Ta reda på systemriskerna – utveckla företaget!

Kartläggning, analys och förslag till åtgärder

Tomas Hellström

Räddningsverkets kontaktperson:

Jan Schyllander Risk-och Miljöavdelningen 054-13 51 41

Innehåll

Sammanfattning

Föreliggande rapport utvecklar begreppet ”systemrisk” mot bakgrund av en rad fallstudier gjorda på svenska företag, där i första hand riskansvariga (sk risk managers) har intervjuats. Systemrisker avser sådana risker där orsaken till ett hot eller faktisk olycka återfinns i komplexa samspel mellan organisationsstruktur, kunskapsbildning och kulturella aspekter, inklusive värderingar.

Rapporten föreslår att ett fokus på sådana bakomliggande faktorer, eller djupstrukturer, fördelaktigt kan komplettera en traditionell risk/säkerhetsanalys på företag. Mot bakgrund av en genomlysning av riskbilden i åtta branschföretag illustrerar rapporten konkret hur begreppet kan användas i analys och riskarbete, samt vilken typ av hot systemriskerna typiskt utgör.

Resultaten från studiet av företagen visar att flera av de underliggande orsakerna till tillbud och brist i överblick faller under följande kategorier:

- Brister i kunskapsutveckling och kommunikation (t.ex. intern och extern riskkommunikation, brister i de anställdas kunskap om risker och produktionsformer).
- Attityder och värderingar (ledningens risktagande och riskkultur på företaget).
- Organisationsfaktorer (t.ex. oklara ansvarsförhållanden, riskhanteringens organisatoriska plats vis a vis kärnprocesser och närheten mellan ledningen och riskansvarig).

Mot bakgrund av dessa resultat rekommenderas ett generellt riskanalysfokus med frågebatteri för kartläggning av systemrisker. Rapporten avslutas med en demonstration av hur en praktisk systemriskanalys genomfördes på ett serviceföretag inom telekombranschen.

Summary

The present report develops the concept of “systemic risks” against the backdrop of a several short case studies conducted at a number of Swedish companies. The case studies are based on interviews with risk managers, which aimed to elucidate some concrete characteristics typical of systemic risk, e.g. where a threat or a realized accident is the result of complex causal interplays between organisational, cultural, epistemic and physical processes.

The report suggests that a focus on such underlying and elusive structures may frutifully complement traditional risk and safety analyses conducted in companies. By looking at the overall pattern of risk and risk reductive practices in eight companies of different branches, the report illustrates how systemic risk may be practically conceived of in risk management. The report further gives illustrative examples of instances of this “family” of risk.

The results from the study show that many of the underlying causes of unwanted events and lack of oversight typically falls within some of the categories below:

- Limitations in knowledge production and communication (e.g. internal and external communication of risk as well as poor employee knowledge of risks and of production processes).
- Attitudes and values (e.g. dysfunctional risk taking practices in top management and corporate risk culture).

- Organisational factors (e.g. differentiated distribution of responsibility and authority, the organisational location of risk management away from core processes, and distance between risk manager and top management).

Drawing on these results a general focus for corporate risk analysis is recommended, and a set of questions for systemic risk analysis is proposed. The report ends with a demonstration of how a practical systemic risk analysis was conducted in a telecom service company.

1. Hur kan jag använda rapporten?

Iakttagelser och slutsatser avser i texten ***företag*** men kan i allmänhet tillämpas ***även på andra slag av verksamheter –*** t.ex. statliga myndigheter, kommuner, landsting och organisationer.

RM (Risk Management) är i rapporten antingen *funktionen* rikshantering eller den *person* (Risk Manager) som driver riskhantering inom företag och andra verksamheter. Det framgår i allmänhet av sammanhanget vilken betydelse RM har.

Underlaget för rapporten är ett smörgåsbord med uppgifter från ett tiotal företag av olika storlek och inom olika branscher. Dessa företag har en rad olika risker – även sådana som inte är föremål för riskhantering i traditionell mening. Flera av riskerna kan vara nya för läsaren, andra är välbekanta.

Meningen med studien är inte att riskhanteringen ska utökas och bli en ännu mer omfattande och komplicerad verksamhet – snarare att läsaren ska få nya intryck och förslag på fokus i riskhanteringen. Det är fokus som gör att företaget kan ersätta eller modifiera gamla verksamheter.

En bra princip i praktisk riskhantering är att betrakta 20 % av företagets risker som tillräckligt allvarliga och påverkbara för att företaget ska lägga ned tid och energi på dem. En tumregel säger att 20 % av riskerna står för 80 % av företagets förluster. *Vilka är dessa 20 %? Det handlar om att välja riskportfölj!*

Att fokusera på riskportföljen är nödvändigt för det företag som vill vara effektivt. Riskerna ser olika ut beroende på t.ex. bransch, företagsstorlek och organisation. *Använd rapporten för att kritiskt granska portföljen! Behöver den förnyas? Behöver nya risker växlas in och gamla växlas ut?* Rapporten kan också användas för att få de riskansvariga att se företaget som en helhet och den mångfald av problem som ofta leder till att riskhanteringen stöter på patrull – alltså fastnar i motstånd från andra ansvarsområden. Rapporten kan hjälpa till att visa på behovet av riskhantering även utanför traditionella gränser för verksamheten.

2. Så här kom studien till

2.1 Räddningstjänsten på 2000-talet

Räddningsverket genomförde i december 1996 ett seminarium under rubriken *Räddningstjänsten in på 2000-talet.* Syftet var att få till stånd en diskussion om viktiga framtidsfrågor. Skydd och säkerhet inom industrin – med inriktning på samspelet mellan företagen och den kommunala räddningstjänsten – var en fråga som enligt verkets mening skulle komma att få stort utrymme i utvecklingsarbetet under de kommande åren.

Räddningsverket hade i samarbete med myndigheter, företag och andra organ utarbetat två scenarier som skulle utgöra grunden för en diskussion om dessa båda framtidsfrågor. Ett av scenarierna beskrev händelsekedjan i samband med ett mycket häftigt åskväder som förstörde datorsystemet för styrning av tillverkningen hos ***Volvo Lastvagnar*** i Sverige och slog ut hela produktionen av tunga lastbilar i Göteborg.

En konferens grundad på innehållet i scenariot om den utslagna lastvagnsproduktionen hos Volvo ägde rum i november 1997. I konferensen deltog ett 70-tal företrädare för industrin och räddningstjänsten. Som ett resultat av överläggningen bildades en *arbetsgrupp* med företrädare för *Volvo Lastvagnar, Ericsson Microwave Systems, SCA Mölnlycke, försäkringsbolaget Skandia, Räddningstjänsten Storgöteborg* och *Räddningsverket.* Till gruppen knöts senare även den för funktionen Säkerhet ansvarige inom *Svenska Arbetsgivareföreningen* och *Näringslivets Säkerhetsdelegation.*

Arbetsgruppen skulle kartlägga innehållet i och formerna för säkerhetsarbetet inom företag och kommunikationen mellan företag och myndigheter. Syftet var ett få till stånd en modell för hantering av dessa frågor. Modellen skulle avse både olycksförebyggande och skadebegränsande åtgärder och kunna användas av stora, medelstora och mindre företag inom olika branscher.

Projektledare blev ***Tomas Hellström,*** som nyligen hade disputerat vid Göteborgs universitet på en avhandling om systemrisker. Räddningsverket sörjde för Hellströms medverkan i arbetet. Arbetsgruppen blev efter detta styrgrupp för projektet.

Ledamöter i *styrgruppen* har varit:	
Nils Andréasson (ordförande)	Räddningstjänsten Storgöteborg
Eva Bergqvist-Flodin	SCA Hygiene Products
Lars Flodin	Svenska Arbetsgivareföreningen
Sven Rune Frid	Räddningsverket
Jan Grönquist	Volvo Lastvagnar
Jan Höst	Ericsson Microwave Systems
Per Nyberg	Skandia

Henrik Rönnqvist	Räddningsverket
Ingvar Svensson	Räddningstjänsten Storgöteborg

2.2 Begreppen som vi använder

2.2.1 Systemrisker

Den teoretiska ramen för denna rapport ingår i projektledarens avhandling **– *Risk-Based Planning*** (1998). En utförligare referens för den som vill veta mer finns i listan över forskarnas arbeten i kapitel 2. Projektledarens avhandling syftar till att beskriva hur *kunskapsbildning och organisatorisk struktur* påverkar tillkomsten och analyser av risker i olika sammanhang. Författaren menar bl.a. att osäkerhet i information, kommunikation och organisation har en avsevärd negativ inverkan på riskbilden och på möjligheterna för riskhantering i företagen. Övervägandena är grundade på studier av ett antal fall som illustrerar sådana "kunskapsosäkerheter".

Författaren vidareutvecklar begreppen ***systemrisk*** och ***systemriskanalys***, som inte fått samma genomslag i praktisk riskhantering som inom forskningen. Ett av syftena med arbetet var att tillhandahålla verktyg för ett samspel mellan riskhantering och kunskapsbildning inom företag och andra slag av verksamheter.

2.2.2 Vad är systemrisker?

Risk definieras traditionellt som

(1) ***Sannolikheten*** *för en oönskad skadehändelse;*

(2) ***Konsekvenserna*** *av denna oönskade händelse;*

(3) ***Sannolikhet x konsekvens*** *(produkten av 1 och 2);* och i en del fall

(4) *Något slag av* ***mått på osäkerheten*** *i bedömningen.*

En sådan definition tar fasta på själva händelsen som risken kan orsaka. Begreppet ***systemrisk*** fokuserar i stället på de ***bakomliggande faktorerna***. Dessa skapar den miljö där risken utvecklas. I stället för att beskriva skadehändelsen – och låta risken "definieras" som t.ex. sannolikheten för att den ska inträffa – börjar systemriskanalysen med de organisatoriska och andra förhållanden som gör att händelsen kan inträffa. I systemriskanalysen blir dessa strukturer "riskerna" som ska beskrivas och hanteras.

Systemrisker kan leda till sak- eller personskador – ofta båda. Orsakerna finns i ett komplext samspel mellan individ, kunskap och organisationsstruktur. Författaren visar i avhandlingen att

- ❑ *Systemrisker går att beskriva och använda i riskanalyser;*
- ❑ *Systemrisker ser ut på i stort sett samma sätt i olika slag av verksamheter;*
- ❑ *Systemrisker är "osynliga" för traditionella riskanalyser;* och
- ❑ *Det är angeläget att finna ett sätt att bedöma systemriskerna.*

Med den "breddning" av riskbegreppet som författaren gör avser risker även det som drabbar företagens ***kärnprocesser*** och s.k. ***humankapital***. Med kärnprocesser menas de verksamheter som är strategiskt grundläggande och värdeskapande i företaget. Humankapitalet skadas t.ex. om företaget systematiskt bränner ut ledare och andra nyckelpersoner i verksamheten.

2.2.3 Vad är systemriskanalys?

Den studie som rapporten beskriver syftar till en inledande empirisk *kartläggning*

av systemrisker – som alltså uppstår i ett samspel mellan individ, kunskap och organisationsstruktur. Avsikten är vidare att med exempel från kartläggningen visa på metoder för en *analys* av sådana risker: *Hur uppstår de? Hur fungerar de? Hur påverkar de företaget?*

Systemriskanalysen omfattar

- *En beskrivning av risker som beror på företagets riskkultur, besluts- och kontrollstruktur och kommunikationsvägar;*
- *En bedömning av företagets riskbenägenhet.*

Det gäller för det första att hitta de verksamheter som är speciellt riskbenägna eller som omvänt är goda exempel på "säkra verksamheter". Det är särskilt viktigt att identifiera risker som inte i första hand resulterar i sak- eller personskador utan som bidrar till att allmänt sett öka riskbenägenheten i företaget. Riskerna verkar i dessa fall under ytan med obestämbara konsekvenser för olika delar av verksamheten. Det är i stor utsträckning fråga om hur de anställda skaffar sig kunskaper, hur risker uppfattas och vilken kontroll företagsledningen utövar över verksamheten.

Systemriskanalys har förutsättningar att bli ett instrument för en allmän förnyelse och utveckling inom företaget. Det innebär att företagsledningen med systemriskanalysen som grund letar efter brister i samordningen och andra fel inom verksamheten. Med hjälp av systemriskanalysen kommer ledningen emellertid också att hitta resurser. Det kan vara fråga om kunskaper och en vilja att samarbeta som gör det möjligt att stimulera ett givande samspel mellan t.ex. produktionen och säkerhetsarbetet.

