Varför följer inte användarna bestämmelser?

En metaanalys avseende informationssäkerhetsbestämmelser

TEODOR SOMMESTAD, JOHAN BENGTSSON,
JONAS HALLBERG

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3524--SE
ISSN 1650-1942

December 2012

Teodor Sommestad, Johan Bengtsson,
Jonas Hallberg

Varför följer inte användarna bestämmelser?

En metaanalys avseende informationssäkerhetsbestämmelser

Bild/Cover: Jonas Hallberg

Titel	Varför följer inte användarna bestämmelser? – En metaanalys avseende informationssäkerhetsbestämmelser
Title	Why do users comply with regulations? – A meta-analysis regarding information security regulations
Rapportnr/Report no	FOI-R--3524--SE
Månad/Month	December
Utgivningsår/Year	2012
Antal sidor/Pages	22 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten/Swedish Armed Forces
FoT område	Ledning och MSI
Projektnr/Project no	E36017
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Införandet av informationssäkerhetsbestämmelser, såsom säkerhetspolicyer och föreskrifter, är en central åtgärd i organisationers arbete med att nå en hög informationssäkerhetsnivå. En förutsättning för att informationssäkerhetsbestämmelser ska ha en positiv påverkan på informationssäkerheten är att de efterlevs. Avseende efterlevnad blir den avgörande frågan: *Vilka faktorer är det som påverkar huruvida informationssäkerhetsbestämmelser efterlevs?*

Det har genomförts forskningsstudier som syftar till att besvara frågan om vilka faktorer som påverkar efterlevnad av informationssäkerhetsbestämmelser. En del av dessa studier inkluderar kvantitativa resultat avseende hur olika faktorer påverkar efterlevnaden av bestämmelser. Denna rapport presenterar en meta-analys för att, utifrån publicerade kvantitativa studier, skapa en sammanställd bild av hur viktiga de olika faktorerna är. Baserat på resultaten från den genomförda metaanalysen besvaras exempelvis följande frågor.

Vem har nytta av denna information?
Alla som formulerar säkerhetsbestämmelser eller försöker se till att de efterlevs.

Vilken vetenskaplig teori är bäst att utgå ifrån?
Det finns inget tydligt svar, men *Theory of planned behavior* förklarar mest, medan *Deterrence theory* förklarar minst avseende vilka faktorer som påverkar efterlevnad.

Varför förklarar de vetenskapliga teorierna så lite av beteendet?
Mänskliga beteenden är komplexa och teorierna försöker förklara dessa med ett fåtal faktorer. Det är mycket begärt att modeller med få faktorer ska kunna förklara beteende med precision.

Vad borde göras för att öka efterlevnad av bestämmelser?
Det borde satsas resurser på att påverka de faktorer som verkar viktiga, exempelvis normer och attityder kopplade till bestämmelserna.

Finns det några problem rörande studiernas kvalitet?
Det finns flera svagheter och problem med studierna, exempelvis bristande metoder för urval av respondenter.

Vilken vetenskaplig teori använder Försvarsmakten idag?
Försvarsmakten verkar använda en kombination av *Deterrence theory* och *Protection motivation theory*.

Spelar inte bestämmelserna i sig någon roll för om de efterlevs?
Bestämmelsernas relevans spelar roll för efterlevnad, men hur de formuleras och kommuniceras tycks vara av ringa betydelse i de fall dessa faktorer har undersökts.

Nyckelord: Informationssäkerhet, säkerhetspolicy, metaanalys

Summary

The introduction of information security regulations is a key element in the efforts of organizations to achieve a high level of information security. In order for information security regulations to contribute to improved information security, the users have to comply with them. Therefore, it is crucial to know: *What affects whether the users comply with the information security regulations?*

A number of research studies have been performed in order to identify what affects the compliance. Some of these studies include quantitative results regarding how different factors affect the information security regulations compliance. This report presents a meta-analysis based on published quantitative studies in order to create a consolidated view of the importance of various factors. Based on the results of the meta-analysis nine questions are addressed, including the following examples:

Who will benefit from this information?
Anyone who creates security regulations or tries to ensure that they are complied with will benefit from this information.

Which scientific theory is best to start from?
There is no clear answer, but the *Theory of planned behavior* seems to explain the most, while *Deterrence theory* explains the least.

Why do the scientific theories explain such a small part of the behavior?
Human behavior is complex and the theories attempt to explain it with only a few variables. There are also measurement problems and weaknesses in the studies.

What should be done to improve the compliance?
Focus should be on the factors that seem important, such as norms and attitudes related to the regulations.

Are there any problems concerning the quality of the studies?
There are several weaknesses and problems with the studies, such as a lack of methods for the selection of respondents.

Which scientific theory do the Swedish Armed Forces use today?
It seems to be a combination of *Deterrence Theory* and *Protection Motivation Theory*.

Do the policies themselves affect whether they are complied with?
The relevance is important, but how the policies are formulated and communicated seems to be irrelevant when these factors have been investigated.

