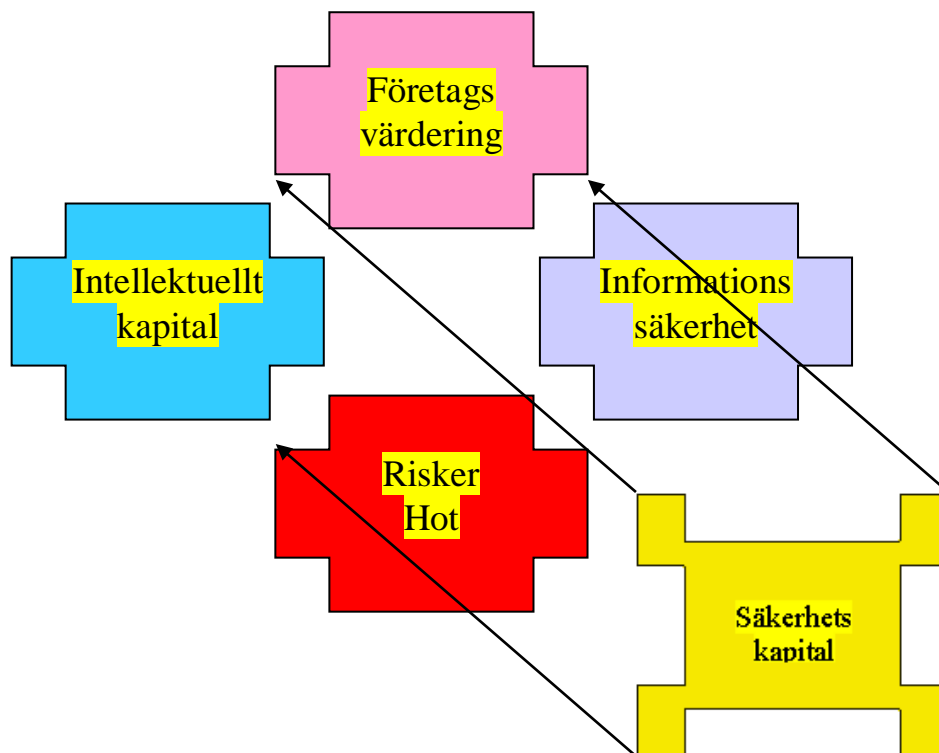


# Säkerhetskapital

## En del av det Intellectuella Kapitalet



# Sammanfattning

Titel	Säkerhetskaptal, en del av det Intellectuella Kapitalet
Författare	Victor Adolfsson
Adress	Folkparksvägen 12:24 372 38 Ronneby
E-mail	pt97vad@student.bth.se
Handledare	Andreas Jacobsson, <a href="mailto:andreas.jacobsson@bth.se">andreas.jacobsson@bth.se</a> Anders Hederstierna, <a href="mailto:anders.hederstierna@bth.se">anders.hederstierna@bth.se</a> Anders Nilsson, <a href="mailto:anders.nilsson@bth.se">anders.nilsson@bth.se</a>
Institution	Institutionen för Ekonomi och Management vid Blekinge Tekniska Högskola.
Kurs	Kandidatarbete i Företagsekonomi
Datum	Rapporten skrevs januari 2002-maj 2002 och presenterades juni 2002.
Nyckelord	Intellectuellt kapital, informationssäkerhet, risk, säkerhetskaptal
Problem	Det saknas metoder att mäta informationssäkerhet inom företag och företagets tillgångar har förändrats från ett fokus på maskiner och råvaror till kunskap (intellectuellt kapital). Rapporten utforskar om det finns delar av företags intellectuella kapital som beskyddar företagets tillgångar och processer. Detta kapital kallas säkerhetskaptal. Hur skulle företags informationssäkerhet kunna tydliggöras genom dess intellectuella kapital och hur kan begrepp inom informationssäkerhet och företagsvärdering hänga samman?
Syfte	Att förstå hur informationssäkerhet är relaterat till intellectuellt kapital.
Metod	Rapporten bygger på litteraturstudier om intellectuellt kapital och informationssäkerhet. Data har samlats in från dels börsnoterade företags årsredovisningar och dels från pressreleaser och börsinformation. Denna information har sedan analyserats både kvantitativt och kvalitativt och begreppet säkerhetskaptal har växt fram.
Teori	Teorier om företagsvärdering, intellectuellt kapital, risk management och informationssäkerhet presenteras och blir den referensram i vilket begreppet säkerhetskaptal sätts i sitt sammanhang.
Analys	Begreppet säkerhetskaptal presenteras i form av modeller och situationer vari olika perspektiv på säkerhetskaptal analyseras och utvärderas.
Slutsatser	Slutsatserna är främst i form av modeller och beskrivningar av hur man kan se på säkerhetskaptal i förhållande till intellectuellt kapital och andra begrepp. Området är komplext men delar av resultaten (som är på en hög abstraktionsnivå) kan användas för att värdera andra typer av immateriella tillgångar.

# ABSTRACT

Title	Security Capital, one part of the Intellectual Capital
Author	Victor Adolfsson
Adress	Folkparksvägen 12:24 372 38 Ronneby
E-mail	<a href="mailto:pt97vad@student.bth.se">pt97vad@student.bth.se</a>
Supervisors	Andreas Jacobsson, <a href="mailto:andreas.jacobsson@bth.se">andreas.jacobsson@bth.se</a> Anders Hederstierna, <a href="mailto:anders.hederstierna@bth.se">anders.hederstierna@bth.se</a> Anders Nilsson, <a href="mailto:anders.nilsson@bth.se">anders.nilsson@bth.se</a>
Department	The Institution for Business Administration and Management, Blekinge Institute of Technology
Course	Bachelor thesis in Business Administration
Date	The report was written January 2002 to May 2002 and was presented in June 2002.
Keywords	Intellectual capital, information security, risk, security capital
Problem	There is a lack of methods to measure information security within companies and the assets of a company have shifted from a focus on machines and material towards knowledge (intellectual capital). This report investigates if there are parts of the intellectual capital that protects the company's assets and processes. This asset is called Security Capital. In what way could a company's information security be visualized through its intellectual capital, and how could the concepts from information security and intellectual capital be related to each other.
Purpose	To understand how information security is related to intellectual capital.
Method	The report is built upon literature studies about intellectual capital and information security. Data has been gathered partly from annual reports and partly from press releases and stock information. This information has been analysed both quantitatively and qualitatively and the concept of Security Capital has grown forth.
Theory	Theories of valuation of companies, intellectual capital, risk management and information security are presented and will be a frame of reference to which Security Capital has been put into context.
Analysis	The concept Security Capital is presented through models and situations from which different perspectives of Security Capital are analysed.
Results	The conclusions are mainly in the shape of models and descriptions of how Security Capital can be looked upon in relation to intellectual capital. The area is complex but parts of the results (which are on a high level of abstraction) can be used to value other types of immaterial assets.

# Förord

Arbetet med denna rapport startade i januari 2002 efter ett kandidatarbetsförslag från Andreas Jacobsson. Jag missförstod hans idéer lite och skrev en beskrivning delvis baserat på hans tankar och delvis på mina egna funderingar om intellektuellt kapital och dess egenskaper. Jag vill tacka Andreas Jacobsson och hans rödpenna som gjort ett bra jobb som handledare med att förbättra och ge feedback till mig i mitt arbete. Jag vill även tacka Anders Nilsson och Anders Hederstierna för givande samtal och feedback på rapporten.

Ett tips till kommande kandidatarbetskrivare är att försök att undvika att skriva ensam då man ibland tappar motivation och inte har någon att bolla idéer och tankar med.

Ronneby, den 28 maj 2002

Victor Adolfsson

# Innehållsförteckning

Problem.....	7
Problembakgrund.....	7
Problemdiskussion.....	7
Problemformulering.....	8
Syfte.....	8
Avgränsning.....	8
Disposition.....	9
Metod.....	10
Litteraturstudier.....	10
Sekundärdata.....	10
Teoriserande.....	11
Empirisk Säkerhetskaptalanlys.....	11
Teoretisk Säkerhetskaptalanlys.....	11
Förkastade metoder.....	12
Övrigt.....	12
Teoretiska perspektiv.....	13
Företagsvärdering.....	13
Marknadsvärde.....	13
Immateriella tillgångar.....	14
Information.....	18
Risk Management.....	20
Operativ risk.....	22
Årsredovisningsundersökning.....	25
Kvantitativt resultat.....	26
Analys.....	26
Behov av tydlig säkerhet.....	27
Försäkra sig mot risker?.....	28
Banker och kapitaltäckningsregler.....	28
Analys.....	30
Företagsvärderingsperspektiv på informationssäkerhet.....	30
Empirisk säkerhetskaptalanlys.....	31
1. Marknaden värderar säkerhetsinvesteringen.....	32
2. Värdera säkerhetsinvesteringen efter kostnad.....	34
3. Säkerhetsinvesteringen värderas efter konsekvenser den skyddar mot.....	34
4. Företaget värderar säkerhetsinvesteringen.....	35
Avrundning.....	36
Teoretisk säkerhetskaptalanlys.....	37
Kapitaltäckningskrav.....	40
Hur förhåller sig säkerhetskaptalanlys till kapitaltäckningsbegreppet?.....	40
Slutsatser.....	42
Årsredovisningsundersökning.....	42
Modeller och metoder.....	42
Värdering av säkerhet.....	42
Egna reflektioner.....	43
Är Edvinssons modell över intellektuellt kapital en absolut sanning?.....	43
Finns det ett optimalt säkerhetskaptalanlys?.....	43
Hur kan man jämföra informationssäkerhet i två företag?.....	43
Hur kommer bankerna att mäta sina operativa risker?.....	43

Hur kan man bestämma ”trögheten” i det intellektuella kapitalet? .....	44
Kritik .....	44
Tillgång till information .....	44
Referenser .....	45
Tryckta källor .....	45
Lagtexter .....	45
Internetkällor .....	45
Årsredovisningar 2001 .....	47
Bilagor .....	50
Bilaga 1 Årsredovisningsundersökning .....	50
Bilaga 2 Förklaring till årsredovisningsundersökningen .....	51
Bilaga 3. Utdrag Microsoft aktiekurser (dollar) .....	52

### **Tabell och figurförteckning**

Tabell 1 Säkerhetsaspekter enligt ISO-17799 .....	21
Tabell 2 Proaktiv och reaktiv säkerhet .....	21
Tabell 3 Riskanalysbegrepp .....	23
Tabell 4 Kvantitativ empirisk undersökning .....	26
Tabell 5 Beskrivning av x-faktorn .....	35
Tabell 6 Perspektiv på riskanalys .....	37
Tabell 7 Säkerhetskapitaltyper .....	38
Tabell 8 Årsredovisningsundersökning .....	50
Tabell 9 Förklaring till årsredovisningsundersökningen .....	51
Tabell 10 Börskurser Microsoft - vid säkerhetsåtgärden .....	52
Figur 1 Marknadsvärde, finansiellt och intellektuellt kapital .....	13
Figur 2 Relativvärdets förändring från jordbrukssamhälle till kunskapssamhälle .....	14
Figur 3 Intellektuellt kapital enligt Edvinsson .....	16
Figur 4 BSC-modellen .....	18
Figur 5 Riskförhållande .....	26
Figur 6 Microsofts börskurs november 2001-maj 2002 .....	32
Figur 7 Säkerhetskapital. Hots inverkan på processer och tillgångar .....	37
Figur 8 Risk-sårbarhetsanalys .....	38
Figur 9 Riskskala .....	39
Figur 10 Kapitaltäckning och säkerhetskapital .....	40

# Problem

*Denna sektion redovisar bakgrunden till rapporten, vilken problemformulering som valts, syftet och vilka avgränsningar som gjorts.*

## **Problembakgrund**

Företag och organisationer består idag till stor del av intellektuellt kapital (se figur sida 16). Då företagets alla delar knyts samman i informationsnätverk och informationssystem så ökar tillgängligheten men även sårbarheten, hoten och riskerna för företaget. Därför behövs en helhetssyn på vad hot, risker och konsekvenser kan kosta företag och organisationer om företagen inte åtgärdar dem. Intellektuellt kapital är en del av företagets värde enligt vissa värderingsteorier. Förespråkare för intellektuellt kapital (Leif Edvinsson, Thomas Stewart) har tagit fram verktyg för hur man kan sätta värde på sådana icketangibla faktorer som humankapital, strukturkapital och organisationskapital. Inom informationssäkerhetsområdet däremot saknas metoder för att mäta informationssäkerhet.

Företag och organisationer för till sina processer in resurser och förädlar dessa och förväntar sig att få ett resultat som är större än summan av alla införda resurser. I affärsprocessen används informationssystem som kan drabbas av incidenter och påverka företagets förädlingsförmåga, effektivitet och lönsamhet. Det kan vara allt från förseningar, kvalitetsförsämringar och oplanerade kostnadshöjningar. Detta påverkar företagets resultat och vinstmarginaler på ett negativt sätt.

## **Problemdiskussion**

Affärsprocessen i dagens kunskapssamhälle består inte längre bara av maskiner, råvaror, energi eller naturtillgångar som går att mäta direkt utan den består till stor del av intellektuellt kapital (se sida 14) som är svårt att mäta. Teorier om intellektuellt kapital fokuserar inte på säkerhet och värdebevarande utan på värdeökning. Mer grundläggande vore att utreda de värdebevarande tillgångarna, de tillgångar i företaget som på olika sätt skyddar verksamheten från kostnadsökningar och intäktsbortfall, i det intellektuella kapitalet. Dessa tillgångar kallas i rapporten för säkerhetskapital. Detta är ett nytt begrepp och ska inte förväxlas med det säkerhetskapital som utgör en buffert för att klara eventuella störningar i driften och på marknaden. Det säkerhetskapitalet<sup>1</sup> är en sorts likviditetsreserv och brukar beräknas som en procentsats av omsättningen.

En analys av ett företags säkerhetskapital kan också användas för att hitta punkter som är överbeskyddade och som därmed är kostnadsineffektiva (kostar mer än de smakar). Konsekvenser av hot kan vara av formen bortfall av finansiellt kapital och vissa hot kan bäst motverkas genom investering i intellektuellt kapital. Frågan är då när och om man ska göra en investering och hur den påverkar företagets lönsamhet. Intellektuellt kapitalområdet och informationssäkerhetsområdet är båda relativt nya och ”omogna” områden där forskning pågår. Företag använder flera olika begrepp och beskriver dessa områden på olika sätt och i olika omfattning vilket upptäcktes i empirin och presenteras i sektionen *Årsredovisningsundersökning* (sida 24).

---

<sup>1</sup> Skärvad Per-Hugo & Olsson Jan, ”Företagsekonomi 99 Faktabok”, 2000, Liber ekonomi, Sverige

### **Problemformulering**

Hur skulle företags informationssäkerhet kunna tydliggöras genom dess intellektuella kapital (i rapporten kallat säkerhetskapital) och hur kan begrepp inom informationssäkerhet och företagsvärdering hänga samman?

### **Syfte**

Syftet med rapporten är att förstå hur informationssäkerhet är relaterat till intellektuellt kapital. I rapporten utforskas de delar av det intellektuella kapitalet som kan klassificeras som ett säkerhetskapital, ett kapital som skyddar företagets totala kapital och förädlingsförmåga. Detta gör att företag kan få en helhetsyn på informationssäkerhet. På sikt leder detta till ökad förståelse för informationssäkerhet genom teorier om intellektuellt kapital så att företag kan operationalisera sin informationssäkerhet och få ett större beslutsunderlag.

Säkerhetskapitalbegreppet kan användas av företag för att hitta svaga punkter som de kan eliminera för att minska sannolikheten för att incidenter får allvarliga konsekvenser. Rapporten försöker också förklara hur säkerhetsåtgärdsbeslut kan påverka marknadsvärdet. Sammanfattningsvis så ska rapporten försöka öka förståelsen för hur informationssäkerhet kan ses som en tillgång i företag.

### **Avgränsning**

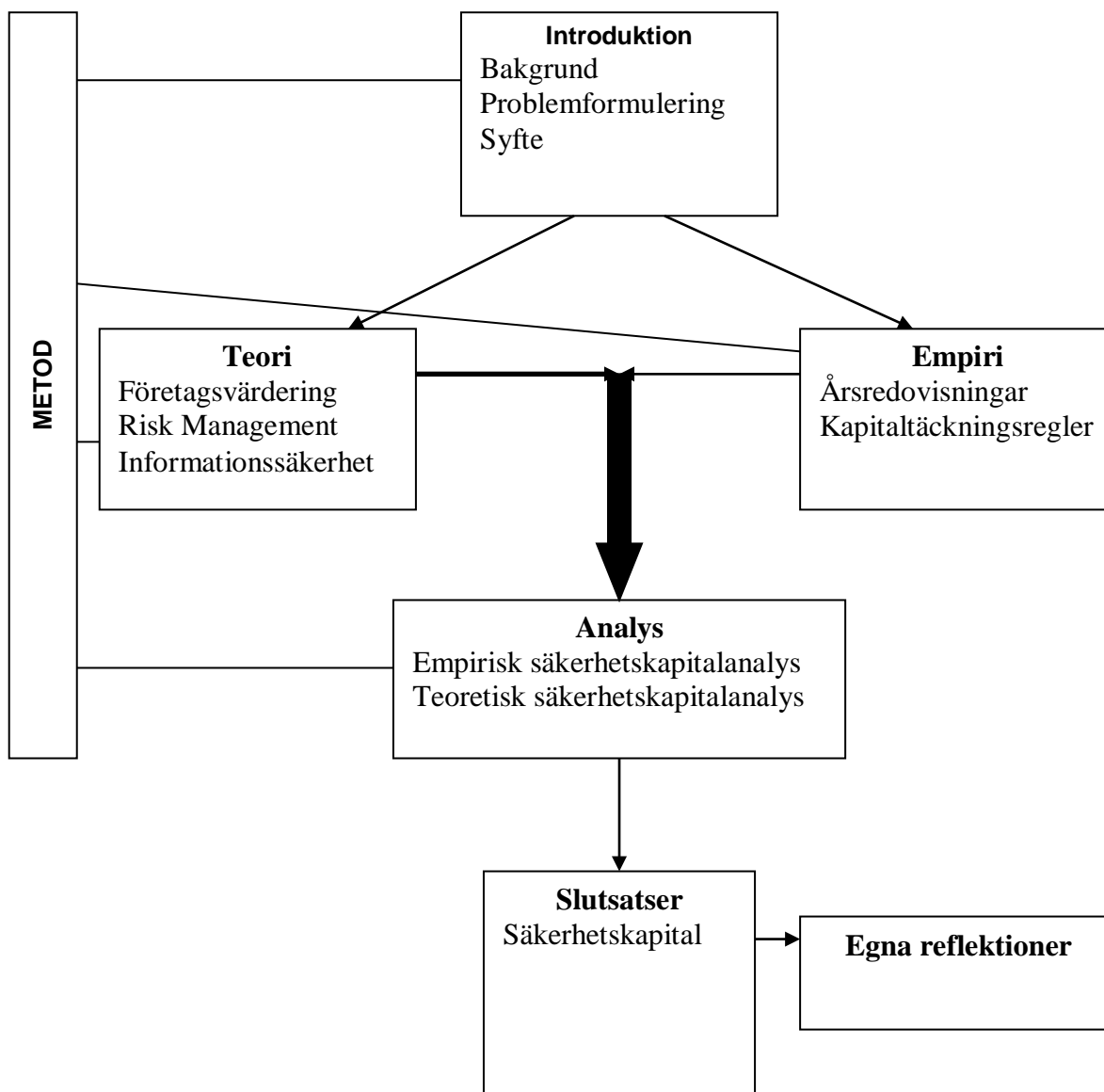
Fokus för rapporten ligger i gränslandet mellan informationssäkerhet och intellektuellt kapital men även kopplingen till finansiellt kapital kommer att göras. Rapporten utger sig inte för att vara heltäckande eller vattentät utan snarare kan den vara en grund att stå på för att förstå förhållandet mellan informationssäkerhet och intellektuellt kapital samt hur man kan använda vetenskapen om detta förhållande för att underlätta beslutsfattande. Rapporten och dess slutsatser kan därmed vara en grund för vidare forskning över hur man kan analysera säkerhet i ett ekonomiskt perspektiv.