Frågor om ***risklärande*** i organisationer och företag handlar i ett systemriskperspektiv om hur företag ska utveckla roller, språk och en organisation som gör det möjligt att sprida kunskap. Det gäller också att klargöra hur motstridiga och utmanande krav på produktion och skydd ska hanteras – utan att företaget går miste om interna synergier och skalfördelar. Strävan bör vara att låta riskhanteringen organisatoriskt ligga inom eller i närheten av företagsledningen.

2.3 Uppläggning och genomförande

2.3.1 Underlaget för övervägandena

Utgångspunkten för övervägandena i rapporten är beskrivningen av den ***teoretiska ramen*** och de redogörelser för ***förhållandena inom ett antal företag*** som har utarbetats. Underlaget för redogörelserna är de samtal som projektledaren har haft med företrädare för de berörda företagen.

Samtalen utgick från några enkla grundfrågeställningar som projektledaren i samråd med styrgruppen hade valt ut som speciellt intressanta. Dessa frågeställningar gällde bl.a.

- *Möjligheter och svårigheter för riskhanteringen inom företaget;*
- *Förhållandet mellan riskhanteringen och företagets kärnverksamhet;*

- ❑ *Förhållandet mellan riskhantering och ledningsfunktioner, beslutsfattande och kommunikation.*

Projektledaren förde loggbok över samtalen med företrädare för företagen och registrerade de ***intryck*** som han fick. Sådana intryck grundades på de synpunkter som kom fram i samtalen och den ***bakgrundsinformation*** om riskhanteringen inom företagen som projektledaren fick tillgång till. Samtalen gav i många fall upphov till spekulativa idéer om hur verksamheten borde bedrivas. Fakta och intryck presenterades för styrgruppen och blev underlag för diskussion och reflektion inom ramen för projektet.

Ur denna process växte det gradvis fram ytterligare ett antal frågor, som ***mer detaljerat beskrev de ursprungliga frågeställningarna***. Sammantaget visade sig frågorna fungera väl som underlag för samtal om systemrisker och kan av det skälet sägas vara ett slags verktyg för tydliggörande av sådana risker.

Iakttagelser och slutsatser avser i texten uttryckligen ***företag*** men kan i allmänhet tillämpas ***även på andra slag av verksamheter –*** t.ex. statliga myndigheter, kommuner, landsting och organisationer.

De ursprungliga och efter hand tillkomna frågorna grupperas i ***nästa avsnitt*** inom de tre olika huvudområden som efter hand växte fram i arbetet.

2.3.2 Frågor i kartläggningen av systemriskerna

(1) Kunskapsutveckling och kommunikation

- ❑ *Vilken kunskap och information behövs för hanteringen av risker inom företaget?*
- ❑ *Var i företaget finns kunskap och information om risker?*
- ❑ *Vilken typ av riskkunskap är lättast att sprida och använda?*
- ❑ *Vad är informationskvalitet i det här sammanhanget?*
- ❑ *Hur går det till att kommunicera kunskap och information om risker?*
- ❑ *Hur använder företaget kunskapen som kommuniceras?*
- ❑ *Hur borde den användas?*

(2) Attityder och värderingar

- ❑ *Finns det några värderingar inom företaget som försvårar riskhanteringen?*

- ❑ *Är det skillnader i "riskkulturer" mellan olika verksamheter i företaget?*
- ❑ *Mellan olika nyckelpersoner?*
- ❑ *Vilka är konsekvenserna av sådana skillnader i värderingar eller kulturer?*
- ❑ *Hur påverkas skapande, spridning och användning av kunskap och information om risker?*
- ❑ *Vad skulle det innebära i stort för företaget om användningen av kunskap och information om risker utnyttjades bättre?*

(3) Organisation

- ❑ *Finns det "systematiska" svårigheter att utnyttja kunskap och information om risker – svårigheter som är "inbyggda" i företagets organisationsstruktur?*
- ❑ *Var finns i så fall flaskhalsarna och var flödar informationen?*
- ❑ *Hur fattas besluten om riskhantering inom företaget? Hur ser beslutsstrukturen ut i förhållande till kommunikationsstrukturen?*
- ❑ *Vad innebär besluts- och kommunikationsstrukturen för riskhanteringen?*
- ❑ *Finns andra verksamheter, t.ex. organisationer, som har betydelse för riskhanteringen i företaget?*
- ❑ *Hur påverkar de företaget – hur ofta och i vilken utsträckning?*
- ❑ *Har företaget god eller dålig kontakt med dessa verksamheter?*

3. Den teoretiska ramen

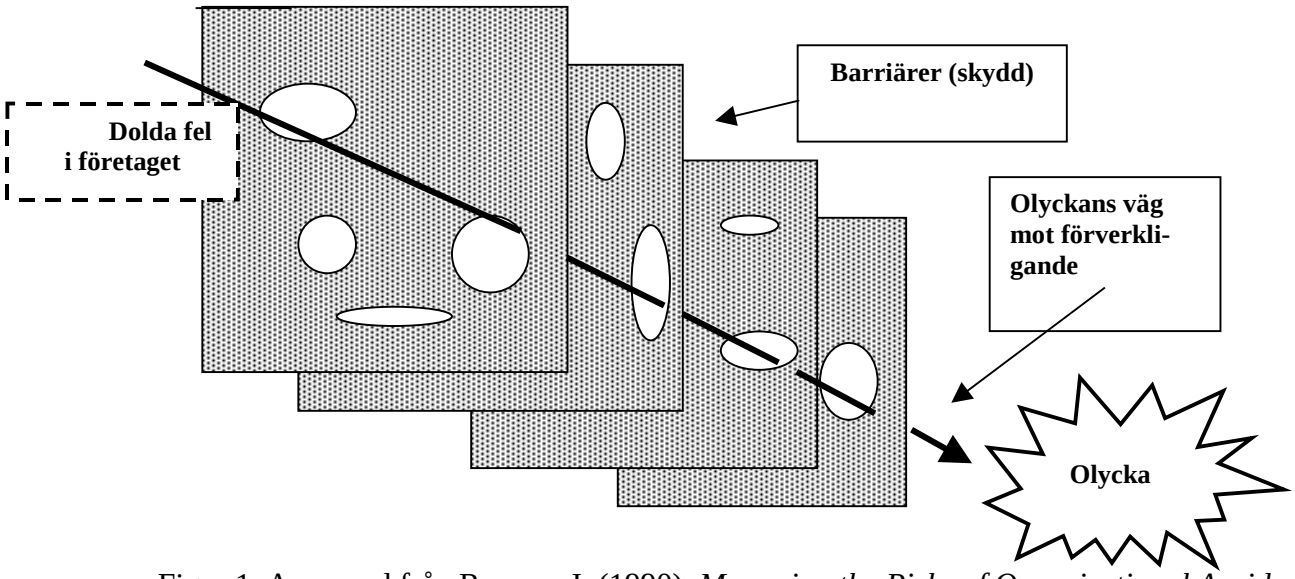
3.1 Vad handlar det om?

En rad forskare har under åren lagt ned mycket arbete på att klargöra begreppet systemrisk och att beskriva orsakssambanden. En typisk utgångspunkt är att varje olycka – oavsett hur liten – är en organisatorisk angelägenhet. Den har sitt ursprung i organisatoriska förhållanden. Det kan vara t.ex. fel person på fel plats, för mycket stress eller andra människors agerande som bryter ned skyddsstrukturer.

En användbar tankebild detta sammanhang är att risken ligger dold i företaget. Det finns ett antal ***skyddande barriärer*** mellan ***risken*** och ***den faktiska olyckan***. Dessa barriärer känner de flesta i företaget kanske till – men inte alla. Det finns hål (defekter) i barriärerna, men sannolikheten är låg för att dessa hål vid något givet tillfälle ska ligga "mitt för varandra", så att risken kan släppas igenom.

Problemet är att individer och grupper i företaget tenderar att manipulera dessa barriärer – ofta utan att veta om det. Detta leder till att barriärerna hela tiden rör sig. Så skedde t.ex. vid Tjernobyl-olyckan, när testpersonalen kopplade bort vissa säkerhetssystem. Ibland ligger barriärerna hål mitt för varandra och en risk kan smita igenom och det uppstår en olycka. ***Figuren*** som följer illustrerar denna princip.

Individer i företaget justerar och manipulerar barriärerna gradvis



Figur 1. Anpassad från Reason, J. (1990). *Managing the Risks of Organizational Accidents.* Cambridge University Press: Cambridge.

Uppgiften för riskhanteringen är att:

(1) Ta reda på vilka barriärer som finns i företaget, hur hålen i dessa ser ut och hur barriärerna kan förstärkas;

(2) *Identifiera beteende i företaget som leder till att barriärerna flyttas* (en del beteende är faktiskt till nytta, t.ex. entreprenörsanda);

(3) *Föra ut kunskap i företaget om hur personalen kombinerar flexibilitet med bra fungerande barriärer mellan risk och olycka.*

På basis av dessa tre aktiviteter går det att urskilja två "traditioner" eller skolor bland forskarna inom systemriskområdet:

- ***Systemanalys-skolan***, som i första hand intresserar sig för människan i de tekniska systemen;
- ***Kunskapshanterings-skolan***, som framför allt ägnar sig åt hur människor i olika verksamheter skapar, kommunicerar och använder (risk)kunskap.

Texten i ***detta kapitel*** ger en bild av de slutsatser som några av de mera inflytelserika forskarna inom de båda skolorna har kommit fram till.

3.2 Människan i det tekniska systemet (Systemanalys-skolan)

3.2.1 Jens Rasmussen

Dansken Jens Rasmussen har en stor vetenskaplig produktion bakom sig. Han har fokuserat sitt arbete på *säkerhet i processindustrier* och på *transport av farligt gods.* Utgångspunkten är att individer arbetar i *socio-tekniska* system som i dessa fall är *komplexa, återkopplade* och synnerligen *dynamiska*. Traditionella organisationsmodeller som enbart bygger på hierarki och instruktioner uppifrån räcker inte för att analysera förhållandena: *"Instruktioner är ett bristfälligt underlag för att bedöma ageranden i samband med praktiskt arbete i ett dynamiskt samhälle"*.

Enligt Rasmussen bör företagen sträva efter att *identifiera gränser för säkert agerande* **–** inte i första hand försöka eliminera orsakerna till mänskliga fel. Det är viktigt att företagen gör dessa gränser synliga och motverkar den *påverkan* från aktörerna som driver systemet mot säkerhetens gränser.

Rasmussen vill alltså att de som svarar för riskhanteringen byter ut sin traditionella *kommandomodell* mot en återkopplande modell där syften, mål och bedömningar hos människor i verksamheten står i centrum. Detta förutsätter att alla *förstår* vilka mekanismer som formar det verkliga agerandet hos aktörerna på olika nivåer i verksamheten, behovet av information, styrande värderingar eller mål och hur dessa olika faktorer påverkas av information över tiden.

3.2.2 James Reason

James Reasons publicerade sin mest inflytelserika bok, *Managing the Risks of Organizational Accidents,* år 1997. Den bygger i stor utsträckning på idéer utvecklade av Rasmussen och på ett tidigare arbete av Reason (*Human Error,* 1990). Reason är psykolog och boken är i stor utsträckning inriktad på *individens* felbeteende, hur individen uppfattar saker och de organisatoriska konsekvenserna av detta.

Reason menar att mänskligt felbeteende i viss mån kan förutsägas: *"I situationer karaktäriserade av otillräcklig information om problemet, eller dålig kunskap om problemområdet, gör man det som brukar fungera i liknande sammanhang."*

Enligt Reason kan mänskliga misstag vara av tre slag: *färdighetsbaserade, regelbaserade* eller *kunskapsbaserade*. Det som skiljer de olika slagen åt är hur de upptäcks – av *individen* själv, av *omvärlden* i form av t.ex. hinder och regler eller av *andra individer.*

Färdighetsbaserade fel beror på brister i kompetens och genomförande (felaktig tillämpning av en bra regel). Regelbaserade fel är inbyggda i stadgar och rutiner (bra tillämpning av en dålig regel). Kunskapsorienterade fel uppstår genom ofullständig kunskap. Dessa fel är svårare att upptäcka genom regler eller genom individen själv. De är dessutom svårare att göra någonting åt.

En olycka orsakas enligt Reason både av ett *aktivt* fel (att någon har gjort ett misstag), och av en uppsättning *latenta* fel (fel i verksamhetens grundförutsättningar). När dessa två fel kombineras uppstår olyckan. Latenta fel har till skillnad från aktiva fel ofta med kunskapsbaserade misstag i ledningen att göra. Med hänvisning till ***Perrow*** (se nedan) anger Reason *komplexitet, koppling* och *tekniska framsteg* som orsaker till den ökande förekomsten av latenta fel. Anställda ska därför inte ses som *orsaker,* utan som *arvtagare* till systemfel skapade av dålig design, dåligt underhåll och dåliga ledningsbeslut.