Keywords: Information security, security policy, regulations, meta-analysis

Innehåll

1 Inledning

Att ha en hög informationssäkerhet är något som eftersträvas av de flesta organisationer. Medlen som kan användas för att nå en hög informationssäkerhet är många. Att definiera informationssäkerhetsbestämmelser som medarbetarna ska följa är i de allra flesta fall en central åtgärd. Informationssäkerhetsbestämmelserna ska beskriva hur organisationens ledning förväntar sig att information ska hanteras i organisationen. Bestämmelserna är ett sätt för ledningen att se till att medarbetarna beter sig på ett sätt som anses välavvägt, exempelvis med hänsyn till de kostnader och nyttor som bestämmelserna för med sig. Informationssäkerhetsbestämmelserna beskrivs ofta i flera olika dokument såsom handböcker, intranätsidor, skriftliga beslut av chefer eller dokument med namn som säkerhetspolicy eller skyddsföreskrift.[1]

En förutsättning för att informationssäkerhetsbestämmelser ska ha en positiv påverkan på informationssäkerheten i en organisation är att bestämmelserna faktiskt följs av de anställda. För att få en bättre förståelse för vad som påverkar huruvida bestämmelser efterlevs har det genomförts flertalet forskningsstudier runt om i världen. Dessa har, på olika sätt, undersökt i vilken utsträckning olika faktorer påverkar graden av efterlevnad. Denna rapport redovisar arbetet avseende genomförandet av en metaanalys för att sammanställa hur viktiga olika faktorer är för efterlevnaden av bestämmelser[2]. Den genomförda metaanalysen är den första som genomförts inom området och resultaten är av stort intresse för både experter och forskare. Denna rapport återger de viktigaste resultaten och slutsatserna från den genomförda metaanalysen.

1.1 Genomförande

För att resultatet av en metaanalys ska vara rättvisande och transparent behövs en systematisk metod för att söka efter studier och för att avgöra vilka som ska inkluderas. Utifrån fördefinierade sökningar i artikeldatabaser identifierades 462 publikationer som skulle kunna vara relevanta för studien. Utöver dessa mer formella sökningar så gjordes även manuella sökningar på Internet efter artiklar som skulle kunna vara av intresse. Exempelvis genomsöktes referenslistor i artiklar som bedömts som relevanta för att hitta ytterligare artiklar.

[1] På engelska används ofta begreppet ”security policy” som ett samlingsnamn för alla de bestämmelser som finns definierade. Eftersom informationssäkerhetspolicy i Sverige oftast syftar till ett specifikt, kortare dokument så används istället begreppet informationssäkerhetsbestämmelser som samlingsnamn.

[2] Sommestad, T. Hallberg, J. Lundholm, K., Bengtsson, J., *Variables influencing information security policy compliance: a systematic review of quantitative studies*. Opublicerad (vetenskplig granskning pågår).

För att en artikel skulle inkluderas i metaanalysen krävdes att studien

1) undersökte vilka faktorer som påverkade efterlevnad av bestämmelser
2) innehöll en kvantitativ analys
3) var vetenskapligt granskad.

Efter flertalet granskningsomgångar identifierades slutligen 29 studier som uppfyllde de tre krav som hade satts upp. Alla dessa 29 studier undersökte området med hjälp av enkäter. Resultaten från studierna sammanställdes kvantitativt för att på så sätt skapa en bild av aktuell status inom området och svara på vilka faktorer som är av betydelse för efterlevnad av bestämmelser och hur viktiga dessa är.

Den kvantitativa sammanställningen, eller metaanalysen som det formellt kallas, görs genom att slå ihop de enskilda resultaten från flera enskilda studier till ett enda (mer tillförlitligt) värde. Det allra vanligaste förfarandet är att beräkna viktade medelvärden för de studier som ingår. Vikten i sammanräkningen bör då återspegla hur stor osäkerhet som studiens enskilda resultat har. En studie med hög osäkerhet bör ges mindre vikt och en studie med låg osäkerhet bör ges mer vikt. I denna sammanställning användes antalet respondenter i enkätundersökningen för att väga samman de olika studierna resultat.

Ett problem vid metaanalyser är att studier med svaga resultat inte publiceras och därmed inte kommer med i metaanalysens sammanställning. Genom analys av resultaten konstaterades att inget uppenbart problem finns med detta så kallade skrivbordsproblem. Det vill säga, det finns inget som talar för att studier med svaga resultat (som att en viss variabel är oviktig) har stoppats undan i byrålådan istället för att publiceras. Denna slutsats baseras på att det är en normal spridning av de genomförda studierna avseende resultatens styrka och antal respondenter.

1.2 Läsanvisning

I kapitel 2 presenteras en sammanfattning av studiens resultat. Denna sammanfattning beskriver resultaten utifrån de beteendevetenskapliga teorier som testats i relation till efterlevnad av informationssäkerhetsbestämmelser. För att undvika missförstånd har de engelska namnen behållits på teorierna.

I kapitel 3 ges svar på nio frågor som läsaren kan tänkas ha. Dessa svarar i huvudsak på hur informationen i kapitel 2 lämpligen bör användas. Även frågor rörande tillförlitligheten i resultaten besvaras.

2 Vad påverkar?

I de 29 utvalda studierna används olika teorier som försöker förklara och prediktera individers beteende avseende efterlevnad av informationssäkerhets-bestämmelser. Av dessa redovisas i denna rapport fem teorier, vilka återges övergripande i Tabell 1 och beskrivs i avsnitt 2.1 - 2.5.

