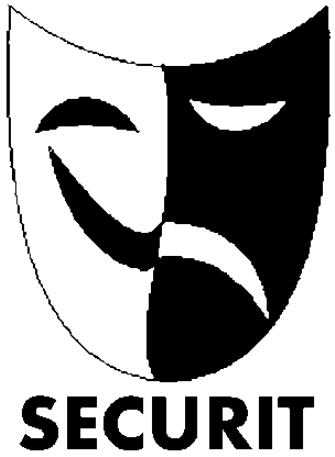


Informationssäkerhetskultur— forskningsprogrammet SECURIT

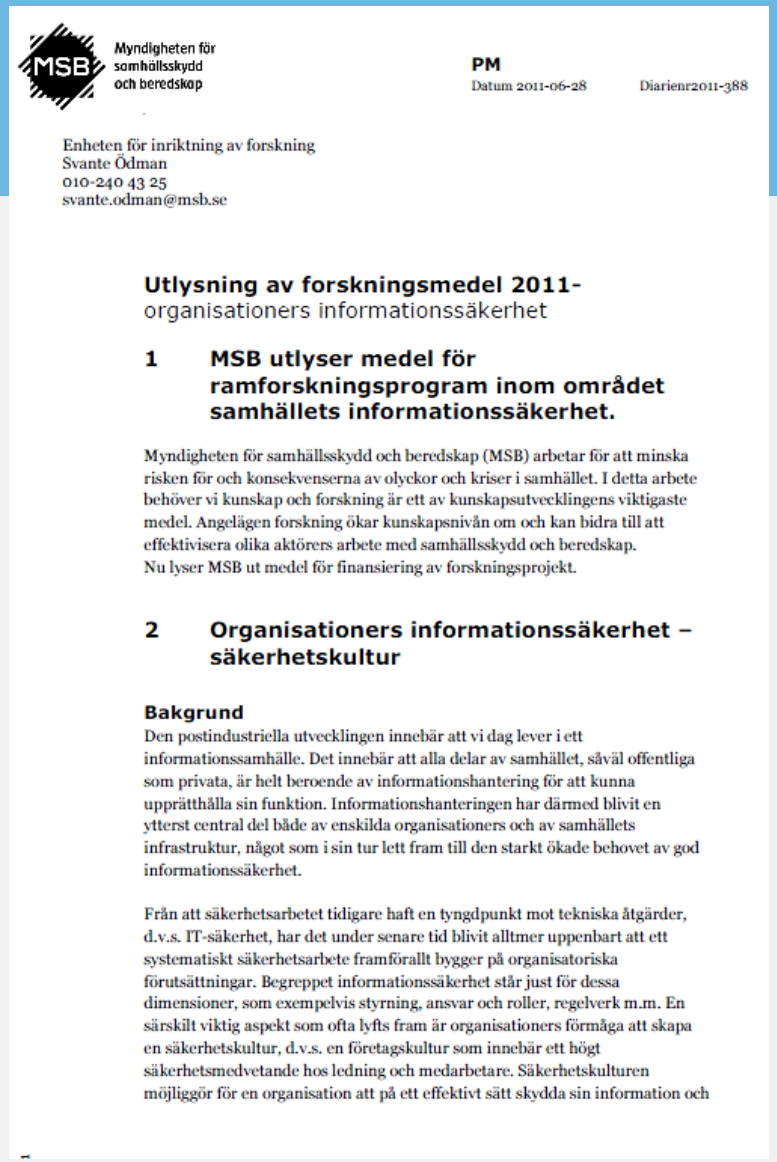
Jonas Hallberg

www.foi.se/securit

FOI

Utgångspunkter

- Behov av förbättrad informationssäkerhet
- Kultur–en central aspekt av informationssäkerhet
- SECURIT studerar
  - säkerhetsrelevanta egenskaper hos individer och organisationer
  - effekter av sociala åtgärder



Myndigheten för samhällsskydd och beredskap

PM
Datum 2011-06-28 Diarienr2011-388

Enheten för inriktning av forskning
Svante Ödman
010-240 43 25
svante.odman@msb.se

