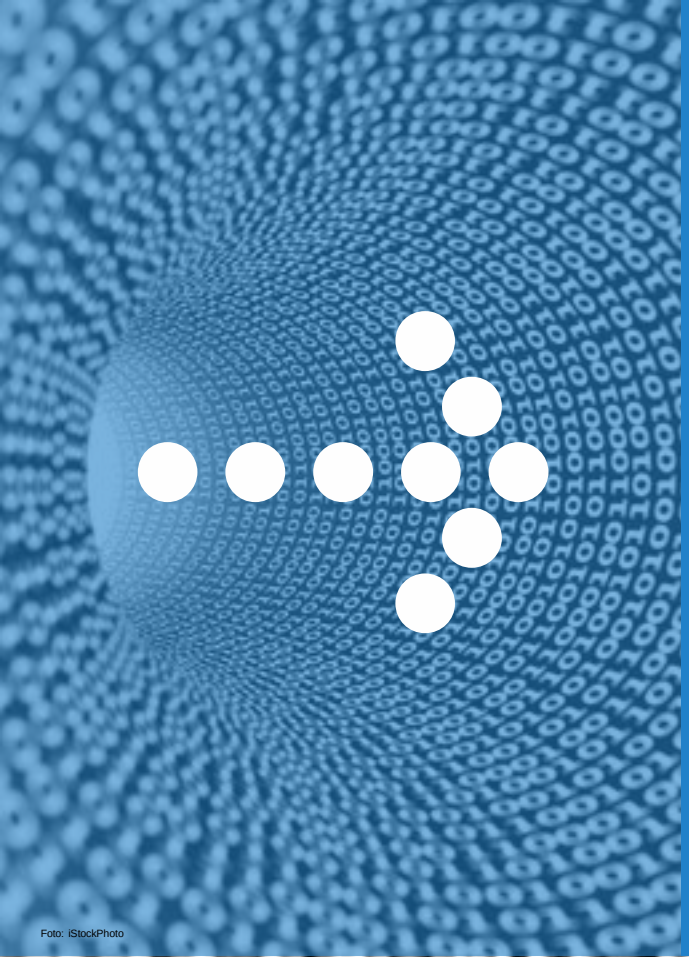


Foto: iStockPhoto

Varför följer inte användarna reglerna?

Säkerhetsbestämmelser hamnar i fokus

Exempel

- Tvingande regler
- Tydliga riktlinjer
- Standardprocedurer
- Normer

Antaganden

- Skrivna av experter med helhetsperspektiv
- Ger rätt risknivå

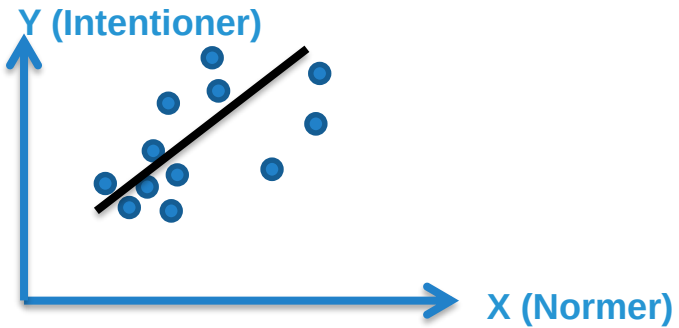
Forskarnas metod: Kvantitativ enkätforskning

X: Mina arbetskamrater tycker att jag ska följa bestämmelserna.

1 – Instämmer inte alls
2 – Instämmer i låg grad
3 – Instämmer delvis
4 – Instämmer i hög grad
5 – Instämmer helt

Y: Jag ämnar följa bestämmelserna.

