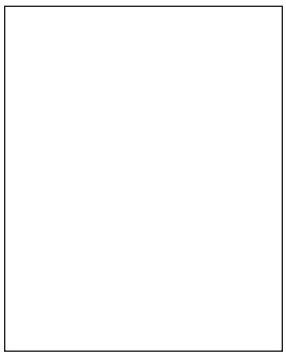
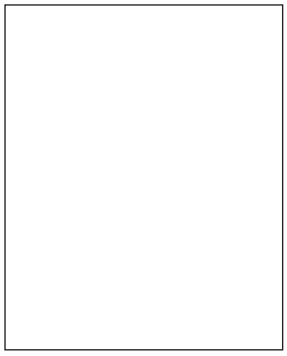
NFT 4/1996

Riskanalys med DEEP-metoden

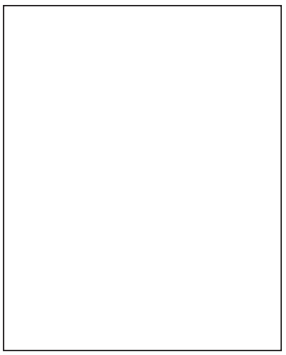
av **Mats Danielson, Love Ekenberg** och **Anders Elgemyr**



Mats Danielson



Love Ekenberg



Anders Elgemyr

Olika metoder har utvecklats för att beräkna skadeutfall och riskpremier. För de kategorier av försäkringar där skadorna har hög frekvens finns detaljerat statistikunderlag som gör det relativt enkelt att räkna fram försäkringsbolagets riskexponering och en rimlig premie.

Vid risker där skadefrekvensen är låg ställer det sig annorlunda. Såväl för företaget som försäkringsbolaget innebär detta ofta avsevärda svårigheter och många befintliga metoder för riskkostnadsberäkningar är mindre lämpliga i sådana fall. Det ligger emellertid i båda parters intresse att man på ett effektivt sätt kan analysera dessa situationer.

1. Bakgrund

Inom säkerhetsområdet arbetar man traditionellt med flera olika modeller för riskanalys i syfte att studera risker i olika verksamheter. Riskanalysen utgör i sin tur en del av den totala riskhanteringen. Granskar man dessa modeller närmare visar det sig att de i grunden arbetar utifrån liknande principer. De flesta modeller brukar innehålla åtminstone följande komponenter för att hantera riskerna inom en verksamhet:

- Identifiera de tillgångar (objekt) som måste skyddas.
- Identifiera hoten (skadehändelser) mot objekten.

Mats Danielson och Love Ekenberg är anställda vid Institutionen för data- och systemvetenskap, Stockholms universitet. Anders Elgemyr är anställd vid ROA.

Projektet har bekostats av Kjell Gunnarssons Risk Management stipendiefond.

- Uppskatta sannolikheten för olika hot.
- Uppskatta värdena som hotas.
- Inventera det befintliga skyddet.
- Analysera vilka hot som skall åtgärdas och vilka som kan lämnas åt sidan.
- Utvärdera vilka alternativa skyddsåtgärder som är rimliga att införa.
- Finansiera återstående risk.
- Genomföra de beslutade åtgärderna.
- Följa upp åtgärderna.

I denna artikel presenterar vi en metod för riskanalys som i väsentliga delar utvidgar och fördjupar värderingsfaserna jämfört med tidigare metodansatser. Begreppet *riskanalys* används här något bredare än vanligt. Ofta innefattas endast identifikation och värdering av skaderisker i begreppet, men här ingår även analys av val av riskbehandlande åtgärder, av riskfinansiering och av de vidtagna åtgärderna. Framställningen koncentreras främst på punkterna identifiering och analys av hot och motåtgärder samt utvärdering av de föreslagna åtgärderna eftersom det är på dessa punkter som metoden DEEP (Damage Evaluation and Effective Prevention) särskiljer sig mest markant. De övriga punkterna är relativt väl täckta i andra skrifter[1], men tanken bakom DEEP-metoden är att erbjuda ett analytiskt ramverk i hela den klassiska kedjan identifiering – värdering – behandling – finansiering.

I hotbildsanalysen jämförs olika hot med varandra och man försöker sålla bort dem som man inte bedömer vara allvarliga och även bestämma i vilken ordning övriga hot skall åtgärdas. Vi kommer i artikeln att kritisera befintliga modeller för att de i många fall är otillräckliga för att närmare avgöra hur allvarliga olika hot är och hur de skall rangordnas.

I inventeringsfasen specificeras närmare vilka alternativa åtgärder som kan företas. Trots att det i verkligheten naturligtvis ofta genomförs sådana analyser med mer eller mindre sofistikerade verktyg så utelämnas denna punkt i de flesta befintliga riskanalysmodeller. Detta är en tydlig brist som avsevärt minskar styrkan hos genomförda analyser.

En annan svaghet som vi skall granska närmare är att ett stort antal modeller inte kan hantera situationer med oprecist informationsunderlag. I många fall måste riskanalytikern arbeta i situationer där det inte finns tillräckligt statistiskt underlag och han kan därför inte heller med rimlig konfidens ange precisa skattningar som t.ex. ”*med 17 procents sannolikhet inträffar konsekvens k*”.[2] Ett problem med ett flertal metoder är att de likafullt förutsätter att de olika parametrarna anges med exakta värden.

Syftet med denna artikel är att beskriva metoden DEEP avsedd för systematisk analys och utvärdering av risk. Modellen fokuserar såväl på riskkostnadsberäkningar som på utvärdering av alternativa skyddsåtgärder. Dessutom tillåter den i dessa moment utvärdering av information som är vag eller numeriskt oprecis. I avsnitt 2 beskrives och kritiseras två kategorier av analysmodeller som används i samband med riskanalyser. Avsnitt 3 presenterar DEEP-metoden och beskriver hur den kan integreras i en process för att analysera risker. Avsnitt 4 visar en mycket enkel tillämpning av delar av metoden och avsnitt 5 sammanfattar våra resultat.

2. Två kategorier av modeller för att beräkna risker

Riskhanteringsmodeller omfattar ofta allt från identifiering och utvärdering av tillgångar såsom egendom och information till hantering av hot som brand, stöld och spionage. Analyserna brukar även innefatta modeller för utvärdering av det befintliga skyddet och effekterna av att modifiera detsamma. Vi avser här att diskutera två kategorier av modeller. Den första kategorin vi behandlar är metoder baserade på förväntade förluster och

därefter följer ett avsnitt om metoder som använder risknivåer.