Reasons huvudpoäng är att när dessa problem ska hanteras räcker det inte med en teknisk ansats. Detta är enligt Reason som att *skala av den aktiva toppen på ett kausalt isberg.* Undersökningen måste omfatta flera faktorer – osäkra handlingar, lokala arbetsplatsfrågor och organisatoriska förhållanden.

3.2.3 Charles Perrow

Perrows bok, *Normal Accidents* från 1984, handlar framför allt om *integrerade sociotekniska system.* Människor särbehandlas inte som hos Reason. Boken kännetecknas av bra analys och intressanta fallstudier – bl.a. haveriet i kärnkraftverket *Three Mile Island* – men innehåller inga direkta rekommendationer.

Perrow menar att flera av de komplexa system som vi idag sätter vår tillit till – t.ex. större processindustrier och kärnkraftverk – är så komplicerade att olyckor inte kan undvikas. De är "inbyggda" i systemet. Perrow kallar dem för *normala* olyckor. De är en *naturlig* del av systemet som vi aldrig helt kan arbeta bort.

En viktig skillnad föreligger enligt Perrow mellan:

- *Komponentfels-olyckor* – en förutsägbar sekvens fel i ett eller flera delsystem i t.ex. en fabrik;
- *Systemfels-olyckor* (normala olyckor) – oförutsägbara interaktioner mellan flera fel.

Det centrala i en "normal olycka" är alltså oförutsägbar interaktion mellan fel.

Vilka system drabbas av normala olyckor? Perrow använder begreppen *komplex* eller *linjär interaktion* och *lös* eller *nära sammankoppling* för att identifiera sådana system. *Komplex* interaktion kännetecknas av oförutsägbarhet, för produktionen "onödiga" konsekvenser av handlingar, fysisk närhet av delar som inte följer varandra i produktionen, oväntade eller obekanta "feedbackloopar", många samverkande kontrollparametrar, indirekta eller störda informationskällor och begränsad förståelse av hela processen. Det linjära systemet å andra sidan är fysiskt utspritt, har entydiga samband mellan olika delar, få feedbackloopar, enkla kontrollsystem och förstås väl av de anställda.

Nära sammankoppling innebär att det inte finns någon buffert eller något "spel" mellan två objekt – t.ex. en mekanisk del eller organisatorisk enhet – i en process. Förändringar i det ena objektet påverkar direkt det andra. Löst sammankopplade system är ofta mer flexibla. Olika enheter kan utvecklas ganska fritt utan att de direkt påverkar intilliggande miljö. Sådana system har ofta tvetydiga och flexibla mått på "performance".

Löst sammankopplade system absorberar lokalt de fel som uppstår. De har liten betydelse för hela verksamheten. I nära sammankopplade system måste buffertar och redundans byggas in från början. Sekvenser kan inte ändras hur som helst. Detta fungerar så länge systemet är linjärt, men om systemet är komplext blir det mycket svårt att veta var sådana buffertar ska byggas in. Perrow drar slutsatsen att verksamheter som kännetecknas av hög komplexitet och nära sammankoppling kommer att producera normala olyckor.

3.2.4 Barry Turner

Barry Turners bok *Man-Made Disasters* från år 1978 är en klar och framsynt bok, som redan för mer än 20 år sedan identifierade kunskaps- och informationsbrist som den väsentliga orsaken till mänskligt orsakade katastrofer. För att kunna hantera katastrofer i komplexa system måste den som svarar för verksamheten ifrågasätta rutiner och söka den expertis som behövs för att kunna förutse katastrofer. Samtidigt är det nödvändigt att beakta det sociala och organisatoriska sammanhang i vilket hela förloppet sker.

En viktig insikt för Turner är att kunskap om risker inte enbart kan sökas rationellt. Ofta finns det en väsentlig faktor utanför det givna området. Det var antagligen därför som olyckan uppstod!

Den viktigaste fasen i de olycksförlopp som Turner beskriver är *inkubationsperioden.* Under denna period äger en rad händelser rum som gradvis för organisationen närmare katastrofen. Faktorer som *stel världsbild, dålig informationshantering, underskattning av fara* och *dåliga regelverk* gör att ingen upptäcker dessa fel. Det finns som regel relevant riskkunskap någonstans i verksamheten men den når inte fram.

Turner menar att tillkomsten av sådan kunskap inte alltid är helt oproblematisk. Våra egna begränsningar som individer omöjliggör optimala lösningar. Ett effektivt arbete fordrar samarbete men innebär också risker för t.ex. hemlighållande av information.

Turner analyserar problemen men kommer inte med några direkta förslag till åtgärder. Mycket i hans analys tyder emellertid på att lösningen kan finnas i ett kun- skapsperspektiv på risker. Det är nödvändigt att analysera relevant riskkunskap, mänskliga barriärer och dålig informationshantering. De flesta av dessa problem behandlas av forskarna inom kunskapshanteringsskolan.

2.3 Människors användning av riskkunskap (Kunskapshanterings-skolan)

3.3.1 Inledning

Denna skola har sitt ursprung inom företagsekonomin. Forskarna intresserar sig först och främst för hur kunskap och information i organisationer skapas, kommuniceras och används. Det är viktigt att förstå de mekanismer som styr verksamhetens kunskapsbildningsprocess. Skälet är att kunskap i en del fall kan reducera risker – men i andra fall också skapa risker. Därför är det viktigt för systemriskanalysen att ta hänsyn till kunskap i verksamheten.

3.3.2 Karl Weick

Karl Weik har bl.a. studerat fundamentala begränsningar och risker förknippade med användningen av IT i olika verksamheter. Många av de sätt vi i vanliga fall använder för att lära oss vad som sker i omvärlden fungerar inte framför datorn, menar Weick. Några exempel på viktiga komponenter i det vardagliga lärandet om omvärlden är:

- *Fri testning – vi ser omedelbart resultaten av något och prövar vidare inom ganska fria ramar;*
- *Triangulering – flera delvis felaktiga källor ger en trovärdig och sannolik bild;*
- *Jämförelse med andras erfarenhet leder till en mer enhetlig bild;*
- *Resonemang – kontemplera och ta sig tid för att nå fram till förståelse;*
- *Stabilisering – sätta in saker i ett sammanhang och kombinera olika typer av kunskaper.*

Dessa processer är mycket viktiga när vi ska lära oss risker och kunna hantera dem. Alla som deltar i verksamheten måste vara involverade i denna hantering och aktivt använda de redovisade inlärningsprinciperna. Enligt Weick hotar en alltför “IT-fierad“ verksamhet att begränsa verklighetens mångfald genom symboler och färre aktiva sinnen. Till detta kommer att stor tillgång på rent kvantifierbar information ofta försvårar och i viss mån omöjliggör överföring av riskrelevant kunskap.

För att kringgå detta föreslår Weick pauser: *Sakta ner arbetsprocessen! Sätt upp rörliga terminaler! Placera personal nära händelser!* Teambuilding, telekonferenser, sponsring och

kulturella aktiviteter är andra hjälpmedel. Framför allt bör den som planerar förändringar i informationssystemen och i riskhanteringen överväga konsekvenserna för inlärningen.

3.3.3 Robert Simons

Simons har utvecklat en metod för att beräkna på vilken "risknivå" en organisation befinner sig. De tre faktorer som utgör kärnan i metoden är verksamhetens *tillväxt*, *kultur* och *informationshantering*. Var och en av dessa kategorier har tre underkategorier eller s.k. "tryckpunkter" på verksamheten. Det är faktorer som ofta ger upphov till en riskfylld verksamhet. Dessa faktorer kan bedömas och ges ett styrka mellan 1-5. Den sammanräknade poängen för olika faktorer visar hur riskfylld verksamheten är.

Tillväxtfaktorer är

- *Prestationskrav (1-5);*
- *Expansionstakt (1-5);* och
- *Brist på erfarenhet hos nyckelpersoner i verksamheten (1-5).*

Kulturfaktorer är

- *Belöningar för entrepreneuriellt risktagande (1-5);*
- *Ledningens motstånd mot "dåliga nyheter" (1-5);* och
- *Intern konkurrens (1-5).*

Informationshanteringsfaktorer är

- *Komplexitet och hastighet i verksamhetens transaktioner (1-5);*
- *Luckor i diagnostiska prestationsmått (1-5);* och
- *Grad av decentralisering i beslutsfattandet (1-5).*

Dessa faktorer kan bedömas informellt av en grupp personer på företaget. Poängen räknas samman och används när ledningen ska besluta om åtgärder. Simons menar allmänt att vid 9-20 poäng är verksamheten relativt säker, vid 21-34 poäng fordras en viss försiktighet. Vid 35-45 poäng är det bara en fråga om tid när katastrofen ska inträffa.

Företaget kan genom riskhantering göra punktinsatser med detta instrument. Om analysen sker vid olika tillfällen går det att klargöra om det finns en trend mot större eller mindre risker i verksamheten. Detta mått beskriver emellertid inte risker för personliga fel utan snarare riskområden. Flera av riskerna kommer enligt Simons från tillväxt. Framför allt kulturproblemen – men i viss mån även de informationshanteringsproblemen – är egentligen symptom på allt för snabb tillväxt. Problemet förefaller att vara den kultur som manar fram tillväxten men också resultaten av expansionen i sig! Den enda systemrisk som egentligen berörs är alltså risk på grund av tillväxt och expansion. Det gör att Simons modell är lämplig vid analyser i tillväxtföretag men kanske inte lika bra för bedömningar inom etablerade företag på stabila marknader.

Rutan som följer innehåller referenser till olika arbeten inom systemriskområdet. Detta är förslag på arbeten för den som vill fördjupa sig inom systemriskområdet.

Förslag på systemriskläsning

Hellström, T. (1998). *Risk-Based Planning*. Institutionen för vetenskapsteori, Göteborgs universitet. Kan beställas från <tomas.hellstrom@fenix.chalmers.se>

Marshall, C., Prusak, L. & Shpilberg, D. (1996). "Financial Risk and the Need for Superior Knowledge Management". *California Management Review*, Vol. 38 No3

Rasmussen, J., Pejtersen, A. M. & Goodstein, L. P. (1994). *Cognitive Engineering Systems*. Wiley: New York.

Reason, J. (1990). *Human Error*. Cambridge University Press: Cambridge.

Reason, J. (1990). *Managing the Risks of Organizational Accidents.* Cambridge University Press: Cambridge.

Simons, R. (1999). "How Risky is Your Company?", *Harvard Business Review*, May-June, 1999.

Turner, B. A. & Pidgeon, N. F. (1997). *Man-Made Disasters 2nd Edition*. Butterworth-Heinemann: Oxford.

Waring, A. & Glendon, I. (1998). *Managing Risk: Critical Issues for Survival and Success in the 21st Century*. Thompson Business Press: London.

Weick, K. (1995). *Sensemaking in Organizations*. Sage Publications: Thousand Oaks.

4. Risksituation och riskhantering i tio svenska företag

4.1 Utgångspunkter

4.1.1 Likheter i systemrisker mellan företagen

Projektledarens samtal med företrädare för företagen illustrerade ett antal grundläggande problem som ibland skapade risker i företagen och samtidigt innebar svårigheter att driva riskhantering i företagen. Dessa grundläggande problem kan sägas ha med *hela* systemet att göra. De faller alltså under det i rapporten behandlade begreppet ***systemrisker***. Riskerna beror i dessa fall på de bakomliggande administrativa, sociala eller kommunikativa förhållandena i företagen men utgör också risker i sig själva, eftersom de i allmänhet inte kommit att identifieras av företagets egen riskhanteringsfunktion.

Studien skulle beskriva riskhanteringen inom ett brett spektrum av branscher. Sedan alla samtalen hade genomförts stod det klart att ***på nivån systemrisker*** hade företagen mycket gemensamt med varandra. Systemrisker är i stor utsträckning generella till sin karaktär men ändå till en del kopplade till branscher. Det allmängiltiga är en följd av riskernas förhållande till organisatoriska och mellanmänskliga faktorer som "går på tvären" genom de flesta verksamheter.

4.1.2 De tio företagen – en kort beskrivning

Företagen i studien täcker ett brett spektrum av verksamheter. Var och en representeras emellertid inte av mer än ett företag. En av fördelarna med detta är att datamängden har blivit relativt hanterlig.