1 – Instämmer inte alls
2 – Instämmer i låg grad
3 – Instämmer delvis
4 – Instämmer i hög grad
5 – Instämmer helt



Utmaning: datainsamling

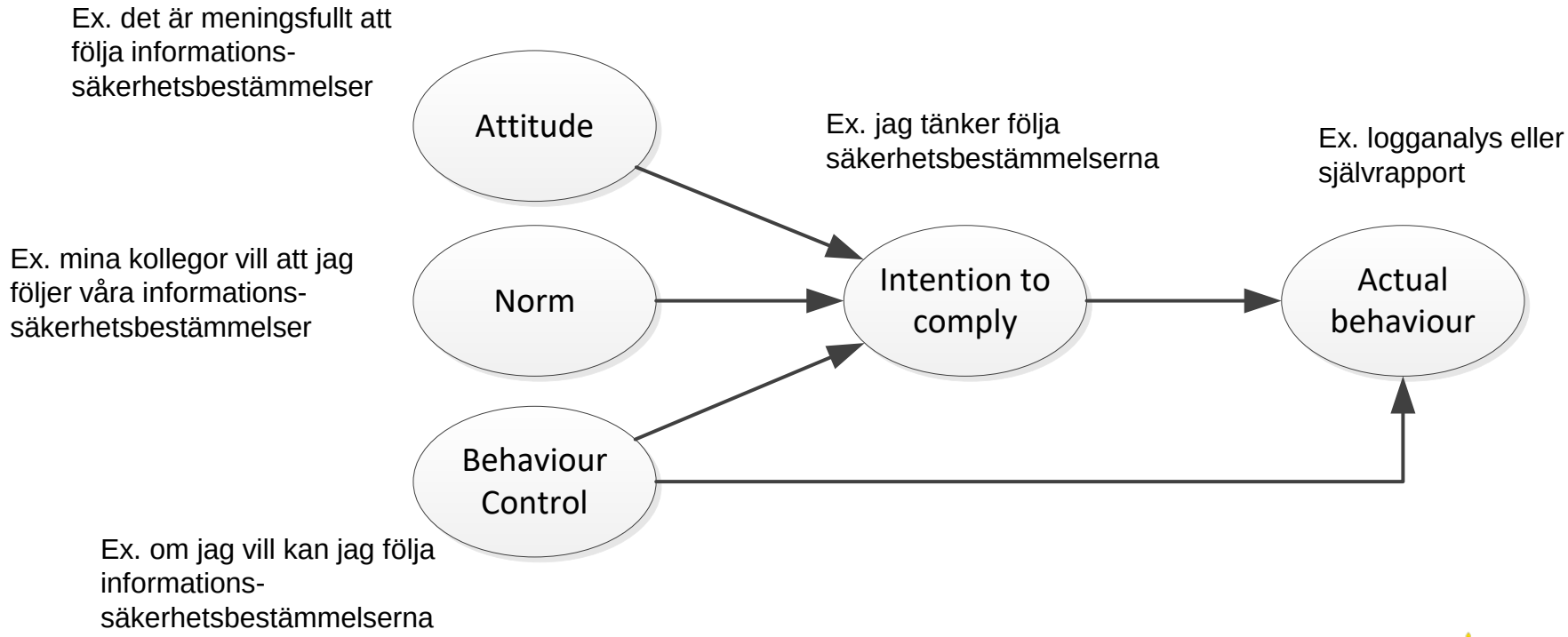
Två metoder för att erhålla data

- Enkäter
- Metaanalyser

Tre populära teorier

	Theory of planned behavior	Protection motivation theory	Deterrence theory
Huvudidé och huvudkoncept	Attityder, normer and upplevd beteendekontroll förklarar intentioner. Intentioner och beteendekontroll förklarar beteende.	Folk är rationella och kommer att efterleva bestämmelser om de ser ett reellt hot och efterlevnad är billigt, enkelt och effektivt.	Beteendet kan styras med straff. Hur hårda, sannolika och snabba straffen är spelar roll.
Normativ vägledning	Jobba på bra attityder, bra normer och att det ska vara lätt att göra rätt.	Se till att folk får ett positivt värde när de jämför kostnader och nyttor med bestämmelserna.	Skräm ordentligt med straff.
Ursprung	Socialpsykologi	Hälsobeteende	Kriminologi

Theory of planned behavior (TPB)



TPB-tolkning av en bestämmelse

Norm?

Ett lösenord till ett IT-system 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. DIfI&ish28smnoli (Dokumentet Instruktionen för IT- och informationssäkerhet har 82 sidor med nyttig och läsvärd information). Lösenord ska bytas minst en gång per år.