2.1. Förväntad förlust

J.F. Broder föreslår en modell i syfte att överbrygga problemet med att tvingas ange orealistiskt precisa värden. "*[…] it is neither necessary nor desirable to make precise statements of impact and probability. The time needed for the analysis will be considerably reduced and its usefulness will not be decreased, if impact (i) and frequency (f) correlations are given in factors of 10.*" [2], s.22. Följande skala föreslås:[3]

Förväntad förlust

$10	i = 1
$100	i = 2
$1.000	i = 3
$10.000	i = 4
$100.000	i = 5
$1.000.000	i = 6
$10.000.000	i = 7
$100.000.000	i = 8

Förväntad frekvens

En gång på 300 år	f = 1
En gång på 30 år	f = 2
En gång på 3 år	f = 3
En gång på 100 dagar	f = 4
En gång på 10 dagar	f = 5
En gång per dag	f = 6
10 gånger per dag	f = 7
100 gånger per dag	f = 8

Den årligen förväntade förlusten approximeras därefter med uttrycket

$$\text{ALE} = \frac{10^{(f+i-3)}}{3}.$$

Ett problem med denna ansats är att de möjliga värdenivåerna är alltför avlägsna varandra. Detta kan naturligtvis lösas genom att använda decimaltal för *i* och *f*, men det är inte tydligt hur precisa sådana angivelser skall tillåtas vara i relation till de fixerade nivåer som modellen är tänkt att appliceras på. Dessutom är möjligheten att effektivt utföra känslighetsanalyser en viktig egenskap hos en metod som tillåter hantering av oprecisa data och detta ställer sig problematiskt om nivåerna inte kan finjusteras. Vidare bör metoden inkludera möjligheten att lokalisera kritiska variabler. Detta är viktigt, inte minst då de möjliga nivåerna är avlägsna varandra. Ytterligare ett problem är att det inte finns något naturligt sätt för en riskanalytiker att uttrycka hur stor tillförlitligheten är för olika angivelser.

2.2. Risknivåer

Ett sätt att delvis undvika dessa problem är att tillåta att olika värden kan uttryckas kvalitativt i form av nivåer. Exempelvis har en modell med tre nivåer använts i [18, 25, 28]. Sannolikheter och värden uttrycks här som i figur 1.[4] Varianter av denna modell är vanligt förekommande. Exempelvis används i såväl [27] som [29] en modell med fyra nivåer. Den sistnämnda brukar betecknas SBA-metoden och har fått ett tämligen stort genomslag i Sverige. Ytterligare en variant förekommer i [24] där en modell för riskklassificering innefattande såväl sannolikheter som värden presenteras. Ibland används ännu enklare modeller.[5]

Risknivån utgörs av summan SV = *sannolikhet + värde*. SV kan anta värden från 2 till 6. När SV är 2 så blir risknivån 1, om SV är 3 eller 4 så blir risknivån 2 och om SV är 5 eller 6 så blir risknivån 3. Se figur 1.

Figur 1. Från [18], s.77.

	Sannolikhet	*Konsekvens*	*Risknivå*
1	Låg/Liten Sällan förekommande	Liten Låg kostnad Liten skada eller förlust	Acceptabel Kan tillåtas Bör åtgärdas
2	Medium Inte ofta men inte heller sällan förekommande	Medium Större kostnad Större skada eller förlust	Oacceptabel Ej tillåten Skall åtgärdas
3	Stor/hög Ofta förekommande	Stor Kostnad som ej kan bäras Totalförlust	Katastrofal Måste omedelbart åtgärdas Oförlåtlig

Ett problem med denna ansats är att skattningarna av sannolikheter och värden omfattar alltför mycket och att det inte finns någon möjlighet till en uppdelning inom dessa. I praktiken utvärderas därför de flesta risker till risknivå 2 utan att ge någon indikation på hur riskerna bör ordnas inbördes. En erfaren säkerhetsansvarig i en organisation kan vanligen skilja mellan katastrofala, oacceptabla och acceptabla risker utan hjälp av analysverktyg. Det egentliga problemet är att avgöra i vilken ordning och omfattning som riskerna skall behandlas, t. ex. genom att utföra mer utvecklade känslighetsanalyser. En annan anmärkningsvärd egenskap hos modellen är att den t.ex. evaluerar sällan förekommande, katastrofala konsekvenser till samma risknivå som ofta förekommande, acceptabla konsekvenser.

2.3. Maximering av den förväntade nyttan

Det är också anmärkningsvärt att utvärderingsmodellen i figur 1 uppenbart skiljer sig från användningen av principen att maximera den förväntade nyttan. Denna princip kan formuleras på följande vis:

En *åtgärd i* har en mängd möjliga konsekvenser $\{k_{i1},\ldots,k_{in}\}$.

Den *förväntade nyttan av en åtgärd i* kan uttryckas med formeln $p_{i1}u_{i1} + \ldots + p_{in}u_{in}$, där u_{ij} betecknar nyttan av konsekvensen k_{ij}, och p_{ij} betecknar sannolikheten för att konsekvensen k_{ij} inträffar förutsatt att man utför åtgärden *i*.

Principen att maximera den förväntade nyttan säger nu att man bör välja att genomföra den åtgärd som har den högsta förväntade nyttan. Definitionerna kan på motsvarande sätt uttryckas i termer av kostnader för möjliga skador varvid kostnaden önskas minimerad.

En *möjlig skada* kan ge upphov till en mängd möjliga konsekvenser $\{k_{i1},\ldots,k_{in}\}$.[6]

Den *förväntade kostnaden av en möjlig skada i* uttrycks med formeln $E_i = p_{i1}c_{i1} + \ldots + p_{in}c_{in}$, där c_{ij} betecknar kostnaden av konsekvensen k_{ij}, och p_{ij} betecknar sannolikheten för att konsekvensen k_{ij} inträffar förutsatt att skadan *i* inträffar.[7]

En rimlig princip kan nu vara att i första hand undvika skadorna med de största förväntade förlusterna. Sådana principer används i en mängd olika sammanhang, inte minst inom ekonomi. Gemensamt för dessa är att de är baserade på principen att maximera den förväntade nyttan. Vi avser emellertid inte att här närmare argumentera för olika tillämpningar av denna princip, utan konstaterar att denna förefaller vara en betydligt mer välgrundad kandidat för en värderingsmodell (se t.ex. [15]). Naturligtvis är denna princip inte den enda rimliga och den är inte okontroversiell [1, 12, 22], men det är på intet sätt klarlagt varför utvärderingsprinciper baserade på risknivåer skulle vara bättre.