I avsnitten nedan kommer betydelsen av en viss faktor att anges med hur många procent av variansen som förklaras med hjälp av denna faktor. Varians är ett mått på variation. I alla studier så varierar det exempelvis mellan personer hur de följer regler – det finns varians. Om en faktor förklarar 100% av variansen så förklarar den all variation och det går att göra exakta förutsägelser med hjälp av den. Om en faktor förklarar 0% av variansen så hjälper den inte alls till att förklara eller prediktera fenomenet i fråga.

Tabell 1. Fem beteendevetenskapliga teorier som har använts för att förklara vad som påverkar efterlevnad av och brott mot informationssäkerhetsbestämmelser. För var och en av teorierna anges referens till beskrivande litteratur, de enligt teorin viktigaste faktorerna och teorins förklaringsförmåga.

Teori	**Huvudfaktorer**	**Förklaringsförmåga**
Deterrence theory (D'Arcy & Herath 2011)	• Sanktioners sannolikhet • Sanktioners allvarlighet • Sanktionssnabbhet • Uttryckliga belöningar för efterlevnad	Dålig. Förklarar varken attityder, intentioner eller faktiska beteenden bra.
Theory of reasoned action & theory of planned behavior (Ajzen 1991)	• Attityd • Subjektiv norm • Beteendekontroll	Förhållandevis bra. Men teorin förklarar långt ifrån all variation som finns i intention och faktiskt beteende.
Neutralization theory (Siponen & Vance 2010)	• Förnekande av ansvar • Förnekande av skada • Fördömmande av de som dömer • Åberopande av högre lojaliteter • Försvar av nödvändighet • Kompensationstänkande (ungefär: "jag är ju så duktig på annat").	Endast två studier är gjorda på denna teori. Men den förklarar variansen i intentioner förhållandevis bra. De olika neutraliseringsteknikerna förklarar ungefär lika mycket vardera.
Protection motivation theory (Norman et al. 2005)	Hotbedömning: • Sårbarhet: upplevd sannolikhet för att hotet realiseras • Allvarlighet: upplevd konsekvens av realiserat hot Genomförbarhetsbedömning: • Beteendeeffekt: hur väl beteendet i fråga anses skydda mot hotet • Beteendekontroll: i vilken utsträckning man tror sig kunna utföra beteendet	Faktorerna tycks vara av betydelse, men förklarar endast en liten del av intention och faktiskt beteende.
Social control theory (Wiatrowski et al. 1981) (Nye 1958)	• Sociala band: hängivenhet, engagemang, involvering. • Kontrolltyper: direkt kontroll, indirekt kontroll, intern kontroll,	Förhållandevis dålig. Sociala band förklarar väldigt lite. Direkt och indirekt kontroll är snarlika Deterrence theory. Intern kontroll tycks ha en viss betydelse.

2.1 Deterrence theory

Deterrence theory (ungefär *avskräckningsteori* på svenska) har sitt ursprung i klassisk kriminologi. Grundidén är att individens beslut om att genomföra eller avstå från brott fattas efter att ha vägt nyttor mot kostnader. Valet faller på beslutsalternativet med mest fördelaktig differens mellan nytta och kostnad för individen. Teorin fokuserade ursprungligen på formella sanktioner (t.ex. legala) och hur dessa upplevs. Numera inkluderas ofta informella sanktioner, exempelvis sådana som är skambeläggande. Sanktionernas upplevda sannolikhet att inträffa, deras allvarlighet och snabbheten de inträffar med är incitament som styr beteendet hos individen enligt *Deterrence theory*.

Av de teorier som prövats, med koppling till efterlevnad av och brott mot informationssäkerhetsbestämmelser, så är *Deterrence theory* en av dem som undersökts i flest studier. Resultaten är förhållandevis tydliga – denna teori är dålig på att förklara varför informationssäkerhetsbestämmelser efterlevs eller ej. Exempelvis förklarar sanktionernas upplevda allvarlighet eller sanktionernas sannolikhet knappt någon del (mindre än 1%) av den variation som mäts i individers intention att efterleva bestämmelser.

Teorins förklaringsförmåga är något bättre då det handlar om direkta brott mot bestämmelserna istället för efterlevnad. Exempelvis förklarar sanktionernas allvarlighet attityd mot regelbrott förhållandevis bra (22% av variansen). Det är dock endast en mindre studie som har undersökt förhållandet utifrån direkta brott.

Tyvärr predikterar inte heller explicit uppmuntrande incitament individers attityder, intentioner eller faktiskt beteende särskilt bra, även om de generellt lyckas bättre än de incitament som kopplas till sanktioner. Exempelvis förklarar upplevda inre och yttre nyttor med ett brott mot informationssäkerhets-bestämmelser endast 10% respektive 2% av variansen i intentionerna att genomföra brotten.

2.2 Theory of reasoned action & Theory of planned behavior

Theory of reasoned action och dess utökning *Theory of planned behavior* försöker främst förklara individers intentioner och i viss utsträckning även individers faktiska beteende. *Theory of reasoned action* proklamerar att intentioner angående ett beteende påverkas av individens *attityd* till beteendet och den *norm* som individen tror gäller. I utökningen *Theory of planned behavior* tas det fasta på att dessa två faktorer inte räcker för att förklara intentioner och beteenden när individer upplever att de saknar möjlighet att påverka sitt beteende. Detta är exempelvis något som en nikotinberoende rökare kan uppleva.