Stärka beteendekontroll?

FOI

Mer TPB-aktig formulering

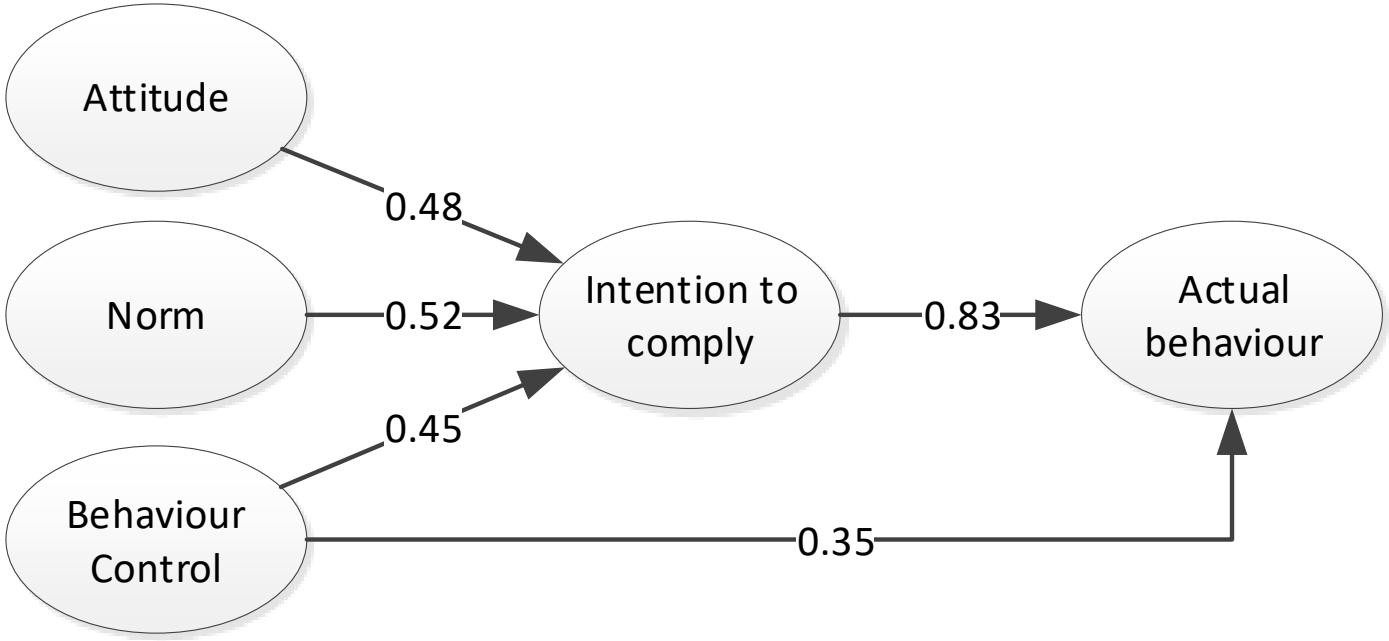
Attityd

Normer

Att skydda IT-system är viktigt. Det förväntas av användarna att de lösenord som används till IT-system 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. Exempelvis kan du skapa ”DIfI&ish28smnoli” från meningen ”Dokumentet Instruktion för IT- och informationssäkerhet har 82 sidor med nyttig och läsvärd information”. Lösenord behöver bara bytas en gång per år.

Upplevd beteendekontroll

The theory of planned behavior (TPB)



Protection motivation theory (PMT)