3. DEEP-metoden för utvärdering av risk

Detta avsnitt beskriver DEEP-metoden och hur man kan utvärdera effekten av olika åtgärder mot möjliga skador. Genom att använda metoden kan man på ett bättre sätt utvärdera vilka hot som är de mest centrala att åtgärda och vilka effekter sådana åtgärder kan ge. Det är också viktigt att metoden kan anpassas till att stämma överens med företagets allmänna riskpolicy.

3.1. Nio steg för riskanalys

DEEP-metoden är en systematisk ansats för riskanalys avsedd såväl att beräkna i vilken ordning olika hot skall åtgärdas som att jämföra olika åtgärder mot varandra. Analysmetoden är uppbyggd kring nio steg, vilka illustreras i nedanstående figur.

De nio stegen följer naturligt efter varandra och omfattar allt från att se över möjliga skador till känslighetsanalyser av analysresultaten. I varje steg dokumenteras resultaten

Riskanalysmodellen DEEP

Damage Evaluation and Effective Prevention

1. Avgränsa riskanalysen

Börja med att bestämma vad riskanalysen skall innefatta och hur den skall läggas upp.

Ex. Maskinhall A

2. Inventera möjliga skador

Sedan inventerar man de skador som kan drabba organisationen och upprättar en lista över objekten.

Inbrottsrisk

3. Inventera befintliga skydd och möjliga åtgärder

Se därefter över det befintliga skyddet och vilka åtgärder som är möjliga för att förbättra säkerheten.

A1 Behåll nuvarande skydd
A2 Inför standardpaket
A3 Standardpaket + extra

4. Uppskatta sannolikheter

När detta är genomfört anger man för varje åtgärd med vilken sannolikhet en skada kan inträffa.

Inbrottskada 30-70%
Inbrottskada 20-50%
Inbrottskada 10-25%
etc.

5. Uppskatta värden

Uppskatta på samma sätt de möjliga skadorna, uttryckt i lämpligt mått, för varje åtgärdsalternativ.

A1 Inbrottskada 2,5-7,5 Mkr
A2 Inbrottskada 3,2-8,7 Mkr
A3 Inbrottskada 4,7-9,8 Mkr
etc.

6. Evaluera värden och sannolikheter

Evaluera problemet. Ofta visar det sig då att den givna informationen är korrekt, behöver kompletteras eller att materialet behöver struktureras på ett annat vis.

S1•V1+...Sn•Vn

7. Känslighets-analyser

Det är nu möjligt att djupare analysera materialet, t.ex. genom att succesivt minska intervallen. Därigenom kan man prova hur stabilt resultatet är samt undersöka om det krävs mer information.

Inbrottskada 35-65%
Inbrottskada 22-48%
Inbrottskada 11-24%

8. Genomför åtgärderna

Med riskanalysen som beslutsunderlag kan sedan de lämpliga åtgärderna beslutats och genomföras. En tid efter genomförandet är det sedan lämpligt att genom föra en uppföljande utvärdering.

Åtgärd A genomförs

9. Utvärdera insatserna

Det är viktigt att man efter en tid kontrollerar de genomförda åtgärderna. Risken finns att dessa egentligen har inneburit en förskjutning av problemen.

Var åtgärden relevant?
Utfördes den på ett riktigt sätt?
Höjde den verkligen skyddsnivån?
Har det tillkommit nya problem?

för att enkelt kunna återkomma till en förnyad analys när förutsättningarna partiellt ändrats. Stegen 1–3 och 8–9 diskuteras översiktligt och i stället fokuserar vi på de mellanliggande analysstegen. De tre första stegen syftar till att ge en bild av organisationens nuvarande riskexponering.

När en riskanalys planeras är det viktigt att ställa upp tydliga avgränsningar och mål för analysen. Det är sällan som en hel verksamhet skall analyseras samtidigt och steg 1 innebär att analysen delas upp i lämpliga hanterbara delar och riskområden. En avgränsning sker ofta också till att behandla rena skaderisker, dvs risk för händelser som enbart genererar kostnader, eftersom det då är lättare att applicera rationella beslutprocesser.

Det andra steget i DEEP innefattar att närmare granska de delar av företaget eller organisationen som analysen omfattar. Vilka skador kan inträffa? Vilka följdverkningar kan dessa få för andra typer av skador? I vilken omfattning kommer driften att störas?, osv. Det är viktigt att så noga som möjligt systematiskt identifiera alla potentiella skadeobjekt och händelser som leder fram till skada avseende egendom, personal, avbrott, ansvar, mm – ej enbart slutresultatet av en skadehändelse.

Därefter är det naturligt att närmare studera det befintliga skyddet. Skyddet består i det allmänna fallet av både direkta skydd och försäkringsskydd. Typiska frågor att ställa i det tredje steget är: Är skydden tillräckligt omfattande? Är de tillräckligt säkra? Vad händer om skyddsmekanismerna trots allt inte fungerar? Hur skall balansen mellan direkta skydd och försäkringar vara?, osv. Steg 3 avslutas med att undersöka tänkbara behandlingsåtgärder. För varje möjlig skada som identifierats anges alternativa åtgärder, vilka torde uppgå till minst två: behålla det nuvarande skyddet eller ersätta eller komplettera det med något annat skydd. Vanligtvis finns flera olika åtgärder att ta ställning till i riskbehandlingen, och de skiljer sig oftast med avseende på hur risken reduceras. Vid behandling genom riskspridning kan risken antingen spridas fysiskt genom förändringar i verksamheten eller monetärt genom försäkringsåtgärder. Vid behandling genom riskreduktion kan antingen skadorna förebyggas (vilket minskar sannolikheterna för att händelserna inträffar) eller begränsas (vilket minskar kostnaderna när händelserna inträffar).