Theory of planned behavior lägger därför till faktorn *upplevd beteendekontroll*. Den upplevda beteendekontrollen påverkar enligt teorin både intentionerna och det faktiska beteendet. Dessa två teorier har undersökts i relation till efterlevnad av bestämmelser i flera studier. De förklarar respondenternas intentioner förhållandevis väl.

Attityd, normer och upplevd beteendekontroll förklarar vardera runt 10% av variansen inom intentionerna att följa regler. Cirka 40% av det faktiska beteendet förklaras av intentionerna att följa regler och cirka 5% av det faktiska beteendet förklaras av upplevd beteendekontroll. Variansen avseende intention att uppsåtligt bryta mot regler förklaras i än större utsträckning av attityd (cirka 18%) och av normen (cirka 12%). Beteendekontrol tycks dock vara av mindre betydelse för brottsintentioner (cirka 2%). Samtidigt som dessa värden indikerar faktorernas styrka överlag så säger inte teorin att det ska finnas en allmängiltig vikt för faktorerna, utan vikten en faktor har kan variera mellan beteende och miljöer. Exempelvis är upplevd beteendekontroll endast viktig då individer upplever att de saknar valmöjligheter.

2.3 Neutralization theory

Neutralization theory togs ursprungligen fram som en förklaringsmodell för ungdomsbrottslingars gärningar. Enligt teorin så bär alla individer på en snarlik bild av vad som är rätt och fel. De vet också om att de har ett moraliskt ansvar att följa reglerna. Enligt teorin är dock vissa individer bättre än andra på att tysta ner (neutralisera) de viljor som uppmanar oss att fullfölja vårt moraliska ansvar.

Det har föreslagits att ett antal tekniker kan användas för att neutralisera (bortförklara/ursäkta) omoraliskt beteende. Kopplat till informationssäkerhets-bestämmelser så har följande faktorer testats (Siponen & Vance 2010): förnekande av ansvar, förnekande av skada, fördömmande av de som dömer, åberopande av högre aktoriteter, försvar av nödvändighet och kompensationstänkande (ungefär: ”jag är ju så duktig på annat”).

Två studier har testat *Neutralization theory.* Båda dessa visar på en relativt god förklaringsförmåga för teorin som helhet. I den större av de två studierna lyckas teorin förklara hela 36% av variansen i intentioner rörande misskötsel. I den mindre studien förklarades 10% av variansen i intentioner rörande misskötsel. De testade neutraliseringsteknikerna tycks bidra ungefär lika mycket var till intentionerna.

2.4 Protection motivation theory

Protection motivation theory säger att individer följer säkerhetsbestämmelserna om de anser att hotet är påtagligt, om de tror att de kan utföra det som står i

bestämmelserna och om de tror att det hjälper. Det finns fyra faktorer som tros styra individers agerande. Dessa faktorer är indelade i två kategorier. I kategorin hotbedömning återfinns följande två faktorer:

- Sårbarhet – upplevd sannolikhet för att hotet realiseras
- Allvarlighet – upplevd konsekvens av realiserat hot.

I kategorin genomförbarhetsbedömning återfinns följande två faktorer:

- Beteendeeffekt – hur väl beteendet i fråga anses skydda mot hotet
- Beteendekontroll – i vilken utsträckning man tror sig kunna utföra beteendet.

Ingen studie har undersökt hur denna teori på egen hand kan förklara beteenden, men faktorerna som ingår i teorin har testats i flera studier. De mätningar som har gjorts har visat förhållandevis svaga resultat. Cirka 4% av variansen i intentionerna kan förklaras med skillnader i den upplevda sannolikheten att hotet realiseras. Ungefär 4% av variansen i beteendet förklaras också med hjälp av konsekvensen om hotet realiseras. En mer övergripande hotbedömning (sårbarhet och allvarlighet) förklarar cirka 10% av attitydskillnaderna, men endast cirka 1% av skillnaderna i beteende. 4% av variansen i beteendet förklaras av hur väl efterlevnad av bestämmelsen upplevs skydda mot hotet. Den självupplevda förmågan en individ har att utföra det önskade beteendet (i princip samma faktor som *upplevd beteendekontroll* i *Theory of planned behavior*) förklarar ungefär 4% av variansen i intentioner och beteende.

2.5 Social control theory

Social control theory har sitt ursprung i kriminologin och säger att socialisationsprocessen och socialt lärande skapar självkontroll hos individen samt minskar avvikande och asocialt beteende. Till skillnad från många andra teorier så säger denna teori när brott *inte* begås, nämligen då det finns en ”bra” social kontroll som ökar förmågan att motstå frestelser. Det finns fyra typer av social kontroll (Nye 1958):

- direkt kontroll (t.ex. monetära straff)
- indirekt kontroll (t.ex. risk för skam)
- intern kontroll (samvete, överjaget och skuldkänslor)
- behovsuppfyllelse (uppfyllda behov minskar benägenheten att begå brott).

Det behöver dessutom finnas alternativa medel än brott att nå målen enligt (Nye 1958). Precis som för *Protection motivation theory* så har ingen studie testat

denna teori enskilt. Istället återkommer delar av den i flera andra studier. De två första kontrolltyperna faller in under *Deterrence theory* och förklarar beteendemönster kopplat till informationssäkerhetsbestämmelser ganska dåligt (se 2.1).