Utlysning av forskningsmedel 2011-
organisationers informationssäkerhet

1 MSB utlyser medel för ramforskningsprogram inom området samhällets informationssäkerhet.

Myndigheten för samhällsskydd och beredskap (MSB) arbetar för att minska risken för och konsekvenserna av olyckor och kriser i samhället. I detta arbete behöver vi kunskap och forskning är ett av kunskapsutvecklingens viktigaste medel. Angelägen forskning ökar kunskapsnivån om och kan bidra till att effektivisera olika aktörers arbete med samhällsskydd och beredskap.
Nu lyser MSB ut medel för finansiering av forskningsprojekt.

2 Organisationers informationssäkerhet – säkerhetskultur

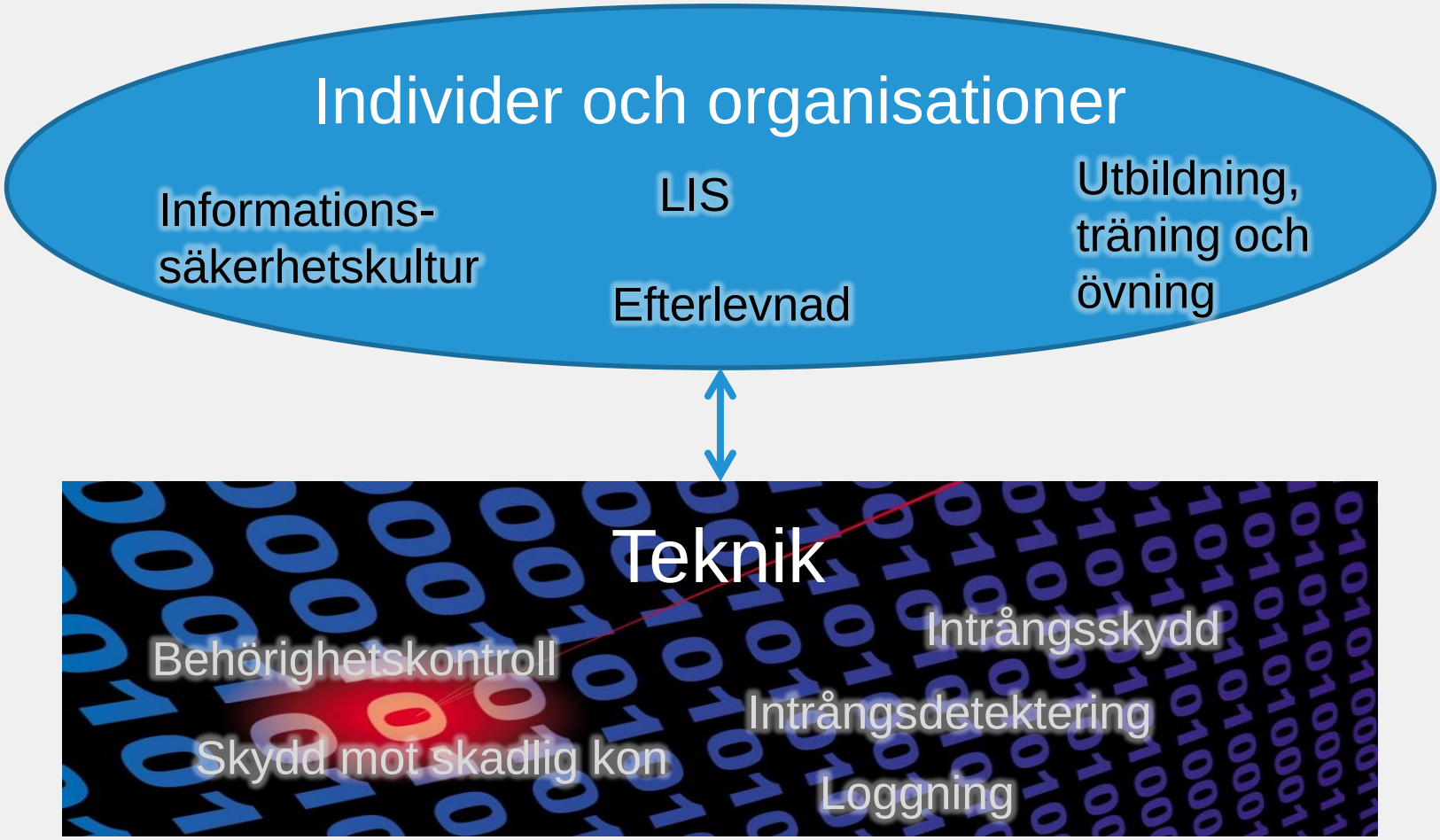
Bakgrund
Den postindustriella utvecklingen innebär att vi dag lever i ett informationssamhälle. Det innebär att alla delar av samhället, såväl offentliga som privata, är helt beroende av informationshantering för att kunna upprätthålla sin funktion. Informationshanteringen har därmed blivit en ytterst central del både av enskilda organisationers och av samhällets infrastruktur, något som i sin tur lett fram till den starkt ökade behovet av god informationssäkerhet.