De fjärde och femte stegen innebär uppskattningar av sannolikheter och värden. För samtliga alternativa åtgärder anges sannolikheten för den möjliga skadan samt värdet (kostnaden) för denna skada givet att respektive åtgärd är vidtagen. Detta görs med avseende på de tänkbara åtgärderna som tidigare framkommit. Steg 4 innefattar sannolikhetsuppskattningar. För att åstadkomma en väl genomtänkt riskanalys är det nödvändigt att på något vis uppskatta hur ofta olika möjliga skador kan inträffa. Ibland finns det noggrant utarbetat underlag, medan man i andra fall får lita till mer eller mindre välunderbyggda uppskattningar. På liknande sätt innebär steg 5 uppskattningar av värden. Detta innebär såväl skydds- som skadekostnader. Värdet kan uttryckas direkt i monetära kostnader eller i någon annan lämplig terminologi.[8] I dessa två steg inträffar det ofta att man upptäcker att informationsunderlaget är otillräckligt och att man därför behöver genomföra kompletterade undersökningar för att kunna genomföra en väl genomtänkt riskanalys. Det kan även visa sig att hela problemet har strukturerats på ett olämpligt sätt och att man därför behöver diskutera igenom förutsättningarna ytterligare en gång.

När alla möjliga skador har identifierats och värderats är det i steg 6 dags att evaluera de alternativa åtgärderna. Detta innebär att åtgärderna värderas mot de möjliga skadorna. En sådan evaluering kan utföras med avseende på olika principer, t.ex. att minimera den förväntade förlusten. En viktig funktion i evalueringssteget är att kunna exkludera ac-

ceptabla risker från fortsatt utvärdering med hjälp av tröskelnivåer.[9] Om den potentiella kostnaden för en specifik skaderisk understiger företagsledningens policy vad gäller tröskelvärden kan den klassas som acceptabel och resurser behöver ej användas för vidare analys av tillhörande hot.

Även en noggrant genomförd analys kan ha mycket att vinna på att kompletteras med en känslighetsanalys vilket är avsikten med steg 7. I detta steg ändrar man successivt de ingående värdena för att se hur stabil analysen är. När värdena justeras kommer förmodligen analysens resultat att påverkas. Exakt var detta sker kan vara av stort intresse eftersom detta indikerar vilka ingångsvärden som är särskilt kritiska. Det är just dessa som bör studeras närmare för att genomföra en mer fullständig analys och förbättra användningen av befintliga resurser.

När denna evalueringsprocess är avslutad genomförs åtgärderna i steg 8. Detta steg är specifikt för den aktuella organisationen och innefattar även finansiering av återstående risk efter behandlingen, t.ex. genom försäkringar. Efter en tid är det viktigt att man verifierar och utvärderar de genomförda åtgärderna. Risken finns att dessa egentligen har inneburit en förskjutning av problemen till andra problemområden, och steg 9 avser att upptäcka sådana förskjutningar.

En principskiss över processen visas i figur 2. Siffrorna i figuren syftar på de olika faserna i DEEP.

- I steg 1 avgränsar man riskanalysen till det relevanta problemet.
- I steg 2 identifieras de möjliga skadorna – hoten.
- I steg 3 analyseras det befintliga skyddet och möjliga åtgärder.
- I steg 4 uppskattas sannolikheterna för de möjliga skadorna med avseende på alternativa åtgärder.
- I steg 5 uppskattas värdena för dessa skador.
- I steg 6 evalueras de alternativa åtgärderna.
- I steg 7 utförs känslighetsanalyser.
- I steg 8 genomförs åtgärderna.
- I steg 9 utvärderas de genomförda åtgärderna.

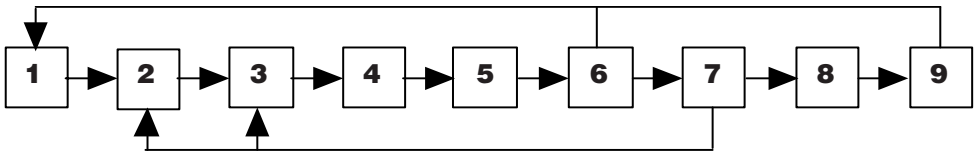
Som vi har förklarat ovan kan det under analysens gång visa sig att ytterligare information eller diskussioner blir nödvändiga. Dessa återkopplingar illustreras i figuren med bakåtriktade pilar.

3.2. Oprecisa uppskattningar

På grund av de svårigheter som är förknippade med att ge precisa uppskattningar av de sannolikheter och kostnader som ingår i en riskberäkning finns det behov av att på ett systematiskt sätt kunna utvärdera situationer där bakgrundsinformationen är vag eller oprecis. Det finns t.ex. ofta inga enkla samband mellan ökade skyddskostnader och minskade skadekostnader, utan de måste uttryckas i tendenser och oprecisa termer. En mängd olika modeller har föreslagits under åren [3, 6, 16, 19, 20, 26].[10]

För att beräkningsmässigt kunna hantera olika typer av omdömen måste de översättas

Figur 2. DEEP-faserna



till en matematisk form, men i stället för att låsa en riskanalytiker till fördefinierade begrepp kan man tillåta en större frihet i vilka omdömen som kan anges. Representationen av sannolikhetsomdömen kan delas in i kvalitativa och kvantitativa omdömen, beroende på vilken typ av problem som skall analyseras. Med kvantitativa omdömen menas omdömen uttryckta i numeriska termer som t.ex. ”denna skada kommer att kosta 70.000–80.000 kr om den inträffar”. Kvalitativa omdömen kan uttryckas som t.ex. ”det är bättre att förbättra skalskyddet än att investera i ett ytterligare larmsystem”. Vi ska nu redogöra för hur detta kan se ut och föreslå en matematisk representation. Omdömen som berör kostnader hanteras på analogt sätt.

I detta sammanhang bör det nämnas att när kostnaderna för konsekvenserna av en möjlig skada beräknas är det inte endast monetära värden som måste beaktas. Vi kommer därför att här använda kostnader i generell mening, dvs med avseende på såväl kvantitativa som kvalitativa aspekter. Detta svarar mot användningen av utilitetsbegreppet inom klassisk beslutsanalys.

DEEP-metoden hanterar kvalitativa omdömen med formen ”konsekvensen c_{ij} är sannolik”, ”konsekvensen c_{ij} är osannolik” eller ”konsekvensen c_{ij} är omöjlig”. Den hanterar även intervalluppskattningar och jämförande omdömen som ”sannolikheten för konsekvensen c_{ij} ligger mellan talen *m* och *n*.” eller ”sannolikheten för konsekvensen c_{rs}, är större än sannolikheten för konsekvensen c_{tu}”. Det väsentliga här är att vi inte nödvändigtvis kräver precisa omdömen.