Texten som följer beskriver de företag som lämnat fakta och synpunkter till studien. Det ska framhållas att företagens karaktäristika inte i alla avseenden är korrekta. Syftet med de ändringar som skett i beskrivningen är att skydda företagens identitet.

- *Verkstadsföretaget*

Det aktuella företaget tillverkar lyftkranar och levererar framför allt till byggbranschen och den internationella varvsindustrin. Det är ett familjeföretag i andra generationen. Verksamheten ligger i västra Sverige. Antalet anställda är ca 500.

- *Basindustriföretaget*

Detta företag ingår i en internationell koncern inom stålindustrin. Företaget har anläggningar i ett tiotal länder spridda över hela världen. Huvudkontoret ligger i norra Sverige i anslutning till en av de större tillverkningsenheterna i koncernen. Där finns hela förädlingsprocessen – från järnmalm till stålplåt.

- *Detaljhandelsföretaget*

Detta företag säljer i första hand dagligvaror i ca 1 500 detaljhandelsbutiker över hela Sverige. Verksamheten omfattar också lager och transport av varorna ut till butikerna.

- *Elproduktionsföretaget*

Detta är ett företag som framställer och distribuerar gas, el och fjärrvärme till ett stort antal hushåll och företag i södra Sverige. Företaget bolagiserades i början av 1990-talet och har ca 500 anställda.

- *Fastighetsföretaget*

Detta företag förvaltar fastigheter både för privat och kommerciellt bruk. Det har fyra filialer utspridda i södra Sverige och ca 230 personer anställda.

- *Konsumentföretaget*

Företaget tillverkar livsmedel vid ett antal anläggningar i södra och mellersta Sverige. Verksamheten omfattar förädling av råvara och distribution av den färdiga produkten.

- *Telekomföretaget*

Detta företag har verksamheter inom en rad olika IT-områden och profilerar sig särskilt som leverantör av tjänster för Internet. Företaget har ca 10 000 anställda och expanderar kraftigt i norra Europa genom allianser med andra infocomföretag.

- *Kunskapsföretaget*

Detta företag arbetar i Stockholms-regionen med uppdragsforskning och annan konsultverksamhet för privata och statliga verksamheter. Företaget sysslar mycket med trafik- och transportsäkerhet och utför även logistikuppdrag.

3.2 Fakta och värderingar om de tio företagens riskhantering

De mest framträdande systemriskerna för de olika företagen i kartläggningen framgår av ***texten som följer.*** Strävan har varit att fånga både riskerna som sådana och att peka på möjliga åtgärder. Det visar sig att en del slag av risker är typiska för vissa branscher. De som är särskilt karaktäristiska för en verksamhet kommer av det skälet att redovisas i matrisen i ***avsnitt 5.2.*** Syftet med matrisen är att läsaren för varje bransch enkelt ska kunna få en uppfattning om den relativa omfattningen av systemrisken, så som den kommit fram i samtalen med företrädarna för företagen.

Texten i ***rutorna inom avsnitten om varje företag*** innehåller mer generella konstateranden grundade på förhållandena i företaget och slutsatser som förekommer i den vetenskapliga litteraturen om systemrisker.

❑ *Verkstadsföretaget (VF)*

De olyckor som resulterat i *personskada* upplevs inte helt oväntat vara den viktigaste riskkategorin hos VF. Skälet är troligen att sådana händelser inträffar förhållandevis regelbundet och att arbetsmiljön ofta är hektisk och "fysiskt påtaglig". riskhantering i företaget har till största del inriktat sina åtgärder på att förebygga denna typ av olyckor. Detta har sannolikt gått ut över systemriskerna.

Företaget samarbetar med räddningstjänsten i kommunen. Det är främst fråga om utbildning av typ Första Hjälpen. Riskhanteringen styrs av en säkerhetskommitté. I den ingår chefer och tjänstemän från olika verksamheter i företaget och skyddsombud, som rapporterar till de fackliga organisationerna. Dessa skyddsombud svarar för olika *skyddsområden* i företaget och gör bl.a. ronder med checklistor. Allting dokumenteras. Klagomål från "golvet" riktas antingen direkt till dessa ombud eller till personalchefen, som är ordförande i säkerhetskommittén.

Rapporteringens innehåll och omfattning beror på hur de anställda ser på riskerna. Det finns flera olika riskkulturer inom VF. Företaget har olika grupperingar som värderar risk på olika vis, utsätter sig för olika mycket risk och har olika slag av förhållanden till företaget. Personalen i basproduktionen – för att ta ett exempel – anser att de är *beroende* av företaget. De tillhör en grupp som arbetar på samma plats varje dag och rapporterar gärna även om enkla brister i arbetsmiljön.

De som arbetar med eftermarknaden – alltså service på maskiner efter försäljning – tenderar i stället att odla en slags machokultur. De reser mycket ofta i riskfyllda miljöer som de inte är bekanta med och ser sig själva som "egna företagare" i förhållande till VF. Det är enligt dem inte någon mening med att "beklaga sig". De underrapporterar risker och tillbud. Följden blir att de som är utsatta för de största riskerna lämnar minst riskinformation till säkerhetskommittén och till skyddsombuden.

Säkerhetskommittén har genom sin sammansättning och sitt sätt att arbeta ett antal svagheter som kan resultera i systemrisker. När ansvariga inom olika delar av linjen är med och definierar samma uppsättning riskfrågor uppstår det lätt informationsflaskhalsar för riskkunskap. Onödiga konflikter och diskussioner infinner sig lätt och säkerhetskommittén kan bli en arena för av olika slag av prestigeutspel.

Risk och "kunskapsarenor"

Hanteringen av risker i en organisation blir ofta en fråga om att se till att rätt typ av kunskap skapas, att rätt person utnyttjar den kunskap som finns, att feltolkningar förhindras, och kanske mer kontroversiellt, att "feltolkningar av personligt intresse" försvåras. Som vi längre fram kommer att se är det säkert naivt att tro att individer gärna lämnar ifrån sig riskkunskap i organisationen. Dels kanske de inte känner igen sådan kunskap, dels "bör" de kanske inte ens ha den! Bristen på kunskap om risker, eller "kunskapsrisker", kommer av att inte veta vad organisationen vet, och att inte veta vad den inte vet. Organisationens riskkunskap finns först och främst hos dess medlemmar, och kunskapsriskhantering blir därför en fråga om att uppmuntra anställda att tänka och tala utanför sin "organisatoriska låda". Det bästa sättet att hantera kunskapsrisker är att bli en kunskapsmäklare i sin organisation. Alltså en individ som har

kontakt med många, som vet var kunskapen finns, och var den inte finns, som kan skapa kontrollerade arenor för diskussioner om risk, där överlämnandet av riskinformation och det utsagda behovet av sådan information belönas. Sådana arenor är troligtvis det enda som kan överbrygga två av de allvarligaste systemriskerna i organisationen, nämligen (1) dåliga kommunikationsvägar och beroende av "djungeltelegrafen" för information, och (2) brist på förtroende hos de anställda gentemot ledningen och vice versa. Det sistnämnda är den riskansvariges yttersta mardröm.

Ordföranden i säkerhetskommittén anser att det är en stor fördel att vara både personalchef och Risk Manager. Det visar hur riskfrågor lätt kan användas för att framhäva vissa ansvarsområden i företaget – i det här sammanhanget personalområdet. Det kan i så fall ske på bekostnad av andra områden. VF har ingen övergripande verksamhet för riskhantering, vilket lätt leder till denna situation och till en brist på överblick.

Säkerhetskommittén föredrar en inriktning på enkla och entydiga risker som "rimmar väl med verksamheten", t.ex. klämskaderisker eller en flimrande datorskärm. Bristen på ett övergripande riskperspektiv gör att företaget lätt fastnar i checklistor, som i sämsta fall är illa anpassade för verksamheten. En person på VF reflekterade över detta och menade att en checklista "måste kombineras med levande diskussioner på företaget runt frågor om struktur, beslut och värderingar. Riskinstrumentet kan inte låsas in i en dator." VF har å andra sidan möjlighet att snabbt reagera på dessa enklare risksignaler genom nära avstånd till VD och genom företagets relativt entydiga verksamhet.

❑ *Basindustriföretaget (BF)*

BF har linjeövergripande rikshantering. En person i styrelsen utgör tillsammans med företagets Risk Manager en grupp som analyserar risker inom samtliga delar av företaget. Risker rankas på samma skala oavsett riskområde. Åtgärderna prioriteras på basis av riskens omfattning. På så sätt kan t.ex. *avtalsrisker* jämföras med risker för *produktionsstopp* och *brandrisker* ställas mot *maskinhaverier*.

Ungefär hälften av riskhanteringen är inriktad på produktionsrisker kopplade till brand och maskinhaveri. Det är två områden för vilka riskanalysen i hög grad har formaliserats inom företaget. Företagets Risk Manager, som har det övergripande riskansvaret, deltar i överläggningar med *specialgrupper* som har bildats för olika riskområden. Utomstående experter anlitas även för specialområden. Efter deras punktutredningar gör företagets Risk Manager ansvar uppföljningar på plats.

Bedömningar och analyser av riskerna hos företagets leverantörer är en mycket viktig del av arbetet. Driftstopp på grund av t.ex. brand hos leverantörer får snabbt effekter i hela produktionskedjan och kan sammantaget leda till mycket höga kostnader. Av det skälet måste även risker i verksamheten hos små leverantörer analyseras med stor noggrannhet.

En ofta oförutsedd systemrisk är att företag faktiskt bygger en "för stark" riskhanteringsfunktion. Om identifieringen och rapporteringen av risker flyttas bort från linjen, eller från den praktiska verksamheten och från "gräsrötterna" i företaget, så försvinner en del av initiativkraften. Informationen om de risker som förekommer flödar sämre – både uppåt och nedåt i organisationen. Det innebär att rikshanteringsfunktionen kan missa ett nytt framväxande ris-

område. Eller också värderas det inte korrekt. Skälet är i så fall att det "faller utanför" den existerande analysen och riskhanteringsapparaten.

En stark riskhanteringsfunktion blir lätt beroende av ett fåtal personers tolkning av de situationer som uppstår. BF har haft en långvarig stabil utveckling med långsam produkt- och affärsförnyelse och en låg personalvårdande profil.

Riskkultur

En organisation kan bara hantera risk om dess medlemmar är villiga att deltaga i riskhantering. Det spelar ingen roll hur många analyser och checklistor som gås igenom, i slutändan kan en organisation inte tvingas till effektiv riskhantering. Individer bestämmer om vad riskhantering är värt för dem, om de ska hantera eller inte hantera risk, och detta kan innebära problem om riskreducerande beteende innebär hög personlig risk. Riskhantering handlar ofta om att "stå upp i båten", och att utmana etablissemanget. Ingen kan hantera risk som inte är beredd att ta risk. Organisationskulturen är viktig inom systemriskanalys, därför att den avgör *hur stora personliga risker en individ måste ta för att sänka riskerna för hela organisationen*. I en positiv riskkultur kan individer fatta beslut och hållas ansvariga för beslut, det är svårt att "gömma sig bakom gruppen". En positiv riskkultur stimulerar ifrågasättande, inte mycket tas för givet, samtidigt som individer på så sätt lättare lär sig rutiner och procedurer. En positiv riskkultur underlättar *erkännande av kunskapsbrister*. – "Hur lär vi oss någonting om nya risker och hot om vi redan vet allting?"

God intern och extern kommunikation – alltså god mediakontakt och god kontakt mellan ledning och anställda – har aldrig varit centrala spörsmål. När samhället i allt högre utsträckning intresserar sig för t.ex. miljön, blir plötsligt goda kontakter med massmedierna en viktig sak även för företagets Risk Manager.

En anställd rapporterade vid ett tillfälle till media om en miljörisk inom BF. Företagets Risk Manager beskriver personen som "lycksökare" och illojal mot företaget. Reaktionen från den riskansvarige säger kanske mer om situationen inom företaget än den anställdes beteende. Fallet illustrerar också *personalfrågans* roll i modern riskhantering. Risker uppstår också vid besked om permitteringar. Vid sådana tillfällen uppstår apati och ilska. Många anställda får en annan syn på verksamheten i företagen. Det leder till nya typer av risker. Det finns många exempel från industriföretag av olika slag på en alternativ informationsstruktur som snabbt byggs upp genom informella kontakter och skvaller. Den nya strukturen kommer att konkurrera med ledningens försök till informationsöverföring. Denna alternativa struktur blir självförstärkande, när ledningen och de anställda hamnar i motsatsställning. Systemrisken uppstår när en radikal förändring i de anställdas värderingar sammanfaller med en förlorad kontroll över informationsflödet från ledningens sida.

