojanc, R., Jerman-Blažič, B. & Tekavčič, M. (2012) Managing the investment in information security technology by use of a quantitative modeling, *Information Processing and Management* 48, 1031-1052.

Boyer, W. & McQueen, M. (2007). Ideal Based Cyber Security Technical Metrics for Control Systems. *Proceedings of the Second International conference on Critical Information Infrastructures Security*, 246-260.

Brotby, W.K. (2009) *Information security management metrics: a definitive guide to effective security monitoring and measurment.* Auerbach Publications, USA

Burns, W. R. & Miller, D. (2004). *JFQ 72 Improving DOD Adaptability and Capability to Survive Black Swan Events*. National defense university press, [www] http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/8318/jfq-72-improving-dod-adaptability-and-capability-to-survive-black-swan-events.aspx (kontrollerad 17/4 2014).

Camp, L. J. & Wolfram, C. (2000). *Pricing Security*. *Proceedings of the CERT Information Survivability Workshop*, Boston, MA.

Camp, L. J., Asgharpour, F., Liu, D. & Bloomington, I. N. (2007). Experimental Evaluations of Expert and Non-expert Computer Users' Mental Models of Security Risks. *Proceedings of Workshop on the Economics of Information Security 2007*.

Cremonini, M. & Martini, P. (2005). Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA). Workshop on the Economics of Information Security. Cambridge, USA, 2-3 Juni.

Davis, A. (2005) Return on security investment – proving it's worth it. *Network Security* 11, 8-10.

Fischhoff B., Slovic, P., Lichtenstein, S., Read S. & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, 9 (2), 127.

Frewer L. J., Hunt, S., Brennan, M., Kuznesof, S., Ness, M. & Ritson, C. (2003). The views of scientific experts on how the public conceptualize uncertainty. *Journal of Risk Research* 6 (1), 75–85.

Friedman, A. A., Mack-Crane, A. & Hammond, R. A. (2013). *Cyber-enabled Competitive Data Theft: A Framework for Modeling Long-Run Cybersecurity Consequences*, Brookings Institution.

Gallaher, M.P., Rowe, B.R., Rogozhin, A.V. & Link, A.N. (2006) *Economic Analysis of Cyber Security.* Final Technical Report (AFRL-IF-RS-TR-2006-227), Research Triangle Institute, USA.

Gao, X., Zhong, W. & Mei, S. (2013) A differential game approach to information security investment under hackers' knowledge dissemination, *Operations Research Letters*, 41, 421-425.

GAO. (2013). *Communications Networks, Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts*. Report to Congressional Requesters, GAO-13-275 (United States Government Accountability Office)

Garvey, P.R, Moynihan, .A. & Servi, L. (2012). A Macro Method for Measuring Economic-Benefit Returns on Cybersecurity Investments: The Table Top Approach. *Systems Engineering* 16 (3), 313-328.

Giroux J. & Burgherr P. (2012). Canvassing the Targeting of Energy Infrastructure: The Energy Infrastructure Attack Database. *Journal of Energy Security*, (kontrollerad 15/4 2014: http://www.ensec.org/index.php?option=com_content&view=article&id=379:canvassing-the-targeting-of-energy-infrastructure-the-energy-infrastructure-attack-database&catid=128:issue-content&Itemid=402)

Goodman, S. E. & Herbert, S. L. (red.). (2007). *Toward a Safer and More Secure Cyberspace*, The National Academies Press.

Gordon, L. A., Loeb M.P. & Lucyshyn W. (2003) Sharing Information on Computer Systems Security: An Economic Analysis. *Journal of Accounting and Public Policy* 22(6), 461-485.

Gordon, L. A. & Loeb, M. P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security* 5 (4), 438-457.