Intern kontroll har mätts i form av frågor kopplade till moral, såsom den subjektiva bilden av normen i *Theory of planned behavior*, och har då förklarat förhållandevis mycket av variansen i intentionerna, men långt ifrån all varians. Även mått på de sociala bandens styrka i en organisation, som tillgivenhet och hängivenhet till organisationen, förklarar ytterst lite av variansen i intentioner. Överlag tycks *Social control theory* ha dåligt stöd i de empiriska studierna kopplade till informationssäkerhetsbestämmelser.

3 Frågor och svar

Sammanställningen av existerande forskning visar att det finns mycket osäkerhet kring vad som får människor att följa (eller bryta mot) säkerhetsbestämmelser. Nedan besvaras frågor som kan ställas kring den genomförda sammanställningen och vad den kan nyttjas till.

3.1 Vem har nytta av denna information?

Försvarsmakten eftersträvar att uppnå så bra informationssäkerhet som möjligt med de medel som finns att tillgå. Det är då viktigt att ha en djup förståelse för användarna av informationssystem och vad som får dem att följa eller bryta mot de bestämmelser som Försvarsmakten har rörande informationssäkerhet. Utan kunskap inom detta område är det svårt att bedöma vilken effekt införandet av olika typer av säkerhetsbestämmelser och säkerhetsfunktioner kommer att få. Bristen på denna kunskap gör det även svårt att veta hur en så stor effekt som möjligt uppnås.

Förståelse för användarnas beteende är värdefullt på flera nivåer i informationssäkerhetsarbetet. Det kan exempelvis vara ett stöd vid prioritering av olika åtgärder. Om forskningen entydigt skulle visa att attitydfrågor är avgörande för huruvida individer följer säkerhetsbestämmelser så bör åtgärder med effekt på dessa attityder prioriteras. När kursmaterial eller instruktioner skapas bör hänsyn tas till attityd. Attityd skulle i så fall kunna användas som ett mått på hur god säkerhetskultur/säkerhetsdisciplin en organisation har. Nu är det (tyvärr) inte så enkelt att allt handlar om attityd, även om attityd verkar vara en av de viktigare faktorerna.

3.2 Vilken teori är bäst att utgå ifrån?

De teorier som gav bäst resultat i de genomförda studierna är *Theory of planned behavior* och *Neutralization theory*. Detta betyder inte att dessa två teorier är de enda som kan användas som utgångspunkt. Eftersom informationssäkerhetsområdet är relativt omfattande och beteende som påverkar informationssäkerheten uppkommer i många olika typer av situationer hos ett brett spektrum av aktörer, kan det vara så att olika teorier passar bäst för olika personer och olika sammanhang. Det är inte orimligt att tänka sig att vissa personer reagerar starkt på attityd och normer (*Theory of planned behavior*), medan andra försöker bete sig rationellt riskhanteringsmässigt (*Protection motivation theory*). Sammantaget kanske det är en kombination av teorier som krävs för att kunna förklara variationer i efterlevnad av informationssäkerhetsbestämmelser, det vill säga att det beror på omständigheterna vilken teori som fungerar bäst.

Ett relativt tydligt resultat är att *Deterrence theory* är dålig på att förklara variation i efterlevnad, men detta behöver inte betyda att teorin är helt irrelevant. Det kan finnas bakomliggande orsaker till att resultaten i de aktuella studierna inte visade på större förklaringsförmåga för *Deterrence theory*, se avsnitt 3.3 och 3.5 nedan.

Ett annat tänkbart mål, än att förändra beteendet hos människor, är att minska variationen i hur de ser på bestämmelseefterlevnad. Detta innebär inte nödvändigtvis att beteenden förbättras generellt, utan att det uppnås en situation med en acceptabel bestämmelseefterlevnad som inte varierar i absoluta mått från person till person. Huruvida arbete enligt en viss teori minskar variationen generellt och gör beteenden mer likformiga har ingen av studierna undersökt. Studierna har undersökt hur den varians som uppmätts mellan individerna kan förklaras med skillnader mellan individerna. Det har alltså inte studerats hur stor varians som finns inom en organisation som angriper problemet på ett visst sätt.

3.3 Varför förklarar teorierna så lite av beteendet?

Ingen av teorierna lyckas med sina faktorer förklara 100% av variansen i beteende. De bättre teorierna förklarar mindre än hälften av variansen i intentioner och cirka hälften av variansen i beteende. Det finns många tänkbara orsaker till varför teorierna inte har större förklaringsförmåga.

Först och främst försöker teorierna förklara något så komplext som mänskligt beteende i organisationer. Det är mycket begärt att modeller med få faktorer ska kunna förklara beteende med precision. Det är rimligt att det egentligen är många faktorer som spelar roll. Teorierna försöker bara fånga de allra viktigaste.

Dessutom är de faktorer som används i teorierna förhållandevis diffusa koncept som är svåra att mäta i praktiken med något tillförlitligt instrument. Typiskt mäts de genom att respondenterna besvarar 3-4 snarlika frågor med givna svarsalternativ. Svarsalternativen är direkt kopplade till siffervärden. Baserat på de erhållna svaren beräknas ett värde för den aktuella faktorn genom att ta medelvärdet av svaren på de enskilda frågorna. Frågorna kan exempelvis handla om respondentens attityd kopplat till ett visst beteende. Även om dessa 3-4 frågor syftar till att mäta samma sak (attityd) varierar de erhållna värdena. Det finns alltså ett mätfel. Med mätfel i indata är det svårt att göra precisa prediktioner av utdata.