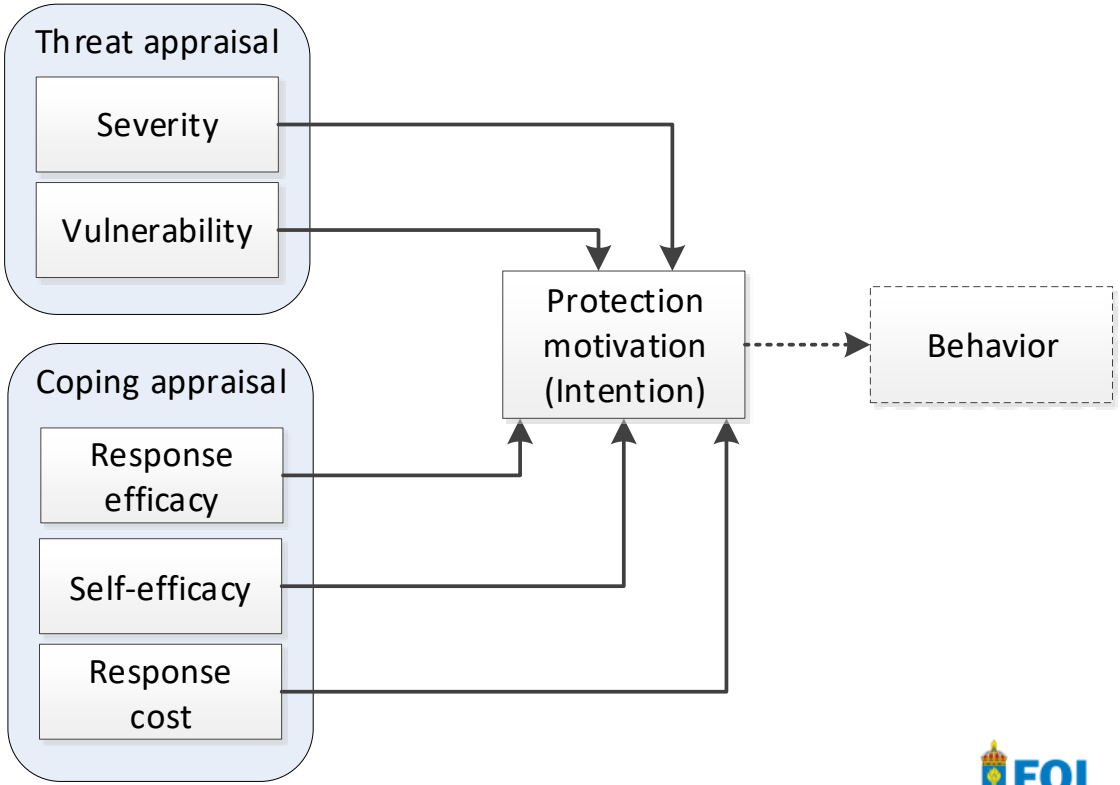
Ex. kostnaden för ett informationsläckage i min organisation skulle vara stor

Ex. informationsläckage kan drabba min organisation

Ex. informationssäkerhetsbestämmelserna minskar risken för informationsläckage

Ex. jag kan följa bestämmelserna om jag vill

Ex. att följa bestämmelserna kräver lite jobb



PMT tolkning av en bestämmelse

Indikerar hot

~Effektivt

Ett lösenord till ett IT-system 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. DIfI&ish28smnoli (Dokumentet Instruktion för IT- och informationssäkerhet har 82 sidor med nyttig och läsvärd information). Lösenord ska bytas minst en gång per år.

Hintar att det är enkelt och billigt

Mer PMT-aktig formulering

Vulnerability

Severity

Svaga lösenord kan användas för obehörigt nyttjande av IT-system, vilket kan få allvarliga följder. Därför bör lösenord vara så konstruerade att det inte kan gissas eller knäckas på ett enkelt sätt och är lätta att använda. Ett lösenord på 15 tecken som innehåller en blandning av versaler, gemener, siffror och specialtecken ger gott skydd om det byts varje år. Genom att utgå från en mening kan du enkelt skapa ett bra lösenord, t.ex. kan du skapa ”DIfI&ish28smnoli” för meningen ”Dokumentet Instruktion för IT- och informationssäkerhet har 82 sidor med nyttig och läsvärd information”.