Insamlandet av empiri avgränsades till att endast omfatta företags årsredovisningar från år 2001 noterade på den svenska börsens A-lista (mest omsatta) samt Microsofts börskurser, pressreleaser och ur informationssäkerhetssynpunkts relevanta nyheter. Detta gjorde att urvalet är avgränsat till storföretag men fördelen är att företagen verkar i olika branscher.



## Disposition

Följande disposition visar hur rapportens olika delar är kopplade till varandra. Analyssektionen är en sammanvävning av Teori och Empirisektionerna. Tonvikten i analysen kommer dock från Teorisektionen. Anledningen till detta förklaras mer i metodavsnittet. Författaren har valt att inte åtskilja empiri från analys i de olika sektionerna i rapporten. Exempelvis så analyseras den insamlade årsredovisningsinformationen i sektionen *Årsredovisningsundersökning*.



# Metod

*Denna sektion tar upp vilka metodöverväganden som gjorts under arbetets gång. Även förkastade metoder och idéer tas upp för att läsaren ska förstå vilka tankebanor som förelåg arbetet med rapporten.*

## Litteraturstudier

Böcker, artiklar och webbsidor har studerats för att få förståelse om de olika begrepp och teorier som är relaterade till informationssäkerhet och intellektuellt kapital. Resultatet av dessa litteraturstudier presenteras delvis i sektionen *Teoretiska perspektiv*. De funna teorierna utgjorde min referensram i de fortsatta studierna och detta var ett deduktivt angreppssätt. Intellektuellt kapital-modellen som presenteras är främst baserad på Edvinssons arbete med intellektuellt kapital. Jag har funnit att det inte finns så stora skillnader mellan de olika förespråkarnas (Stewart, Saint-Onge, Roos) teorier och inom ramen för detta arbete hade vilken av deras modeller som helst fyllt sin funktion som ”ankare” eller bas för säkerhetskapitalet. Det fanns tyvärr ingen direkt information att tillgå inom det område jag valt att utforska, nämligen gränslandet mellan intellektuellt kapital och informationssäkerhet.

## Sekundärdata

För att få en aktuell bild på företagens syn på vikten av informationssäkerhet och intellektuellt kapital och vilka begrepp som används så studerades årsredovisningar för år 2001. Urvalet av företags årsredovisningar gjordes genom att studera de bolag som noterats på Stockholmsbörsens A-lista som mest omsatta<sup>2</sup>.

Följande sökord användes i datainsamlingen:

*sårbarhet, säkerhet, kapital, intellektuell, risk och information.*

Dessa sökord användes för att få en bild av hur de utvalda företagen ser på riskhantering, typer av risker, informationssäkerhet, värdering av intangibelt kapital såsom humankapital, strukturkapital och kundkapital. Resultatet av den undersökningen presenteras kvantitativt i Tabell 4 Kvantitativ empirisk undersökning, på sida 21. Undersökningen var både kvantitativ och kvalitativ då jag ville finna så många nyanser av begreppen som möjligt för att bättre kunna förstå dem i sitt sammanhang och även för att öka förståelsen på hur dessa begrepp höll på att utvecklas. ”Nätet” som här kastades ut gav nämligen i sin tur upphov till nya områden att utforska, bland annat om nya regler för mätning av operativa risker. Resultatet av denna empiriska undersökning presenteras i sektionen *Årsredovisningsundersökning*.

Under undersökningens gång hittade jag ett begrepp (kapitaltäckningsregler) som presenteras under rubriken Kapitaltäckningsregler under analyssektionen. Detta begrepp fann jag viktigt då det tar upp kopplingen mellan kapital och risker, två centrala begrepp inom det område jag valt att utforska, nämligen informationssäkerhet och intellektuellt kapital. I den sektionen byggs en modell upp i form av en figur som visar hur jag ser på sambandet mellan risk, kapitaltäckningskrav och det nya begreppet säkerhetskapital. Säkerhetskapital är främst beskrivet på sida 37

---

<sup>2</sup> [http://epi.bolagsfakta.se/borsbolag/default.asp?f\\_companyalpha=&f\\_tickeralpha=&f\\_swestocklist=33&f\\_search=&f\\_reportalpha=&f\\_lineofbusiness=](http://epi.bolagsfakta.se/borsbolag/default.asp?f_companyalpha=&f_tickeralpha=&f_swestocklist=33&f_search=&f_reportalpha=&f_lineofbusiness=)

## **Teoriserande**

Då denna rapport är mer av utforskande, skrivbordsforsknings- eller teoriserande karaktär så fann jag det svårt att hitta direkt relaterad empiri att använda i analysen. Med skrivbordsforskning menas sådan forskning där man enbart samlar in sekundärdata<sup>3</sup>. Därför har jag valt att dela upp analysen i två delar *Empirisk Säkerhetskaptalanalys* och *Teoretisk Säkerhetskaptalanalys*.

## **Empirisk Säkerhetskaptalanalys**

I Empirisk Säkerhetskaptalanalys utgår jag från en verkligt uppmätt situation och försöker analysera den ur ett företagsvärderings och informationssäkerhetsperspektiv och samtidigt applicera begreppet säkerhetskaptal på den situationen och utifrån fyra perspektiv där säkerhetskaptalet värderas på olika sätt.

Detta är ett slags dynamiskt perspektiv och jag fann det intressant att sätta in säkerhetskaptalet i en halvtentativ situation för att förstå förändringar i företagets olika "värdebärare" (intellektuellt kapital, finansiellt kapital, se sektionen *Kapitalvärdering och Informationssäkerhet*) över tiden när man fattar beslut<sup>4</sup>.

Den empiriska säkerhetskaptalanalysen utgick från en sökning på [www.idg.se](http://www.idg.se) efter ordet säkerhetssystem för att hitta en situation där ett börsnoterat företag tillkännagivit ett beslut om en säkerhetsåtgärd. På den fjortonde platsen fanns exemplet som sedan valdes för analys, att Microsoft utsett en säkerhetsstrateg. Kurserna för Microsoftaktien hämtades från Nasdaq ([www.nasdaq.com](http://www.nasdaq.com)) medan pressreleaser hämtades från Microsofts hemsida. Fyra olika perspektiv på hur man kan värdera säkerhet identifierades och testades. Dessa var marknads-, kostnads-, konsekvens- och företagsvärderingsperspektiv. Därefter analyserades dessa halvt empiriska, halvt tentativa situationer i tur och ordning.

## **Teoretisk Säkerhetskaptalanalys**

Här analyserar jag och teoriserar kring det nya begreppet säkerhetskaptal i text och modeller och hur det förhåller sig till de begrepp som presenteras i teorisektionen (*Teoretiska perspektiv*). En brist i denna analys är att modellerna helt baseras på teoretiska perspektiv och egna tankar, d.v.s. den är inte kopplad till någon direkt empiri. Anledningen till detta beror på att ämnet jag valde var ett mer teoretiskt och abstrakt, vilket gjorde det svårt att hitta och använda något slags empirimaterial. Jag försöker med introspektion<sup>5</sup> förstå och förmedla hur informationssäkerhet och intellektuellt kapital kan vara relaterat till varandra, d.v.s. hur säkerhetskaptalet skulle kunna vara uppbyggt. Detta presenteras i figurer som ska korrelera med övriga relaterade begrepp som beskrivs i teorisektionen *Kapitalvärdering och Informationssäkerhet*. De olika begreppen kopplas samman i figurer som används för att beskriva för läsaren hur säkerhetskaptalet skulle kunna verka i olika situationer. Då introspektion bygger på iakttagelse av egna föreställningar och ens föreställningar i sin tur beror på vad man lärt sig så är föreställningarna på något sätt påverkade av en verklighet man har iakttagit. Därmed anser jag att jag har belägg för att introspektion är en gångbar teknik vid sådan här typ av vetenskaplig forskning (teoriserande) när ingen direkt empiri fanns att tillgå.

<sup>3</sup> <http://www.san.fuf.org/forskningsprocessen.pdf>

<sup>4</sup> Eneroth Bo, "Hur mäter man vackert", 1987, Bokförlaget Natur och Kultur, Sverige

<sup>5</sup> Ibid

Då rapporten syftar till att förstå hur informationssäkerhet är relaterat till intellektuellt kapital så valde jag att utveckla ett begrepp (säkerhetskaptal) som ska täcka en given bit av verkligheten (informationssäkerhet som en del av det intellektuella kapitalet) så används en kvalitativ ansats i analysarbetet. För detta arbete har jag valt att arbeta efter en variant av begreppsbildningsmetoden<sup>6</sup>.

1. Avgränsa företeelsen (säkerhetskaptal)
2. Hämta data ur företeelsen
3. Sammanför lösryckta data till olika kvaliteter

Om man ansätter denna metod på problemet med säkerhetskaptal får metoden följande mer explicita riktlinjer.

1. Beskriv säkerhetskaptal i relation till övriga teorier och begrepp
2. Utsätt modellen (säkerhetskaptal) för en situation och olika perspektiv
3. Dra slutsatser från de teoretiskt beskrivna situationerna för att beskriva och revidera säkerhetskaptal som begrepp

I denna analys studeras säkerhetskaptal ur ett statistiskt perspektiv i den meningen att säkerhetskaptalens beståndsdelar och relationer med existerande begrepp klargörs.

### **Förkastade metoder**

Metoder som tidigare varit i diskussion var att intervjua företagsledare om deras intellektuella kapital och informationssäkerhet. Flera problem identifierades rörande detta. En första tanke var att djupstudera två företag med avseende på vad som går att mäta vad gäller informationssäkerhet och intellektuellt kapital. Utfallet från dessa två intervjuer skulle sedan kunna användas när man studerade och intervjuade de övriga företagen. Resultatet hade förmodligen blivit mediokert då företag inte mäter intellektuellt kapital i någon egentlig bemärkelse och dessutom skulle en del företag kunna vara återhållsamma med att lämna ut information rörande informationssäkerhet. Dessutom skulle intervjuareffekten göra sig påmind då flera företagare inte använder begreppet intellektuellt kapital. Den intervjuade skulle därmed bli påverkad av min beskrivning av vad intellektuellt kapital var och risken var att intervjuerna enbart skulle bekräfta mina egna tankar om intellektuellt kapital och informationssäkerhet. Även enkätvarianten var uppe på diskussion men då kopplingen intellektuellt kapital och informationssäkerhet ej gjorts tidigare så bestämdes att tyngden skulle ligga på att just analysera den kopplingen utifrån ett teoretiskt perspektiv ("skrivbordsforskning"). Därmed har ingen primärdata samlats in utan empirin är begränsad till sekundärdata i form av årsredovisningar, nyheter och börsinformation som dock endast använts i begränsad omfattning i analysen utan mer förstärkt bilden av att det är ett relevant problem att diskutera (oklarheter i hur företag presenterar sitt intellektuella kapital och att det inte finns några egentliga sätt att mäta och värdera informationssäkerhet).

### **Övrigt**

Jag har valt att redovisa källor i fotnoter på den sida där källan använts för att öka läsbarheten och snabbt tillåta läsaren av rapporten att dra slutsatser över de olika påståendenas trovärdighet. När jag använder ordet investering i denna rapport är det inte bundet till att investeringen sätts upp som en tillgång i balansräkningen. Vidare så används ordet åtgärd synonymt med ordet investering i rapporten.

---

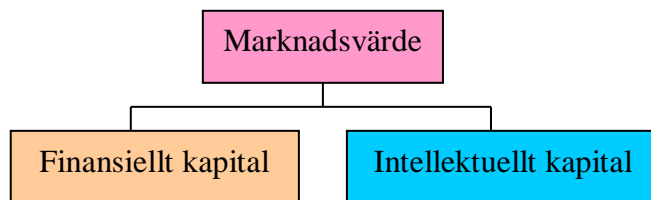
<sup>6</sup> Eneroth Bo, "Hur mäter man vackert", 1987, Bokförlaget Natur och Kultur, Sverige

# Teoretiska perspektiv

*Företag kan idag värderas utifrån många olika modeller. Denna sektion belyser några av dessa olika modeller och tillhörande begrepp för att ge en bild av hur företag kan värderas och vad risker och informationssäkerhet är för något. Dessa begrepp behöver klargöras och förstås då de sätts in i säkerhetskaptalsammanhanget i analyssektionen. Det finns olika tolkningar av dessa begrepp men dessa är de stipulativa definitioner som används genomgående i rapporten om det inte specifikt anges annorlunda.*

## Företagsvärdering

Företag kan värderas på flera sätt. Några olika perspektiv på företagsvärdering presenteras här, med utgångspunkt från Leif Edvinssons uppdelning av marknadsvärdet i finansiellt kapital och intellektuellt kapital<sup>7</sup>.



Figur 1 Marknadsvärde, finansiellt och intellektuellt kapital

### Marknadsvärde

Marknadsvärdet är det belopp som marknaden värderar företaget till. Det räknas ut genom aktiekursen multiplicerat med antalet aktier. Aktiekursen varierar beroende på marknads förhoppningar och förtroende för företaget i fråga samt de beslut företaget tar. Ett annat ord för marknadsvärde är börsvärde<sup>8</sup>. Man kan också se marknadsvärdet som nuvärdet av företagets framtida intjäningsförmåga.

Förr värderades bolag efter företagets substans (byggnader, maskiner, kassa). Idag är det ett stort gap mellan företagets marknadsvärde och dess fysiska värde. Detta är speciellt tydligt i kunskapsintensiva branscher som telecom/IT<sup>9</sup>. Microsoft värderades 1996 till 86 miljarder kronor medan de fasta tillgångarna endast uppgick till 930 miljoner kronor<sup>10</sup>.

Skillnaden mellan ett företags marknadsvärde och dess finansiella kapital kallas enligt vissa modeller för intellektuellt kapital.

Marknadsvärde = aktiekurs \* bolagets totala antal aktier<sup>2</sup>

<sup>7</sup> Edvinsson Leif & Malone Michael S., "Intellectual Capital", 1998, HarperCollins Publishers Inc, USA

<sup>8</sup> <http://web2.nettradeswedbank.se/skolan/ordlista/a-d.html#börsvärde>

<sup>9</sup> [http://www.ericsson.com/about/publications/kon\\_con/kontakten/kont07\\_98/k07\\_kronika.html](http://www.ericsson.com/about/publications/kon_con/kontakten/kont07_98/k07_kronika.html)

<sup>10</sup> Stewart Thomas A, "Intellektuellt kapital", 1999, Fakta info direkt N & S, Sverige

## Marknadseffektivitet<sup>11</sup>

Med marknadseffektivitet menas i vilken grad marknaden tar till sig information som leder till att aktiekursen förändras. Variabler som påverkar effektiviteten är antalet handlare, informationsstillgång och transaktionskostnader.

Svag marknadseffektivitet implicerar att aktiekursen endast reflekterar information som finns i historiska kurser. Enligt detta synsätt sker förändringar i kurserna oberoende av tillgänglig information och följaktligen är aktiekurserna slumpmässiga och oförutsägbara.

Semistark marknadseffektivitet medför att investeraren intar ett vanligt förhållningssätt till marknaden och dess aktörer. Marknaden reagerar på information som offentliggörs om inflation, tillväxttakt och vinster.

Stark marknadseffektivitet betyder att marknaden omedelbart reagerar på all information, inklusive sådan ej tillgängligt för marknaden, såsom insiderinformation.

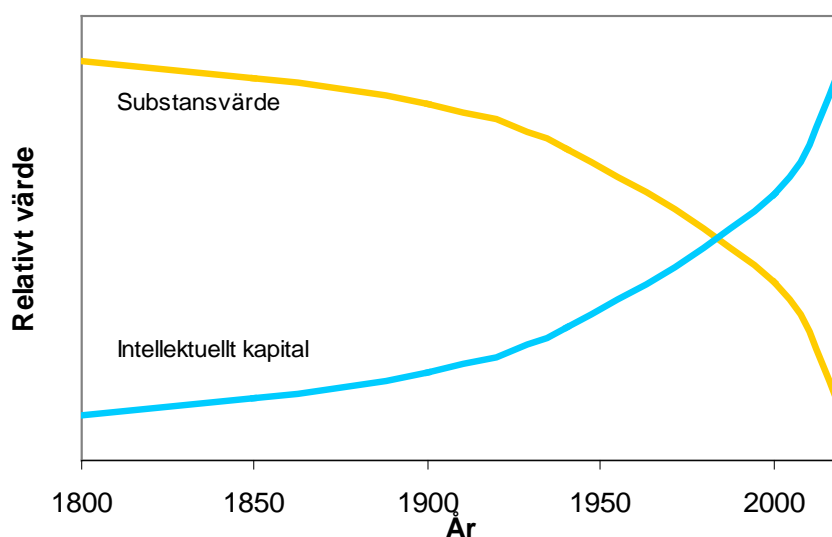
## Finansiellt kapital

Med finansiellt kapital<sup>12</sup> menas här både omsättningstillgångar (kassa) och anläggningstillgångar (byggnader maskiner, land). Det finansiella kapitalet presenteras i företagets balansräkning.

Finansiellt kapital= Anläggningstillgångar + Omsättningstillgångar

## Immateriella tillgångar

Immateriella tillgångar är tillgångar som inte har någon fysisk existens men som ändå kan vara av värde för företaget. Exempel på immateriella tillgångar är intellektuellt kapital och därmed kunskap. I dagens samhälle har dessa tillgångar blivit en allt större andel av tillgångsmassan och en allt viktigare konkurrensfaktor.



Figur 2 Relativvärdets förändring från jordbrukssamhälle till kunskapssamhälle<sup>13</sup>

<sup>11</sup> <http://www.ep.liu.se/exjobb/eki/2001/allek/004/exjobb.pdf>

<sup>12</sup> Skärvad Per-Hugo & Olsson Jan "Företagsekonomi 99 Faktabok", 2000, Liber ekonomi, Sverige

Konkurrensfördelarna ligger bland annat i företagets kunskaper, dess patenterade produkter, dess rykte hos konsumenterna och dess varumärken. För att man ska få ta upp en immateriell tillgång i balansräkningen så måste tillgången ha ett väsentligt värde för rörelsen under kommande år. Detta regleras i årsredovisningslagen<sup>14</sup>. Därmed kan exempelvis inte anställdas kunskaper tas upp i balansräkningen då det är osäkert om de kommer att vara kvar i företaget kommande år. Redovisningspraxis är att man är försiktig när det gäller att ta upp immateriella tillgångar<sup>15</sup>. Med det intellektuella kapital som benämns i denna rapport menas sådana immateriella tillgångar som ej tas upp i balansräkningen.

### **Intellektuellt kapital**

Det finns flera olika modeller om vad skillnaden mellan marknadsvärde och finansiellt kapital utgörs av. Intellektuellt kapital är en av dessa modeller. Stewart<sup>16</sup> beskriver det som summan av de kunskaper som företagets anställda har och som ger företaget en konkurrensfördel. Det kan vara utbildning och kreativitet som en grupp kemister har som gör att de upptäcker ett nytt värdefullt läkemedel eller expertisen hos medarbetare, som kommer på nya sätt att förbättra effektiviteten i verksamheten.

Kleins och Prusak<sup>17</sup> beskriver intellektuellt kapital som intellektuellt material som har formaliserats, tagits om hand och blivit använt som hävstång för att producera en tillgång av större värde.

Edvinsson<sup>18</sup> beskriver det som förpackad användbar kunskap, summan av en organisations patent, tillverkningsmetoder, kompetens hos de anställda, teknologi, information om kunder och leverantörer samt traditionell erfarenhet.

Det intellektuella kapitalet är därmed kunskap som genererar finansiellt kapital till företaget. Intellektuellt kapital visar även på företagets förmåga att lära och förändras.

I industrisamhället var mark, naturtillgångar, malm, energi, mänskligt och maskinellt arbete de beståndsdelar som byggde upp förmögenheten. Idag, i kunskapssamhället är förmögenhet och välstånd en kunskapsprodukt<sup>19</sup>. Ledningens viktigaste uppdrag i kunskapssamhällets arbetsliv är därför att förvalta det intellektuella kapitalet enligt Edvinsson<sup>20</sup>.