En sådan representationsmodell kan översättas till ett system av linjära olikheter som medför att de blir beräkningsmässigt hanterbara. Så kan t.ex. omdömet ”sannolikheten för konsekvensen c_{ij} ligger mellan talen *m* och *n*” översättas till uttrycken $p_{ij} \geq m$ och $p_{ij} \leq n$, vilket skrivs som $p_{ij} \in [m, n]$. Även kvalitativa omdömen kan ges en sådan representation. Exempelvis kan omdömet ”konsekvensen c_{ij} är osannolik” översättas till $p_{ij} \in [k_1, k_2]$. De positiva talen k_1 och k_2 ligger i intervallet [0,1] och används för att uttrycka sådana kvalitativa påståenden. Dessa översättningar är naturligtvis inte okontroversiella eftersom det inte finns några a priori grunder till varför man skulle välja några bestämda tal för k_1 och k_2. Det bör emellertid betonas att detta inte är kritiskt. Allteftersom analysen fortskrider kan effekten av olika översättningar studeras. Om riskanalytikern fortfarande är skeptisk mot att hantera kvalitativa omdömen på detta sätt kan denne i stället arbeta uteslutande med intervallpåståenden och jämförelser.

Mängden av översatta sannolikhetsomdömen kommer vi att beteckna *sannolikhetsbasen*. Motsvarande system för omdömen rörande kostnaderna betecknas *kostnadsbasen*. Sannolikhetsbasen och kostnadsbasen tillsammans utgör *informationsbasen*.[11]

4. Ett exempel

Följande exempel avser att tydliggöra hur metoden fungerar i stegen 4–7. Den mycket förenklade kalkylen omfattar en inbrottshändelse under en period och uppskattningarna är oprecisa. Avsikten är att illustrera att DEEP-metoden kan möjliggöra en bedömning av vilka åtgärder som är rimliga att genomföra trots att endast ofullständig information finns att tillgå.

Ett företag önskar reducera sin riskexponering genom att införa ytterligare skyddsutrustning och skyddsmekanismer för en viss produktionsanläggning. Avskrivningstiden för sådana åtgärder antas vara fem år, varför analysen nedan baserar sig på uppskattningar av sannolikheter för händelser under en femårsperiod.

Först inventeras de möjliga skadorna under femårsperioden. Denna inventering utmynnar i följande skadelista:

K_1 Inget inbrottsförsök
K_2 Alla inbrottsförsök misslyckas
K_3 Inbrottsskada inträffar

Det befintliga skyddet inventeras och eventuella åtgärder listas. Inventeringen utmynnar i tre möjliga åtgärder.

A_1 Behålla det nuvarande skyddet
A_2 Införa de av försäkringsbolaget rekommenderade förbättringarna
A_3 Dessutom införa tilläggsfunktioner rekommenderade av säkerhetskonsulten

Den analys som därefter vidtas ger nedanstående grova uppskattningar av sannolikheterna och kostnaderna för olika möjliga skador med avseende på de olika åtgärderna. Kostnaderna innefattar anskaffningskostnader samt uppskattade kostnader för inträffade händelser.[12]

I detta exempel finns tre konsekvenser (K_1–K_3) till varje åtgärd – de två åtgärdstyperna samt alternativet att behålla det befintliga skyddet under perioden.[13] Med avseende på dessa har man uppskattat sannolikheter och värden för olika utfall. Dessa uppskattningar kan mer komprimerat skrivas på följande sätt. p_{ij} betecknar sannolikheten för den j:te möjliga skadan då den i:te åtgärden har genomförts. På motsvarande sätt betecknar c_{ij} kostnaden om den j:te möjliga skadan inträffar då den i:te åtgärden har genomförts. p_{11}–p_{13} utgör här således variabler för sannolikheterna till åtgärden A_1 och c_{11}–c_{13} utgör variabler för kostnaderna för konsekvenserna av åtgärden A_1. På motsvarande sätt representeras samtliga omdömen.[14] Kostnaderna har normerats till intervallet [0,1] genom att skalans spännvidd valts till 10 miljoner kronor. Således motsvarar 0.1 en kostnad på 1 miljon kronor.

$p_{11} \in [20\%, 50\%]$ $c_{11} \in [0.00,0.00]$
$p_{12} \in [10\%, 20\%]$ $c_{12} \in [0.01,0.03]$
$p_{13} \in [30\%, 60\%]$ $c_{13} \in [0.25,0.65]$
$p_{21} \in [30\%, 50\%]$ $c_{21} \in [0.06,0.08]$
$p_{22} \in [20\%, 50\%]$ $c_{22} \in [0.08,0.12]$
$p_{23} \in [15\%, 30\%]$ $c_{23} \in [0.33,0.75]$
$p_{31} \in [35\%, 55\%]$ $c_{31} \in [0.22,0.26]$
$p_{32} \in [30\%, 60\%]$ $c_{32} \in [0.24,0.31]$
$p_{33} \in [10\%, 20\%]$ $c_{33} \in [0.52,0.91]$
$p_{11} < p_{21} < p_{31}$
$p_{12} < p_{22} < p_{32}$
$c_{22} - c_{21} \in [0.02,0.04]$
$c_{32} - c_{31} \in [0.02,0.05]$

Sannolikheter i procent	*Inget inbrottsförsök*	*Alla försök misslyckas*	*Inbrottsskada*
A_1 – Nuvarande skydd	20–50%	10–20 %	30–60 %
A_2 – Förs.bolagets förslag	30–50%	20–50 %	15–30 %
A_3 – Förs.bolaget + konsult	35–55%	30–60 %	10–20 %
Kostnader i miljoner kr.	*inbrottsförsök*	*Alla försök misslyckas*	*Inbrottsskada*
A_1 – Nuvarande skydd	0	0,1–0,3	2,5–6,5
A_2 – Förs.bolagets förslag	0,6–0,8	0,8–1,2	3,3–7,5
A_3 – Förs.bolaget + konsult	2,2–2,6	2,4–3,1	5,2–9,1

Övriga omdömen

- Sannolikheten för att det inte blir något inbrottsförsök ökar ju kraftfullare åtgärder som vidtas.
- Sannolikheten för att inbrottsförsök misslyckas ökar ju kraftfullare åtgärder som vidtas.
- Skillnaden mellan kostnaderna vid uteblivna och misslyckade inbrottsförsök då A_2 väljs är liten. Den uppskattas ligga mellan 0,2 och 0,4 miljoner kronor.
- Även skillnaden mellan kostnaderna vid uteblivna och misslyckade inbrottsförsök då A_3 väljs är relativt liten. Den uppskattas ligga mellan 0,2 och 0,5 miljoner kronor.