Från att säkerhetsarbetet tidigare haft en tyngdpunkt mot tekniska åtgärder, d.v.s. IT-säkerhet, har det under senare tid blivit alltmer uppenbart att ett systematiskt säkerhetsarbete framförallt bygger på organisatoriska förutsättningar. Begreppet informationssäkerhet står just för dessa dimensioner, som exempelvis styrning, ansvar och roller, regelverk m.m. En särskilt viktig aspekt som ofta lyfts fram är organisationers förmåga att skapa en säkerhetskultur, d.v.s. en företagskultur som innebär ett högt säkerhetsmedvetande hos ledning och medarbetare. Säkerhetskulturen möjliggör för en organisation att på ett effektivt sätt skydda sin information och

www.foi.se/securit

SECURIT

Informationssäkerhet



SECURIT

Vad är kultur?

Hofstede:

“Culture is the collective programming of the mind distinguishing the members of one group or category of people from others”

http://geert-hofstede.com/national-culture.html

Edgar Schein:

There are three distinct levels

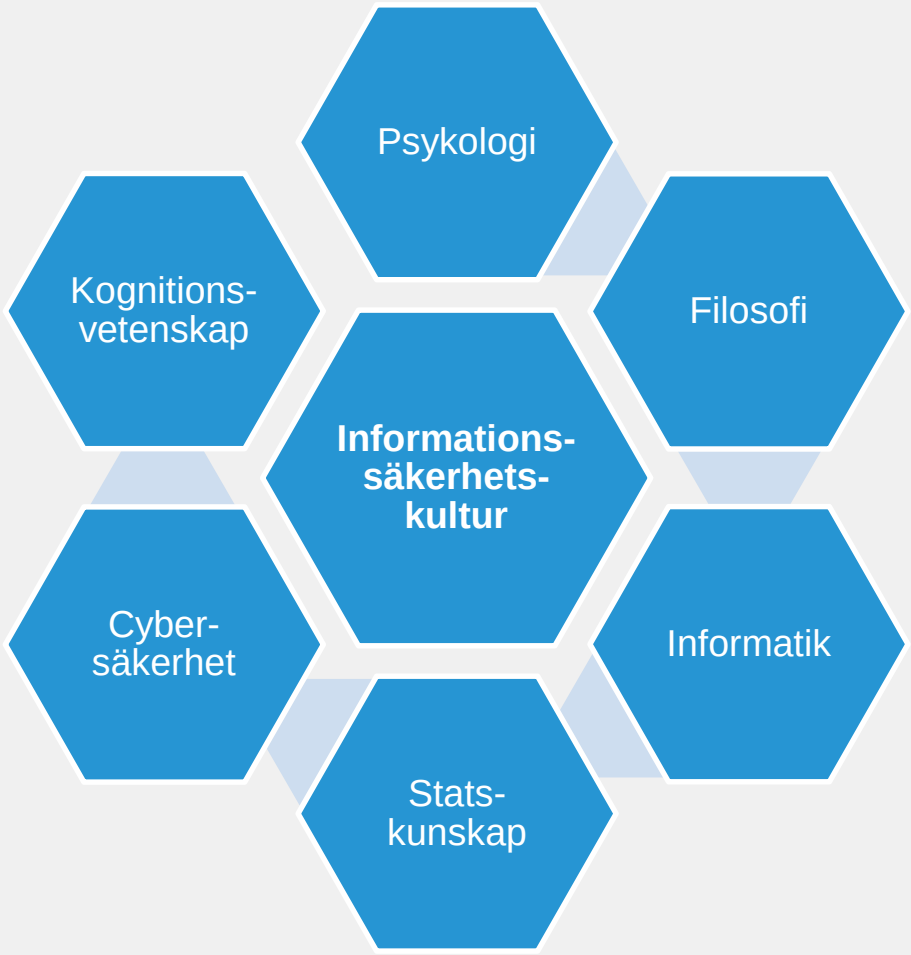
- Artifacts
- Espoused values
- Basic assumptions