Det finns idag exempel på företag, såsom snabbväxande IT-bolag som nästan inte äger något alls. De hyr lokaler, leasar sina datorer, har något eller några hundrat

---

<sup>13</sup> Wik Manuel, "Perspektiv på Informationssäkerhet. IT Säkerhet 2000, IT-säkerhet ur ett organisations- och integritetsperspektiv", presentationslides vid konferens vid BTH, Försvarets Materialverk

<sup>14</sup> Årsredovisningslagen (SFS 1995:1554) 2 § 4 kap

<sup>15</sup> Hallgren Örjan, "Finansiell metodik", Tionde omarbetade upplagan, Ekonomibok förlag AB, 1998

<sup>16</sup> Stewart Thomas A, "Intellektuellt kapital", 1999, Fakta info direkt N & S, Sverige

<sup>17</sup> Ibid

<sup>18</sup> Edvinsson Leif & Malone Michael S., "Intellectual Capital", 1998, HarperCollins Publishers Inc, USA

<sup>19</sup> Stewart Thomas A, "Intellektuellt kapital", 1999, Fakta info direkt N & S, Sverige

<sup>20</sup> Edvinsson Leif & Malone Michael S., "Intellectual Capital", 1998, HarperCollins Publishers Inc, USA

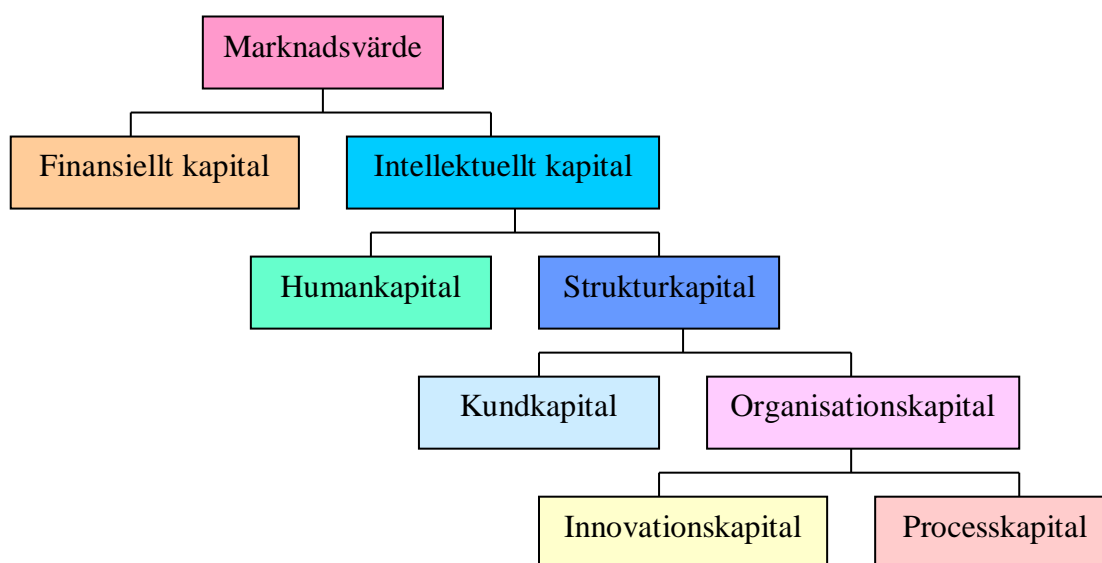
personer anställda, tjänar ännu inte pengar men är ändå värderade till hundratals miljoner amerikanska dollar på börsen<sup>21</sup>. Det finansiella kapitalet är lågt men marknadsvärdet är högt. Skillnaden utgörs av det intellektuella kapitalet.

Leif Edvinsson (före detta VD för intellektuellt kapital på Skandia) är en av grundarna till begreppet intellektuellt kapital och han beskriver det som "roots of value". Det är den första gemensamma måttstocken för att mäta och jämföra värdeökning i alla typer av företag och organisationer. Till skillnad mot årsredovisningar som skrivs i imperfektum så ska Intellektuell kapitalredovisning ge intressenter underlag för att bedöma den uthålliga lönsamheten och den framtida intjäningsförmågan. Detta ligger väl i linje med definitionen av marknadsvärde som är nuvärdet av företagets framtida intjäningsförmåga. En systematisk förvaltning av intellektuellt kapital anses också öka verksamhetens värde<sup>22</sup> eftersom man då kan återvinna och dra fördel av de kunskaper och erfarenheter, som finns i organisationen, för kreativa ändamål. Just detta tar WM-Data upp i sin årsredovisning<sup>23</sup>. Sektionen *Årsredovisningsundersökning* undersöker bland annat i vilken utsträckning och hur begreppet Intellektuellt Kapital används av företag i sina årsredovisningar.

Intellektuellt kapital består främst av humankapital och strukturkapital. Se Figur 3 Intellektuellt kapital enligt Edvinsson. Strukturkapitalet delas sedan upp ytterligare.

Marknadsvärde = Finansiellt kapital + Intellektuellt kapital

Intellektuellt kapital = Humankapital + Strukturkapital



Figur 3 Intellektuellt kapital enligt Edvinsson<sup>24</sup>

<sup>21</sup> [http://www.ericsson.com/about/publications/kon\\_con/kontakten/kont07\\_98/k07\\_kronika.html](http://www.ericsson.com/about/publications/kon_con/kontakten/kont07_98/k07_kronika.html)

<sup>22</sup> Edvinsson Leif & Malone Michael S., "Intellectual Capital", 1998, HarperCollins Publishers Inc, USA

<sup>23</sup> [http://www.wmdata.se/wmwebb/Menu6/reports/pdf/WM-Data\\_01\\_Swe.pdf](http://www.wmdata.se/wmwebb/Menu6/reports/pdf/WM-Data_01_Swe.pdf)

<sup>24</sup> Edvinsson Leif & Malone Michael S., "Intellectual Capital", 1998, HarperCollins Publishers Inc, USA



**Humankapital:** Humankapitalet<sup>25</sup> fokuserar på människors förmåga att lösa problem och hur de tar tillvara på möjligheter. Humankapitalet omfattar den sakkunskap, förnyelseförmåga, ledningsförmåga och entreprenörs- och förvaltningsförmåga som finns hos en organisations anställda. Humankapitalet är flyktigt och bundet till de anställda. Humankapitalet blir mer produktivt när det stöds av strukturerade lättillgängliga och intelligenta arbetsmetoder (strukturkapital, se nedan).

**Strukturkapital:** Strukturkapital kan till skillnad från humankapitalet ägas av företaget och det finns kvar på företaget när de anställda lämnat företaget. Det består delvis av databaser, datornätverk, patent och bra ledarskap som kan öka verkningsgraden i ingenjörsarbetet<sup>26</sup>. För att klara detta behöver kompetensen struktureras och förpackas med hjälp av teknologier och med metodbeskrivningar såsom manualer och nätverk. När kompetensen är strukturerad, förpackad och lätt tillgänglig blir den en del av företagets strukturkapital. Det blir därmed en tillgång som tillhör organisationen och som inte är bunden till individer. Då finns förutsättningar för snabbt kunskapsutbyte och oavbruten gemensam kunskapsutveckling. Ledtiderna mellan inläring och kunskapsutbyte förkortas systematiskt<sup>27</sup>.

En del av strukturkapitalet gäller juridiska rättigheter såsom teknologier, uppfinningar, data, publikationer och tillverkningsmetoder som kan patentskyddas, skyddas av copyright eller skyddas genom lagar som rör företagshemligheter. Delar av strukturkapitalet kan därmed säljas och företaget kan stämna den som använder det utan tillstånd<sup>28</sup>.

Strukturkapital = Kundkapital + Organisationskapital

**Kundkapital:** Kundkapitalet ger en ekonomisk bas för verksamheten och kan vidareutvecklas som drivkraft för vidare utveckling och partnerskap. Kundkapital är värdet av kundbas, kundrelationer och kundpotential, det vill säga värdet av företagets relationer med organisationer som man gör affärer med (även leverantörer och andra intressenter). Rent praktiskt kan kundkapital komma i uttryck som klagomål och rekommendationer för förbättringar. Om hänsyn tas till dessa synpunkter torde detta öka värdet av kundkapitalet ytterligare och kunderna vill förbli kunder hos företaget.

Saint-Onge (vice VD för Strategic Capabilities på Clarica Insurance) definierar det som ”*djupet (penetrationen), bredden (täckningen) och trofastheten (lojaliteten) i vår franchise*”. Edvinsson definierar kundkapitalet som sannolikheten att företagets kunder kommer att fortsätta att göra affärer med det<sup>29</sup>.

Kundkapital innefattar även värdet av relationerna till leverantörerna. Kundkapitalet kommer till uttryck i klagomål, dröjsmålsräntor och rekommendationer för förbättringar.

**Organisationskapital:** Organisationskapital är företagets investeringar i system, verktyg och verksamhetsfilosofi som ökar kunskapsflödet samt förbättrar leverantörs

---

<sup>25</sup> Stewart Thomas A, "Intellektuellt kapital", 1999, Fakta info direkt N & S, Sverige

<sup>26</sup> Ibid

<sup>27</sup> Ibid

<sup>28</sup> Ibid

<sup>29</sup> Ibid

och distributionskanaler. Organisationskapital består av innovations- och processkapital<sup>30</sup>.

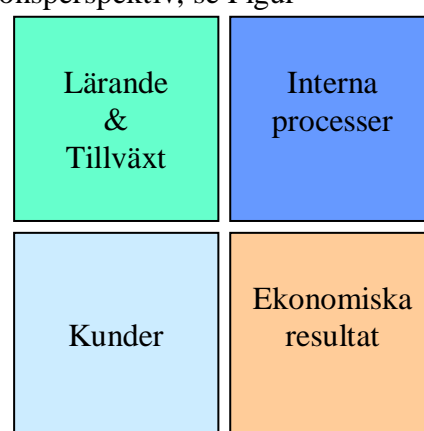
Organisationskapital = Innovationskapital + Processkapital

**Processkapital:** (PK) Processkapital omfattar arbetsprocesser, tekniska lösningar och personalprogram som stärker och ökar effektiviteten<sup>31</sup>. Däri ingår databaser och andra strukturer som kompletterar humankapitalet och ger det hävstångseffekter.

**Innovationskapital:** (InK) Innovationskapital är både förnyelseförmåga och sådana immateriella tillgångar som patent, juridiska rättigheter, immateriell egendom och affärshemligheter<sup>32</sup>.

**Balanced ScoreCard:** Balanced ScoreCard<sup>33</sup> är en modell för att mäta och styra det intellektuella kapitalet. Den bygger på fyra distinkta organisationsperspektiv, se Figur 4. Modellen förväntas ge en ”balanserad” syn på en organisations aktuella och framtida resultat.

Tillståndsanalysen skall hjälpa organisationer att bedöma vad de måste göra för att öka sina interna möjligheter att förbättra det framtida resultatet, inklusive investeringar i människor, system och procedurer. Anledningen till att modellen presenteras här är att flera företag använder modellen vilket visas senare i årsredovisningsundersökningen. Anledningen till att modellen inte används mer i denna rapport i relation till begreppet säkerhetskapital är att det inte finns någon koppling till några kapitalenheter (såsom kronor) i modellen.



Figur 4 BSC-modellen

## Information

Information är dels kunskap som enskilda medarbetarna besitter men även uppgifter som finns lagrade i en databas, på band, på skivor, talad information, tryckt information, faxmeddelanden, information i datorer på web och intranät. Information är en tillgång i alla organisationer; den är nyckeln till deras tillväxt och framgång<sup>34</sup>. Information har också ett värde som går att mäta i olika termer. Det kan vara i form av kostnader för att återskapa förlorad information, inkomstbortfall beroende på stillestånd i produktionen på grund av informationsförlust, kostnader för förlorade kunder, skadestånd, förlorat förtroende på marknaden. Det kan också vara den kostnad som uppstått då man skaffade informationen. Vilket värde informationen har för organisationen avgör hur stora resurser man bör lägga ner på att skydda den. Detta besvaras genom kartläggning av vilka tillgångarna är och vilka risker och sårbarheter som är förknippade med dem. Hur detta kan ske diskuteras i analyssektionen i Tabell 6 Perspektiv på riskanalys på sidan 37.

## Goodwill

<sup>30</sup> Stewart Thomas A, "Intellektuellt kapital", 1999, Fakta info direkt N & S, Sverige

<sup>31</sup> Ibid

<sup>32</sup> Mounteney Simon & Hosford Pen, "Protect and survive", Financial World; Canterbury; Oct 2001

<sup>33</sup> [http://www.union-network.org/UNISite/Groups/PMS/publications/IntelCap00\\_sw.pdf](http://www.union-network.org/UNISite/Groups/PMS/publications/IntelCap00_sw.pdf)

<sup>34</sup> [http://www.sisforum.se/verktyg/pdf/LIS\\_broschyr2002.pdf](http://www.sisforum.se/verktyg/pdf/LIS_broschyr2002.pdf)

Det mervärde utöver tillgångarnas värde som man ibland betalar vid köp av ett företag. Goodwillen utgör ersättning för övertagande av det köpta företags kundkontakter, organisation, personalstruktur med mera. Goodwill måste avskrivas med minst 10 % årligen.<sup>35</sup>

## Finansiering

Då den här rapporten tar upp hur tillgångar värderas och vad man baserar finansiella beslut på så presenteras här vissa för ämnet relevanta begrepp.

Det vidgade finansieringsbegreppet enligt Ezra Solomon behandlar 3 frågor<sup>36</sup>:

1. Hur stort kapital bör företaget disponera över (expansionsproblemet, storleksutvecklingsproblemet)?
2. Hur bör kapitalet fördelas på olika användningsmöjligheter (kapitalanvändningsfördelning)?
3. Hur bör kapitalet fördelas på skilda kapitalformer (kapitalanskaffningsfördelning)?

Fokus i analyssektionen ligger på de delar av finansiering som behandlar hur kapitalet bör fördelas på användningsmöjligheter.

Beslutsfattande inom finansiering måste ta hänsyn till företagets olika mål<sup>37</sup>:

1. Räntabilitetsmål eller vinstmål
2. Riskmål
3. Kontroll (nuvarande ägare vill förbli i en maktposition)

Ledningen styr företaget och söker samtidigt en acceptabel kombination av vinst och risk. I och med att företaget har flera mål är inte bästa alternativet att optimera ett mål utan att sätta dem alla. Viktfördelningen av de olika målen beror på företaget och det kan förändras med tiden. Exempelvis torde riskvilligheten vara högre i ett nystartat tillväxtföretag än i ett etablerat företag i konsolideringsfasen (stabiliseringsfasen).

Företag kan analyseras på olika sätt, bland annat kan dessa faktorer studeras: storleksutveckling, kapitalbindning, kapitalanskaffning, likviditet, soliditet, effektivitet, lönsamhet och flexibilitet. Rapporten fokuserar på de tre senaste då de påverkas av hur man använder kapitalet.

*Kostnad för eget och främmande kapital:* Kostnaden beror på realräntan (säker ränta i en ekonomi utan inflation), inflationstäckning (kompensation till långivaren för fallande penningvärde) och riskpremien (ersättning till kapitalägaren för risken att kapitalet inte kommer tillbaka)<sup>38</sup>. Detta begrepp är relevant då det är den lägsta alternativkostnad företaget har att jämföra med då man bestämmer sig för att göra en satsning på säkerhet. Om man satsar 100 000 kronor på säkerhet så kostar det kapitalet egentligen mer än 100 000 kronor då realräntan, inflationstäckning och riskpremie tillkommer. Därmed måste nyttan av säkerhetsåtgärden värderas till högre än 100 000 kronor för annars fattar företaget ett dåligt beslut.

---

<sup>35</sup> Hallgren Örjan, "Finansiell metodik", Tionde omarbetade upplagan, 1998, Ekonomibok förlag AB, Sverige

<sup>36</sup> Ibid

<sup>37</sup> Ibid

<sup>38</sup> Ibid

Det finns flera beslutsmodeller när det gäller att bedöma investeringars nuvärde. Två av dessa är CAPM (Capital Asset Pricing Model)<sup>39</sup> och APT (Arbitrage Pricing Theory). En annan modell är PENG<sup>40</sup> (Prioritering Efter Nyttogrunder) som främst används för att bedöma nyttan av IT-investeringar. Just prioritering efter nyttogrunder är möjlig väg att gå när det gäller säkerhetsåtgärder då kostnaderna ofta är direkt mätbara medan det stora problemet är att värdera nyttan av investeringen.

Företag kan göra olika typer av investeringar såsom realinvesteringar, finansiella investeringar och strategiska investeringar. Fokus för den här rapporten ligger på strategiska investeringar. Strategiska investeringar<sup>41</sup> definieras som immateriella investeringar i forskning, produktutveckling, reklam, personalutbildning, personalvård, organisationskostnader etc. Dessa poster får omkostnadsföras direkt, vilket är anledningen till att de ofta saknas på balansräkningen. Denna typ av investeringar har blivit en allt viktigare del av företagets kapitalplaceringar. Dock är de svårare att bedöma, dels på planeringsstadiet och dels vid uppföljningen än vad andra investeringar är.

**CASE:** Vad är värdet av att man utbildar en nätverkstekniker i nätverkssäkerhet? Utbildningen kommer inte att resultera i några intäktshöjningar eller kostnadsreduktioner i kärnverksamheten. Dock kan utbildningen minska kostnader för konsekvenser som är relaterade till nätverkssäkerhet. Vid planeringen inför investeringen vet man inte utbildningens värde då det är svårt att avgöra vilka hot som verkligen blir incidenter och får konsekvenser för verksamheten. Man kan bara uppskatta ett intervall och en sannolikhet. I uppföljningen kan man konstatera att incidenter har inträffat men de kan vara svåra att direkt koppla till utbildningen och särskilt vet man inte vilka konsekvenserna skulle ha blivit då utbildningen gjorde att incidenten inte fick några konsekvenser som gick att mäta.

Den strategiska investeringen avgör förmågan att överleva på lång sikt. Personalens kunskaper förbättras och nya produkter utvecklas och man blir konkurrenskraftigare. Dessa strategiska investeringar är inte en del av det finansiella kapitalet men ökar företagets framtida intjäningsförmåga och är därmed en del av företagets värde. Därmed måste de logiskt sett vara en del av det intellektuella kapitalet. Se Figur 3.

## Risk Management

Risk management är ett centralt begrepp för informationssäkerhet. Risk management (eller riskhantering) omfattar riskanalys och säkerhetsbedömning (skyddsvärdering). Man fastställer en hotbild genom identifikation av riskkällor eller hot, samt uppskattar skyddsvärdet genom att bedöma konsekvenser och sannolikheten för incidenter. Risk Management relaterade ord presenteras här för att öka läsarens förståelse för risk management och informationssäkerhet. Dessa begrepp kommer sedan att användas främst i sektionen *Teoretisk Säkerhetskaptalanalys*.

---

<sup>39</sup> [http://www.ungaaktiesparare.se/dep\\_stockmagazine/artiklar/modern\\_prissttningsteori.asp](http://www.ungaaktiesparare.se/dep_stockmagazine/artiklar/modern_prissttningsteori.asp)

<sup>40</sup> Dahlgren Lars Erik & Lundgren Göran & Stigberg Lars, "Gör IT Lönsamt! – PENG – Ett praktiskt hjälpmedel för ekonomisk värdering av IT-nytta", 1997, Ekerlids förlag, Sverige

<sup>41</sup> Hallgren Örjan, "Finansiell metodik", Tionde omarbetade upplagan, 1998, Ekonomibok förlag AB, Sverige

## Informationssäkerhet

Med informationssäkerhet menas att man genom olika åtgärder minskar sannolikheten för oönskade händelser eller att man mildrar konsekvenserna av dem<sup>42</sup>.

För företag kan rätt information vid rätt tidpunkt innebära skillnaden mellan vinst och förlust, framgång och misslyckande<sup>43</sup>. Samma sak gäller för offentliga organisationer där läckande information kan skada både samhälle och den enskilda människan.

Bristande informationssäkerhet kan få ödesdiga konsekvenser för företaget<sup>44</sup>:

1. Otillräcklig säkerhet lämnar företaget sårbart för finansiella förluster.
2. Stöld av ett företags intellektuella kapital kan leda till förlust av konkurrensövertag.
3. Ett företags rykte och varumärke kan komma till skada.

Uttryckt i företagsvärderingstermer så betyder finansiella förluster att det finansiella kapitalet har minskat, förlust av konkurrensövertag är bland annat knutet till förlust av human och strukturkapital medan en skada på varumärket främst är kopplat till kundkapital och försvårar vidare kundrelationer.