Nu kan evalueringen utföras. Detta görs här genom att den förväntade kostnaden beräknas, och den kan uttryckas i ett intervall. Den övre ändpunkten i detta intervall utgör den maximala förväntade kostnaden och den lägre ändpunkten den minimala. Beräkningen utförs med algoritmer som i detalj är beskrivna i [5, 10, 11, 23].

För åtgärderna A_1, A_2 och A_3 ovan erhålls nu uttryck för de förväntade kostnaderna. Dessa betecknas med E_1, E_2 respektive E_3. För varje åtgärd har såväl förväntade minimisom maximikostnader beräknats. Observera att dessa är de minsta och största *förväntade* värdena givet de osäkra intervalluppskattningarna, inte de globalt minsta eller största möjliga värdena. Alla värden anges i tiotal miljoner kronor.

$\min E_1 = 0{,}087$
$\min E_2 = 0{,}110$
$\min E_3 = 0{,}257$
$\max E_1 = 0{,}395$
$\max E_2 = 0{,}296$
$\max E_3 = 0{,}407$

Detta innebär att den förväntade kostnaden för att välja åtgärd A_1 ligger i intervallet 870.000 till 3.950.000 kronor. På motsvarande sätt ligger den förväntade kostnaden för att välja åtgärderna A_2 och A_3 mellan 1.100.000 och 2.960.000 respektive 2.570.000 och 4.070.000 kronor. Som synes är dessa intervall överlappande och det kan vara svårt att avgöra vilken åtgärd som egentligen bör väljas, varför ytterligare analys fordras.

När en riskanalytiker möter ett komplext problem så uppmanar DEEP-metoden denne att vara medvetet oprecis i sina uppskattningar. Värden nära intervallgränserna förefaller därför vara något mer otillförlitliga. Detta påverkar naturligtvis intervallet för den förväntade kostnaden. I många fall är detta intervall för brett för att ge ett rimligt underlag till en åtgärdsplan. Analysen kan emellertid fördjupas genom att introducera olika typer av känslighetsanalyser i modellen. Ett exempel på hur sådana kan utföras är att man samtidigt beskär de olika intervalluppskattningarna i informationsbasen för att studera vilken effekt detta får på kostnadsintervallet. Intervallen i sannolikhets- eller kostnadsbasen kan modifieras på en mängd olika sätt, varav några beskrivs i [5, 9].

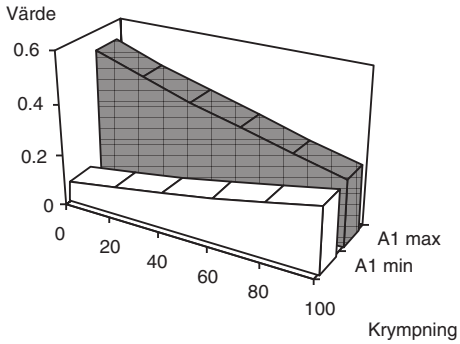
Genom att använda sådana metoder kan man noggrannare studera förhållandena mellan de tre åtgärderna. Ett sätt är att studera deras max- respektive min-värden med avseende på kostnader. För att en åtgärd ska vara bättre än en annan måste den förstnämnda ha lägre värden i kolumnerna. Av tabell 1 framgår därför att åtgärd 3, det extra skyddet, framträder allt tydligare som en sämre åtgärd ju mer intervallgränserna skärps. Däremot kvarstår överlappningen mellan åtgärd 1 och 2 trots successiva krympningar, varför ytterligare analyser rekommenderas.[15]

Tabell 1.
Minsta och största förväntade värden

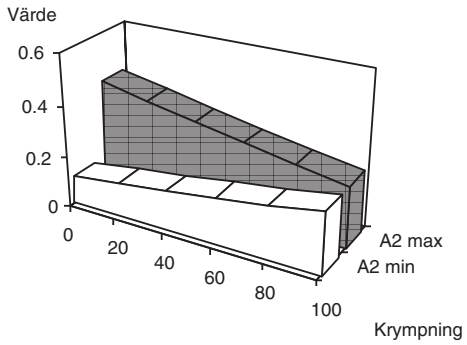
Min och max	*0%*	*20%*	*40%*	*60%*	*80%*
$\min E_1$	0,087	0,109	0,132	0,158	0,186
$\min E_2$	0,110	0,124	0,139	0,154	0,171
$\min E_3$	0,257	0,269	0,282	0,295	0,309
$\max E_1$	0,395	0,355	0,317	0,281	0,247
$\max E_2$	0,296	0,273	0,250	0,229	0,208
$\max E_3$	0,407	0,389	0,372	0,355	0,339

Figurerna 3 till 5 utgör en grafisk representation av tabellen.

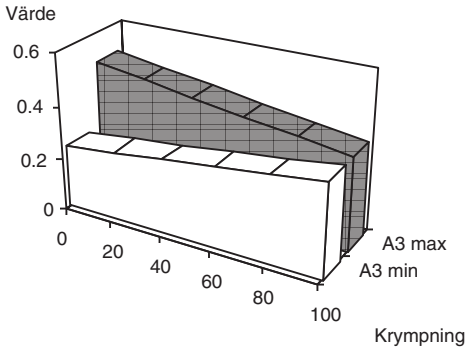
Figur 3. Alternativ 1 – behåll skyddet



Figur 4. Alternativ 2 – försäkringsbolaget



Figur 5. Alternativ 3 – förs.bolaget + konsult

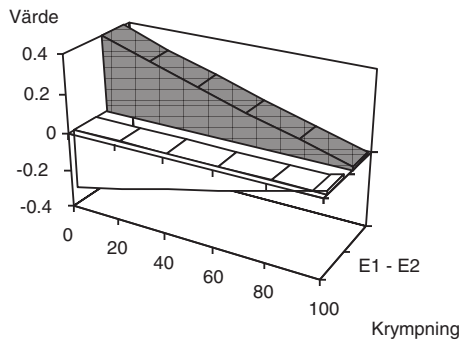


För att tydligare kunna studera skillnaderna mellan åtgärderna jämför vi dem nu parvis. Detta illustreras i tabell 2 och i de tre jämförande graferna i figurerna 6 till 8. Tabellen visar de minsta respektive de största skillnaderna mellan de olika åtgärderna. Man kan nu se att krympningar av informationsbasen tämligen tidigt ger negativa resultat för åtgärd 3, vilket innebär att den är avsevärt mer kostsam än de övriga.