Aktörerna bakom SECURIT

www.foi.se/securit

SECURIT

Forskningsprogrammet SECURIT, 2012-2017



www.foi.se/securit

SECURIT

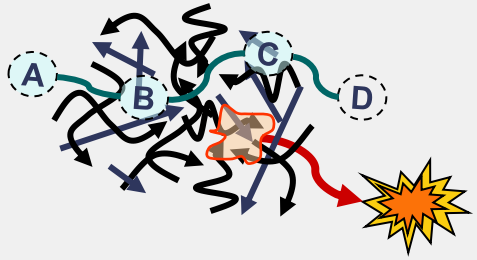
Informationssäkerhetskultur

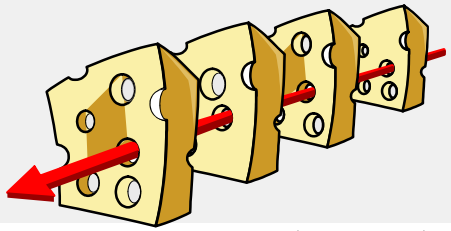
Gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer baserade på inre och yttre krav, som traderas till nya medlemmar och som har implikationer för informationssäkerhet

http://foi.se/sv/Sok/Sammanfattningssida/?rNo=FOI+MEMO+5253

Forskningsprojekten i SECURIT

- Security culture
- User acceptance of information security policies
- Attitude, culture, and information security
- Discourse and security practice
- Balanced IT-based Organizational development
- ATTITUDE
- INTERORG
- CONGRUENCE
- Cultural aspects in information security standard development



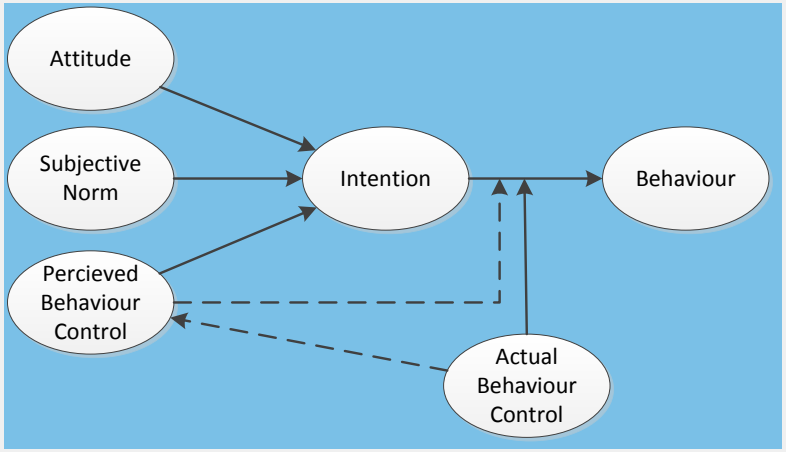


www.foi.se/securit

SECURIT

Exempel: följa bestämmelser

- Vilka faktorer påverkar anställdas intention att följa informationssäkerhetsbestämmelser och faktiska beteende?