❑ *Detaljhandelsföretaget (DF)*

Företaget har delat upp riskhanteringen mellan detaljhandelsledet och koncernen i övrigt. Det senare innebär framför allt lagerhållning och transporter. DF har två ytterst riskansvariga – en som täcker säkerhetsförfarandet i det stora antalet butiker och en som svarar för mer övergripande riskfrågor inom företaget. Dessa två roller överlappar varandra men har delats upp organisatoriskt. Det leder lätt till svårigheter när det är nödvändigt att lösa gemensamma problem som uppstår. Det gäller t.ex. att avgöra i vilken grad lokala säkerhetsrutiner ska anpassas till en generell koncernstandard?

En av de allvarligaste riskerna är rökskador på grund av brand i butikerna. Orsaken till sådana bränder är ofta fel i elinstallationerna. Även anlagda bränder förekommer. Den koncernövergripande riskbilden säger att händelser som leder till materiella skador och personskador är flest i antal, medan datastopp och stölder leder till de högsta kostnaderna. De senare problemen matchar inte butikssidans bedömning, som säger att rökskador är den största risken.

DF har eget captive. Verksamheten administreras av ett stort svenskt försäkringsbolag. Bolagets säkerhetskonsulter står för en del av riskhanteringen – framför allt riskanalyserna – vilket ger en mer allsidig bild och minskar riskerna för felbedömningar. När det gäller skydd mot t.ex. bedrägerier, rån och svinn har DF enligt den koncernriskansvariges mening inte hunnit anpassa sig till den efter hand förändrade brottsligheten. Polisiära insatser räcker inte på långa vägar för att lösa dessa problem på ett tillräckligt bra sätt. Säkerhetsnivån har passat den traditionella folksjälen väl, men svarar inte mot dagens hårda samhällsklimat. Många av problemen beror sannolikt på brister i rutiner och utbildning. Skrivna och oskrivna regler misstolkas lätt av personal, antingen de kommer nya till en arbetsplats eller får nya chefer.

Flera åtgärder skulle förbättra situationen i detta sammanhang: ökad internrevision inom olika områden, bättre uppmärksamhet med chefsattityder, fler analyser av seder och bruk, ökad kommunikation på arbetsplatserna, bättre incident- och skaderapportering och effektivare etablering och upprätthållande av säkerhetsnormer. Visionen för DF är "högsäkerhetsbutiken". Den koncernriskansvarige anser att företagets Risk Manager ska vara ett föredöme för annan ledning i företaget. Om det ska kunna ske är det nödvändigt att alltid ekonomiskt kunna motivera de åtgärder som vidtas. En viss rapportering har i det sammanhanget större betydelse än annan. Det behövs en snabbare uppgifter om händelser och tillbud från logistiken på företagsnivå, medan rapporteringen från butikerna kan tillåtas gå något långsammare.

Riskanalys och val av kontext

Vilken är riskens kontext? Denna fråga kan ge oss svaret på hur vi bör hantera risken. Inom RM kan kontext tolkats på tre olika sätt. Först och främst *platsen* där risken börjar och utvecklas och *förutsättningarna* för att risken ska utvecklas. Det kan vidare påstås att en negativ händelse är en kombination av plats, förutsättningar och *omständigheter*. Riskanalysens "systemkänslighet" kommer av hur flexibla vi är att lyfta oss från den omedelbara platsen (från kassaapparaten till butikens närområde), från de omedelbara förutsättningarna (från brist på kassaspeglar till brist på träning av personal), och från de omedelbara omständigheterna (från tillgång på pengar i kassan till tillgång på pengar i samhället). Riskhantering inbegriper alltid ett val av kontext. Detta val är aldrig självklart – det måste reflekteras över och motiveras. Anledningen till detta är att en åtgärd som tas på en "lägre" nivå, kan omintetgöras av faktorer "högre upp" eller åtminstone begränsas i sin effektivitet. Risken för stöld av cigaretter minskar när skatterna på cigaretter ökar, därför att smugglingen ökar när skatterna ökar, vilket sänker priserna på cigaretter i kriminella led. Både butikssäkerhetschefen och koncernsäkerhetschefen kan bli effektivare genom att förbättra sin syn på riskens kontext!

❑ *Elproduktionsföretaget (EF)*

EF hanterar el, gas och fjärrvärme och utnyttjar branschföreningar inom alla dessa områden för riskinformation och övrigt utvecklingsarbete inom riskhanteringen. De mest uppenbara riskerna för EF är skador i produktionsanläggningarna. Det kan vara fråga om turbin- eller rotorskador. Kostnaderna för dessa kan uppgå till mellan en halv och en miljon kronor per år.

Även riskerna för personskador är stora – framför allt för elinstallatörerna. Dessa risker hanteras emellertid väl med hjälp av regelverk och certifierande utbildning av olika slag.

Personsäkerhet och skador på anläggningarna har traditionellt stått i fokus för riskhanteringen i företaget. Systemrisker som börjat uppträda är en följd av bolagiseringen av företaget, marknadsanpassningen och den informationsteknologiska utvecklingen. Några av dessa systemrisker framstår som särskilt allvarliga. Utformningen av avtalen med kunderna har blivit decentraliserat och förlagts till marknadsavdelningen. Verksamheten växer snabbt genom bl.a. nyanställningar av försäljare, som i många fall saknar kunskap om branschens kärnprocesser men som har en hel del entusiasm.

En *entreprenörskultur* som rimmar dåligt med EF:s traditionella anda håller på att utvecklas inom marknadsavdelningen. Detta har tagit ledningen "på sängen". Verksamheten har med jämna mellanrum kommit att bli bundet av avtal som är ofördelaktiga för företaget eller rent av omöjliga att genomföra. Till detta kommer att kostnader i en del fall har hamnat på "andras konton" – även utanför företaget!

Risk och "informationsdemokratin"

"Information wants to be free" har varit datahackerns stridsrop under 1980/90-talet, som skrämt slag på större affärsidkare och på militära organisationer runt om i världen (speciellt i USA). Idag går trenden hos storföretag mot att öppna "kompetens-torg", tekniska diskussionslistor och "datawarehouses" på sina intranät. Dessa initiativ går under samlingsnamnet *Knowledge Management*. Information ska delas, göras fri, så att växande företag ska kunna behålla sin dynamik och öka de anställdas närhet till kunskap som är relevant för deras arbetsuppgifter. Samtidigt ökar personalomsättningen på företagen, speciellt på stora företag som befinner sig inom snabbt utvecklande affärsområden (IT, telecom). Knowledge management bygger på insikten att kunskap är pengar. Men lägg till personalomsättningskomponenten, och ekvationens andra sida av uppenbarar sig. Din kunskap riskerar att bli andras pengar. Kunskapsspridning inom företaget utgör en konkurrensfördel så länge kunskapen inte sprids till dina konkurrenter, eller på annat sätt används mot ditt intresse. I *motsvarande utsträckning* som kunskapsspridning inom företaget byggs ut, måste företagets "kunskapsskydd" byggas ut för att denna kunskap ska kunna fortsätta att vara värdefull.

EF arbetar mycket med kartor över sina elnät. Dessa kartor utgör företagets viktigaste kunskapsresurs. Kartorna har nyligen digitaliserats och lagts ut på företagets intranät. De har vidare blivit tillgängliga för ändring och uppdatering genom nätoperatörerna. Detta var tidigare en relativt seg process i flera led. Allt skulle prövas och godkännas innan justeringar fick ske direkt på kartan. De elektroniska kartorna har inneburit två saker. Allt fler i organisationen kan gå in och ändra i kartorna. Ett stort antal anställda har möjligheter att på sin arbetsstation framställa kartor över ledningsnätet och skicka dem vidare – med t.ex. e-post – till i princip vem som helst. En del kartor har ett speciellt känsligt innehåll. De som inte är hemliga kan användas – eller kombineras med annan information – för planering av sabotage. Säkerhetsprövningen i företaget är viktig. Det finns emellertid få utarbetade rutiner för att hantera denna form av säkerhet. De säkerhetsnivåer som EF uppnår genom användningen av begreppet *skyddsobjekt* bedöms inte som tillräckliga.

På grund av att kommunen har aktiemajoritet i EF tillämpas offentlighetsprincipen för alla dokument. Enligt företagets Risk Manager är många av de IT-relaterade problemen inom företaget egentligen administrativa och organisatoriska.

❑ *Fastighetsföretaget (FF)*

På FF ligger riskhanteringen på var och en av fyra lokala fastighetsförvaltare, vilka har ansvar för företagets distriktskontor direkt under VD. Detta innebär ett mycket kort avstånd till VD i beslutsfrågor, men samtidigt ett lite längre avstånd mellan distriktcheferna och svårigheter i samordningen av riskarbetet. Distriktscheferna är ansvariga för att informera anställda om risker och förändringar, samt att samordna arbetarskydd. FF har rutinmässigt kontakt med Räddningstjänsten, som förutom sina årliga kontroller av fastigheterna även engageras när kontrakt ska skrivas och när verksamheter i lokalerna ändrar karaktär. Den fastighetsansvarige går då med brandinspektören både för att "kunskapen ska hamna på rätt ställe" och för att den fastighetsansvarige vet mer om huset och dess egenheter. Grundinställningen är att uppfylla kraven från myndigheterna. Moralen anses vara hög i bolaget.

Cheferna på FF är i stor utsträckning medvetna om företagets risker men saknar ett utvecklat system för att hantera dessa. En av cheferna rapporterade att han saknade kunskap om sitt informationsansvar. *Vad bör regleras i kontrakten med hyresgästerna? Vem svarar för att information om olycksrisker sprids till uthyrare i andra, tredje och fjärde hand? Hur når information om avtalsskrivande och om innehållet i avtal dem "längst ner" i verksamheten, alltså t.ex. fastighetskötarna?*

Mycket av riskkunskapen inom fastighetsbranschen är informell. Golvbelastning, och skyldigheter som gäller skyddet av vattentäkter brukar inte regleras i kontrakten. Under sådana omständigheter blir det svårt att informera och förutse risker.

FF har nyligen utvecklat ett enkelt system för att kunna hantera åtminstone några av dessa kunskapsrisker. Det sker genom ett nytt kontraktsförfarande som reglerar entreprenörernas skyldigheter. Fyra fastighetsförvaltare ansvariga för var sitt område satt och "spånade" om dessa problem – om skyddsåtgärder och priset på tjänster och material. De kom då på idén att integrera rikshanteringskraven och affärskraven på den kontraktsblankett som de anställda använder när de beställer tjänster och material. De framstod som naturligt att tydligt knyta riskhanteringen till inköpen. Blanketten utvecklades under tre-fyra frukostmöten mellan förvaltare och övrig administrativ personal. Den ger uppgifter om priser, varor och leveranstider men även information om vem som svarar för skyddsåtgärder enligt AML, vem som är brandskyddsansvarig vid heta arbeten och vem som är arbetsmiljöansvarig. Dessa personer ska skriva under blanketten och därmed bindas vid sin uppgifter.

❑ ***Konsumentvaruföretaget (KVF)***

Företagets risker – framför allt på systemrisknivå – gäller *ekonomisystemet*, *logistiken* för verksamheten som helhet och *produkten*. Ekonomisystemets känslighet beror på att det är kopplat till detaljhandelns ordersystem. Efterfrågan på produkterna varierar med tiden. Om det skulle inträffa ett datorhaveri kan KVF leverera "på förra veckans order", men därefter kraschar logistiken och kan inte ens temporärt ersättas av ett ordersystem med manuell expediering som innebär att butikerna ringer in sina beställningar.

Flera av företagets systemrisker sammanhänger med ett starkt "sammankopplat" ekonomi- och logistiksystem. Den höga genomströmningen av varorna späder på riskerna. Detta är ett exempel på att ökad effektivitet och försäljning kan komma att ske på bekostnad av säkerheten i verksamheten.

Som koncern och logistiskt sett omfattar KVF råvaruproducenter och är samtidigt leverantör till detaljhandeln. Företaget har en stor producerande organisation och en mycket omfattande transportverksamhet. Lastbilsflottan består av nästan 700 bilar med släp. De traditionella transportriskerna är avsevärda. En systemrisk är även den riskexponering KVF utsätter sig för genom användningen av djur i produktionen. Sabotage är i det sammanhanget den största risken företaget är utsatt för.