Hansson, S. O. (2005). The Epistemology of Technological Risk. *Techné: Research in Philosophy and Technology*, 9 (2). http://scholar.lib.vt.edu/ejournals/SPT/v9n2/hansson.html (kontrollerad 15/4 2014)

Hole K. J. & Netland, L.H. (2010). Toward Risk Assessment of Large-Impact and Rare Events. *IEEE Security and Privacy Magazine* 8, 21-27.

Hua, J. & Bapna, S. (2013) The economic impact of cyber terrorism. *Journal of Strategic Information Systems* 22, 175-186.

Huang, C. D., Hu, Q. & Behara, R. S. (2008) An Economic analysis of the optimal information security investment in the case of a risk-aversive firm. *International Journal of Production Economics* 114, 793-804.

Hubbard, D. W. (2009). *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley & Sons.

ISBS (2008). *Information Security Breaches Survey*. Technical Report (URN 08/788). Department for Business Enterprise and Regulatory Reform, London, Storbritannien.

ISBS (2012). *Information Security Breaches Survey*. Technical Report. PricewaterhouseCoopers, London, Storbritannien.

ISBS (2014). *Information Security Breaches Survey*. Technical Report. Department for Business, Innovation and Skills, London, Storbritannien.

Jaquith, A. (2007). *Security metrics – Replacing Fear, Uncertainty, and Doubt.* Pearson

Jenkin, C. M. (2006). Risk Perception and Terrorism: Applying the Psychometric Paradigm. *Homeland Security Affairs* 2 (2).

Kaaniche, M., Deswarte, Y., Alata, E., Dacier, M. & Nicomette, V. (2006). Empirical analysis and statistical modeling of attack processes based on honeypots. Workshop on empirical evaluation of dependability and security, Philadelphia,USA, 25-28 Juni.

Kahneman, D. (2011). *Thinking, Fast and Slow*, Farrar, Straus and Giroux.

Kwon, J. & Johnson, M.E. (2011). An Organizational Learning Perspective on Proactive vs. Reactive Investment in Information Security. *Workshop on Economics of Information Security*, George Mason University, USA, Juni 14–15.

Lelarge, M. (2012) Coordination in Network Security Games: A Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications*, 30(11).

Liu, D., Ji., Y. & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support System* 51, 95-107.

McQueen M., Boyer W., Flynn M. & Alessi S. (2006). Quantitative Risk Reduction Estimation Tool for Control Systems – Suggested Approach and Research Needs. *International Workshop On Complex Network and Infrastructure Protection*.

Mell, P., Scarfone, K. & Romanosky,S. (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [www] http://www.first.org/cvss/cvss-guide.html (kontrollerad 17/4 2014).

MSB (2012). *Nationellt system för it-incidentrapportering.* (2012-2637) Myndigheten för samhällsskydd och beredskap (MSB)

National Research Council (NRC) (2010). *Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop*, The National Academies Press.

NIST (2008). *Performance Measurement Guide for Information Security*. NIST Special Publication 800-55 Revision 1, National Institute of Standards and Technology.

Öğüt, H., Raghunathan, S. & 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).

Oram A. & Viega J. (red.) *Beautiful Security*. O'Reilly Media, 2009.

Page, S. E. (2007). *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies*, Princeton Univ. Press.

Panton, B.C., Colombi, J.M., Grimaila, M.R. & Mills, R.F. (2013). Secure DoD Software: Considerations for the Vulnerability Market. *Crosstalk* November/December.

Paté-Cornell, E. (2012). On "Black swans" and "Perfect storms": Risk analysis and management when statistics are not enough, *Risk Analysis* 32 (11), 1823–1833.

Paté-Cornell, E. & Guikema, S. (2002). Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures, *Military Operations Research* 7 (4).

Paté-Cornell, M. E. (1996). Uncertainties in risk analysis: Six levels of treatment. *Reliability Engineering & System Safety* 54, 2-3.

Paté-Cornell, M. E. & Fischbeck, P. S. (1995). Probabilistic interpretation of command and control signals: Bayesian updating of the probability of nuclear attack. *Reliability Engineering & System Safety* 47 (1).