Informationssäkerhetsstandarden SS-ISO/IEC 17799<sup>45</sup> definierar informationssäkerhet i termerna:

<b>Tillgänglighet</b>	Att behöriga användare har tillgång till de resurser de är behöriga till i rätt tid och omfattning.
<b>Riktighet</b>	Att information inte obehörigt ändras eller modifieras.
<b>Sekretess</b>	Att endast behöriga användare kommer åt informationen.
<b>Spårbarhet</b>	Att kunna se vem som gjort vad och vid vilken tidpunkt.

Tabell 1 Säkerhetsaspekter enligt ISO-17799

Informationssäkerhet kan delas upp i proaktiv och reaktiv säkerhet.

<b>Proaktiv</b>	Säkerhetsåtgärd som hjälper till att förebygga och förhindra att hot blir incidenter som får konsekvenser för företaget. Exempel på proaktiva säkerhetsåtgärder är brandväggar och antivirusprogram
<b>Reaktiv</b>	Säkerhetsåtgärd som hjälper till att mildra konsekvenser när incidenter inträffat. Exempel på reaktiva säkerhetsåtgärder är försäkringar, backuprutiner och loggning

Tabell 2 Proaktiv och reaktiv säkerhet

Jag har under litteraturstudierna inte funnit något exempel på vare sig något säkerhetsindex eller säkerhetskapital, d.v.s. ingen som försökt presentera någon metod på hur man kan värdera eller gradera informationssäkerhet. Därmed finns det möjligheter att utöka informationssäkerhetsbegreppet så att det blir tydligare och även kanske sätta ett värde på det. För att kunna göra det måste informationssäkerhet värderas på något sätt och sättas in i situationer för att antingen empiriskt eller introspektivt testa dess gångbarhet.

<sup>42</sup> Keisu Thomas, "Riktlinjer för god informationssäkerhet SSR97ETT", 1997, SIG Security, Sverige

<sup>43</sup> [http://www.sisforum.se/verktyg/pdf/LIS\\_broschyr2002.pdf](http://www.sisforum.se/verktyg/pdf/LIS_broschyr2002.pdf)

<sup>44</sup> Woods Bob, "Quashing cyber mayhem", 2001, Chief Executive New York, USA

<sup>45</sup> [http://www.sisforum.se/verktyg/pdf/LIS\\_broschyr2002.pdf](http://www.sisforum.se/verktyg/pdf/LIS_broschyr2002.pdf)

## Risk

”Sannolikheten för att en störning som medför skada eller förlust ska inträffa”.<sup>46</sup>

Företagande handlar till viss del om att ta risker. Exempelvis så kan risktagande innebära att man är innovativ och testar nya saker som man inte vet om man kommer att lyckas med eller inte. Beslutet man tar kan leda till framgång eller misslyckande. Att inte ta risker innebär att man står still och då kommer företaget att föråldras, särskilt om det befinner sig i en snabbt rörlig marknad, och kommer på sikt att gå under<sup>47</sup>. Skickliga entreprenörer hanterar risker och tar hem vinsten av sina risktagningar. Med risk menas att man inte säkert vet vad utfallet kommer att bli<sup>48</sup>.

Risker relaterade till informationssäkerhet kallas operativa risker och rapporten fokuserar på denna typ av risker.

<b>Operativ risk</b>	Risken för förlust till följd av såväl händelser i omvärlden (naturkatastrofer, extern brottslighet etc.) som interna faktorer (datafel, bedrägerier, bristande efterlevnad av lagar och interna föreskrifter, övriga brister i den interna kontrollen etc.) <sup>49</sup> . Kvalitativ risk, som bland annat hänför sig till ledningens och personalens kompetens, systemens funktionssäkerhet samt eventuellt missbruk. Operativ risk kan också omfatta legal risk och anseenderisk <sup>50</sup> .
----------------------	---

Det finns mängder av olika typer av risker som företag och organisationer kan ta hänsyn till. AstraZeneca tar till exempel i sin årsredovisning<sup>51</sup> upp valutakursrisker, risk att forsknings- och utvecklingsverksamheten inte resulterar i nya produkter som ger kommersiell framgång, risken för att patent- och varumärkesrättigheter löper ut eller förloras.

Hur företag ser på olika risker undersöks i empirisektionen

*Årsredovisningsundersökning* då risk var ett av sökorden vid genomgången av årsredovisningarna.

## Riskanalys

Med kännedom om riskerna är det lättare att fatta riktiga och effektiva beslut.

En riskanalys gör det möjligt för företaget att fatta rationella investeringsbeslut och samtidigt tillgodose affärsverksamhetens krav. Grunden för riskanalysen då man ska fatta beslut rörande säkerhet är en bedömning av situationen man är i. Detta kan göras på olika sätt beroende på situation. Olika faktorer som man kan uppskatta är chansen att beslutet får önskad effekt och även risken att hot inträffar om man inte fattar beslutet. Man kan även värdera konsekvenserna om en risk blir en incident och det kan man göra på olika sätt såsom att beräkna kostnaden för att återskapa förlorad information, kostnaden för missbruk av information, förlorade intäkter, förlorat förtroende. Det är också intressant att ta reda på vad som kan hända i värsta fall, vilka konsekvenser detta får på verksamheten, och göra en uppskattning av sannolikheten

<sup>46</sup> Keisu Thomas, ”Riktlinjer för god informationssäkerhet SSR97ETT”, 1997, SIG Security, Sverige

<sup>47</sup> [http://intellectualcapital.org/intelcap/tour.hc\\_risk.html](http://intellectualcapital.org/intelcap/tour.hc_risk.html)

<sup>48</sup> <http://www.fi.se/index.asp?x=/Publikationer/debatt/t20000907.asp>

<sup>49</sup> <http://www.waymaker.net/bitonline/2002/03/15/20020409BIT01090/wkr0001.pdf>

<sup>50</sup> [http://www.rata.bof.fi/svenska/Tillsyn/data/data\\_riskanalys.html](http://www.rata.bof.fi/svenska/Tillsyn/data/data_riskanalys.html)

<sup>51</sup> [http://www.astrazeneca.com/annualrep2001/pdf/az\\_report2001\\_front.pdf](http://www.astrazeneca.com/annualrep2001/pdf/az_report2001_front.pdf)

att incidenter inträffar (till exempel elavbrott, stöld, brand som minskar tillgångarnas värde). För att man ska fatta ett sunt företagsekonomiskt beslut så bör man väga förväntad nytta mot uppskattad kostnad. Dessutom kan man ställa sig frågan om pengarna får högre avkastning om de placerats på något annorlunda sätt (kapitalets alternativkostnad). Dessa frågeställningar tas upp i finansieringsavsnittet på sidan 19.

Följande begrepp är ser jag som relevanta inom riskanalys och informationssäkerhetsområdet. Begreppen hänger samman som i en orsaks-verkan-kedja. Hot och sårbarhet kan ge upphov till en incident. Incidenten kan ge upphov till konsekvenser.

Hot	Alla oönskade händelser eller situationer som kan störa verksamheten <sup>52</sup> . Saker som kan gå fel eller som kan attackera en organisation, exempelvis bedrägeri <sup>53</sup> .
Sårbarhet	Risken för oförutsedda eller oförutsebara händelser som medför att verksamheten skadas eller drabbas av oönskade konsekvenser <sup>54</sup> . Detta ökar risken att ett hot verkligen blir en incident som kan påverka en organisation på ett negativt sätt <sup>55</sup> . Om hotet är bedrägeri så skulle dålig lojalitet vara en sårbarhet som ökar risken för hotet bedrägeri.
Incident	Ett hot ”inträffar”. Företaget blir utsatt för bedrägeri och hemlig affärsdata kommer andra till dels.
Konsekvens	Detta är följderna av en händelse. Om bedrägeri inträffar så påverkar detta företaget på olika sätt. En konsekvens kan vara ett minskat förtroende för företaget.

**Tabell 3 Riskanalysbegrepp**

### Affärsprocesser

Det finns mängder av affärsprocesser inom ett företag, till exempel bokföring, tillverkning, management, rapportering, löneutbetalning, försäljning, marknadsföring. Till dessa affärsprocesser förs resurser in och något förädlas inom processen och ger ett resultat som värderas högre än de införda resurserna. Om processen utsätts för incidenter så kan resultatet av processen försämrats.

Hot, sårbarhet, incident, konsekvens och affärsprocesser sätts i relation till varandra och till säkerhetskapital i Figur 7 i analyssektionen.

### Beslutsstöd

Den här rapporten tar upp informationssäkerhet och värdering i relation till fattade beslut eller beslutssituationer. Därför har jag valt att inkludera det här beslutsstödsavsnittet för att ge läsaren samma möjlighet som jag haft vad gäller att förstå de bakomliggande faktorerna som man kan basera beslut på.

Förr i tiden använde man ofta bara instinkt, sunt förnuft och gissningar när man fattade beslut. Till viss del används fortfarande ”gut feeling” när man fattar beslut.

<sup>52</sup> Keisu Thomas, ”Riktlinjer för god informationssäkerhet SSR97ETT”, 1997, SIG Security, Sverige

<sup>53</sup> <http://www.security-risk-analysis.com/introduction.htm>

<sup>54</sup> Keisu Thomas, ”Riktlinjer för god informationssäkerhet SSR97ETT”, 1997, SIG Security, Sverige

<sup>55</sup> <http://www.security-risk-analysis.com/introduction.htm>

Dock går processen att formalisera och det finns olika tekniker för detta. Drucker<sup>56</sup> sammanfattar arbetsprocessen att fatta beslut som;

1. Klassificera problemet eller hotet. Är det ett vanligt eller unikt problem?
2. Definiera problemet. Vad vet vi om problemet?
3. Specificera hur problemet kan inramas. Vilka gränser finns?
4. Vad är rätt att göra som håller sig inom ramarna?
5. Vad behöver göras? Vem behöver veta om det?
6. Utvärdera beslutet (dess validitet och effektivitet) efter hand som det genomförs.

Hammond, Keeney och Raiffa<sup>57</sup> har tagit fram en beslutsstödst teori som de kallar Even Swaps (jämna byten). I den ska man göra jämförelser mellan beslutsalternativens olika mål. Problemet är att olika mål har olika jämföringsbaser, till exempel precisa nummer, relationer eller beskrivningar. Metoden underlättar jämförelsen av olika alternativ genom att man simplificerar och kodifierar effekterna av olika mål. Metoden låter beslutsfattaren fokusera på att bestämma det reella värdet av beslutet eller alternativet. I Even Swaps utgår man från att göra en konsekvenstabell, där man sätter mål till vänster i en kolumn och alternativen på en rad överst. I matrisen beskrivs sedan konsekvensen som alternativet har för de olika målen. Man börjar med att ta bort dominerade alternativ, alternativ som inte är bättre på något mål. Gradera eller ranka sedan konsekvenserna, vilket gör det lättare att hitta dominerade alternativ som sedan kan strykas från valmängden. Därefter börjar man göra Even Swaps. Man gör de lätta bytena först. Detta gör att man kan stryka ännu fler alternativ. Med Even Swaps menas att man eliminerar ett mål genom att jämföra hur mycket en skillnad i ett mål är värt enligt något kvarvarande mål.

Att använda rationella beslutstöd kräver mycket kunskap om beslutssituationen för att kunna fatta ett korrekt och rationellt beslut, det vill säga det beslut som gör att företaget hamnar i bästa möjliga situation i förhållande till sina uppsatta mål. Den här beslutstekniken kan vara svår att använda då företagets beslutstider är korta och då det finns informationsöverskott eller informationsunderskott. Andra tekniker som då föreslås för beslutsfattande är humble decision making<sup>58</sup> som är en mer adaptiv metod där man tar hänsyn till nya fakta efterhand som man fattar experimentella beslut och använder utfallet för att fatta nya beslut.

I incrementalism-tekniken<sup>59</sup> så söker man inte målet utan man försöker undvika det sämsta alternativet genom små beslutsmanövrar. Fördelen är att man inte behöver all information vid varje beslutssituation men nackdelen är att den är konservativ, i den mening att beslutsvägen inte avviker så mycket från den tidigare inslagna.

Det beslutsstöd som jag kommer att förespråka i relation till säkerhetsåtgärder är ett rationellt beslutsstöd. Det är bättre att fatta beslut från den information man kan samla in och uppskatta än att fatta beslut i blindo.

---

<sup>56</sup> Drucker et al, "Harvard business review on decision making", 2001, Harvard Business School Press, USA

<sup>57</sup> Ibid

<sup>58</sup> Ibid

<sup>59</sup> Ibid



# Årsredovisningsundersökning

*I denna sektion undersöks hur svenska företag ser på sårbarhet, intellektuellt kapital, säkerhet och risker och hur de presenterar detta i sina årsredovisningar. Även förändringar och nya krav vad gäller redovisningsskyldigheter undersöks. Sektionen är tänkt att öka läsarens förståelse för hur företag använder begreppen intellektuellt kapital och informationssäkerhet i årsredovisningar.*

Företagen som studeras är de mest omsatta börsbolagen på A-listan. Dessa valdes då de har stor omsättning (omfattande verksamhet) och för att få en bredd på typen av företag. Det har gjorts undersökningar om intellektuellt kapital tidigare men då har man exempelvis gjort ett urval endast på så kallade IT-bolag som ansågs vara extra kunskapsintensiva. En sådan undersökning är ”*HUMANKAPITAL - ur ett Stakeholderperspektiv*”<sup>60</sup>. Anledningen att årsredovisningar studeras i denna rapport är för att ta reda på hur en spridd grupp företag ser på de säkerhetskaptalrelaterade begreppen idag och vilken vokabulär de använder när de tar upp risker etc. Årsredovisningar valdes också för att de är lättillgängliga. Företaget presenterar det som de är lagstadgade att presentera samt sådant som förstärker bilden av deras företag. Nackdelen med att studera årsredovisningar är att de ger en ofta subjektiv och ofullständig bild av företaget. Man får inte reda på vad som ligger bakom deras påståenden och hur olika saker fungerar i praktiken.

De säkerhetskaptalrelaterade begreppen som användes vid genomsökningen av årsredovisningarna var **sårbarhet, säkerhet, kapital, intellektuell, risk** och **information**. Dessa orden valdes då jag anser att de är relaterade till säkerhetskaptalbegreppet. Hade man sökt efter redan sammansatta ord såsom ”intellektuellt kapital” hade man missat sektioner som tagit upp exempelvis strukturkapital och kundkapital.

Arbetsgången var att söka efter sökorden i årsredovisningarna genom sökfunktionen i Acrobat Reader, då årsredovisningarna fanns tillgängliga i pdf-format. De stycken som tog upp något av ovanstående ord kopierades till ett separat dokument. Därefter gjordes en kategorisering och empirin sammanställdes i tabeller, som presenteras i denna sektion samt som bilagor.

De studerade företagen var ABB, ASSA ABLOY, AstraZeneca, Atlas Copco, Autoliv, Electrolux, Ericsson, Föreningssparbanken, Gambro, Handelsbanken, Holmen, Industrivärden, Investor, Kinnevik, Nobel Biocare, Nokia, Nordea, OM, Pharmacia, Sandvik, SCA, Scania, SEB, Securitas, Skandia, Skanska, SKF, SSAB, StoraEnso, Swedish Match, Telia, Volvo, WM-Data.

---

<sup>60</sup> <http://www.ep.liu.se/exjobb/eki/2000/allek/006/exjobb.pdf>

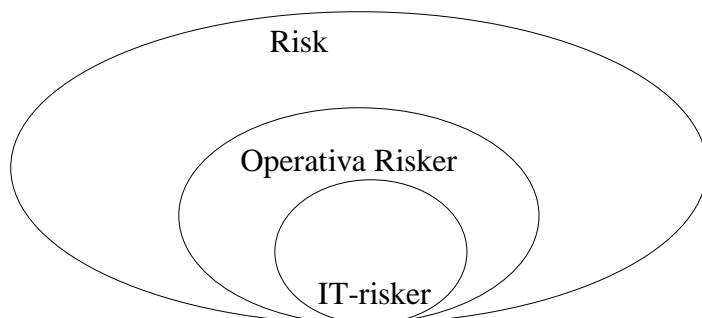
## Kvantitativt resultat

Undersökningens kvantitativa resultat sammanfattas i Tabell 4 Kvantitativ empirisk undersökning. Tabellen visar hur många procent av de studerade företagen som tar upp de olika begreppen i sina årsredovisningar

Område	Andel (%)
Risker	91 %
Operativa risker	24 %
Intellektuellt kapital	48 %
IT	48 %
IT-säkerhet	45 %

Tabell 4 Kvantitativ empirisk undersökning

Det man kan utläsa ur resultatet är att risker är ett centralt begrepp i företagens årsredovisningar (91 %). Dock tar bara en fjärdedel av företagen upp operativa risker på något sätt. Istället ligger tonvikten i årsredovisningarna på att redovisa de finansiella risker (valutarisk, ränterisk etc.) som företaget lider under. Operativa risker däremot är de som kan vara informationssäkerhetsrelaterade (se sektionen *Kapitalvärdering och Informationssäkerhet* sida 22). Värt att notera är att alla operativa risker inte behöver vara informationssäkerhetsrelaterade. Följande bild visar vilket förhållande mellan risker jag identifierat i undersökningen.



Figur 5 Riskförhållande

Bilaga 1 (sida 50) presenterar mer specificerat vad de olika företagens årsredovisningar innehöll uppdelat på begreppen IT-säkerhet, intellektuellt kapital, risk och informationssystem. De olika elementen i tabellen, såsom IK, r, k, FR förklaras i bilaga 2 (sida 51).

## Analys

Cirka hälften av företagen beskriver intellektuellt kapital och vikten av detta kapital på något sätt i sina årsredovisningar men inget av företagen kopplar någon kapitalsiffra till det. Det finns, som Tabell 8 Årsredovisningsundersökning på sida 50 visar, ingen enad bild eller standardiserad metod att beskriva sitt intellektuella kapital med kapitalsiffror. Företagen använder över 10 olika begrepp som går att återfinna i teorier om intellektuellt kapital. Båda dessa faktorer (inga kapitalsiffror och olika begrepp) bidrar till att det idag är svårt att jämföra företags intellektuella kapital. Detta faktum talar också emot möjligheten att bryta ut delar av det intellektuella kapitalet till ett säkerhetskapital som kan användas för att mäta informationssäkerhet. Det finns alltså luckor i användandet av intellektuellt kapital som begrepp och ingen verkar konkretisera Edvinssons modell fullt ut, i alla fall inte i årsredovisningarna.

Det är möjligt att företagen håller reda på sitt intellektuella kapital och värderar detta i andra forum än årsredovisningar och detta får anses vara en brist att denna rapport inte tagit reda på det men det har fått utelämnats på grund av tidsbrist.

Just att företagen beskriver säkerhet och intellektuellt kapital på olika sätt försvårar också möjligheterna att jämföra säkerhet i två företag. Att kunna göra en jämförelse av säkerheten i två företag skulle kunna vara intressant ur exempelvis investerarsynvinkel (investeraren vill veta risken som är förknippad med en investering) och kundsynvinkel (kunden vill veta vilket företag som det är säkrast för honom att göra affärer med). I USA finns den statliga organisationen Securities and Exchange Commission (SEC) för att skydda just investerare från att fatta icke väl underbyggda beslut. De beskyddas genom en lag som säger att företagen måste tillhandahålla information till SEC som gör de tillgängliga för allmänheten. Exempel på information är årsredovisningar, kvartalsrapporter, information om fusioner. SEC sammanfattar lagen:

*”Companies publicly offering securities for investment dollars must tell the public the truth about their businesses, the securities they are selling, and the risks involved in investing.”<sup>61</sup>*

Återigen är det främst finansiella risker som dominerar de SEC-filings som finns tillgängliga i SEC-databasen liksom det är i de svenska årsredovisningarna. Däremot verkar de visa allt större intresse av även operativa risker<sup>62,63</sup>.

### **Behov av tydlig säkerhet**

Därmed kan man identifiera att det finns ett behov av ett sätt att beskriva säkerhet som underlättar tydliggörande och jämförande av säkerheten i företag. Denna slutsats kan dras även på det faktum att ett flertal årsredovisningar tog upp att vi lever i ett allt osäkrare samhälle och de tar upp händelserna den 11 september (World Trade Center-attackerna) som exempel på detta. Att kunder ser informations säkerhet som en viktig faktor vid exempelvis handel via Internet kan man utläsa ur en artikel från Computer Sweden:

*”Kostnaden är inte det främsta hindret mot att handla på webben, utan att det känns obekvämt och riskfyllt. Det visar en rapport från analysföretaget IDC, som avser 14 europeiska länder.”<sup>64</sup>*

Även SIS Forum (dotterbolag till Swedish Standards Institute) tar upp vikten av att se säkerhetsarbete som en god investering.