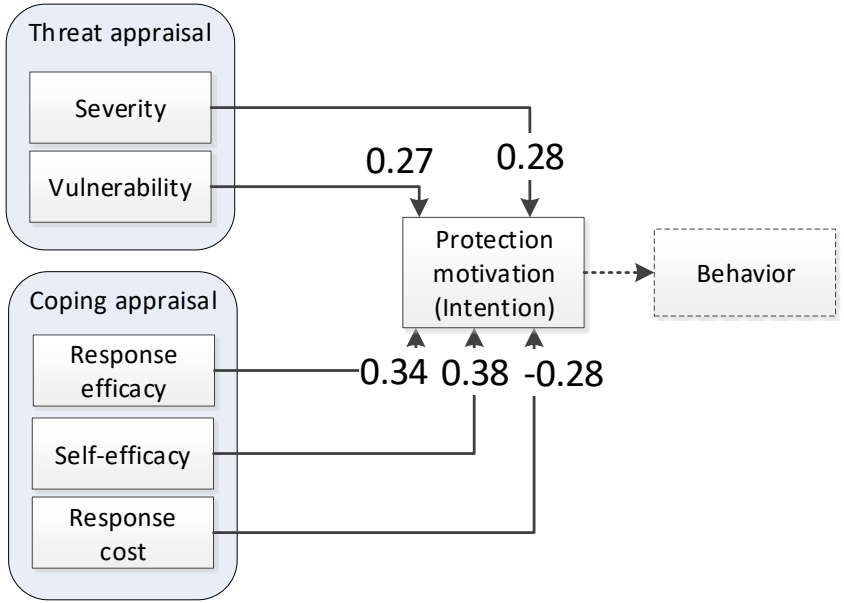
Response efficacy

Self-efficacy

Protection motivation theory (PMT)

Fungerar bättre

- för frivilliga beteenden än tvingande
- om hotet är riktat mot individen snarare än organisationen
- för precisa beteenden snarare än generella (lösenordshantering vs. bestämmelser i allmänhet)