En tredje möjlig orsak till teoriernas begränsade förklaringsförmåga är att vad som är viktigt skiljer sig från person till person. Till exempel är det rimligt att vissa personer bryr sig mycket om vad andra tycker medan andra personer bryr sig mer om faktiska risker kopplade till beteenden. Det finns flera resultat som pekar åt detta håll. Exempelvis svarar olika personlighetstyper olika på olika

former av träning (Workman & Gathegi 2007) och personer med olika moralisk mognad tilldelar olika vikt till sanktioner (D'Arcy & Herath 2011). Mer komplexa samband av dessa slag har förbisetts i de flesta studier och ges ingen vikt i teorierna. Ytterligare metodmässiga problem som kan bidra till sämre förklaringsförmåga ges i avsnitt 3.5.

3.4 Vad borde göras för att öka efterlevnaden av bestämmelserna?

Teorierna försöker förklara beteenden och intentioner med olika faktorer. För att öka efterlevand av bestämmelser bör de faktorer som är möjliga att påverka och samtidigt har en effekt på efterlevnaden adresseras.

Tyvärr är det inte nödvändigtvis så att faktorer som förklarar variansen även har en kausal påverkan på efterlevnaden. Exempelvis har tidigare beteende visat sig vara en ypperlig faktor för att prediktera kommande beteende. Trots detta tror få människor att dagens beteende har en direkt påverkan på morgondagens beteende. Vanor är med andra ord ingen kausal faktor (men de samvarierar med sådana). Teorierna i kapitel 2 försöker att använda vad som tros vara kausala faktorer, men det är inte uppenbart att de lyckas. Då studierna inte undersökt teorierna i form av välutformade experiment är beläggen för kausalitet (eller avsaknad av det) rena argumentationer.

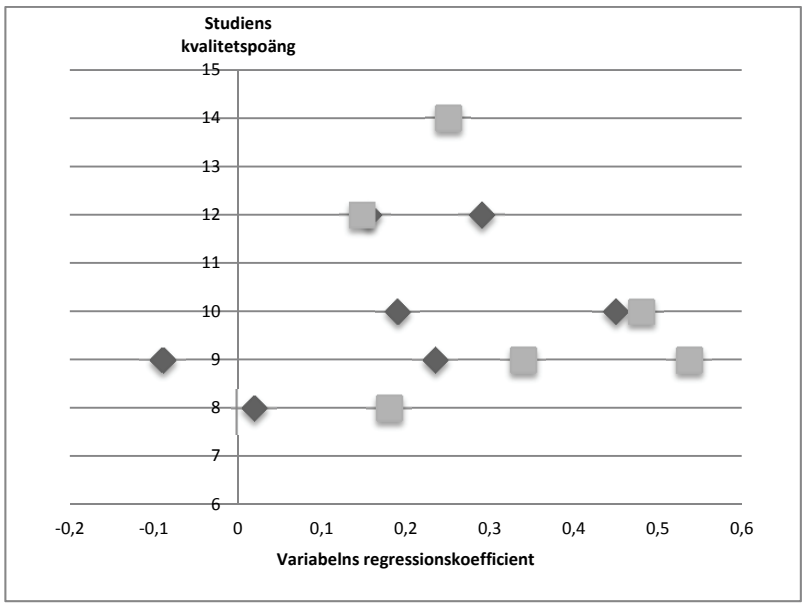
Ett svar på frågan om vad som borde göras är att påverka just kausala faktorer. Allt som samvarierar med efterlevnad är inte kausala faktorer. Det lämnas till läsaren av denna rapport att själv bedöma hur stor kausal påverkan en faktor har.

Förutom distinktionen mellan kausal påverkan och prediktiv förmåga så kan det vid informationssäkerhetsarbete vara meningsfullt att utgå från miljön och vad som kan vara effektivt i just denna miljö. Det kan vara stor skillnad på hur stor effekt en faktor har i olika miljöer. Exempelvis i en studie som undersökte olika former av informationssäkerhetsträning så fann man att cirka hälften av variationen i effekt som två gruppers träning (etikbaserad eller hotbaserad) hade berodde på deltagarnas syn på hur viktiga normer var (Workman & Gathegi 2007). Med detta menas att de personer som anser att normer är viktiga reagerar på etikbaserad träning och de som inte gör det reagerar på hotbaserad träning. Flera liknande exempel finns. Studier inom andra domäner än informations-säkerhet har bland annat funnit att människors attityd är viktigare när det kommer till beteenden som det saknas en tydlig moralisk norm för.

Förutom att inriktas på kausala faktorer så bör åtgärder alltså tänka på hur viktiga dessa kausala faktorer kan vara just i denna miljö. Det finns förhållandevis lite forskning på hur styrkan som olika kausala faktorer har påverkas av miljön och andra betingelser (som individen). Detta gör det svårt att ge ett konkret och fullständigt svar på frågan om vad som borde göras. Det verkar "bero på".