*”Och god säkerhet är ett konkurrensmedel, särskilt i kunskapsföretag, där kundernas förtroende är det som ger affärer.”<sup>65</sup>*

Därmed går företag miste om potentiella intäkter till följd av att kunder uppfattar att de tar på sig risker om de inleder relationer med detta företag. Om företaget kunnat tydliggöra dess säkerhet på ett accepterat och standardiserat sätt så skulle den potentiella kunden kunnat välja vilket företag att inleda relation med baserat på vilken

---

<sup>61</sup> <http://www.sec.gov/about/whatwedo.shtml>

<sup>62</sup> <http://www.sec.gov/pdf/annrep01/ar01econanal.pdf>

<sup>63</sup> <http://www.sec.gov/pdf/annrep01/ar01marketr.pdf>

<sup>64</sup> Computer Sweden, 2001-04-04

<sup>65</sup> [http://www.sisforum.se/verktyg/pdf/LIS\\_broschyr2002.pdf](http://www.sisforum.se/verktyg/pdf/LIS_broschyr2002.pdf)

risk den tolererar. Därmed finns incitament för företag att tydliggöra sin säkerhet och vilka risker de lider under.

### **Försäkra sig mot risker?**

Flera företag tar i sina årsredovisningar upp just att de försäkrar sig mot risker av olika typer. Detta kan ses som en reaktiv säkerhetsåtgärd och där går det att mäta värdet av säkerhetsåtgärden. Kostnaden för säkerhetsåtgärden är försäkringspremien och självriskan. I Trygg-Hansas försäkring KontorsPlus<sup>66</sup> kan man försäkra bland annat ritningar, arkivalier och datamedia likväl som man kan försäkra sig mot databrott och dataintrång. En förändring som skett i försäkringsbranschen i år är att försäkringsbolagen inte längre ersätter företag för skador som uppstått på grund av datavirus<sup>67</sup>. Värt att notera är att försäkringsbolagen värderar informationssäkerhet på något sätt då de avgör vilken premie ett visst företag måste betala samt avgör hur stor skadeersättning företagen kan få. Däremot är det oklart i vilken mån det intellektuella kapitalets storlek och utformning (om de har ett stort säkerhetskaptal) påverkar vilken premie som företaget måste betala.

### **Banker och kapitaltäckningsregler**

En grupp företag som påtalar ett behov av att mäta sina operativa risker i större utsträckning än i andra branscher är bankerna (Föreningssparbanken, Handelsbanken och Nordea). De relaterar i sina årsredovisningar till Basel-kommittén som förespråkar att banker ska mäta sina operativa risker för att utvärdera vilket kapitaltäckningskrav som ska råda<sup>68</sup>. Kapitaltäckningsreglerna<sup>69</sup> föreskriver den minsta mängd kapital som en bank måste hålla för att få lov att driva sin verksamhet. Detta kapital ska utgöra en buffert om det uppkommer stora förluster i verksamheten som inte täcks av de löpande intäkterna.

Kapitalet ska finnas till skydd för bankens långivare och insättare och andra som har fordringar på banken. Storleken på kapitalet som krävs beror på de risker som banken utsätter sig för. Utsätter sig banken för stora risker krävs ett större kapital för att eventuellt kunna täcka för förluster som kan uppstå om riskerna leder till incidenter och får konsekvenser för banken. Frågor man kan ställa sig då man ska beräkna kapitaltäckningen är

- Hur stora förluster ska man räkna med att det kan bli under riktigt dåliga år?
- Ska man behöva räkna med flera förlustår i följd?

De kapitaltäckningsregler<sup>70</sup> som finns idag gäller finansiella risker men Baselkommittén och Finansinspektionen<sup>71</sup> börjar dock lägga mer fokus på operativa risker, framförallt storbankernas IT-användning, säkerhetslösningar och de utvecklingsarbeten som är kopplade till Internet. Finansinspektionens ger ut allmänna råd om styrning, intern information och intern kontroll och där specificeras IT-risker, andra tekniska risker, administrativa risker och legala risker som sådana operativa risker som banker bör ägna särskild uppmärksamhet. I Finansinspektionens rapport

---

<sup>66</sup> <http://www.trygghansa.se/foretag/Frame2827.html>

<sup>67</sup> <http://computersweden.idg.se/text/020424-CS29>

<sup>68</sup> <http://www.bis.org/bcbs/aboutbcbs.htm>

<sup>69</sup> <http://www.fi.se/index.asp?x=/Publikationer/debatt/t20000907.asp>

<sup>70</sup> Lag om årsredovisning i kreditinstitut och värdepappersbolag (SFS 1995:1559) 1 § 2 kap. och 3 § 6 kap. Sida B:717 lagboken

<sup>71</sup> <http://www.fi.se/index.asp?x=/Publikationer/nyhetsbrev/info0102.asp>

den 14 februari 2001: ”Riskmätning och kapitalkrav – Baselkommitténs förslag till kapitaltäckningsregler ur ett svenskt perspektiv” står följande att läsa:

*”En nyhet är att de operativa riskerna skiljs ut och åsätts ett separat krav på kapitaltäckning. Operativa risker innefattar bland annat risken för förluster på grund av störningar i datasystem, dålig intern kontroll och bedrägerier. Att dessa slag av risker nu behandlas särskilt kan ses som ett uttryck för den ökade betydelse de fått under senare år, inte minst genom det växande IT-beroendet. Förmågan att mer systematiskt hantera dessa risker har dessutom förbättrats, även om mät- och värderingsproblemen fortfarande är stora på många områden.”*<sup>72</sup>

Bankerna verkar därmed vara den bransch som har kommit längst, delvis säkert på grund av de krav finansinspektion och lagar ålägger dem, vad gäller främst finansiella risker. När Baselkommittén är klar så måste bankerna dessutom beräkna sitt kapitaltäckningskrav för sina operativa risker, det vill säga på sätt och vis sätta en prislapp på sina risker. Då kapitaltäckningsreglerna innebär att man värderar sina risker och eftersom det är ett begrepp som redan finns och används i viss utsträckning så är det relevant att ta upp det i denna rapporten. Kapitaltäckningsregler och dess möjliga koppling till säkerhetskaptalbegreppet analyseras i sektionen *Teoretisk Säkerhetskaptalanalys*.

---

<sup>72</sup> [http://www.fi.se/Publikationer/rapporter/rapport2001\\_1.pdf?from=](http://www.fi.se/Publikationer/rapporter/rapport2001_1.pdf?from=)

# Analys

*Denna sektion försöker bringa klarhet i vad begreppet säkerhetskaptal är och hur det förhåller sig till intellektuellt kapital, informationssäkerhet och hot. Säkerhetskaptalbegreppet sätts i relation till ett studerat fall (Microsoft) och olika värderingsperspektiv på säkerhetskaptal samt olika modeller presenteras.*

## **Företagsvärderingsperspektiv på informationssäkerhet**

Målet med analysen är att bekantgöra det som är främmande, nämligen informationssäkerhet och risker, uttryckta i ett företagsekonomiskt sammanhang. Att detta är främmande och att det finns problem med att mäta risker tas bland annat upp i Finansinspektionens rapport "Riskmätning och kapitalkrav – Basalkommitténs förslag till kapitaltäckningsregler ur ett svenskt perspektiv"<sup>73</sup>. Det perspektiv som presenteras i denna rapport är att via teorier om intellektuellt kapital, kunna beskriva företags informationssäkerhet/sårbarhet och de risker som företaget är utsatta för. Denna lösning är författarens egen ide och det har ej samlats in något empirimaterial direkt rörande detta fenomen, utan empiriinsamlandet har skett rörande delarna av problemet (och den möjliga lösningen), nämligen intellektuellt kapital, risker och informationssäkerhet. Författaren av denna rapport har inte kunnat hitta något material som explicit kopplat samman dessa begrepp.

Analysen är uppdelad i två delar som kallas *Empirisk Säkerhetskaptalanalys*, respektive *Teoretisk Säkerhetskaptalanalys*. Båda analyssektionerna har en stark bas i teorier om marknadsvärde och intellektuellt kapital. I *Empirisk Säkerhetskaptalanalys* sätts dock Säkerhetskaptal-begreppet in i en riktig situation för att få ner abstraktionsnivån på en något konkretare nivå. Sektionen *Teoretisk Säkerhetskaptalanalys* är främst till för att förmedla författarens bild genom introspektion av hur säkerhetskaptal skulle kunna hänga samman med företags tillgångar och processer samt till de hot och risker som företaget är utsatt för d.v.s. de begrepp som tas upp i sektionen *Teoretiska perspektiv*.

---

<sup>73</sup> [http://www.fi.se/Publikationer/rapporter/rapport2001\\_1.pdf?from=](http://www.fi.se/Publikationer/rapporter/rapport2001_1.pdf?from=)

## Empirisk säkerhetskapitalanalys

I denna sektion följer vi ett verkligt fall från våren 2002 där jag anser att Microsoft fattade ett strategiskt beslut att tillsätta och utse en chefstrateg. Material kring denna situation analyseras och de teoretiska begreppen om marknadsvärdering sätts i relation till situationen. Därmed vägs också säkerhetskapitalbegreppet in i situationen.

Följande artikel i Computer Sweden utgör upptakten till analysen.

### **Microsoft utser säkerhetsstrateg**<sup>74</sup>

(2002-02-01 11:20) Scott Charney har blivit utsedd till chefsstrateg för säkerhet på Microsoft. Hans jobb blir att göra Microsofts produkter, tjänster och infrastruktur säkrare. Utnämningen, som offentliggjordes igår, är ett led i Bill Gates nya satsning på produkter och tjänster "att lita på".

Scott Charney tillträder tjänsten 1 april och flyttar då från Pricewaterhousecoopers där han är chef för enheten mot cyberbrott. Där har han varit delaktig i att förse stora företag med säkerhetslösningar, bygga säkerhetssystem från grunden, testa existerande system och göra cyberbrottsundersökningar, skriver IDG News.

Den ursprungliga pressreleasen skrevs på engelska och den ovan presenterade är en förkortad variant av originalet<sup>75</sup>.

Utifrån tillgänglig information analyseras situationen och olika perspektiv på att se på den gjorda säkerhetsinvesteringen presenteras.

De olika perspektiv som testas på denna verkliga situation är

1. Marknaden värderar säkerhetsinvesteringen
2. Värdera säkerhetsinvesteringen efter kostnad
3. Säkerhetsinvesteringen värderas efter konsekvenser den skyddar mot
4. Företaget värderar säkerhetsinvesteringen

### **Följande regler och förkortningar används i analysen.**

Marknadsvärde = Finansiellt kapital + Intellectuellt kapital = FK+IK

Intellectuellt kapital = Humankapital + Strukturkapital = HK+SK

Strukturkapital = Kundkapital + Organisationskapital = KK+OK

Organisationskapital = Innovationskapital + Processkapital = InK+PK

MV=FK+IK

MV=FK+HK+SK

MV=FK+HK+KK+OK

MV=FK+HK+KK+InK+PK

Säkerhetskapital i det här exemplet utgörs främst av humankapital men sett i ett tidsperspektiv kommer säkerhetsstrategens kunskaper och arbete leda till att kunskaperna även konverteras in i organisationens processer och organisation i helhet. För enkelhetens skull värderas ökningen enkom som säkerhetskapital vid beräkningarna och jag går därmed inte in på säkerhetskapitalets utformning här.

<sup>74</sup> <http://nyheter.idg.se/display.asp?id=020201-cs50>

<sup>75</sup> <http://www.microsoft.com/presspass/press/2002/jan02/01-31CharneyPR.asp>

## 1. Marknaden värderar säkerhetsinvesteringen

Empiri, börsinformation<sup>76</sup> och finansiell information hämtade från Nasdaq, pressreleaser hämtade från [www.microsoft.com](http://www.microsoft.com) samt övriga nyheter från [www.idg.se](http://www.idg.se). Totalt antal Microsoft-aktier: 5 415 463 000<sup>77</sup>



Figur 6 Microsofts börskurs november 2001-maj 2002

Den för analysen insamlade börskursinformationen finns i rapporten som en bilaga på sida 52.

### 2002-01-30 - Före ”investering”

Marknadsvärde 2002-01-30=5 415 463 000\*62.85=340.4 miljarder dollar

Finansiellt kapital 2001-12-31<sup>78</sup>= 51.5 miljarder dollar

Intellektuellt kapital 2002-01-30=340.4-51.5 (miljarder dollar)=288.9 miljarder dollar

**2002-01-31** tillkännages att Microsoft förstärker sin kompetens inom säkerhet. Aktien höjs under dagen med 0.86 dollar per aktie (marknadsvärdet ökade med 4.6 miljarder dollar).

Marknadsvärde 2002-01-31=5 415 463 000\*63.71=345.0 miljarder dollar

Finansiellt kapital 2001-12-31= 51.5 miljarder dollar

Intellektuellt kapital 2002-01-31=345-51.5 (miljarder dollar)=293.5 miljarder dollar

Möjlig säkerhetskaptalökning= Intellektuellt kapital (2002-01-31)- Intellektuellt kapital (2002-01-30)=293.5-288.9 miljarder dollar=4.6 miljarder dollar

### 2002-03-28 - Före tillträde

Marknadsvärde 2002-03-28=5 415 463 000\*60.31=326.6 miljarder dollar

Finansiellt kapital 2002-03-31= 54.3 miljarder dollar

Intellektuellt kapital 2002-03-28=326.6-54.3 (miljarder dollar)=272.3 miljarder dollar

**2002-04-01** tillträder personen ifråga och humankapitalet ökar (säkerhetskaptalet ökar). Aktiekursen höjs under dagen med 0.07 dollar (marknadsvärdet ökade med 0.38 miljarder dollar)

Marknadsvärde 2002-04-01=5 415 463 000\*60.38=327.0 miljarder dollar

Finansiellt kapital 2002-03-31= 54.3 miljarder dollar

Intellektuellt kapital 2002-04-01=327-54.3 (miljarder dollar)=272.7 miljarder dollar

<sup>76</sup> <http://quotes.nasdaq.com/quote.dll?page=charting&mode=DrilldownFrameset&symbol=MSFT%60&selected=MSFT%60&months=6&elem=0>

<sup>77</sup> <http://quotes.nasdaq.com/quote.dll?page=full&mode=basics&symbol=MSFT%60&selected=MSFT%60>

<sup>78</sup> <http://www.nasdaq.com/asp/ExtendFund.asp?kind=extendfund&symbol=MSFT`&selected=MSFT&documentType=balance&period=qtr>



Möjlig säkerhetskaptalökning= Intellektuellt kapital (2002-04-01)- Intellektuellt kapital (2002-03-28)=272.7-272.4 miljarder dollar=0.4 miljarder dollar

Vid båda situationerna var aktiekurserna på neråtgående. Det allmänna neråtgäendet kan bero på lågkonjunktur men någon händelse gjorde att aktiekursen gick upp just dessa dagar. Av detta borde slutsatsen vara att det värde vi sätter på humankapitalökningen (säkerhetskaptalökningen i detta fall) är lågt räknat om något (d.v.s. ett slags minimivärde, förutsatt att inga andra positiva ting (beslut) föreligger kring de studerade situationerna).

Genom analysen av aktiekursförändringarna kan man dra slutsatsen att marknadens förväntningar på Microsoft ökade. Marknadsvärdesökningen var 4.6 miljarder dollar (januari-februarifallet). Säkerhetskaptalökningen kan dock uppskattas på flera sätt.

- a. Under 4.6 miljarder dollar. Detta vore fallet om andra intellektuellt kapitaldelar ökade, alternativt det finansiella kapitalet ökade. En pressrelease från 31 januari berättar om samarbete med TRUSTe angående förtroende och tillit i kommersiella mail. Detta skulle kunna påverkat exempelvis kundkapitalet positivt, men även delar av säkerhetskaptalet då tillit är nära kopplat till integritet och säkerhet.
- b. 4.6 miljarder dollar. Detta vore fallet om inga andra faktorer påverkade aktiekursen under dagen, varken positiva eller negativa, eller om dessa positiva och negativa faktorer var lika stora och därmed eliminerade varandra.
- c. Över 4.6 miljarder dollar. Detta vore fallet om andra delar av det intellektuella kapitalet och finansiella kapitalet drabbades av en värdeminskning. Trots dessa värdeminskningar höjdes marknadsvärdet med 4.6 miljarder dollar. Då har det skett ett skift till säkerhetskaptal med dels 4.6 miljarder dollar och dels det som övriga tillgångar har minskats med. Det som talar för detta var att aktiekursen i stort varit på nedgång.

Problemet är då att förstå vad som hände dagen efter när börskursen vände nedåt. Minskade det finansiella kapitalet på något sätt? Förlorades viktiga kunder? Blev säkerhetskaptalet något äldre och därmed ej värt lika mycket längre. En frågeställning som då uppstår är om och hur man borde skriva av säkerhetskaptal (och övrigt intellektuellt kapital)? Värderades nyheten om tillsättningen för högt från början? Hursomhelst måste, om inte det finansiella kapitalet minskades, någon del av det intellektuella kapitalet minskas.

Därmed är det svårt att analysera utifrån en aktiekurs vilket värde marknaden sätter på en säkerhetskaptalinvestering (eller vilken investering som helst), då flera olika faktorer kan påverka men som modell torde en analys av säkerhetskaptalet med hjälp av marknadsvärdet fungera, om ceteris paribus råder. Då är problemet istället hur man ska beskriva eventuella marknadsvärdesförändringar när inget har beslutats/investerats. Betyder det att det intellektuella kapitalet på sätt och vis skrivs av med tiden vid marknadsvärdesänkningar och skrivs upp vid marknadsvärdeshöjningar?

Vid beräkningarna har ingen extrapolering av det finansiella kapitalet skett från sista december till sista januari men om man gjort det så hade det bara påverkat den möjliga säkerhetskaptalökningen marginellt (0,7 %).

## 2. Värdera säkerhetsinvesteringen efter kostnad

Att anställa en person medför främst en lönekostnad men även vissa kringkostnader i form av kontorsytanvändande (hyra), datorer (avskrivningar) mm. Låt säga att Scott Charney kostar Microsoft 1 miljon dollar (A nedan) om året. Om man värderar säkerhetskapitalet till 1 miljon dollar så påverkas inte marknadsvärdet direkt då lika mycket finansiellt kapital försvinner. Följande formler förklarar det sambandet.

$$MV=FK+IK$$

Säkerhetsinvestering görs (man anställer Scott Charney)

$$FK'=FK-A$$

$$IK'=IK+A$$

$$MV=FK-A+IK+A$$

Därmed bryts inte sambandet  $MV=FK+IK$  då man värderar efter kostnad.

På detta sättet förändras aldrig marknadsvärdet efter att beslut tagits.

Dock kommer, om anställningen var ett bra beslut, Scott att påverka företaget på olika sätt genom att införa säkerhetsrutiner vars kostnader är lägre än de konsekvenser som annars skulle kunna ha uppstått om rutinerna inte införts. Detta ger ett skift från FK till IK under året, och i slutet av året kommer FK att ha ökat jämfört med om rutinerna inte införts. Om FK har höjts utan att marknadsvärdet har förändrats så måste säkerhetskapitalet (det intellektuella kapitalet) skrivas ned för att jämvikten  $MV=FK+IK$  ska råda. Om FK höjts jämfört med förväntningarna kommer dock marknadsvärdet att följa med. Fluktuerar marknadsvärdet även då FK inte ändras så är värdering efter kostnad ingen bra modell av verkligheten, då kostnad bestäms när man tar beslutet.

Dessutom kan en sådan strategisk investering (se sidan 20) inverka på marknadsvärdet och bör därför värderas högre om marknadsvärdet ökar. Dessutom kan dåliga investeringar värderas för högt, exempelvis om företaget anställer en högavlönad nätverkstekniker med utdaterade och inaktuella kunskaper. Därmed anser jag att värdering efter kostnad inte ger en rättvis bild av de säkerhetsåtgärder (det säkerhetskapital) företaget har. Dock är den enkel att göra och kan göras lika för alla företag och underlättar jämförandet. Dock tror jag inte kostnadsvärdering ger en rättvisande bild av säkerheten i ett företag.