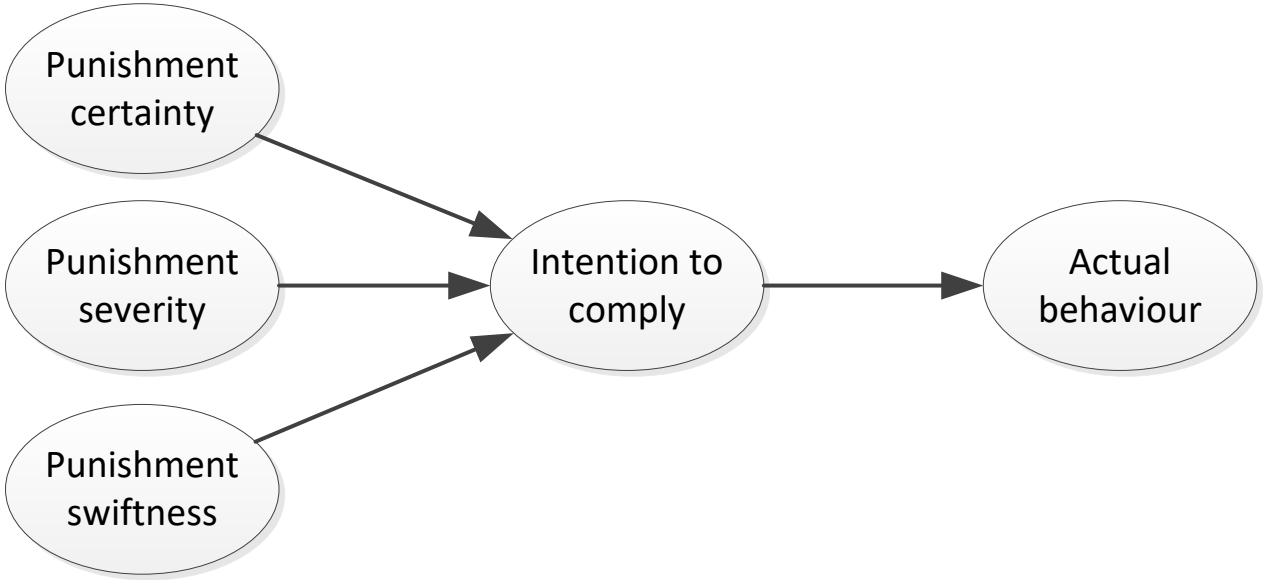


Deterrence theory

Ex. om jag bryter mot bestämmelserna kommer det att upptäckas

Ex. straffet mot att bryta mot bestämmelserna är kännbart

Ex. eventuella bestraffningar kommer att utfärdas fort efter upptäckt



DT-aktig formulering av en bestämmelse

Punishment certainty

Om inte IT-systemet i sig är begränsande, ska lösenord i IT-system bestå av minst 15 tecken samt innehålla en blandning av versaler, gemener, siffror och specialtecken. Organisationen genomför regelbundet tester av lösenord i sina IT-system och utreder alltid orsaken till incidenter. Medarbetare som bryter mot denna instruktion kommer omedelbart att rapporteras. Det kan i enlighet med 7 § i lagen om anställningsskydd leda till uppsägning och i enlighet med 19 kapitlet 9 § i brottsbalken leda till två års fängelse.

Punishment swiftness

Punishment severity

FOI

Sammanfattning av de populära teorierna

	Theory of planned behavior	Protection motivation theory	Deterrence theory
Huvudidé och huvudkoncept	Attityder, normer and upplevd beteendekontroll förklarar intentioner. Intentioner och beteendekontroll förklarar beteende	Individer är rationella och kommer att efterleva bestämmelser om de upplever ett hot och efterlevnad är billigt, enkelt och effektivt	Beteendet kan styras med straff. Hur hårda, sannolika och snabba straffen är spelar roll
Förmåga att förklara efterlevnad av informations-säkerhets-bestämmelser	45% av variansen i intentioner förklaras	38% av variansen i intentioner förklaras	Svag. Vissa studier pekar på omvänd effekt
Speciellt för informations-säkerhetsområdet	Inga tydliga säkerhetsspecifika fynd har gjorts	Inga, men teorin funkar bäst för säkerhetshot mot personen själv	Funkar förvånansvärt illa

FOI

Ytterligare en teori

	Neutralization theory
Huvudidé och huvudkoncept	Alla vet vad som är rätt och fel, men vissa är bra på att hitta på ursäkter för sitt beteende (att neutralisera)
Normativ vägledning	Oklart hur detta ska hanteras annat än vid val
Förmåga att förklara efterlevnad av informations-säkerhets-bestämmelser	Bra förklaringsförmåga i de två studier som har publicerats

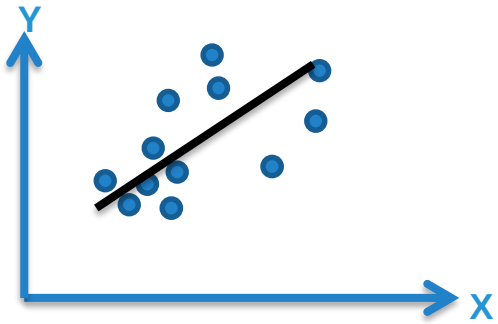
Utvidga Theory of planned behavior med fler variabler	(Ifinedo, 2012)	(Siponen et al., 2014)	(Sommestad et al., n.d.)	(Dugo, 2007)	(Bulgurcu et al., 2010)	(Herath and Rao, 2009)	(Zhang et al., 2009)	(Al-Omari et al., 2012)	(Hu et al., 2012)
Severity	0.00	0.01	0.03			0.00			
Vulnerability	0.02	0.01	0.00		0.01	0.00			
Response cost	0.02	0.00	0.02		0.03	0.01			
Response efficacy	0.03	0.00	0.00		0.00	0.02	0.01		
Anticipated regret			**0.07**		**0.01**				
Organizational Commitment				0.00		0.03			
Security culture				0.00					
Punishment certainty				0.02		0.02			
Punishment severity				0.01		0.00			
Rewards					0.02				
Benefit of compliance					0.00				
Work Impediment					0.03				
General information security awareness					**0.08**			**0.04[a]**	
Technology awareness								0.02	
Information security policy awareness					0.02				
Perceived cost of noncompliance					0.00				
Intrinsic Benefit					0.00				
Sanctions					0.00				
Threat appraisal (concern)						0.00			
Resource availability						0.00			
Descriptive norm						0.01			
Perceived top management participation									0.00
Perceived rule orientation									0.01
Perceived goal orientation									0.02

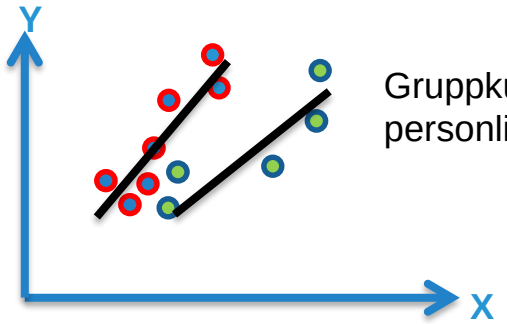
[A] Påverkan är omvänd mot den i (Bulgurcu et al., 2010).