3.5 Finns det några problem rörande studiernas kvalitet?

Inom ramen för metaanalysen gjordes en allmän bedömning av enkätstudiernas kvalitet. Kvalitetsbedömningen baserades på kriterier, framtagna för enkätstudier, av Malhotra och Grover (1998). Överlag är kvaliteten på de studier som genomförts god. Som förväntat tycks en studies kvalitet ha betydelse för hur väl studiens resultat överensstämmer med resultat från andra studier. Studier av sämre kvalitet borde rimligen få mer spridda resultat, medan studier av bättre kvalitet rimligen borde ha mindre varierade resultat som hamnar närmare medelvärdet. Kvalitetspoäng och regressionskoefficient (variabelns viktighet) visas i Figur 1 för de två relationer som studerats i flest antal studier (sex respektive sju studier).



Figur 1: Kvalitetspoäng för olika studier, som försöker förklara samband mellan normativ uppfattning respektive attityd till efterlevnad och intention att efterleva bestämmelser, kopplad till den styrka som erhölls.

Det största problemet med studiernas kvalitet finns i hur respondenterna valts ut. Det är alltigenom bekvämlighetsurval där antingen en svårdefinierad grupp av blandade respondenter (exempelvis från en webbpanel) eller medarbetare från ett fåtal utvalda organisationer har använts. Många av studierna har dessutom en relativt låg svarsfrekvens. Denna oförsiktighet i urvalet kan innebära att urvalet är skevt i olika avseenden. Exempelvis kan ett oförsiktigt urval ge en övervikt av respondenter som

- ser säkerhet som något intressant och viktigt
- har gott om tid över (för att svara på enkäter)
- ifrågasätter nuvarande bestämmelser.

Skeva urval som dessa skulle kunna leda till resultat som inte stämmer överens med hur hela populationen av respondenter ser på saker och ting.

Ett annat stort problem som följer av hur respondenter valts är att populationen i sig sällan är väldefinierad. Det tas dessutom sällan hänsyn till att bakomliggande faktorer kan vara helt olika i olika miljöer. Om dessa bakomliggande faktorer har en inverkan så kommer den inte att märkas i resultatet. Resultat från andra domäner än informationssäkerhet antyder exempelvis att svar från människor som lever i kollektivistska miljöer (Sydkorea) inte bör blandas med svar från individualistiska miljöer (USA) (Park 2009) eftersom de ger olika vikt till sociala attityder och subjektiva normer. Att blanda mer eller mindre okontrollerat bland respondenter döljer sådana skillnader och leder till otydliga resultat.

Ytterligare ett potentiellt problem är att de allra flesta av studierna är gjorda enkom genom mätningar och inte med hjälp av kontrollerade experiment. Det innebär att bakomliggande faktorer kan missas. Exempelvis kan det vara så att avskräckningsmetoder (d.v.s. *Deterrence theory*) används i situationer där allt annat är omöjligt eller redan har gjorts, men där individer fortfarande vill bryta mot bestämmelser av någon anledning. En sådan anledning kan exempelvis vara att personen anser att det är moraliskt rätt. I så fall skulle det kunna förklara varför just resultaten kopplade till hot om sanktioner har så liten inverkan. Sådana bakomliggande faktorer skulle i princip kunna leda till att avskräckningsmetoder leder till mindre efterlevnad enligt mätningarna – avskräckningsmetoder används för de bestämmelser som människor är notoriskt dåliga på att följa, vilket innebär att användning av avskräckningsmetoder ofta sammanfaller med låg efterlevnad av bestämmelserna. Notera att sådana risker finns med alla teorier och alla faktorer, *Deterrence theory* används enbart som ett exempel. Bakomliggande faktorer kan lika väl få effekter på andra teorier i testerna, exempelvis då regler oftast skrivs för de situationer där medarbetare inte begriper att hotet är stort och sårbarheten är allvarlig så skulle det påverka hur väl *Protection motivation theory* kan förklara beteenden.

3.6 Gäller de erhållna resultaten inom Försvarsmakten?

Som tidigare diskuterats i 3.4 påverkar personegenskaper och miljörelaterade betingelser förmodligen hur viktiga olika faktorer är. Ingen av de 29 studierna har studerat Försvarsmakten, eller någon jämförbar organisation. Studierna har genomförts vid olika typer av företag och, oproportionerligt ofta, vid universitet

eller forskningsinstitut. Ofta har paneler används och miljön som respondenter kommer ifrån är blandad, eller i värsta fall oklar. En gissning är att miljön inom Försvarsmakten är mer homogen än den är i de miljöer som typiskt studerats i de 29 studierna. I så fall skulle resultaten (exempelvis teoriers förklaringsförmåga) bli mer tydliga och förutsägbara inom Försvarsmakten än de är generellt. I Försvarsmaken varierar personegenskaper och miljörelaterade betingelser mindre än de gör generellt och mellan olika organisationer. Av samma skäl är det rimligt att anta att de generella resultaten inte är direkt applicerbara i Försvarsmakten, utan att vissa teorier passar bättre på Försvarsmakten medan andra passar sämre.

3.7 Vilken teori använder Försvarsmakten idag?

Författarna har inte gjort någon djupare analys av Försvarsmaktens syn på hur regelefterlevnad uppnås. Det verkar dock vara en blandning av *Protection motivation theory* (motivering med informationssäkerhetsrisker och acceptans för sämre effektivitet) och *Deterrence theory* (hänvisningar till lagar och straff vid brott) som är mest förekommande i den skriftliga kommunikationen av bestämmelser.