## 3. Säkerhetsinvesteringen värderas efter konsekvenser den skyddar mot

Vid konsekvensvärdering uppskattar man vilka konsekvenser som införandet av säkerhetsåtgärden skyddar mot. Man kan också ta hänsyn till sårbarheter och sannolikheter att hot verkligen får dessa konsekvenser och speciellt skillnaden mellan om man inte inför åtgärden och om man inför åtgärden. Problemet som finns här är det som kännetecknar många företagsekonomiska problem, att man inte vet hur framtiden ter sig, d.v.s. informationsbrist.

I fallet med anställningen av en säkerhetsstrateg så skulle han arbeta med "tjänster och produkter att lita på". Sett i det perspektivet så verkar det inte vara Microsofts säkerhet som ökar utan snarare säkerheten i deras produkter och därmed även hos deras kunder. Detta kan leda till större kundkapital, d.v.s. fler som vill göra affärer med Microsoft och handla dessa produkter av dem. Detta gör konsekvensvärderingen svårbedömd. Dock står det att läsa i den ursprungliga pressreleasen från Microsoft att Charney även ska förbättra säkerheten i Microsofts infrastruktur. Detta betyder att han kan komma att förbättra företagets strukturkapital, d.v.s. företagets processer, arbetsmetoder och datornätverk. Förbättras dessa så minskar risken att företaget skadas av diverse hot, exempelvis datorvirus, hackerattacker och insiderbrott. Ett datorvirus kan få ödesdigra konsekvenser för ett företag.

Exempelvis så drabbades datortillverkaren Dell av ett virus i november 1999<sup>79</sup> som ledde till ett två dagars stopp i produktionen i en fabrik och att återkalla 12000 smittade datorer som fick saneras. Uppskattningsvis så kostade det hela 180 miljoner kronor och det hade kunnat undvikas med ett uppdaterat virussydd. Ur det exemplet kan man utläsa att genom små kostnader kan man undkomma stora ekonomiska konsekvenser.

Utän tvekan kan en säkerhetsstrateg bidra till att sådana konsekvenser motverkas men problemet är hur man värderar det hela. Om man tar alla konsekvenser som personen kan bidra till att förhindra så kan konsekvenssumman komma att överstiga marknadsvärdet för företaget. Det gör den här värderingstypen orimlig. Att värdera på det sättet bryter mot jämvikten  $MV=FK+IK$  som måste råda. Dessutom är det osannolikt att företaget skulle drabbas av alla dessa konsekvenser. Detta löses genom att väga in sannolikheterna att hoten blir incidenter som leder till konsekvenser. Återigen lider detta angreppssätt av att man inte vet sannolikheterna exakt utan man endast kan uppskatta dem. Fördelen är att i arbetet med att värdera åtgärden kan man hitta aspekter på säkerhet som varit eftersatta som man borde åtgärda och därmed kan säkerhetskapitalanalysen hjälpa till att inte bara värdera säkerheten utan även att höja den.

#### 4. Företaget värderar säkerhetsinvesteringen

När säkerhetsinvestering görs används FK för att höja IK.

A. Före investering

$$MV=FK+IK$$

B. Säkerhetsinvestering på A kr görs (kostnaden för Charney). Företaget bedömer värdet av investeringen genom att estimera variabeln x. Variabeln x har tre lägen.

x=1	Företaget har inte förbättrat sin situation (minskat risken, höjt kontrollen, förbättrat räntabiliteten). x=1 motsvaras av att placera pengarna med en avkastning enligt den riskfria bankränta
x>1	Företaget har gjort en bra säkerhetsinvestering (d.v.s. risk har minskats, kontroll och räntabilitet kan ha höjts).
x<1	Företaget borde placerat pengarna på en annan aktivitet eller åtgärd, alternativt ha satt in pengarna på banken för att få riskfri ränta som avkastning, d.v.s. nå x=1.

Tabell 5 Beskrivning av x-faktorn

$$FK=FK-A$$

$$IK=IK+A*x$$

$$MV=FK-A+IK+A*x-Z$$

Då marknadsvärdet inte förändras direkt när beslut tas så måste man ta detta i hänsyn med variabeln Z. Z beror i detta fall på stark/svag marknadseffektivitet, om företaget fattat ett korrekt beslut (hur rätt deras x-variabel är), hur omvärlden uppfattar företagets beslut, hur snabbt beslutet har fått önskad effekt på verksamheten. Vid stark marknadseffektivitet, ju korrektare beslut och beroende på hur väl omvärlden uppfattar företagets beslut så kommer Z att sjunka neråt noll, varvid marknadsvärdet höjs successivt. Om  $x<1$  så kommer Z att vara negativt men kommer att stiga mot noll

<sup>79</sup> <http://nyheter.idg.se/display.asp?id=991118-cs21>

varvid marknadsvärdet sjunker. Ju snabbare Z går mot noll desto starkare marknadseffektivitet råder. Alla företag med positiva räntabilitetsmål och som önskar bibehålla kontrollen och som har ett uns av riskmedvetenhet kommer endast att fatta beslut där de uppskattar  $x$  till ett värde som överstiger 1.

C. Z har blivit noll. Marknadsvärdet har förändrats (om  $x < 0$ ). Då  $x$ -variabeln uppskattades av företaget och kan ha varit felaktig så införs en ny variabel ( $y$ ), detta då det kan uppstå skillnader mellan uppskattad nytta/effekt och verklig nytta/effekt.

$$MV = FK - A + IK + A * y$$

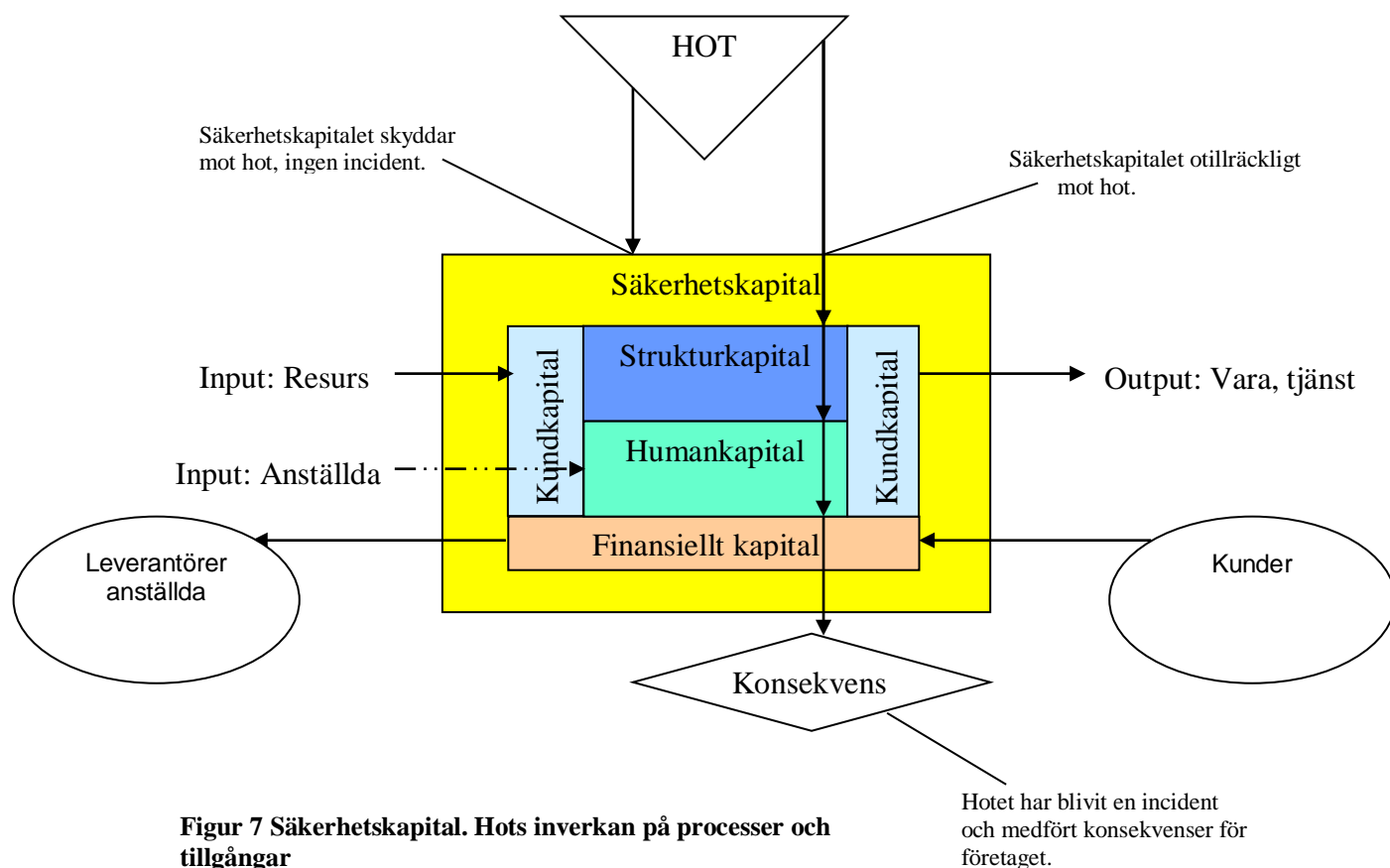
Denna modell ska ses som ceteris paribus, d.v.s. allt annat lika. Man måste kunna isolera en åtgärd och följa marknadsvärdesförändringen som uppstår till följd av den åtgärden. Detta är inget trivialt problem. Ju kortare tid Z verkar desto lättare är det att urskilja åtgärdens effekt på marknadsvärdet och därmed även få marknadsvärdering av åtgärden ( $A * y$ ). Den uppskattade värderingen är  $A * x$ . Ju färre nyheter som berör företaget som publiceras och ju mindre fluktuationer i konjunkturen desto lättare blir det att bedöma riktigheten i det uppskattade värdet ( $A * x$ ) av en säkerhetsåtgärd. De problem som uppstår här är dels företagets uppskattning av  $x$ , som kan ske på diverse sätt, baserade på saker såsom kostnad, konsekvens, sannolikhet mm. Det stora problemet är dock att avgöra när Z har nått noll för att se den verkliga värderingen av säkerhetsåtgärden (och därmed den delen av säkerhetskapitalet). Likaså är problemet att många beslut tas under tiden som Z går mot noll vilket ger upphov till en mängd Z som ska gå mot noll. Detta gör att den verkliga värderingen ( $A * y$ ) blir svår att göra, på samma sätt som den är svår att göra i fallet där marknaden värderar säkerhetsinvesteringen.

### **Avrundning**

Här presenterades olika sätt på hur man kan värdera informationssäkerhet i kapitaltermer. De kopplingar som gjorts här var främst i form av säkerhetsbeslut och företagsvärdering. I nästa sektion *Teoretisk Säkerhetskapitalanalys* kommer istället informationssäkerhet och intellektuellt kapital-begrepp att sättas samman till begreppet säkerhetskapital och presenteras i figurer.

## Teoretisk säkerhetskapitalanalys

**Definition:** Säkerhetskapital är de tillgångar i företaget (både immateriella och materiella) som skyddar företagets tillgångar och processer. Säkerhetskapitalet ligger som ett lager mot potentiella hot i enlighet med Figur 7 nedan.



**Figur 7 Säkerhetskapital. Hots inverkan på processer och tillgångar**

Utifrån denna bild kan man sedan använda två perspektiv för att göra riskanalyser, dels ett processperspektiv och dels ett tillgångsperspektiv.

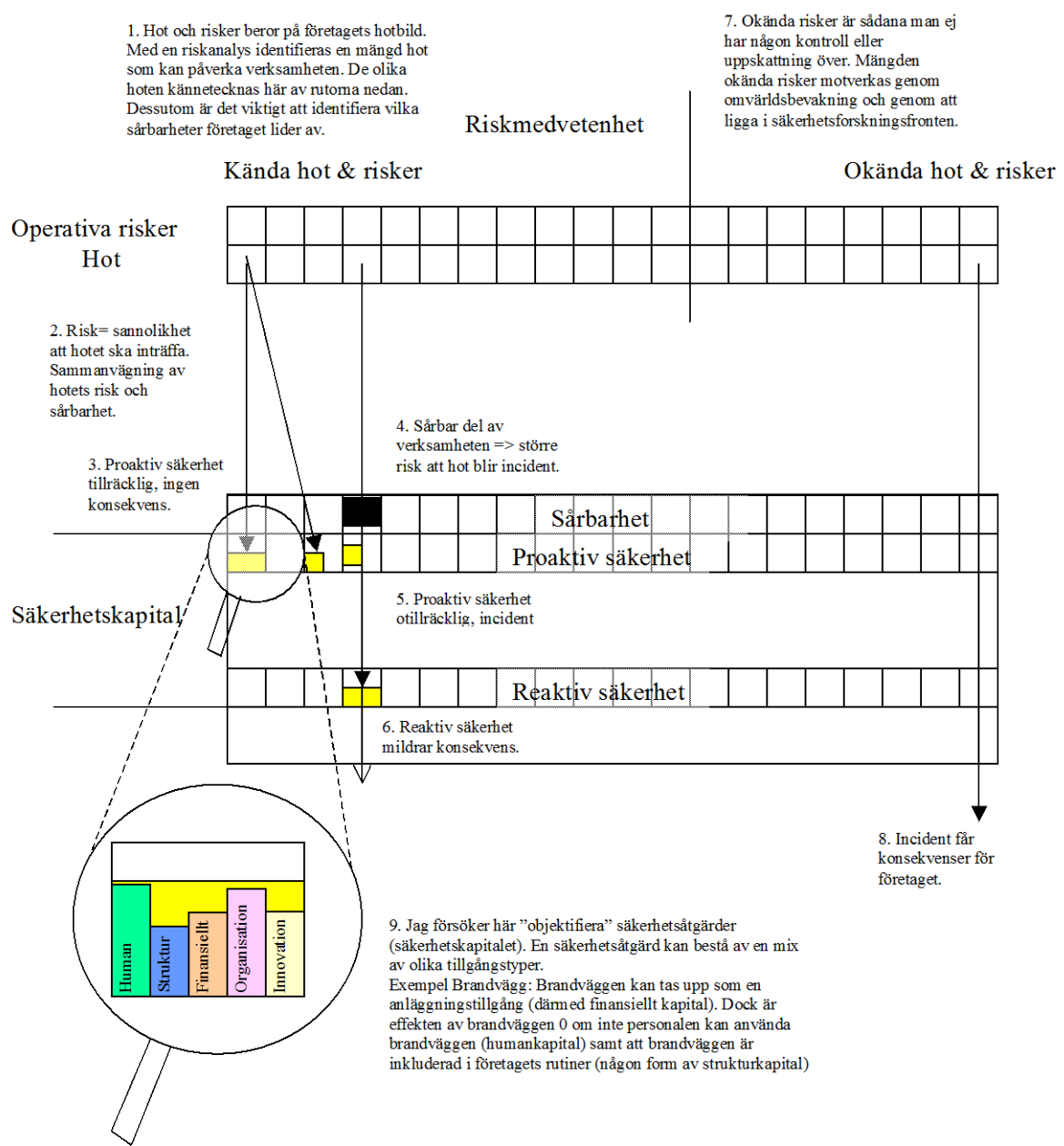
<b>Processperspektiv</b>	Vilka affärsprocesser finns i företaget och vilka sårbarheter finns inom dessa, vilka hot är de drabbade av och hur stor är risken (sannolikheten) att de inträffar?
<b>Tillgångsperspektiv</b>	Vilka tillgångar finns inom företaget (både materiella och immateriella), hur är de skyddade, på vilket sätt är de sårbara och vilka hot finns det att dessa tillgångar på något sätt skadas eller stjäls?

**Tabell 6 Perspektiv på riskanalys**

Exempel på tillgångar som klassificeras som säkerhetskapital enligt denna definition har tidigare varit oklassificerade och dess betydelse i ett företags verksamhet har ej visats på detta sätt. En utbrytning på detta sätt gör att beslutsfattare förhoppningsvis kan få ett nytt perspektiv på vad informationssäkerhet i företaget är och var det finns. Detta nås genom att dels sätta in säkerhetskapital i relation till de affärsprocesser företaget driver och dels vad det består av och beskyddar. Säkerhetskapitalenheter kan bestå av olika tillgångstyper.

Kapitaltyp	Exempel
Humankapital	Företaget kan ha anställda utbildade i informationssäkerhet
Strukturkapital	Företaget kan ha backuprutiner som följs (reaktiv säkerhetsåtgärd)
Finansiellt kapital	Företaget kan ha kortläsare och bra lås på kontoret och till datorerna.
Kundkapital	Företaget kan ha säkerhetsmedvetna och lojala kunder som inte vill skada företaget

**Tabell 7 Säkerhetskapytyper**



**Figur 8 Risk-sårbarhetsanalys**

Figur 8 visar hur säkerhetskapytalet kan objektifieras och delas upp i proaktiva och reaktiva åtgärder. Den sätter också samman företagsekonomiska begrepp (värderingsbegreppen) med de informationssäkerhets och risk managementbegreppen

som presenterades i *Teoretiska perspektiv*-sektionen (hot, risk, sårbarhet, konsekvens och säkerhet).

För att öka riskmedvetenheten i företag så måste man identifiera och definiera risker som företaget är utsatt för. Detta är det första ledet i att hantera risker och eliminera dem.

*”En väl definierad risk är till hälften eliminerad”<sup>80</sup>*

Vikten av att kartlägga hotbild och risker tas även upp av Dan Larsson vid projektet Ledningssystem för Informationssäkerhet, som även varit med om att utveckla standarden SS7799-2 (standard för informationssäkerhet).

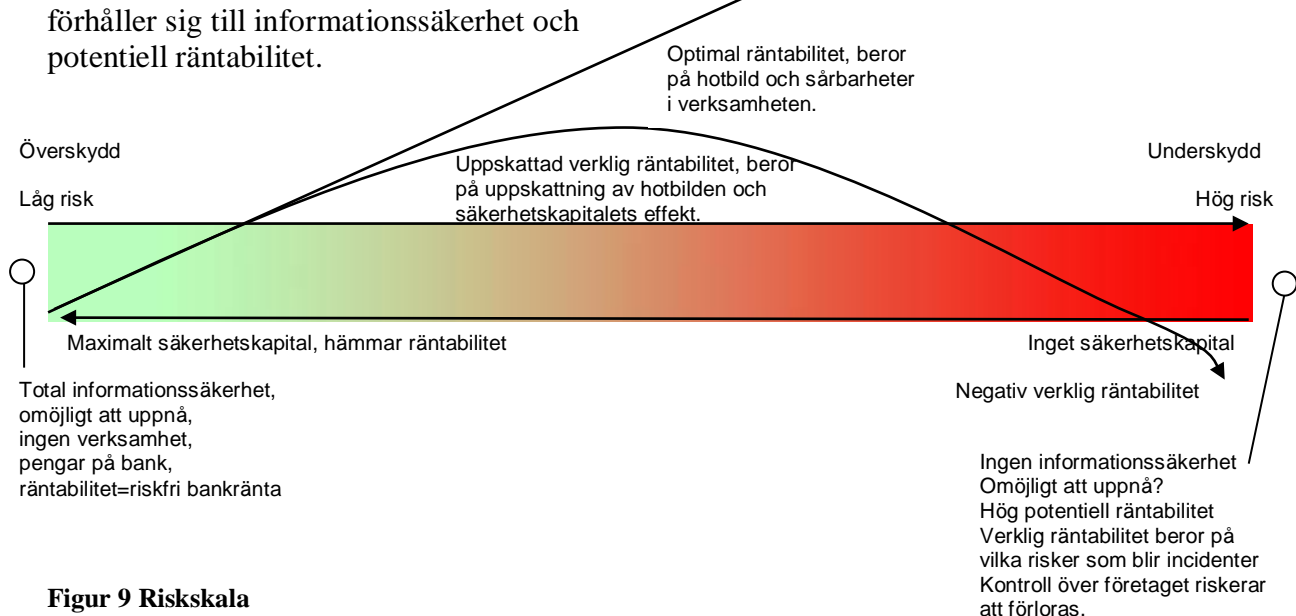
*”För att kunna förbättra företagets informationssäkerhet krävs ett omfattande arbete där företaget kartlägger hotbilden. Man analyserar alla risker - tekniska, organisatoriska och fysiska. Utifrån analysen skrivs en säkerhetspolicy som ligger till grund för hela företagets informationssäkerhet.”<sup>81</sup>*

Företag gör i sin verksamhet en avvägning mellan risk och räntabilitet.