- Testa teorin
  - Litteraturstudie
  - Metaanalys
  - Egen datainsamling

	Regression model							
	1	2	3	4	5	6	7	8
Theory of planned behavior	•	•	•	•	•	•	•	•
Threat Appraisal (PMT)		•			•	•	•	
Coping Appraisal (PMT)			•		•	•		•
Anticipated Regret				•		•	•	•
Explained variance (R^2)	0.36	0.40	0.37	0.43	0.41	0.45	0.44	0.44

www.foi.se/securit

SECURIT

TPB-tolkning av en bestämmelse

Norm?

- Ett lösenord till ett IT-system vid FOI ska vara så konstruerat att det inte kan gissas eller knäckas på ett enkelt sätt. För närvarande gäller att lösenord, om inte IT-systemet i sig är begränsande, bör bestå av minst 15 tecken samt innehålla en blandning av Versaler, gemener, siffror och specialtecken. T.ex. FIfs&ish84#snli (FOI Instruktion för säkerhetsskydd & informationssäkerhet har 82 # sidor nyttig läsvärd information). Lösenord ska bytas minst en gång per år.

Stärka beteendekontroll?

SECURIT

Mer TPB-anpassad formulering

Attityd

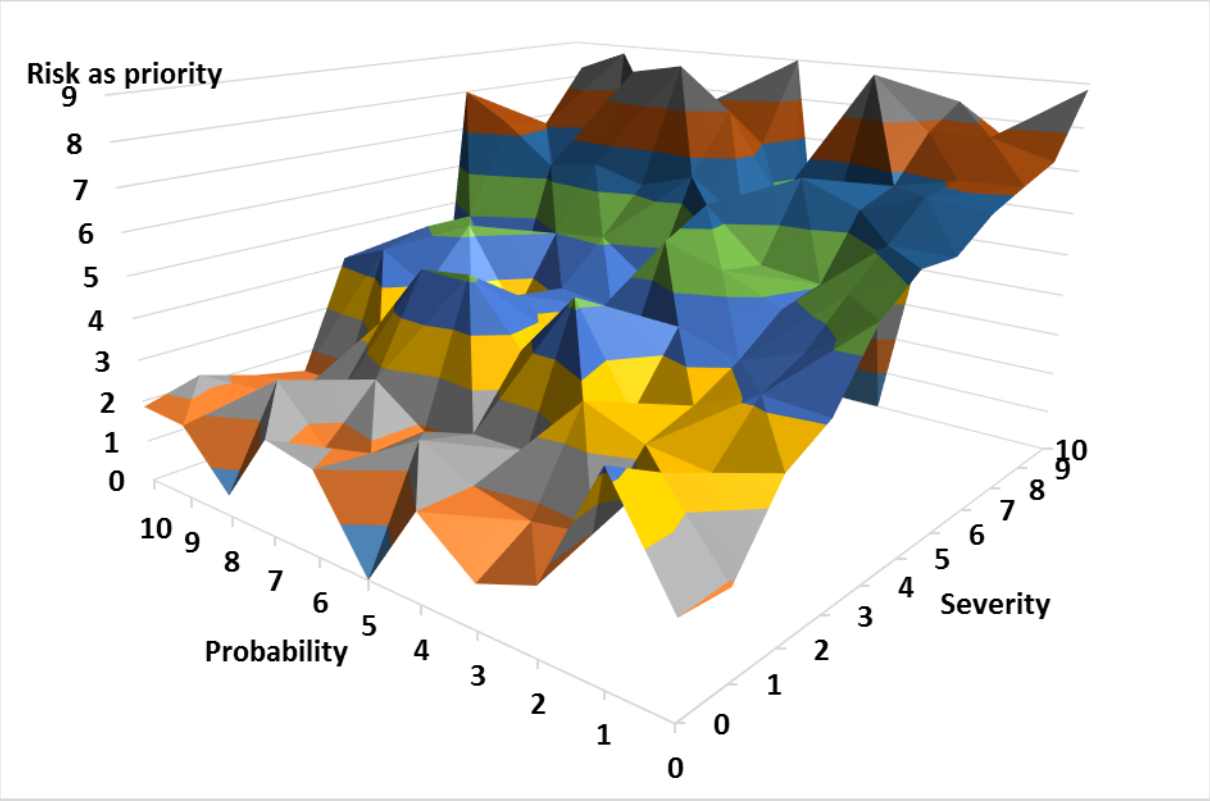
Normer

Att skydda IT-system vid FOI är viktigt. Det förväntas av medarbetare och uppdragsgivare att de lösenord som används till IT-system vid FOI är konstruerade så de inte kan gissas eller knäckas på ett enkelt sätt. Om inte IT-systemet i sig är begränsande bör lösenordet bestå av minst 15 tecken samt innehålla en blandning av Versaler, gemener, siffror och specialtecken. Du kan enkelt skapa ett bra lösenord genom att utgå från en mening. T.ex. kan du skapa ”FIfs&ish84#snli” från meningen ”FOI Instruktion för säkerhetsskydd & informationssäkerhet har 82 # sidor nyttig läsvärd information”. Lösenord behöver bara bytas en gång per år.

Upplevd beteendekontroll

SECURIT

Exempel: bedöma risker



T. Sommestad, H. Karlzén, P. Nilsson, J. Hallberg, (2016) "An empirical test of the perceived relationship between risk and the constituents severity and probability", Information & Computer Security, Vol. 24 Iss: 2

Datainsamling

- SCB-enkät
- Frågor från flera av SECURIT-projekten
- Utskick till
  - 11 000 anställda
  - 6 branscher
  - Organisationer och arbetsställen