KVF anser den ledande risken är hotet mot deras produkter. Verksamheten är sedan flera år utsatta för både hot och attentat från radikala intressegrupper – djurrättsaktivister och militanta veganer. Även om KVF tar juridiskt ansvar för produkten enbart under den del av produktionscykeln som de kontrollerar – från upphämtning hos råvaruproducenten till leverans i detaljhandeln – är det uppenbart att företaget i ett affärsriskperspektiv är mycket sårbart. Produkterna kan manipuleras med giftiga ämnen antingen hos råvaruproducenterna eller i butikerna. Det är omöjligt för KVF att kontrollera detta.

KVF bedömer att ett attentat mot t.ex. ett tiotal detaljhandelsbutiker i landet skulle kunna sätta stopp för försäljningen under lång tid. Det skulle kunna slå omkull koncernen, med oerhörda finansiella och sociala skador som följd. Det förefaller som om KVF relativt framgångsrikt hanterar ett antal vardagliga risker inom ett ganska smalt område på riskskalan. De risker som utgör hot mot företaget som helhet ligger emellertid inom ett område som verkar okontrollerbart.

KVF har genomgått en utveckling som varit vanlig för traditionella konsumentvaruföretag. Företaget har gått från en historiskt relativt oproblematisk produktion av en relativt oproblematisk produkt till att hamna i en konflikt med värden och attityder som befinner sig i snabb förändring hos ett antal människor i samhället. Detta problem tenderar att eskalera i takt med informationssamhällets utveckling. Det gör att många företag inte längre bara är beroende av en säker produktion, ordning och reda, systematisk rapportering och kontroll över linjen. Av minst lika stor betydelse är företagets "ansikte utåt" – distributionen av produkterna och förmågan att bevaka och anpassa sig till snabba förändringar. Det är viktigt att också kunna dra nytta av omvärldsförändringarna. Företagets Risk Manager anser att riskhanteringsfunktionen i detta avseende har i stort sätt samma intresse som marknadsavdelningen.

Företaget måste inom ramen för sin riskhantering kunna identifiera de radikala intressegrupper som kontinuerligt bildas och ombildas. *Hur ser sådana grupper ut? Hur sprider de information? Var söker de information? Vilka värderingar har de? Hur organiserar de sig?* Det är genom sådana frågor riskförebyggande aktiviter måste börja. Företaget har skapat ett nätverk med andra som sysslar med djur. Tillsammans diskuterar de erfarenheter, problem och åtgärder. De rapporterar händelser till SÄPO, som sammanställer uppgifterna och får underlag för åtgärder som syftar till att förebygga nya attentat.

❑ *Telekomföretaget (TF)*

TF expanderar framför allt på sin hemmamarknad i Norden genom fusioner. Baltikum är ett annat viktigt expansionsområde. Företaget har delägare över hela världen. Nya marknader och spridda intressen innebär nya risker. TF är i första hand ett serviceföretag. Produktionen som ska skyddas – i det här fallet *nätet* med tillhörande produktutveckling – skiljer sig kraftigt från ett företag som t.ex. BF. TF har ingen fabrik som kan skyddas. De allvarligaste hoten föreligger mot det mycket omfattande nätet samt mot den *information* som transporteras på nätet.

Företaget har en riskhanteringsfunktion för varje större verksamhetsområde. Arbetet leds operativt från linjen. En s.k. *RM & Security Group* koordinerar dessa åtgärder och rapporterar till ledningen, där gruppen har en rådgivande funktion. Ett problem med att riskhanteringen finns i linjen är att verksamheten ofta får stå tillbaka för produktutvecklingen. Företaget har blivit en *processorganisation* uppbyggd kring den dynamiska produktutvecklingen. Utvecklingsprocessen — och de risker som denna skapar — går på ett oförutsägbart sätt på tvären över affärsområdena. Detta leder till samordningsproblem för den linjebaserade riskhanteringen.

TF bolagiserades i början av 1990-talet. Innan dess lades stora resurser ned på traditionell infrastruktur för säkerhet — brandskydd och skydd mot inbrott eller annan skadegörelse. Ett skäl var att företaget som offentlig verksamhet inte kunde försäkra sig. Följden har blivit att verksamheten i dag i många delar är klart överskyddad. Resurserna läggs numera i stället på affärsrisker och informationsrisker kopplade till framför allt nätet och processerna, upprätthållandet av servicefunktioner och återställandeåtgärder. Affärsrisker, finansrisker och politiska eller kulturella risker är exempel på de många nya "dynamiska risker" som blir allt

Riskhantering och organisation

Om riskhantering ska kunna utgöra en verklig förändringskraft i organisationen måste den anpassas till de processer som verkligen skapar värde, inte till de officiella, fasta organisationsstrukturerna. I telecomföretaget är riskhanteringen anpassad till en linjeorganisation, när företaget egentligen använde sig av en processorganisation för att driva utvecklingsprojekt. Istället för att sitta i linjen och se produktutvecklingsprojekten svischa förbi, borde riskhanteringsfunktionen sitta i projektet och se linjerna svischa förbi! Annars riskerar funktionen att hamna utanför de fora där beslut med verkliga konsekvenser fattas och där information delas. Den kan komma att bli isolerad i en linje som saknar relevans. Placeringen av riskhanteringen måste ta hänsyn till ett antal grundläggande krav med avseende på organisation: (1) Aktiv bevakning: Var är företagets föryngringsytor lokaliserade? Om rikshanteringen förläggs dit är chansen till riskkänslighet i analysen god. (2) Anpassligt riskhanteringssystem: Förlägg riskhanteringen till *början* snarare än *slutet* av viktiga processer (t.ex. projekt), så att riskarbetet kan utvecklas *med* de värdeskapande processerna snarare än *mot* (jämför att sätta in riskhanterin "fem i 12", då alla väsentliga beslut redan har fattats). (3) Flexibelt lärande: Knyt samman organisatoriska processer i ett gemensamt risklärande t.ex. genom riskseminarier. (4) Tillgång på resurser: De processer som skapar värde är också de som har störst behov av samt störst potentiella resurser för riskhantering. Lokalisera dessa processer och omorganisera riskhanteringsfunktionen för att passa dessa.

viktigare för expanderande företag i marknader med snabb utveckling. Dessa risker är emellertid svåra att "komma åt" inom en traditionell RM-funktion kopplad till linjen eller affärsområdena. Detta problem kan möjligtvis hanteras genom att en övergripande "hotbildsanalys" läggs till grund för all produktutveckling. TF håller på att utveckla ett sådant förfarande.

❑ *Kunskapsföretaget (KF)*

Inom ett kunskapsföretag står alltid information och kunskap i centrum. De är både verktyg och produkter. Samtidigt används de i mycket hög grad när företaget organiserar själva verk-

samheten. Brister i kunskapsspridning inom det egna företaget blir för KF en uppenbar systemrisk.

Storleken på det aktuella företaget ― 15 anställda ― begränsar dessa problem. Ett tydligt problemområde är enligt KF sambandet mellan information och organisation hos kunden. Erfarenheten visar att svårigheterna att utnyttja rapporter och annan information i den beställande organisationen ofta är mycket stora. Sådana svårigheter påverkar kundens bedömning av kvaliteten i KF:s verksamhet. I förlängningen innebär det en affärsrisk för KF. Varje uppdrag borde vara kombinerat med en parallell studie av hur kunden bäst ska tillgodogöra sig det beställda materialet.

Den vanligaste formen av informationsöverföring mellan KF och beställaren är *rapporten*. En rapport som inte kommer till användning kan vara riskskapande i sig. Den kan få konsekvenser för kunden i följande tre avseenden: (1) Resurser har slösats på ett arbete som inte används; (2) Problemet som rapporten handlar om hanteras inte rätt, vilket kan förvärra problemet; och (3) En "informations-apati" riskerar att infinna sig. Det senare innebär att aktörerna hos beställaren inte känner något behov att varken ta upp problemet eller att söka ny information, eftersom "en studie redan har gjorts".

Problemet kan vara av den karaktären att det ständigt förändrar sig. Ingen letar emellertid längre efter information. *Det är legitimt, eftersom det finns en rapport!* Till detta kommer att en rapport med låg läsbarhet eller relevans kan bli mer användbar som maktmedel hos beställaren än som kunskapskälla. Information kan brytas ut eller omtolkas för att stödja en viss uppfattning om situationen och vad som bör göras. Alla dessa aspekter verkar menligt på avsättningen för KF:s tjänster och dess största resurs, nämligen ryktet att kunna förbättra verksamheten hos kunderna.

KF har goda erfarenhet av att *kurser* med personalen hos beställarna underlättat utnyttjandet av tjänsterna. Svårigheten med denna lösning är att kunskapen riskerar att bli bunden i tillfälligt närvarande konsulter eller kursledare. Detta skapar intensivt, lokalt utnyttjande av kunskapen under en kort period. Överföringen i stort till kunden eller under längre tidsperioder är emellertid låg. Vid en sådan kurs identifierade KF motståndet mot informationsanvändning i ett företag. *Flaskhalsen* var förhållandet mellan ledning och personal. Konsultföretaget lyckades förebygga problemet genom samtal mellan parterna. Detta säkrade en mer långsiktig kunskapsöverföring i kundens verksamhet.

5. Våra slutsatser och rekommendationer

5.1 Tre huvudområden för systemrisker

5.1.1 Utgångspunkter

Underlaget för redogörelserna i kapitel 2 var samtalen mellan projektledaren och de riskhanterings- eller säkerhetsansvariga i ett antal svenska företag. Samtalen hade karaktären av öppna diskussioner om framför allt systemrisker.

Efter samtalen – och vid de genomgångar som styrgruppen hade – gick det som tidigare framgått att urskilja ***tre huvudområden*** för systemrisker och inom dessa ***ett antal delområden***. Huvudområdena omfattar de övergripande faktorer i organisationen som leder till risker av olika slag och delområdena de särskilda processer som ibland orsakar systemrisker inom företagen.

Huvudområdena är

(1) Kunskapsutveckling och kommunikation;

(2) Attityder och värderingar; och

(3) Organisation.

Avsnitten som följer innehåller en kort beskrivning av de tre huvudområdena.

5.1.2 Kunskapsutveckling och kommunikation

Detta huvudområde avser organisationens informationsstruktur – hur information och kunskap uppstår, kommuniceras och används. Slutsatserna gäller både överföringen av riskspecifik kunskap och sådan generell kunskap som påverkar organisationens processer och dess produktion. Se t.ex. avsnittet om telekomföretaget.

Särskilt intressant är tillgången på riskkunskap för rikshantering och möjligheten för den riskansvarige att kommunicera denna kunskap till ledningen för beslut. Dessa två faktorer har betydelse för varandra. Kunskap utan kommunikation är meningslös och kommunikation utan kunskap är farlig. Se avsnittet om kunskapsföretaget.

Några frågor i detta sammanhang: *Hur säker eller osäker är informationen? Hur viktig är den för att företaget ska kunna fatta rätt beslut?*

5.1.3 Attityder och värderingar

Detta huvudområde avser de anställdas attityder till företaget och till riskerna i verksamheten. Det gäller både ledningens och de anställdas riskbenägenhet. Till bilden hör företagets risk-

kultur (se verkstadsföretaget) och vidare de anställdas och ledningens förmåga och intresse att dela kunskap.

Några frågor i detta sammanhang: *Hur påverkar attityder och värderingar hu-vudområdet kunskapsutveckling och kommunikation? Finns det en obenägenhet i organisationen att kommunicera uppåt eller nedåt? Är strävan att skapa kunskapsbarriärer med hänsyn till grupptillhörighet (se basindustriföretaget)? Hur stor är risken för ett "vi-och-dom-tänkande"?*

5.1.4 Organisation

Detta huvudområde gäller organisationsformen – både den som representeras i organisationsschemat och den verkliga. Det gäller att klara ut om organisationsformen och riksanteringen är funktionellt anpassade till varandra (se telekomföretaget) och om ansvarsfördelningen i företaget och inom riskhanteringen svarar mot riskbilden (se detaljhandelsföretaget).

Några frågor i detta sammanhang: *Är de administrativa rutinerna funktionella eller dysfunktionella (se elförsörjningsföretaget)? Hur lätt är det att få gehör och snabba beslut (se verkstadsföretaget)?*

5.1.5 En systemrisktriad

Tillsammans bildar de tre huvudområdena en systemrisktriad som kan illustreras så här:

De tre områdena interagerar med varandra. Kunskap och kommunikation är både beroende av värderingar och attityder inom företaget och av själva organisationen. Det handlar om t.ex. ***benägenheten att kommunicera***. Information kan forma inställningar i olika frågor. Attityder och värderingar är av det skälet också ett resultat av kommunkation och kunskap. Organisation och värderingar påverkar varandra genom att värderingar ofta skiljer sig mellan olika avdelningar i företaget samt mellan "högt" och "lågt" i organisationen.