Noll-risk innebär att företaget inte har någon verksamhet och räntabiliteten blir den riskfria bankräntan (realräntan som nämns på sidan 19 i finansieringsavsnittet i *Teoretiska Perspektiv*-sektionen). När företag accepterar risk blir den förväntade räntabiliteten högre än bankräntan. Den verkliga räntabiliteten beror dock på hur skyddat företaget är och utfallet på företagets affärsprocesser. Ju optimalare säkerhet desto närmare förväntad optimal räntabilitet kan företaget komma.

**Högre risk innebär att företaget förväntar sig hög räntabilitet men tar en stor risk och ledningen kan förlora kontrollen över företaget.**

Figur 9 presenterar min modell över hur risk förhåller sig till informationssäkerhet och potentiell räntabilitet.



**Figur 9 Riskskala**

Skalan visar ytterligheterna av risker, låg risk respektive hög risk. Den potentiella räntabiliteten är lägst vid låg (ingen risk) och ökar ju mer riskvilligt företaget är. Den

<sup>80</sup> Keisu Thomas, ”Riktlinjer för god informationssäkerhet SSR97ETT”, 1997, SIG Security, Sverige

<sup>81</sup> <http://www.sis.se/projekt/lis/pdf-filer/Montera%20inte%20bromsen%20utanpå%20bilen.pdf>

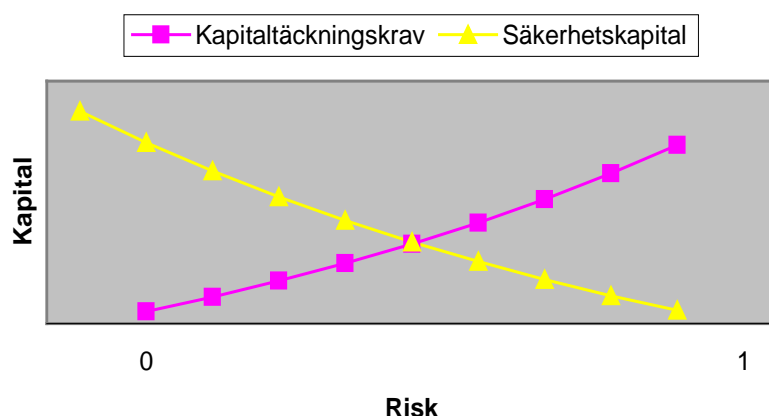
verkliga räntabiliteten däremot är endast ”given” vid nollrisk, och då är det den riskfria bankräntan. Dock gör jag en rimlig uppskattning vad gäller hög risk-, inget säkerhetskaptal-, underskyddssituationen till höger på skalan. Där torde den verkliga räntabiliteten vara negativ och att företagets kontrollmål är i fara. Någonstans däremellan på risk och säkerhetskaptalskalorna borde verkligt optimum ligga. Det optimala läget beror företagets hotbild, sårbarheter och vilka incidenter som inträffar under året. Med en förståelse för hur säkerhetskaptal (säkerhetsinvesteringar i intellektuellt kapital och finansiellt kapital) hänger samman med risker och om företaget kan uppfatta sin hotbild så får de ett större beslutsunderlag och kan på det sättet närma sig ett för det företaget optimal säkerhets-, risk- och räntabilitetsnivå.

### Kapitaltäckningskrav

Kapitaltäckningsregler presenterades på sidan 28 i sektionen *Årsredovisningsundersökning*. Detta är ett begrepp som används redan idag för att koppla risker till kapital. Om man kan minska riskerna i företaget så minskar även kapitaltäckningskravet på företaget. Enligt tidigare presenterade modeller så minskas risker och sårbarheter genom investering i säkerhetskaptal.

Figur 10 nedan visar min modell över sambandet mellan kapitaltäckning och det nya begreppet säkerhetskaptal (för förklaring av begreppet säkerhetskaptal, se sida 37) och hur det är relaterat till begreppet risk.

#### Kapitaltäckning och säkerhetskaptal



Figur 10 Kapitaltäckning och säkerhetskaptal

#### Hur förhåller sig säkerhetskaptalbegreppet till kapitaltäckningsbegreppet?

Har banken stora operativa risker så ligger man till höger på riskskalan (närmare 1) och större kapitaltäckningskrav. Företaget kan minska sina risker (gå från höger på riskskalan till vänster) genom att öka sitt säkerhetskaptal och därmed minska risken för negativa konsekvenser.

Stort säkerhetskaptal leder till att banken inte utsätter sig för så stora risker och får därmed mindre krav på sig om storleken på täckningskapitalet. Stort säkerhetskaptal nås genom investering i säkerhet med finansiellt kapital som man annars varit tvungen att ha som buffert för att täcka eventuella skador som riskerna kunnat leda till. En väl definierad risk-skala och vilket kapitaltäckningskrav som råder för varje risk företaget gör tillåter företaget att beräkna vad det kostar att åtgärda eller minska sannolikheten för olika risker. Företaget kan alltså göra en avvägning om man vill tvingas ha kapitaltäckning för en risk (kapital kostar) eller om man vill åtgärda den



genom att investera i säkerhetskapital. För att en åtgärd ska vara kostnadseffektiv så måste kostnaden för säkerhetskapitalökningen understiga kapitaltäckningskravkostnaden. Differensen mellan kapitaltäckningskravkostnaden och säkerhetsinvesteringskostnaden torde vara ett rimligt värde på säkerhetskapitalet.

# Slutsatser

*Denna sektion presenterar uppsatsens slutsatser som jag kunnat dra från rapportens olika delar och från arbetet med rapporten.*

## **Årsredovisningsundersökning**

De undersökta företagen i sektionen *Årsredovisningsundersökning* använder olika begrepp när de beskriver sitt intellektuella kapital och de lägger vikt vid informations säkerhet, ett område som blir allt viktigare för företag och organisationer. Undersökningen visade också att det börjar komma krav som säger att bankväsendet måste börja mäta operativa risker. Risk är ena sidan och intellektuellt kapital och företagets andra tillgångar är den andra sidan av problemet som här analyserats. Däremellan finns informations säkerhet. För att få förståelse för hur man kan börja mäta säkerhet kan man införa begreppet säkerhetskaptal, kopplingen som finns mellan risker och företagets tillgångar, då främst det intellektuella kapitalet.

## **Modeller och metoder**

Resultatet av rapportarbetet är främst i form av de modeller jag presenterar i *Analyssektionen*. Dessa modeller är Figur 7 Säkerhetskaptal. Hots inverkan på processer och tillgångar på sida 37, Figur 8 Risk-sårbarhetsanalys sida 38, Figur 9 Riskskala sida 39 och Figur 10 Kapitaltäckning och säkerhetskaptal på sida 40. Den modell över säkerhetskaptal som begrepp och metod som jag analyserat i sektionen *Empirisk Säkerhetskaptalanalys* som jag anser viktigast och med störst nyhetsvärde är den där jag inbegriper variablerna  $x$ ,  $y$  och  $Z$ , se sidan 35. Där anser jag att det tas mest hänsyn till komplexiteten och problematiken att mäta sådana intangibla egenskaper som säkerhet. Där värderas säkerhet på ett sätt av företaget ( $x$ ), ett sätt av marknaden ( $y$ ) och olika faktorer påverkar marknadens omvärdering från  $x$  till  $y$  och det faktum att det tar tid ( $Z$ ). Att verkligen undersöka dessa samband kvantitativt vore intressant men det har ej hunnits med i ramen för detta arbete. Dessutom är modellen generell och skulle kunna användas för att även värdera andra immateriella tillgångar i företaget än just säkerhetskaptal. Därmed kan det ses som en konkretisering av Edvinssons modell över intellektuellt kapital.

## **Värdering av säkerhet**

Om man kan värdera säkerhetskaptalet objektivt och om man kan göra jämförelser mellan företag och kunna förmedla detta ut till kunder och investerare så kan förtroendet för företaget öka och risktagandet och spekulerandet i företag minska. Dock är det inte säkert att ett alltför högt säkerhetskaptal är det bästa ur alla perspektiv. De pengarna som lagts på säkerhetskaptal kanske istället borde ha lagts på någon intäktsökande process eller tillgång istället för på en kostnadsminskande åtgärd som säkerhetskaptal tenderar att vara. Det är i relation till sådana frågor som jag finner att säkerhetskaptal kan ha sitt existensberättigande som en modell för att beskriva delar av företagets tillgångar. Jag har funnit att värdering av immateriella tillgångar som informations säkerhet är ett komplext problem med många påverkande faktorer. De slutsatser och modeller jag kommit fram till och presenterar i denna rapport ligger på en hög abstraktionsnivå, kanske en för hög abstraktionsnivå för att vara användbara i nuvarande skick. Dock har jag visualiserat det nya begreppet säkerhetskaptal i relation till intellektuellt kapital, dess uppbyggnad och hur det är positionerat bland företagets processer och övriga tillgångar.

# Egna reflektioner

*I denna sektionen tillåter jag mig att skriva fritt om de olika begrepp och teorier som använts i rapporten. Jag kommenterar på det sättet här brister och kommenterar vissa delar av det jag kommit fram till och det jag funderat över under arbetets gång. Dessa kommentarer kan också ses som mina förslag på framtida arbete som är relaterat till det område som jag presenterat i rapporten.*

## **Är Edvinssons modell över intellektuellt kapital en absolut sanning?**

Författaren har i rapporten inte tagit hänsyn till den kritik som finns mot Edvinssons modell för intellektuellt kapital utan har i analysen ansatt  $MV=FK+IK$  som en slags absolut jämviktsformel och sanning vad gäller företagsvärdering. Modellen är som sagt en modell och därmed en förenkling av verkligheten och jag ställer mig passiv till om Edvinssons modell över skillnaden mellan marknadsvärde och finansiellt kapital är den bästa. Dock har den sina pedagogiska poänger i dess uppdelning av intellektuellt kapital och jag tror man kan placera en väldigt stor del av företagets värde i just det intellektuella kapitalets olika delar.

## **Finns det ett optimalt säkerhetskapital?**

Om man kan sätta en kapitalsiffra på säkerhetskapitalet i ett företag, hur vet man då om den är optimal eller ens bra? Detta tror jag har att göra med företagets mål (räntabilitetsmål, kontrollmål och riskmål). I riskmålet tar man hänsyn till hotbilden som företaget är drabbat av. Exempelvis så kräver ett företag med en liten hotbild inget stort säkerhetskapital för att ligga i linje med sina riskmål. Ett företag med en stark hotbild däremot behöver ett större säkerhetskapital för att ligga i linje med sina mål, främst risk och kontroll-målen då de torde ha störst betydelse för ett angreppsutsatt företag. Vidare tror jag att ett stort säkerhetskapital minskar den potentiellt högsta räntabiliteten men det kan ge en högre verklig räntabilitet än om man haft ett lågt säkerhetskapital. Detta försöker jag illustrera på sidan 39 med Figur 9 Riskskala.

## **Hur kan man jämföra informationssäkerhet i två företag?**

För det första borde företagen använda samma måttstock för att värdera informationssäkerhet (eller säkerhetskapital) på samma sätt. Detta är det första problemet då det är en svårvärderad tillgång. Jag har här i rapporten försökt presentera flera sätt att mäta just säkerhetskapital men inte gått in i hur man kan jämföra informationssäkerhet. Det som faller mig på intuitivt är att om man får två företag att värdera sitt säkerhetskapital med samma metod och med samma vikter och värderingar så borde kvoten säkerhetskapital/finansiellt kapital tydligt visa företagets inställning till säkerhet. Ett maximerande av säkerhetskapital är dock inte det bästa för företaget i alla lägen utan det beror på företagets mål och de viktigaste målen är förmodligen räntabilitet. Jag tror att räntabiliteten i företaget hämmas av ett stort säkerhetskapital då företaget tar mindre risker i det fallet vilket visas i Figur 9 Riskskala på sidan 39.

## **Hur kommer bankerna att mäta sina operativa risker?**

Här tror jag det finns stora möjligheter att göra undersökningar och följa bankernas arbete med att implementera hur de ska mäta sina operativa risker och riskernas

koppling till kapitaltäckningskrav. Kan erfarenheterna från bankernas mätning av operativa risker appliceras på andra branschers företag? Bankerna är de som kommer att få krav på sig att mäta sina operativa risker inom en snar framtid och detta öppnar upp för undersökningar av risk och kapitaltäckning.

### **Hur kan man ändra bokföringslagarna så att företags bokförda värde bättre återspeglar verkligheten?**

Detta är ett område som inte är direkt relevant för säkerhetskaptal och informationssäkerhet utan det är något som täcker hela spektrumet av intellektuellt kapital (och därmed immateriella tillgångar). Exempelvis så bokförs utbildningskostnader löpande som kostnader men en utbildning skulle istället kunna redovisas som en tillgång i alla fall till den kostnad som förknippats med utbildningen och skrivs av efter hand som utbildningens värde minskar med tiden. Detta gör att företagets balansräkningar blir mer nyanserade och faktiskt säger mer, de tar inte bara upp hur statusen på företaget är idag och har varit utan den ger även en indikation över hur företaget mår för att klara av morgondagen. Det är alltså på sätt och vis att diskutera vilken roll årsredovisningar ska ha och vad de ska presentera.

### **Hur kan man bestämma ”trögheten” i det intellektuella kapitalet?**

Detta är kopplat till marknadseffektivitet. När företag fattar ett beslut så påverkar det företagets ekonomiska status och på sikt marknadsvärdet. Det intellektuella kapitalet borde justeras när beslutet genomförs. Därför kan det vara relevant med två intellektuella kapital. Företagets uppfattade intellektuella kapital och det som sätts genom marknadsvärdet. Intellektuellt kapital<sub>marknad</sub> (som är en variant av  $y$ ) närmar sig Intellektuellt Kapital<sub>företag</sub> (som är en variant av  $x$ ). Jag presenterade ett sätt att se på detta problem genom att införa begreppen  $x$ ,  $y$  och  $Z$  i avsnittet *Empirisk Säkerhetskaptalanalys* på sidan 35 där begreppen  $x$ ,  $y$  och  $Z$  också är förklarade. Jag tycker att det hade varit intressant att utforska begreppet  $Z$  närmare, vad som styr dess gång mot en nollpunkt och vad som påverkar hastigheten det gör det i.

### **Kritik**

Empiriinsamlande som har gjorts har skett med ett visst mått av subjektivitet då jag medvetet letade efter samband intellektuellt kapital (och varianter därav) samt informationssäkerhet, delvis baserat på min förförståelse. Därmed bör man vara försiktig om man drar slutsatser utifrån empirin. Jag tror det finns reliabilitetsbrister<sup>82</sup>, en annan undersökare skulle kunna komma fram till ett annat resultat med samma metodbeskrivning, detta då jag är färgad av mina förvärvade kunskaper inom ämnet och mina idéer rörande intellektuellt kapital och informationssäkerhet (som inte gått att få ner i metodbeskrivningen).

### **Tillgång till information**

Beroende på mitt val av ämne (hur intellektuellt kapital är relaterat till informationssäkerhet) så har informationen varit bristfällig alternativt svårtillgänglig. Detta beror främst på att företag idag inte värderar sitt intellektuella kapital på det sätt som man skulle kunna göra det. Detta har givetvis påverkat uppsatsens innehåll och disposition.

---

<sup>82</sup> Wiedersheim-Paul Finn & Eriksson Lars Torsten ”Att Utreda Forska och Rapportera”, 1997, Liber ekonomi, Sverige

# Referenser

## Tryckta källor

Dahlgren Lars Erik & Lundgren Göran & Stigberg Lars, "Gör IT Lönsamt! – PENG – Ett praktiskt hjälpmedel för ekonomisk värdering av IT-nytta", 1997, Ekerlids förlag, Sverige

Drucker et al, "Harvard business review on decision making", 2001, Harvard Business School Press, USA

Edvinsson Leif & Malone Michael S., "Intellectual Capital", 1998, HarperCollins Publishers Inc, USA

Eneroth Bo, "Hur mäter man vackert?", 1987, Bokförlaget Natur och Kultur, Sverige

Hallgren Örjan, "Finansiell metodik", Tionde omarbetade upplagan, 1998, Ekonomibok förlag AB, Sverige

Keisu Thomas, "Riktlinjer för god informationssäkerhet SSR97ETT", 1997, SIG Security, Sverige

Mounteney Simon & Hosford Pen, "Protect and survive", Oct 2001, Financial World, Canterbury, USA

Skärvad Per-Hugo & Olsson Jan, Företagsekonomi 99 Faktabok, 2000, Liber ekonomi, Sverige

Stewart Thomas A, "Intellektuellt kapital", 1999, Fakta info direkt N & S, Sverige

Wiedersheim-Paul Finn & Eriksson Lars Torsten, "Att Utredda Forska och Rapportera", 1997, Liber ekonomi, Sverige

Wik Manuel, "Perspektiv på Informationssäkerhet. IT Säkerhet 2000, IT-säkerhet ur ett organisations- och integritetsperspektiv", presentationslides vid konferens vid BTH, Försvarets Materialverk, Sverige

Woods Bob, "Quashing cyber mayhem", 2001, Chief Executive New York, USA

## Lagtexter

Lag om årsredovisning i kreditinstitut och värdepappersbolag (SFS 1995:1559) 1 § 2 kap. och 3 § 6 kap.

Årsredovisningslagen (SFS 1995:1554) 2 § 4 kap

## Internetkällor

Länkarna testades senast 2002-05-22. Alla länkarna nedan har försetts med en beskrivande text, exempelvis titel, källa/författare, datum. Beskrivningarna har inte kunnat utformas homogent beroende på sidornas olika innehåll och upphovsmän.