- Svarsfrekvens: 33,6 %

Resultat

SECURIT

Security Culture and Information Technology

Forskningsprogrammet Security Culture and Information Technology, SECURIT, har som mål att förbättra organisationers informationssäkerhet. I moderna informationsdrivna organisationer utgör god säkerhetskultur en viktig förutsättning för informationssäkerheten.

För att uppnå målen studerar SECURIT:

- Egenskaper hos individer och organisationer som är relevanta för informationssäkerheten
- Effekter av åtgärder som syftar till att förbättra informationssäkerheten genom att påverka individer och organisationer

SECURIT finansieras av Myndigheten för samhällsskydd och beredskap, MSB, och koordineras av Totalförsvarets forskningsinstitut, FOI. Forskningen genomförs gemensamt av Chalmers, Göteborgs universitet, FOI, KTH och Örebro universitet i samarbete med Linköpings universitet. Karlstad universitet koordinerar och stödjer nätverket Swedish IT Security Network for PhD students (SWITS) inom ramen för SECURIT.

Relaterat material

Rapporter

Definition of information security culture

Dokument

Projektbeskrivning (eng)

Länkar

Forskningsprojekt

Resultat

Resultaten från SECURIT kommer att spridas på flera olika sätt till ett antal olika mottagare. Forskningen kommer främst att dokumenteras i form av artiklar som skickas till vetenskapliga tidskrifter och konferenser. Resultat kommer också att spridas via fackpress, seminarier, fallstudier etc. på så sätt nås forskare, informationssäkerhetsexperter och beslutsfattare inom såväl näringsliv som den offentliga sektorn.

Informationssäkerhetskultur

Gemensamma tanke-, beteende- och värderingsmönster som uppstår och utvecklas i ett socialt kollektiv genom kommunikativa processer baserade på inre och yttre krav, som traderas till nya medlemmar och som har implikationer för informationssäkerhet

Forskningen inom SECURIT syftar till att besvara följande frågor.

- Vad är förhållandet mellan säkerhetskultur och det generella sociala och intellektuella klimatet i organisationer?

www.foi.se/securit

Antologi

SECURIT