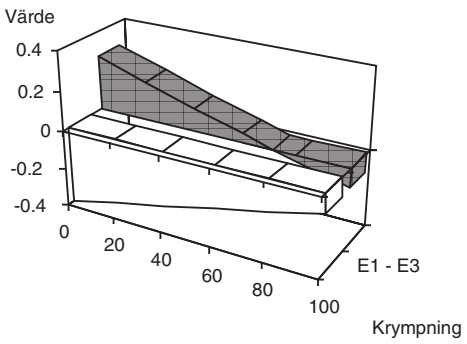
Tabell 2.
Parvisa jämförelser mellan alternativen

Parvisa jfr	*0%*	*20%*	*40%*	*60%*	*80%*
min (E_1-E_2)	-0,201	-0,160	-0,115	-0,069	-0,023
min (E_1-E_3)	-0,314	-0,276	-0,237	-0,197	-0,153
min (E_2-E_3)	-0,274	-0,246	-0,220	-0,196	-0,168
max (E_1-E_2)	0,284	0,231	0,178	0,127	0,076
max (E_1-E_3)	0,137	0,085	0,035	-0,014	-0,062
max (E_2-E_3)	0,038	0,002	-0,033	-0,067	-0,101

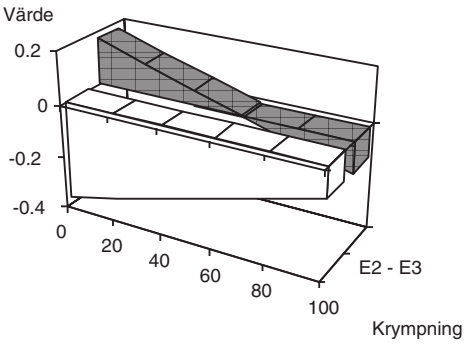
Figur 6. Alternativen 1 och 2



Figur 7. Alternativen 1 och 3



Figur 8. Alternativen 2 och 3



För att korrekt bedöma förhållandet mellan åtgärderna 1 och 2 rekommenderas ytterligare känslighetsanalyser, t.ex. genom att man krymper olika intervall var för sig. Vi avstår emellertid här från att genomföra dessa fördjupade analyser, men kan konstatera att de två åtgärderna är relativt likvärdiga givet den

befintliga informationen. Ytterligare information bör tillföras innan ett definitivt avgörande sker. I synnerhet skattningarna för sannolikheterna för att inbrottsförsök misslyckas givet de båda åtgärderna är kritiska. Om det inte heller efter ytterligare analys går att komma fram till ett avgörande indikerar detta att alternativen är ungefärligt likvärdiga relativt den givna modellen och det kan vara värt att undersöka ytterligare åtgärder, t.ex. att kontakta alternativa leverantörer.

5. Sammanfattande slutsatser

Vi har i denna artikel försökt att påvisa vissa brister i många av de modeller för riskanalys som används idag. Problemet med befintliga modeller är att de endera kräver alltför stor exakthet av användaren eller att de ger alltför lite vägledning i hur olika risker tydligt särskiljs. Vi föreslår DEEP-metoden som täcker analysbehov i hela riskhanteringskedjan och fokuserar på riskkostnadsberäkningar och utvärdering av alternativa skyddsåtgärder. En utmärkande egenskap hos metoden är att den inte tvingar användaren att ange orealistiskt precis information då denne inte har kännedom om exakta sannolikheter för olika skador och kostnader som dessa kan resultera i. Metoden bygger på klassisk beslutsanalys och finns implementerad i datorprogrammet DELTA.

Metoden förutsätter inte något specifikt verksamhetsområde utan kan tämligen enkelt integreras i befintliga processer inom risk management. Den medger även olika typer av känslighetsanalyser i syfte att studera stabiliteten hos resultaten. Det är viktigt att notera att metoden i en del fall, beroende på att tillräckligt särskiljande data inte föreligger, inte finner väsentliga skillnader i olika åtgärdsplaner och utvärderingar och uppmanar då användaren att, där det så krävs, insamla ytterligare information. Den är därför även lämplig för att lokalisera parametrar som är särskilt kritiska för resursallokering.

Referenser

[1] M. Allais, *Fondements d'une Théorie Positive des Choix Comportant un Risque et Critique des Postulats et Axioms de L'Ecole Americane*: D. Reidel Publishing Company, 1953.

[2] J. F. Broder, *Risk Analysis and the Security Survey*: Butterworth Publisher, 1984.

[3] G. Choquet, "Theory of Capacities," *Ann. Inst. Fourier*, vol. 5, s. 131–295, 1953/54.

[4] R. H. Courtney, "Security Risk Assessment in Electronic Data Processing," *AFIPS NCC 46*, 1977.

[5] M. Danielson och L. Ekenberg, "A Framework for Analysing Decisions under Risk," 1996, under revision för publicering i *European Journal of Operational Research*.

[6] A. P. Dempster, "Upper and Lower Probabilities Induced by a Multivalued Mapping," *Annals of Mathematical Statistics*, vol. xxxviii, s. 325–339, 1967.

[7] G. Dixon, *Riskanalys*: SBF – Svenska Brandförsvarsföreningen, 1990.

[8] L. Ekenberg, "Modelling Decentralised Decision Making," Proceedings of ICMAS'96, 1996.

[9] L. Ekenberg och M. Danielson, "A Support System for Real-Life Decisions in Numerically Imprecise Domains," Proceedings of the International Conference on Operations Research '94, s. 500–505, 1994.

[10] L. Ekenberg och M. Danielson, "Handling Imprecise Information in Risk Management," in *Information Security – the Next Decade*, J. Eloff and S. von Solms, Eds.: Chapman & Hall, 1995.

[11] L. Ekenberg, M. Danielson och M. Boman, "From Local Assessments to Global Rationality," *International Journal of Intelligent and Cooperative Information Systems*, 1996.

[12] L. Ekenberg, M. Danielson och M. Boman, "Imposing Security Constraints on Agent-Based Decision Support," *Decision Support Systems International Journal*, 1996.