Vad beror resterande del av variansen på!?

- Ekvationerna som används antar att alla respondenters beteende predikteras av samma variabler, med samma vikter på variablerna

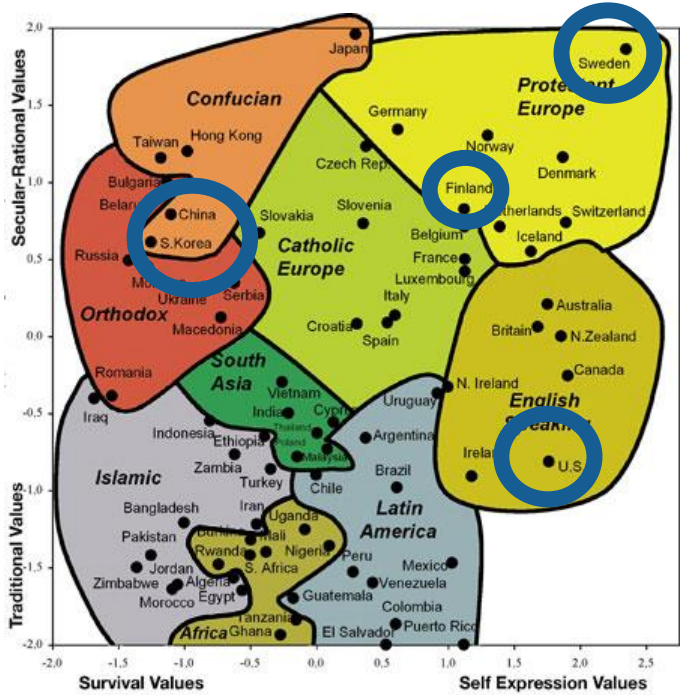
- Enkäterna är gjorda i olika kulturer och mot personer med olika personlighet





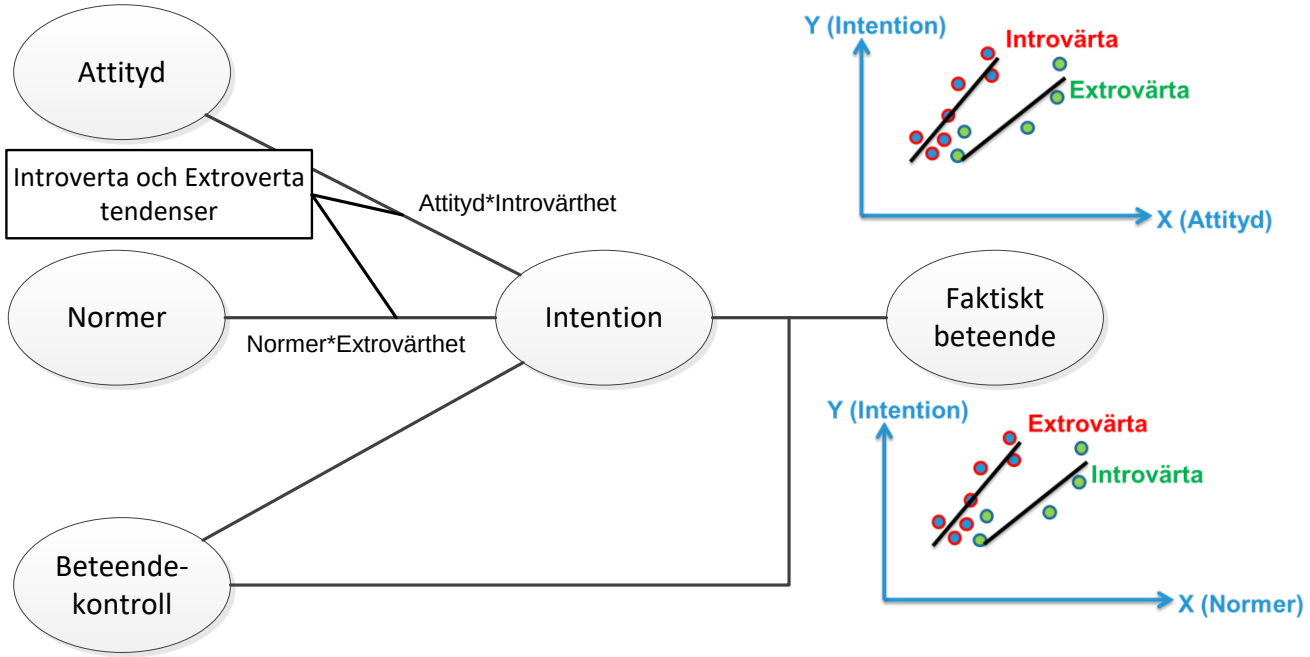
Gruppkultur och/eller personlighetstyper?