Det är också möjligt att vrida på det och spekulera i vilken teori som skulle kunna förklara mest av den variation som antas finnas i Försvarmakten avseende intentioner och faktiskt regelföljande. En gissning är att det i Försvarmakten ibland kan vara nödvändigt att bryta mot bestämmelser för att kunna genomföra sina uppgifter, exempelvis vid speciellt utsatta eller stressade situationer. Denna faktor finns med i *Neutralisation theory* (”Försvarande av nödvändighet”), *Protection motivation theory* (”Genomförbarhetsbedömning”) och *Theory of planned behavior* (”Beteendekontroll” och ”Genomförbarhetsbedömning”).

Vad gäller mer slentrianmässiga brott mot bestämmelserna vågar författarna inte gissa vad som är viktigast. Vid undersökningar av detta kan *Neutralisation theory* vara en bra utgångspunkt eftersom den teorin syftar till att ta reda på vilka ursäkter personer intalar sig själva är rimliga.

3.8 Spelar inte bestämmelserna i sig någon roll för om de efterlevs?

Bestämmelserna i sig kan ha betydelse för om de efterlevs. Ingen studie har tittat specifikt på det. Hur vettiga bestämmelserna upplevs vara är dock en central del av *Protection motivation theory*.

Det bör noteras att de som har svarat på de enkäter som har använts i studierna är

1) personer som lyder under uttryckliga informationssäkerhets-bestämmelser
2) personer som vet var de hittar bestämmelserna och oftast även har tittat på dem.

Ett rimligt antagande är att det blir svårare att uppnå efterlevnad om inte informationssäkerhetsbestämmelserna är nerskrivna och kommunicerade. Kvaliteten på själva dokumentationen tycks dock vara av liten vikt enligt den enda studie som har tittat på den frågan. Det verkar inte heller spela roll i vilken utsträckning respondenterna har förtroende för de som har skrivit dokumentationen. Dessa faktorer har förklarat mindre än 1% av variansen i intentionerna när de har studerats.

3.9 Vilka frågor borde forskningen gå vidare med nu?

Nedan listas forskningsfrågor som bör besvaras för att förbättra kunskapen kring vad som påverkar efterlevand av informationssäkerhetsbestämmelser.

- Vilka grundprinciper utgår designen av informationssäkerhets-bestämmelser ifrån? Är valet av grundprincip organisationsberoende och konsistent för de olika delarna av bestämmelserna? Hur tolkas bestämmelserna?
- Hur skiljer sig riskuppfattningen mellan användare, säkerhetsexperter och beslutsfattare? Hur skiljer sig dessa riskuppfattningar från de risker som möts med informationssäkerhetsbestämmelser? När bör man skriva allmänna bestämmelser och när bör man förlita sig på individers goda omdöme?
- Hur kan teorierna anpassas eller kompletteras så att de bäst passar en viss typ av personlighetstyp och/eller organisation?
- Missas något viktigt genom att bara göra observationer och inte kontrollera miljön (se avsnitt 3.5 ovan)?

Förutom att studera dessa frågor bör det vara intressant att genomföra specifika studier inom Försvarsmakten för att ge underlag till informationssäkerhetsarbetet på alla nivåer i organisationen.

4 Referenser

Ajzen, I., 1991. The theory of planned behavior. *Organizational behavior and human decision …*. Available at: http://www.cas.hse.ru/data/816/479/1225/Oct 19 Cited %231 Manage THE THEORY OF PLANNED BEHAVIOR.pdf [Accessed October 15, 2012].

D'Arcy, J. & Herath, T., 2011. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), pp.643–658.

Malhotra, M. & Grover, V., 1998. An assessment of survey research in POM: from constructs to theory. *Journal of Operations Management*, 16(4), pp.407–425. Available at: http://www.sciencedirect.com/science/article/pii/S0272696398000217 [Accessed March 5, 2012].

Norman, P., Boer, H. & Seydel, E., 2005. Protection motivation theory. In M. C. and P. Norman, ed. *Predicting Health Behaviour: Research and Practice with Social Cognition Models*. Open University Press, pp. 81–126. Available at: http://psycnet.apa.org/psycinfo/1997-36396-006 [Accessed October 15, 2012].

Nye, F.I., 1958. *Family relationships and delinquent behavior*, Oxford: John Wiley.

Park, H.S., 2009. Testing the theory of reasoned action across cultures. , (October 2012), pp.37–41.

Siponen, M. & Vance, A., 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly: Management Information Systems*, 34(SPEC. ISSUE 3), pp.487–502. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-77957068563&partnerID=40&md5=c6ecfa7e63590aa13b8e6870bbc9c576.

Wiatrowski, M., Griswold, D. & Roberts, M., 1981. Social control theory and delinquency. *American Sociological Review*, 46(5), pp.525–541. Available at: http://www.jstor.org/stable/10.2307/2094936 [Accessed October 15, 2012].

Workman, M. & Gathegi, J., 2007. Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, 58(2), pp.212–222. Available at: http://onlinelibrary.wiley.com/doi/10.1002/asi.20474/full [Accessed March 7, 2012].