[13] L. Ekenberg, S. Oberoi och I. Orci, "A Cost Model for Managing Information Security Hazards," *Computers & Security*, vol. 14, s. 707–717, 1995.

[14] A. Elgemyr och L. Mattsson, *Stora säkerhetsboken*: Publica, 1992.

[15] P. Fishburn, "Subjective Expected Utility: A Review of Normative Theories," *Theory and Decision*, vol. 13, s. 139–199, 1981.

[16] I. J. Good, "Subjective Probability as the Measure of a Non-measurable Set," i *Logic, Methodology, and the Philosophy of Science*, Suppes, Nagel, and Tarski, Eds.: Stanford University Press, 1962, s. 319–329.

[17] B. Green, "Vad kan bankerna lära sig av en entrepenör som utvecklas till organisationsforskare," i *Riskbedömning – kunskap om risker*. Stockholm: NUTEK, 1992, s. 121–126.

[18] G. Hamilton, *Detta är Risk Management*: Studentlitteratur, 1985.

[19] P. J. Huber, "The Case of Choquet Capacities in Statistics," *Bulletin of the International Statistical Institute*, vol. 45, s. 181–188, 1973.

[20] P. J. Huber och V. Strassen, "Minimax Tests and the Neyman-Pearsons Lemma for Capacities," *Annals of Statistics*, vol. 1, s. 251–263, 1973.

[21] Kemikontoret, *Riskhantering 1: Administrativ SHM - revision, 4:e uppl*, 1996.

[22] P-E. Malmnäs, "Axiomatic Justification of the Utility Principle," *Synthese*, vol. 99, s. 233–249, 1994.

[23] P-E. Malmnäs, "Towards a Mechanization of Real Life Decisions," in *Logic and Philosophy of Science in Uppsala*, Prawitz and Westerståhl, Eds.: Kluwer Academic Publishers, 1994.

[24] Räddningsverket, *Att skydda och rädda liv, egendom och miljö: Handbok i kommunal riskanalys inom räddningstjänsten*: Räddningsverket, 1989.

[25] SAF, *Riskanalys*: Näringslivets Beredskapsbyrå, 1986.

[26] C. A. B. Smith, "Consistency in Statistical Inference and Decision," *Journal of the Royal Statistic Society, Series B*, vol. xxiii, s. 1–25, 1961.

[27] Statskontoret, *Vägledning i ADB-säkerhet 1-8*, 1989–91.

[28] H. Wermdalen, *Securitas – Säkerhetsboken 1992*: Studentlitteratur, 1991.

[29] R. Wrede, "The SBA Method: A Method for Testing Vulnerability," Proceedings of IFIP/SEC'84, s. 313–320, 1984.

Noter

[1] Riskanalysen är i de inledande stegen mindre generell. Det som skall skyddas och hotbilden helt olika ut beroende på bransch. Det är därför naturligt att t ex Kemibranschen ger ut en skrift som syftar till att täcka just deras medlemsföretags behov [21]. Även analyssteget i riskanalysen behandlas ofta som vore den branschspecifik. Detta beror antagligen på att det hittills har saknats en generell metod som varit naturlig att använda inom olika verksamheter. En mängd aspekter på detta behandlas exempelvis i [14].

[2] Metoder för att uppskatta den monetära kostnaden för en möjlig skada genom att använda numeriskt precisa data finns t.ex. i [7], s.86 ff.

[3] Denna modell föreslogs från början i [4].

[4] Värden brukar något missvisande kallas konsekvenser i många modeller. Detta val av terminologi är tämligen olyckligt eftersom det kan finnas anledning att skilja på det som inträffar och värdet av det inträffade. Det som inträffar är något faktiskt men detta faktum kan värderas utifrån en mängd olika aspekter. Därigenom uttrycks faktumet med olika värde- eller nyttofunktioner beroende på sammanhanget och de kriteria som upplevs vara relevanta för detta sammanhang.

[5] Många modeller exkluderar sannolikhetsuppskattningar helt och hållet. Exempelvis anser många försäkringsrådgivare att det är svårt eller omöjligt att uppskatta sannolikheten för vissa typer av olyckor pga att de förekommer så ytterligt sällan och att det därför inte finns någon möjlighet att finna en frekvensfördelning för dessa. EML-metoder (Estimated Maximal Loss) rangordnar risker enbart efter den största tänkbara förlusten om skadehändelsen inträffar. I [17] föreslås en femnivåers modell utan sannolikhetsuppskattningar.

[6] Vid en generell riskanalys bör det inte förutsättas att en möjlig skada endast resulterar i en konsekvens i någon given konsekvensmängd. Detta är ingen nödvändig restriktion och DEEP-metoden kan hantera möjliga skador som ger upphov till såväl konsekvenser som nya skador. De sistnämnda kan i sin tur resultera i ytterligare möjliga skador och konsekvenser, etc. Genom att introducera nya begrepp kan metoden hantera ännu mer generella riskanalyser. Detaljerna rörande hur den förväntade kostnaden kan utvärderas i mer generella fall finns beskrivna i [8].

[7] [10] ger en mer formell definition av detta.

[8] Sannolikheter och värden är uttryckta som intervalluppskattningar i figur 2. Detta kommer att behandlas närmare i nästa avsnitt.

[9] Säkerhetsnivåer införda genom tröskelvärden beskrivs mer detaljerat i [12].

[10] En beskrivning av olika evalueringsmodeller finns i [5].

[11] Formellt inkluderas även ekvationerna $\Sigma p_{ij}=1$ för varje möjlig skada i sannolikhetsbasen. Detta sker pga att vi antar att analysen är uttömmande med avseende på konsekvenserna, dvs att vi har beaktat alla relevanta konsekvenser.

[12] [10, 13] föreslår en metod för att systematiskt uppskatta kostnader. Vi behandlar därför inte detaljerna i detta förfarande här.

[13] I exemplet är det samma konsekvenser till alla alternativ, något som inte krävs för att använda DEEP-metoden.

[14] En förutsättning för den modell som här presenteras är att konsekvenserna är parvis disjunkta, dvs att endast en av dessa kan inträffa i taget. Denna restriktion kan emellertid mildras till priset av att mängden av möjliga kostnadsfunktioner begränsas [10].

[15] I denna och följande tabell representeras 1 miljon kronor av 0,1