Nationell kultur



World Values Survey, http://www.worldvaluessurvey.org

Personlighetsdrag (exempel)



Rekommendationer

- Nästan alla säger att de tänker följa bestämmelser
  - Se till att de vet vad som står i bestämmelserna!
- Normer verkar vara lika viktigt som folks egna attityder
  - Jobba på normer!
- Om du berättar om risker …
  - … berätta också hur enkelt och effektivt det är att följa bestämmelserna!
- Straff verkar inte fungera på kontorsarbetare som hanterar känslig information
  - Hota inte med straff!
- Det finns etablerade teorier som förklarar informationssäkerhetsbeteende
  - Använd dessa teorier!

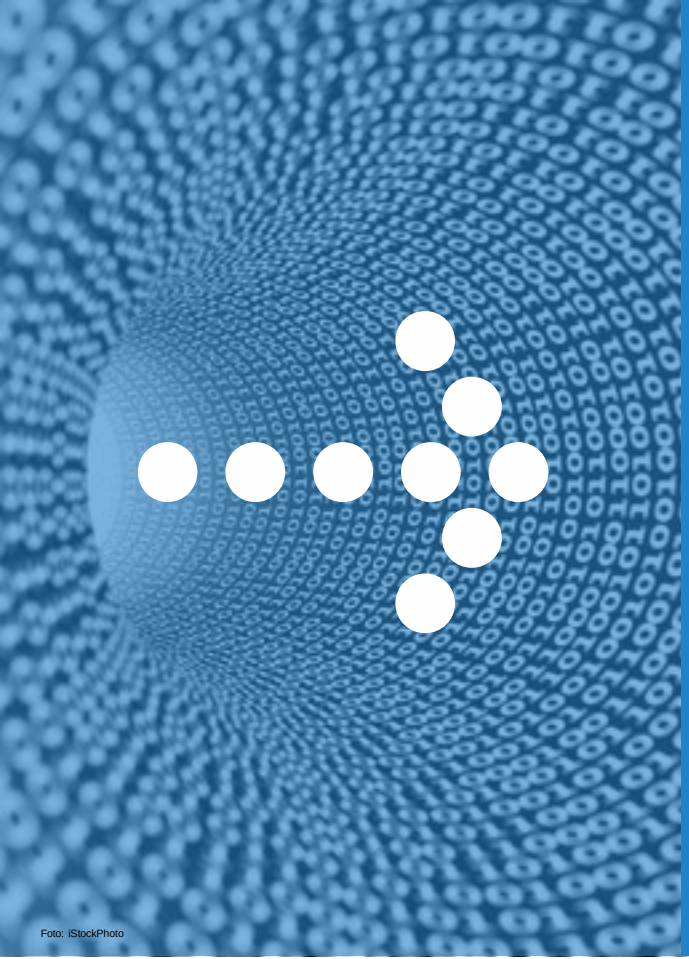


Foto: iStockPhoto

www.foi.se/securit

FOI