Attityder påverkar även organisationen. Strukturen är självförstärkande på grund av de attityder som den skapar. Organisationen med sina administrativa rutiner och sin ansvarsfördelning påverkar kommunikation och kunskap. Ledningen fattar beslut om organisationsformer med ledning av information som flödar i dessa kanaler. Med detta är systemrisktriaden sluten!

I varje företags systemrisktriad kommer naturligtvis omfattningen av systemriskerna att falla lite olika beroende på t.ex. verksamhetens karaktär. Urvalet av företag i den här rapporten ger en vägledning av den vikt som systemriskfaktorerna inom de tre huvudområdena har för olika branscher. Viktningarna framgår av ***matrisen som följer på nästa sida.*** Ett kryss markerar låg omfattning av systemrisken. Fem kryss innebär omvänt att systemrisken är hög.

Lägg märke till att viktningarna på detta stadium i arbetet ska betraktas som ***illustrationer av en princip*** och inte som exakta resultat av studien.

Illustration av systemriskviktning för de deltagande företagen

Huvudområden för systemrisker	*Verkstadsföretaget*	*Basindustriföretaget*	*Detaljhandelsföretaget*	*Elproduktionsföretaget*	*Fastighetsbolaget*	*Konsumentvaruföretaget*	*Telekomföretaget*	*Kuskapsföretaget*
Kunskapsutveckling och kommunikation	×××	×××××	×××××	××××	××××	××	×	××××
Attityder och värderingar	×××××	×××	×××	×××	×	×××××	×	×
Organisation	×	××	××××	×	×××	×××	××××	××

5.2 En metod för systemriskanalys?

Kunskaperna om systemriskerna ökade efter hand som samtalen med företagens företrädare fortskred. Det framkom att flera av detta resultat knappast skulle ha kommit till genom traditionella metoder för riskanalys. Slutsatsen blev att just samtalen var ett mycket effektivt analysintrument för systemrisker. Samma resultat skulle kunna uppnås genom seminarieliknade gruppdiskussioner mellan flera personer med kunskaper om risker.

Den som svarar för riskhanteringen eller en arbetsgrupp inom ett företag borde med hjälp av en mer specifik riskmatris som ledning eller ”trigger”, och en ganska strikt hållen diskussionsform kunna genomföra systemriskanalys på egen hand. En sådan diskussion borde kunna äga rum under en halv dag och inkludera VD, linjecheferna, riskanvariga samt några företrädare för de anställda. Diskussionen borde ledas av en samtalsledare som styr överläggningarna och som ser till att det blir en öppen anda och att temat följs.

Systemriskområdena skulle kunna behandlas genom fokus på några av de frågor som redovisas i avsnitt 1.2 eller fokuseras på de delområden som förekommer i matrisen nedan. Dessa delområden diskuteras utifrån de medverkande personernas perspektiv och får en ranking efter problemets omfattning. Det är viktigt att låta dessa överläggningar resultera i en kort beskrivning av problemet, motiveringar av riskernas omfattning, förslag till åtgärder och ansvariga personer.Det dokument som växer fram under en sådan diskussion bör vara ett “levande“ dokument som följs upp med nya möten, regelbundet blir ifrågasatt och skickas runt till lämpliga personer inom företaget för kommentarer och kompletteringar. Fördelarna med ett sådant förfarande är flera:

- *En systemriskanalys som fokuserar på underliggande orsaker är sannolikt mycket effektiv i ett förebyggande perspektiv;*

- *En sådan analys kan användas för att skapa mer robusta och standardiserade instrument;*
- *Mindre företag som inte har råd med en specialiserad riskhanteringsfunktion eller med ett mer genomarbetat system för riskhantering kan få snabb och god överblick av hot och risker;*
- *Större företag som har dessa funktioner får en alternativ informationskälla för riskhantering och ett bättre förhållande mellan riskhanteringsfunktionen och övrig ledning;*
- *Kommunikationsvägarna i företaget blir klargjorda;*
- *Systemriskansatsen för upp riskfrågorna till en övergripande ledningsnivå och motiverar riskhantering i ett generellt managementperspektiv;*
- *Systemriskanalysen gör riskhanteringen mer känslig för andra centrala frågor i företaget och vice versa.*
- *Den som svarar för riskhanteringen utvecklas från en expert till en utvecklare i företaget.*

Matrisen på nästa sida tillsammans med exemplet ”Riskanalys på IT-serviceföre-taget” kan fungera som struktur för genomförande och rapporteringsform för denna typ av riskanalys. Det är viktigt att understryka att informationen som framkommer vid en sådan här analys är viktig, men lika viktigt kan vara att sätta igång en process där samtal förs om dessa risker på ledningsnivå i företaget. Systemriskanalys enligt den modell som beskrivs här kan ses som en metod att skapa och vidmakthålla en sådan process.

Systemriskområden	
1. Kunskapsutveckling och kommunikation	1.1 Hur fungerar risk kommunikationen internt i bred mening?
	1.2 Hur fungerar risk kommunikation externt? Alltså med organisationer som påverkar er risk?
	1.3 Hur är de anställdas kunskap om produkter och produktionsformer? --Om företagande och problem? Hur påverkar detta de risker ni tar?
2. Attityder och värderingar	2.1 Ledningens risktagande (å sina egna vägar... samt å företagets vägnar)?
	2.2 De anställdas risktagande? Hur ser företagets risk-kultur ut?
	2.3 Är det lätt eller svårt att kommunicera dåliga nyheter uppåt?
3. Organisation	3.1 Ansvarsfördelning i företaget: täcks alla risker in? Vad faller utanför?
	3.2 Organisationsform och RM i harmoni? Var skapas värde resp. var finns RM?
	3.3 Administrativa rutiner funktionella? Är administrationen riskfylld?
	3.4 Beslutsvägar – ledningens närhet. Känner VD till företagets risker?

Exempel på användning:

Systemriksanalys på ”IT-Serviceföretaget”

Bakgrund

Nedanstående riskanalys bygger på en inbjudan från IT-serviceföretaget att genomföra en interaktiv riskanalys under en halv dag. Övningen genomfördes tillsammans med Tomas Hellström och Ulf Malmquist på FENIX forskarprogram vid Chalmers Tekniska Högskola i Göteborg, samt Handelshögskolan i Stockholm. IT-serviceföretaget är ett bolag inom en större IT/Infocom-koncern, och har ca 800 anställda. De levererar service och helhetslösningar inom IT till hela Sverige.

Metod

Övningen gick ut på att ett antal nyckelpersoner på Serviceföretaget (se deltagarlista) träffades i en seminariemiljö under tre timmar och genomförde en modifierad sk. "metaplansanalys" av risker och hot mot verksamheten. Metaplansanalys är ett sätt att fokusera en problemdiskussion och få snabba och samtidigt djupa svar på en fråga. Frågan för denna övning var "Vilka är de viktigaste riskerna/hoten mot att uppfylla vår verksamhets mål". Övningen inleddes med att deltagarna fick överväga ett antal systemriskfaktorer, (se matrisen ovan) i syfte att få några "triggers" för hur man kan tänka om risk. Deltagarna fick sedan skriva ner ett antal sådana risker sett ur sitt eget perspektiv (minst fem per person) på lappar, med kort beskrivning av varje risk. Därefter satte deltagarna upp dessa lappar på väggen och ordnade dem tillsammans i kluster, eller relevansområden (riskområden). Dessa områden diskuterades sedan i termer av orsak-verkan. Deltagarna fick därefter ett antal markörer var med vilka de kunde vikta de olika riskområdena efter allvarlighet. Avslutningsvis diskuterades de viktade riskområdena av hela gruppen och man försökte fastställa orsaker till riskerna, samt interventioner som skulle kunna avhjälpa några av dem.

Följande arbetsschema användes vid övningen:

Tid	**Aktivitet**
10.00 -- 10.15	Introduktion av vilka mötesledarna är. Presentation av deltagarna. Syftet med övningen. Presentation av riskexempel (se matrisen).
10.15 -- 10.30	Skriva lappar: Minst 5 var och hur många som helst. Ca 1-2 meningar om risker/hot mot verksamheten. *Det går att komplettera med fler lappar under hela övningen/dagen.*
10.30 -- 10.40	Fram till tavlan och sätt upp lapparna, alla på en gång.
10.40 -- 11.00	Flytta lappar och kommunicera fram kluster av lappar som passar ihop. Det är OK att flytta andras lappar. Skriv nya om man vill komplettera.
11.00 -- 11.05	Bensträckare.

11.05 -- 11.45	Diskutera kluster av lappar. Är de giltiga? Verklighetstrogna? Namnge kluster/grupper. Diskutera bakomliggande struktur, kategoriernas karaktär.
11.45 -- 11.50	Dela ut till varje person lika många markörer som kluster. (små magneter eller klisterlappar kan användas)
11.50 -- 12.00	Hela gruppen går fram och viktar grupperna/klustren samtidigt, med hjälp av markörererna (får sättas ut hur som helst)
12.00 -- 13.00	Lunch.
13.00 -- 14.00	Tolkning, reflektion och åtgärdsdiskussion om de viktade riskklustren. Uppsummering.

Resultat av övningen

Deltagarlista

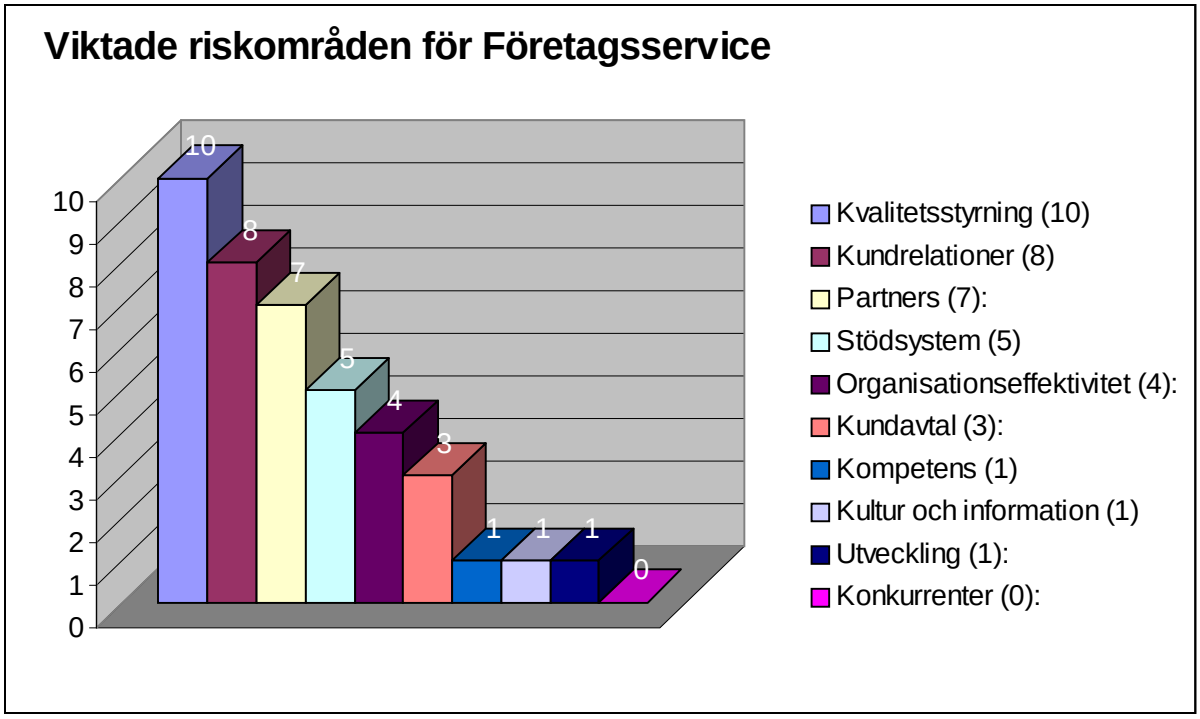
BH, specialistsäljare.

BJ, serviceteamsledare.

AJ, medlem av ledningsgrupp.

LL, ansvarig för marknad och försäljning, medlem av ledningsgrupp.
PL, analystekniker.

I diagrammet på nästa sida redovisas de riskområden som deltagarna identifierade, samt viktningen av dessa områden. Det är viktigt att notera att flera av områden hänger samman på olika sätt, vilket vi kommer att återkomma till senare. Nedan följer dessa riskområden sammanfattade för Serviceföretaget.