Aktiekurs för Microsoft (senaste 6 månaderna), NASDAQ

<http://quotes.nasdaq.com/quote.dll?page=charting&mode=DrilldownFrameset&symbol=MSFT%60&selected=MSFT%60&months=6&elem=0>

Aktieskolan, Börsvärde

<http://web2.nettradeswedbank.se/skolan/ordlista/a-d.html#börsvärde>

Balansräkning för Microsoft, NASDAQ

<http://www.nasdaq.com/asp/ExtendFund.asp?kind=extendfund&symbol=MSFT`&selected=MSFT&documentType=balance&period=qtr>

Basel Committee on Banking Supervision

<http://www.bis.org/bcbs/aboutbcbs.htm>

Bolagsfakta Finans, Svenska börsbolag

[http://epi.bolagsfakta.se/borsbolag/default.asp?f\\_companyalpha=&f\\_tickeralpha=&f\\_swestocklist=33&f\\_search=&f\\_reportalpha=&f\\_lineofbusiness=](http://epi.bolagsfakta.se/borsbolag/default.asp?f_companyalpha=&f_tickeralpha=&f_swestocklist=33&f_search=&f_reportalpha=&f_lineofbusiness=)

Börsinformation för Microsoft, NASDAQ

<http://quotes.nasdaq.com/quote.dll?page=full&mode=basics&symbol=MSFT%60&selected=MSFT%60>

Börsvärdering av bioteknologiska forskningsbolag, Kristoffer Öhman, Fredrik Söder, D-uppsats företagsekonomi

<http://www.ep.liu.se/exjobb/eki/2001/allek/004/exjobb.pdf>

Förbundet unga forskare, om forskningsprocessen

<http://www.san.fuf.org/forskningsprocessen.pdf>

HUMAN CAPITAL – ur ett Stakeholderperspektiv, Bengtsson Linda & Maglica

Mikaela & Rydén Anna Sofia, D-uppsats företagsekonomi

<http://www.ep.liu.se/exjobb/eki/2000/allek/006/exjobb.pdf>

Human Capital – Risk, Intellectualcapital.org

[http://intellectualcapital.org/intelcap/tour.hc\\_risk.html](http://intellectualcapital.org/intelcap/tour.hc_risk.html)

Informationssäkerhet- nyckeln till nya affärer, Broschyr Ledningssystem för informationssäkerhet, projekt inom SIS (Swedish Standards Institute)

[http://www.sisforum.se/verktyg/pdf/LIS\\_broschyr2002.pdf](http://www.sisforum.se/verktyg/pdf/LIS_broschyr2002.pdf)

KontorsPlus, Försäkringspaket från försäkringsbolaget TryggHansa

<http://www.trygghansa.se/foretag/Frame2827.html>

Microsoft Names Scott Charney as Chief Security Strategist, PricewaterhouseCoopers Principal to Lead Microsoft Security Efforts, 2002-01-31, Microsoft

<http://www.microsoft.com/presspass/press/2002/jan02/01-31CharneyPR.asp>

Microsoft utser säkerhetsstrateg, 2002-02-01, ComputerSweden

<http://nyheter.idg.se/display.asp?id=020201-cs50>

Modern prissättningsteori -prissättning på en effektiv marknad, Unga aktiesparare

[http://www.ungaaktiesparare.se/dep\\_stockmagazine/artiklar/modern\\_prisstningsteori.asp](http://www.ungaaktiesparare.se/dep_stockmagazine/artiklar/modern_prisstningsteori.asp)

Montera inte bromsen utanpå bilen, Konsensus vintern 1998/1999, Anette Karlsson  
<http://www.sis.se/projekt/lis/pdf-filer/Montera%20inte%20bromsen%20utanpå%20bilen.pdf>

Nya regler för kapitaltäckning i kreditinstitut och värdepappersbolag, Samlade riskbedömningar, Finansinspektionen 2001-02-22 Nyhetsbrev Nr 2/2001  
<http://www.fi.se/index.asp?x=/Publikationer/nyhetsbrev/info0102.asp>

Riskanalys, kapitaltäckning, Finansinspektionen (Finland)  
[http://www.rata.bof.fi/svenska/Tillsyn/data/data\\_riskanalys.html](http://www.rata.bof.fi/svenska/Tillsyn/data/data_riskanalys.html)

Riskanalys, Security Risk Analysis Group  
<http://www.security-risk-analysis.com/introduction.htm>

Riskmätning och kapitalkrav, Baselkommitténs förslag till nya kapitaltäckningsregler ur ett svenskt perspektiv, Finansinspektionen  
[http://www.fi.se/Publikationer/rapporter/rapport2001\\_1.pdf?from=](http://www.fi.se/Publikationer/rapporter/rapport2001_1.pdf?from=)

Securities and Exchange Commission  
<http://www.sec.gov/about/whatwedo.shtml>  
<http://www.sec.gov/pdf/annrep01/ar01econanal.pdf>  
<http://www.sec.gov/pdf/annrep01/ar01marketr.pdf>

Stopp för försäkring mot virus 2002-04-24, Computer Sweden  
<http://computersweden.idg.se/text/020424-CS29>

Vad betyder nya kapitaltäckningsregler för företag och tillsynsmyndigheter?  
Finansinspektionens generaldirektör Claes Norgren  
<http://www.fi.se/index.asp?x=/Publikationer/debatt/t20000907.asp>

Vem är mest värd? Kontakten Direkt, NUMMER 07, 1998  
[http://www.ericsson.com/about/publications/kon\\_con/kontakten/kont07\\_98/k07\\_kronika.html](http://www.ericsson.com/about/publications/kon_con/kontakten/kont07_98/k07_kronika.html)

Virus slog till mot DELL-fabrik, 1999-11-18, Computer Sweden  
<http://nyheter.idg.se/display.asp?id=991118-cs21>

## **Årsredovisningar 2001**

**ABB**

[http://www.abb.se/GLOBAL/ABBZH/ABBZH259.nsf/99ad595c32e0c2d9c12566e1000a4540/afc85168a4be341cc1256b8700338bec/\\$FILE/\\_685144bbbdtn66pbidpimssp0gpp76sj5chnncqbjdpkmspqv68o30c8\\_.pdf](http://www.abb.se/GLOBAL/ABBZH/ABBZH259.nsf/99ad595c32e0c2d9c12566e1000a4540/afc85168a4be341cc1256b8700338bec/$FILE/_685144bbbdtn66pbidpimssp0gpp76sj5chnncqbjdpkmspqv68o30c8_.pdf)

**ASSA ABLOY**

[http://www.assaabloy.net/overview/fileobjects/AA\\_AR01\\_SE.PDF](http://www.assaabloy.net/overview/fileobjects/AA_AR01_SE.PDF)

**ASTRAZENECA**

[http://www.astrazeneca.com/annualrep2001/pdf/az\\_report2001\\_front.pdf](http://www.astrazeneca.com/annualrep2001/pdf/az_report2001_front.pdf)  
[http://www.astrazeneca.com/annualrep2001/pdf/az\\_report2001\\_back.pdf](http://www.astrazeneca.com/annualrep2001/pdf/az_report2001_back.pdf)

**ATLAS COPCO**

[http://www.atlascopco-group.com/ACGROUP/acgroup.nsf/lookup\\_pdfs/Annual+Report+2001+sv/\\$File/Arsredovisning+2001.pdf](http://www.atlascopco-group.com/ACGROUP/acgroup.nsf/lookup_pdfs/Annual+Report+2001+sv/$File/Arsredovisning+2001.pdf)

Autoliv

[http://www.autoliv.com/appl\\_alv/Autoliv.nsf/Files/AR2001/\\$file/AR2001.pdf](http://www.autoliv.com/appl_alv/Autoliv.nsf/Files/AR2001/$file/AR2001.pdf)

Electrolux

<http://investors.electrolux.com/files/Elux-annual-2001-sv.pdf>

Ericsson

[http://www.ericsson.com/investors/pdf/annualreport2001\\_swe\\_business\\_review.pdf](http://www.ericsson.com/investors/pdf/annualreport2001_swe_business_review.pdf)

Föreningssparbanken

[http://www.foreningssparbanken.se/ir/rapporter/FSPA\\_arsred2001.pdf](http://www.foreningssparbanken.se/ir/rapporter/FSPA_arsred2001.pdf)

Gambro

[http://www.gambro.com/upload/Annual%20Reports/2001/arsredov\\_01\\_sv.pdf](http://www.gambro.com/upload/Annual%20Reports/2001/arsredov_01_sv.pdf)

Handelsbanken

[http://www.handelsbanken.se/shb/INeT/ICentSv.nsf/vLookUpPics/Investor\\_Relations\\_HB\\_01\\_sv\\_ar\\_medfoto/\\$file/HB01sv\\_medfoto.pdf](http://www.handelsbanken.se/shb/INeT/ICentSv.nsf/vLookUpPics/Investor_Relations_HB_01_sv_ar_medfoto/$file/HB01sv_medfoto.pdf)

Holmen

[http://www.holmen.com/pdf/ar01\\_se.pdf](http://www.holmen.com/pdf/ar01_se.pdf)

Industrivarden

<http://www.industrivarden.se/files/pdf/arsredovisning2001.pdf>

Investor

<http://www.waymaker.net/bitonline/2002/03/26/20020326BIT00320/wkr0003.pdf>

Kinnevik

[http://www.kinnevik.se/images/textFile/Kinnevik\\_AR\\_2001\\_S.pdf](http://www.kinnevik.se/images/textFile/Kinnevik_AR_2001_S.pdf)

Nobel Biocare

[http://www.nobelbiocare.se/cms/files/Corporate\\_Financial\\_Reports\\_2002/NB\\_annual\\_report\\_2001\\_SE.pdf](http://www.nobelbiocare.se/cms/files/Corporate_Financial_Reports_2002/NB_annual_report_2001_SE.pdf)

Nokia

[http://nds1.nokia.com/aboutnokia/pdf/Annual\\_Accounts\\_2001.pdf](http://nds1.nokia.com/aboutnokia/pdf/Annual_Accounts_2001.pdf)

Nordea

[http://www.nordea.com/appx/eng/pdf/annual\\_2001/report.pdf](http://www.nordea.com/appx/eng/pdf/annual_2001/report.pdf)

OM

[http://www.om.com/company/pdf/OM\\_AR\\_2001\\_SWE.pdf](http://www.om.com/company/pdf/OM_AR_2001_SWE.pdf)

Pharmacia

<http://www.pharmacia.com/investor/pdf/annrept2001.pdf>

Sandvik

<http://www3.sandvik.com/pdf/annualreports/swedish2001.pdf>



SCA

<http://www.sca.com/Pdf/2001SVE.pdf>

Scania

<http://www.scania.com/ir/archive/acrobat/sca01SE.pdf>

SEB

<http://www.waymaker.net/bitonline/2002/03/15/20020409BIT01090/wkr0001.pdf>

Securitas

[http://www.securitasgroup.com/www/secgroup/securitas.nsf/46269fabcb1b1991c1256a0e0029cc4a/a8f6c18745b33c8ec1256a0e00317452/\\$FILE/Securitas+2001+Sve.pdf](http://www.securitasgroup.com/www/secgroup/securitas.nsf/46269fabcb1b1991c1256a0e0029cc4a/a8f6c18745b33c8ec1256a0e00317452/$FILE/Securitas+2001+Sve.pdf)

Skandia

[http://www.skandia.com/se/includes/documentlinks/annualreport2001/Skandia2001\\_sv.pdf](http://www.skandia.com/se/includes/documentlinks/annualreport2001/Skandia2001_sv.pdf)

Skanska

[http://www.skanska.se/files/documents/pdf/Skanska2001\\_de11\\_sve.pdf](http://www.skanska.se/files/documents/pdf/Skanska2001_de11_sve.pdf)

SKF

[http://vp009.alertir.com/files/SKF\\_annual2001\\_sv.pdf](http://vp009.alertir.com/files/SKF_annual2001_sv.pdf)

SSAB

[http://www.ssab.se/arsredo\\_2001/pdf/ssab\\_arsredo\\_2001.pdf](http://www.ssab.se/arsredo_2001/pdf/ssab_arsredo_2001.pdf)

StoraEnso

<http://www.storaenso.com/CDAvgn/showDocument/0,,1485,00.pdf>

Swedish Match

<http://www.swedishmatch.com/archive-pdf/annual-2001-sve.pdf>

Telia

<http://www.telia.com/eFocus/DOCUMENT/20020328/TeliasArsredovisning2001.pdf>

Volvo

[http://www3.volvo.com/investors/finrep/volvo\\_ar\\_01\\_sv.pdf](http://www3.volvo.com/investors/finrep/volvo_ar_01_sv.pdf)

WM-Data

[http://www.wmdata.se/wmwebb/Menu6/reports/pdf/WM-Data\\_01\\_Swe.pdf](http://www.wmdata.se/wmwebb/Menu6/reports/pdf/WM-Data_01_Swe.pdf)

# Bilagor

## Bilaga 1 Årsredovisningsundersökning

<b>Företag</b>	<b>IT-säkerhet</b>	<b>Int-kap</b>	<b>Risk</b>	<b>Infosys</b>
<b>ABB</b>		IK	r	IT
<b>ASSA ABLOY</b>	Dsak+	KUNK	rkiFr	
<b>ASTRAZENECA</b>			BIRM, RAC,FrP	
<b>ATLAS COPCO</b>			FrP	
<b>AUTOLIV</b>		IK	Fr	
<b>ELECTROLUX</b>			Fr	IT
<b>ERICSSON</b>			Fr	
<b>FÖRENINGSSPARBANKEN</b>	enhet	HK, KUN	RM,FrP,OrPks	IT
<b>GAMBRO</b>			FrP	IT
<b>HANDELSBANKEN</b>	JA		MIOr,Fr,ITr	IT
<b>HOLMEN</b>			FrP	IT
<b>INDUSTRIVÄRLDEN</b>	sakprod		Fr	
<b>INVESTOR</b>	JA	HK	RM,Fr,OrP	
<b>KINNEVIK</b>				
<b>NOBEL BIOCARE</b>		KUN	RM,FrP	IT
<b>NOKIA</b>	sakprod		RMOrFr	IT
<b>NORDEA</b>	JA	BSC	RM,MOrP,i,Fr	IT
<b>OMGRUPPEN</b>	JA	InK,SK,KUNK	RMFrP	IT
<b>PHARMACIA</b>		IP	Fr	
<b>SANDVIK</b>			Fr	IT
<b>SCA</b>	JA		RMFr	IT
<b>SCANIA</b>			Fr	
<b>SEBANKEN</b>	JA		RMOrFr	IT
<b>SECURITAS</b>	Dsak+,JA,prod	KUN	RM,MFr	
<b>SKANDIA</b>	JA	HK,Nav	OrFr	
<b>SKANSKA</b>		KUN	RMFrOr	
<b>SKF</b>			FrP	
<b>SSAB</b>			Fr	IT
<b>STORAENSO</b>			R	
<b>SWEDISH MATCH</b>			RMFrPOr	
<b>TELIA</b>	JA		Fr	IT
<b>VOLVO</b>	JA	ORG	FrP	IT
<b>WM-DATA</b>	JA	SK,Kund		IT

Tabell 8 Årsredovisningsundersökning

De olika tabellelementen (HK, JA, RM o.s.v.) förklaras i Tabell 9 Förklaring till årsredovisningsundersökningen på sida 51.

## Bilaga 2 Förklaring till årsredovisningsundersökningen

<b>Kolumn</b>	<b>Benämning</b>	<b>Beskrivning</b>
<b>IT-säkerhet</b>	enhet	Företaget skriver att de har en enhet som ansvarar för IT-säkerheten i företaget
	JA	Företaget beskriver IT-säkerhet på något sätt. De kan ha instruktion för IT-säkerhet, styrelsen har ägnat uppmärksamhet åt frågan under året, de har arbetat med att säkra processer eller tillgångar
	sakprod prod	Företaget är involverat i produktion av IT-säkerhetslösningar Företaget är involverat i produktion av säkerhetsprodukter/tjänster (ej nödvändigtvis IT-relaterat)
	Dsak+ (blankt)	De skriver att behovet av säkerhet ökar (ej IT-specifik) Företaget nämner inte IT-säkerhet (säkerhet) på något sätt
	<b>Intellektuellt kapital</b>	IK
	KUNK	Företaget skriver om sitt kunskapskapital, synonymt med intellektuellt kapital i vissa företag
	HK	Företaget skriver om sitt humankapital
	InK	Företaget skriver om sitt individkapital, synonymt med humankapital i vissa företag.
	SK	Företaget skriver om sitt strukturkapital
	Kund	Företaget skriver om sitt kundkapital (det samlade, långsiktiga värdet av företagets affärsrelationer)
	BSC	Företaget använder Balanced Score Card
	IP	Företaget skriver om patent (engelska "intellectual property")
	Nav	Företaget har en modell (Navigator) som berör human, kund, finans, process samt utvecklingsfokus
	ORG	Företaget beskriver organisationsstrukturförändringar som ett sätt att förbättra konkurrenskraft
	KUN	Företaget skriver om kunskap som en viktig faktor i verksamheten
<b>Risker</b>	ITr	Företaget skriver om IT-risker
	MOrP	Företaget skriver om att mäta operativa risker samt har policy för de riskerna
	MOr	Företaget skriver om att mäta operativa risker
	OrP	Företaget skriver om policy för operationella risker
	Or	Företaget skriver om operationella risker
	s	Företaget skriver om sårbarhet
	r	Företaget skriver om risker (endast ospecificerat)
	k	Företaget skriver om konsekvenser
	i	Företaget skriver om incidenter
	MFr	Företaget skriver om att mäta finansiella risker
	FrP	Företaget skriver om att de har en policy för finansiella risker
	Fr	Företaget skriver om finansiella risker
	RM	Företaget skriver om sin Risk Management
	BIRM	Business Interruption Risk Management, process som ser över risksituationen inom produktion och varuförsörjning. Risker minimeras med beredskapsplaner
RAC	Företaget har en Risk Advisory Committee	
<b>Infosystem</b>	IT	Företaget skriver om IT, exempelvis att de har standardiserad IT-infrastruktur

Tabell 9 Förklaring till årsredovisningsundersökningen

### Bilaga 3. Utdrag Microsoft aktiekurser (dollar)

Datum	Slutpris	Volym	Pressreleaser <sup>83</sup>
01/28/2002	63.820	20809800	<ul style="list-style-type: none"> <li>• MSN Carpoint Announces People's Choice Best of Show Award Winner For North American International Auto Show 2002 . Heritage, Legendary Appeal and a Sexy Silhouette Drive Ford's GT40 Concept To the Top of the List With More Than 50,000 Consumer Votes</li> <li>• Microsoft Helps Healthcare Organizations Acquire Extension For HIPAA Implementation Deadline . "Nightingale," a Comprehensive HIPAA Offering, Includes BizTalk Accelerator for HIPAA And Training, Consulting and Testing Services</li> <li>• Xbox and Linkin Park Team Up for Promotional Partnership. Hot Video Game Console and Leading Artist to Hit the Road to Entertain Fans</li> <li>• Microsoft Personal Collection 2002 Provides Home Office Users With an Affordable Edge . Collection of Four Programs Is Perfect Complement to Microsoft Office for Home Users And Helps Families Do More, Learn More and Enjoy More</li> </ul>
01/29/2002	62.320	29332600	<ul style="list-style-type: none"> <li>• Microsoft to Offer Popular SQL Server 2000 Driver For JDBC at No Charge . New Beta Version of Driver Is Available for Download</li> </ul>
01/30/2002	62.850	33047800	<ul style="list-style-type: none"> <li>• Membership Has Its Benefits: Microsoft Announces Mobility Partner Advisory Council . Microsoft Mobility Development Gains Momentum; Company Invests In the Growing Economy</li> <li>• ESPN.com on MSN Delivers Everything Fans Need For Super Bowl Sunday . One-Click Access to Chats, Up-to-the-Minute News and Analysis, Leading Services, And ESPN.com's Premier Sports Content Are on MSN</li> <li>• Los Angeles-Area Children Benefit From Software Piracy Recoveries . Microsoft's \$1.35 Million Anti-Piracy Recoveries Donation Helps Bridge the Digital Divide At Laguna Nueva Elementary</li> </ul>
01/31/2002	63.710	34782500	<ul style="list-style-type: none"> <li>• Microsoft Names Scott Charney as Chief Security Strategist. PricewaterhouseCoopers Principal to Lead Microsoft Security Efforts</li> <li>• Microsoft to Participate in the Beta Testing of New "Trusted Sender" Program . Launched by TRUSTe and ePrivacy Group to Promote Trust and Confidence in Commercial E-mail</li> </ul>
02/01/2002	62.660	31730700	<ul style="list-style-type: none"> <li>• First "Blacks in Technology" Summit Offers Digital Opportunities. Microsoft Sponsors Gathering as Part of Outreach to Diverse Communities Nationwide</li> </ul>
02/04/2002	61.120	35153300	<ul style="list-style-type: none"> <li>• 10 stycken pressreleaser.</li> </ul>
03/26/2002	59.080	34674600	<ul style="list-style-type: none"> <li>• Microsoft President and COO Rick Belluzzo Announces Expansion Of Club Tech Program at Boys &amp; Girls Clubs of America in Arizona. U.S. Sen. John McCain on Hand to Discuss Benefit to State's Children and Teens Through Technology Access at Approximately 30 Boys &amp; Girls Clubs</li> </ul>
03/27/2002	59.440	23659200	<ul style="list-style-type: none"> <li>• MSN Vice President Judy Gibbons Named to List Of Most Successful Businesswomen in Europe. Stellar Leadership Guides Unique User Growth of More Than 50 Percent For MSN Europe During Past Year</li> <li>• Microsoft Releases Shared Source CLI and C# Implementation. Availability of Over 1 Million Lines of Source Code for FreeBSD and Windows Underscores Microsoft's Commitment to Open Standards, Academia and Developers</li> </ul>
03/28/2002	60.310	21720600	
04/01/2002	60.380	23504200	<ul style="list-style-type: none"> <li>• Microsoft Releases UltimateTV Service Upgrade. New Service Is Faster, Easier to Use and Introduces Innovative New Features</li> </ul>
04/02/2002	57.300	38193800	<ul style="list-style-type: none"> <li>• Microsoft Celebrates 10 Years of Success With Microsoft Certified Professionals. MCP Community Is Primed to Deliver Another 10 Years of Excellence</li> </ul>
04/03/2002	56.330	38462500	<ul style="list-style-type: none"> <li>• Microsoft Realigns Business Structure, Belluzzo to Transition</li> <li>• Study Finds SQL Server 2000 Saves Customers \$3 Million Vs. Oracle9i . Microsoft/Unisys Business Intelligence Solution Demonstrates Lowest Total Cost of Ownership</li> </ul>

Tabell 10 Börskurser Microsoft - vid säkerhetsåtgärden

<sup>83</sup> <http://www.microsoft.com/presspass/todaynews1.asp?indextype=pr&month=Apr02>