Post, G.V. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computer & Security* 26, 229-237.

Qian, Y., Fang, Y. & Gonzalez, J.J. (2012) Managing information security risks during new technology adoption. *Computer & Security* 31, 859-869l.

Rakes, T. R., Deane, J. K. & Rees, L. P. (2012) IT security planning under uncertainty for high-impact events, *Omega* 40, 79-88.

RTI (2014). *Predict, Protected Repository for the Defense of Infrastructure Against Cyber Threats*, tillgänglig på https://predict.org 13 maj 2014.

Sawik, T. (2013) Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems* 50, 156-164.

Schechter, S. (2002). Quantitatively Differentiating System Security. Workshop on Economics and Information Security. Berkeley, USA, 16-17 Maj.

Schechter, S. E. (2004). Toward econometric models of the security risk from remote attacks. *Security & Privacy* 3 (1).

Schmidt, M. (2004). *Investigating risk perception: a short introduction. Chapter 3 in: Schmidt M. 2004. Loss of agro-biodiversity in Vavilov centers, with a special focus on the risks of genetically modified organisms (GMOs)*. PhD Thesis, Vienna, Austria.

Schudel G. & Wood B. (2000). Adversary Work Factor as a Metric for Information Assurance. Workshop on new security paradigms. Ballycotton, Cork, Irland, 18-21 September.

Sjöberg, L. (1999). Consequences of perceived risk: Demand for mitigation. *Journal of Risk Research* 2 (2).

Sjöberg, L., Moen, B-E. & Rundmo, T. (2004). Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. *Rotunde nummer 84.*

Soo Hoo, K.J. (2000). *How Much Is Enough? A Risk-Management Approach to Computer Security*. Doktorsavhandling, Stanford University, USA.

Starr, C. (1969). Social Benefit versus Technological Risk. *Science* 165 (3899), 1232-1238.

Steinbart, P.J., Raschke, R.L., Gal, G. & Dilla W.N. (2012) The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems* 13 (3), 228-243.

Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*, First Chapter. New York Times, April 22. [www] http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html?_r=0 (kontrollerad 19/4 2014)

Taleb, N. N. (2007b). The A Priori Problem of Observed Probabilities, *Wilmot Mag.* 2, 5-8. [www] http://www.fooledbyrandomness.com/central.pdf (kontrollerad 13 maj 2014).

Taleb, N. N. (2008). The Fourth Quadrant: A Map of the limits of statistics, An Edge Original Essay. Edge. [www] http://edge.org/conversation/the-fourth-quadrant-a-map-of-the-limits-of-statistics (kontrollerad 19/5 2014).

Taleb, N. N. (2009). Ten principles for a Black Swan-proof world. Financial Time, 7 april. [www] http://www.ft.com/intl/cms/s/0/5d5aa24e-23a4-11de-996a-00144feabdc0.html (kontrollerad 19/4 2014)

Thomason, J. S. (2009*) IDA's Integrated Risk Assessment and Management Model.* Institute for defense analyses IDA Paper P-4470, Log: H 09-001006

Verendel, V. (2009). Quantified Security is a Weak Hypothesis, A critical survey of results and assumptions. New Security Paradigms Workshop. Oxford, Storbritannien, September 2009.

Wallace, L., Lin, H. & Cefaratti, M.A. (2011) Information Security and Sarbanes-Oxley Compliance: An Exploratory Study. *Journal of Information Systems* 25 (1), 185-211.

Wallsten, T. S., Budescu, D.V., Erev, I. & Diederich, A. (1997). Evaluating and Combining Subjective Probability Estimates. *Journal of Behavioral Decision Making*, 10 (3), 243-268.

Wang, S-L, Chen, J-D, Stripe, P. A. & Hong, T-P (2011) Risk-neutral evaluation of information security investments on data centers. *Journal of Intelligent Information Systems* 36, 329-345.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se