Kvalitetsstyrning (viktning 10)
Gruppen observerade ett glapp mellan försäljning och utförande av tjänster, vilket får konsekvenser för kvalitet. Detta glapp innebär att samarbetskedjan mellan projekt, försäljning och service riskerar att bli lidande. Specifikt två aspekter stod ut som viktiga, nämligen (1) fokuserade och regelmässiga kontraktsgenomgångar saknas i denna kedja, samt (2) dokumentation och kunskapsspridning av kunders kommunikationslösningar var bristande. Konsekvensen är i första hand bristande snabbhet i implementeringen av nya affärer. Bättre samarbete behövs med rollfördelning mellan marknadsbolagen inom Koncernen, samt rutinmässig återförsäkran av kontrakt och kundkontakter i produktion och service.

Kundrelationer (8)
Marknadskapitalet är lågt. Hög komplexitet i den kundunika lösningen generar ett högre pris som möts av bristande förståelse hos kund, med betalningsovilja som följd. Ytterligare konsekvenser av hög kundanpassning och samtidig komplexitet i produkten är att kundkraven riskerar att bli orimliga. “Ingen kund vill betala för kundanpassade lösningar, men alla vill ha det”. Hur sker kommunikation/utbildning *vis a vis* kund i dessa frågor? Serviceorganisationen är byggd på standardkoncept och då måste man även göra de kundunika lösningarna mer standardbetonade. En risk som identifierades av gruppen var även kundernas konkurser. Finns framförhållning och kunskap om kundens solvens?

Partners (7)
Partners/leverantörer riskerar att ej tillhandahålla den utlovade servicenivån, visa bristande kompetens i komplex problemlösning, inte hålla leveranstider samt ha ofördelaktig prissättning. I vissa fall håller inte produkterna leverantörernas utfästelse. Det upplevs att det finns dåliga avtal med underleverantörer samt att dessa riskerar att inte förstå (leva upp till) sin del av avtalet. Detta kan avhjälpas med hjälp av en bättre återförsäkran mot leverantörer. En annan riskfaktor utgör reservdelsförsörjningen med problem som utgående sortiment, kvalitetsbrister, logistik och lagerbrister. Lönsamhet kan försvinna pga högre kostnader, skrotning, material samt nya revisioner. Det finns även negativa effekter av intern konkurrens inom Koncernen. Detta är möjligtvis inte en partnerfråga utan snarare en fråga om den övergripande styrmodellen (se organisationseffektivitet).

Stödsystem (5)
Stödsystemen hindrar effektivt arbete, och är sällan anpassade för situationen. Detta innebär att flexibla stödsystem saknas för kundunika lösningar. Stödsystem med sådan flexibilitet skulle bl.a. innehålla uppdaterad kundinformation om avtal samt vilken utrustning som kunden sedan tidigare har, vilket skulle leda till att kundens förtroende ökar.

Organisationseffektivitet (4)
Organisationen måste strukturera erbjudande mot kund och effektivt kommunicera behov internt samt möjligheter att uppfylla dessa behov. Detta försvåras av bl.a. två faktorer. (1) En ekonomisk styrmodell byggd på intern konkurrens och nyttomaximering främjar inte samarbete inom Serviceföretaget, eller mellan Serviceföretaget och övriga Koncernen. (2) Organisationen är inte anpassad efter kund utan snarare tvärtom, med andra ord Serviceföretaget bör eftersträva anpassning mot att arbeta process/kundorienterat med klar avvägning mot linjeorganisation. Det upplevs som om det finns för många beröringspunkter (interface) inom både Koncernen och Serviceföretaget. Det processorienterade arbetssättet har inget stöd i organisationen i stort.

Kundavtal (3)
Komplexiteten i stora avtal gör att marknadsbolagens säljkår tecknar avtal utan att tillräckligt väl kontrollera täckning av servicesidan. Först efter det att affären är gjord uppdagas brister i möjligheterna att leva upp till det slutna avtalet. Detta påverkar lönsamheten då prissättningen blir för låg, det påverkar kundrelationer då avtal ej kan uppfyllas, reservdelar ej finns tillgängliga, kompetens, inställelse- och åtgärdstid inte matchar behov (geografiska orsaker såväl som tekniska finns för dessa problem).

Kompetens (1)
Risken att förlora personal, främst med hög teknisk kompetens är alltid närvarande. Viktigt i detta avseende är hög kompetens i säljled för affärsutveckling och för drivande av komplexa affärer. Ett annat behov som nämns är att skaffa kompetens i takt med teknikutveckling, samt egen resursinventering i termer av sådana kompetensbehov. Dessutom krävs kunskap och framförhållning inom Serviceföretaget för att kunna parera då personal slutar och tar sin egen kompetens såväl som kundkompetens med sig. I kompetenshänseende identifierades även risken i att åldersammansättningen inom Serviceföretaget är hög med många medarbetare som är +50 år. Tas deras kompetens tillvara, samt hur mottagliga och motiverade är de för att utveckla ny kompetens?

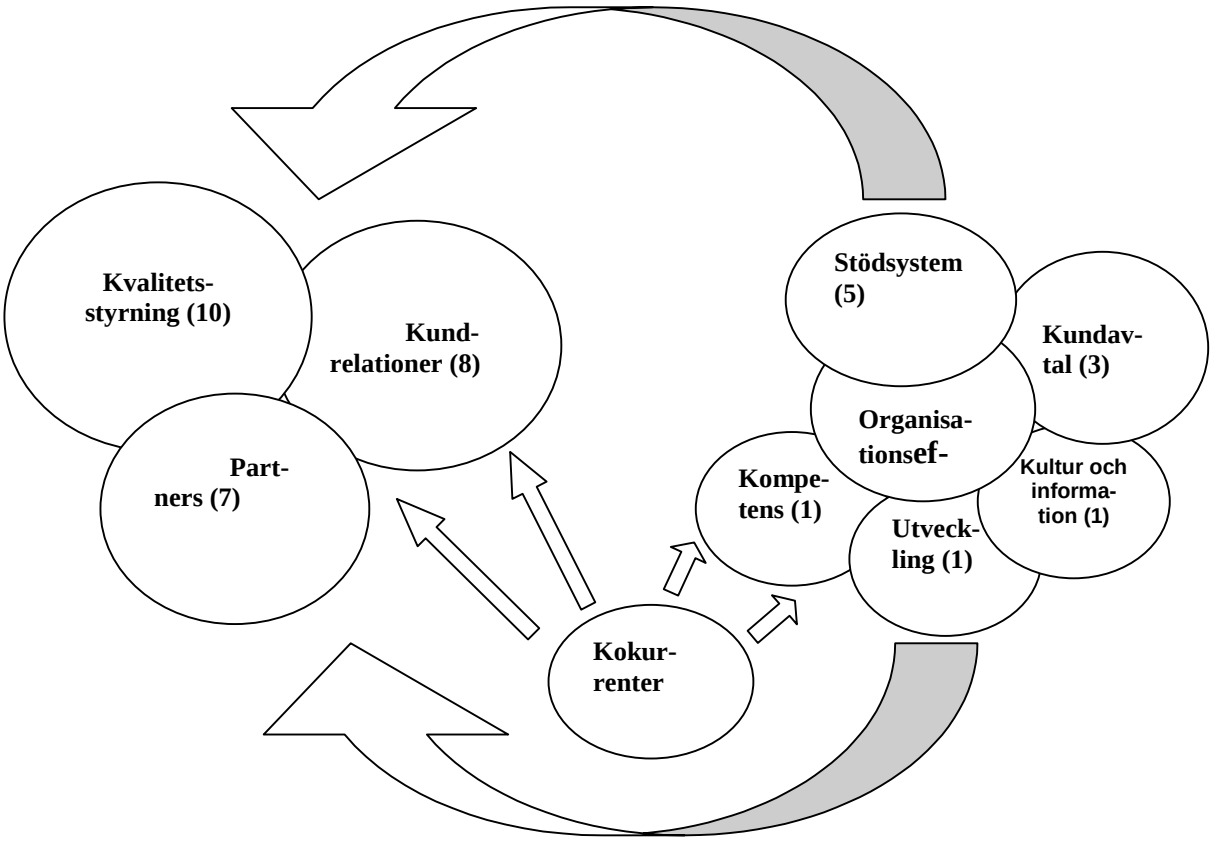
Kultur och information (1)
Inom Serviceföretaget finns en äldre mentalitet från tiden innan bolagiseringen med hänsyn till kundbemötande och arbetseffektivitet. Denna mentalitet passar inte Serviceföretaget nya affärslogik med dynamiska och kundanpassade lösningar. Samtidigt är den svår att förändra, då attityder och värderingar hos enskilda medarbetare tar lång tid att påverka och förändra. En upplevd risk med avseende på information är personalens bristande insikt i överenskommelser och kundavtal med avseende på totalaffären. Detta gäller även säljares insikt i produktion.

Utveckling (1)
Ett av gruppen identifierad risk är utvecklandet av tjänster i takt med teknikutveckling och kundbehov. Detta pga en upplevelse av att många utvecklingsprojekt ej blir genomförda.

Konkurrenter (0)
Risk med avseende på konkurrenter är att dessa vinner kunder från Koncernen genom att utveckla nya produktkoncept, samt genom att kunna erbjuda förmånliga priser för kunderna. Även rekrytering av egen kompetent personal till konkurrenter upplevs som en risk.

Reflektion och slutsatser

Efter att ha analyserat riskområdenas beskrivning och viktning, har en preliminär riskmodell vuxit fram vilken ser ut på följande sätt:



Vi ser *kvalitetsstyrning, kundrelationer* och *partners* (vänster sida) som de områden som är mest utsatta för risk, samt *stödsystem, kundavtal* etc. (höger sida), som faktorer som i första hand orsakar risk. I den senare gruppen av faktorer bör i denna tolkning åtgärder sättas in för riskreducering, snarare än direkt i den första gruppen. Den vänstra gruppen utgörs av generellt

mycket komplexa faktorer vilka troligtvis är svåra att utöva direkt påverkan på. Några korta slutsatser med avseende på riskreducerande åtgärder är som följer.

Gruppen ser marknadsbolagen som en återförsäljarkanal, och relationen där emellan fungerar inte alltid till belåtenhet. Det finns brister i processen, främst avseende på överlämning mellan olika enheter. Det upplevs som om de koncerninterna bindningarna hindrar. Ytterligare ett problem som upplevs är att marknadsbolagens säljare inte är lika intresserade av servicefrågor, mycket beroende på att service endast omfattar ca 15% av marknadsbolagens omsättning.

Serviceföretaget har en kordinatorroll för leveransen. Denna roll finns mellan flera, både interna och externa, partners. Dessutom finns en tveksamhet om vilka krav som Serviceföretaget kan rikta mot dessa partners, mycket beroende på att Serviceföretaget inte kunnat påverka avtalet/affären från början utan kommer in i ett senare skede.
Synpunkt: *Ett samarbete bör utarbetas mellan de ingående parterna, och ett sätt är att göra en gemensam genomgång av kontrakt/avtal innan detta sluts. En förutsättning för detta är att klart tydliggöra den egna affären, och göra Serviceföretaget erbjudande tydligt. För denna process bör bildas ett specifikt forum.*

Kvalitetsstyrning, affärsstöd och implementering av avtal är tre faktorer som upplevs påverka varandra.

Synpunkt: *Information om affärer och avtal i god tid till teknikersidan är en åtgärd som kan förhöja kvaliteten i det utförda arbetet, då förberedelsetiden ökar för att ta fram kunduppgifter och förvärva nödvändig kompetens. Detta skulle ge en lönsamhet på sikt, om än en initial tidsåtgång.*

Ytterligare åtgärd som nämns vid analysen är att utse ansvariga från servicesidan vid kontraktsgenomgångar.

Synpunkt: *Möjligheten att diskutera olönsamma uppdrag från servicesidan upplevs som begränsad och bör stödjas.*

Ledarskapet, både på högre och lägre nivå, uppfattades som viktigt. Mandatet upplevs som utdelat från högre (verkställande ledning) till lägre (teamledare) nivå, främst vid handhavandet av olönsamma uppdrag. Men samma mandat upplevs inte i verkligheten av den lägre nivån. En uppfattning är att problem löser sig bättre i en konfliktsituation, då det är påtagliga meningsskiljaktigheter som skall lösas. En mentalitet som innebär att ständigt remitera beslut till lägre instans finns, med resultatet att information stannar i mellanledet och inte når den enskilde medarbetaren. Detta då besluten saknar förankring i lägre led, vilket gör att i diskussion mellan teamledare och medarbetare om fattat beslut, slutar med att teamledaren inte kan föra fram beslutet med samma kraft som högre nivå.

Synpunkt: *Det är viktigt på medarbetarnivå att veta vilka personer och funktioner som finns inom Serviceföretaget.*