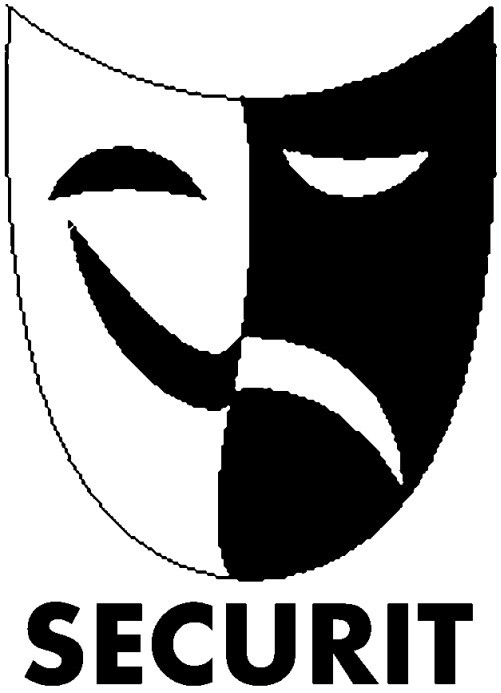
FORSKNINGSPROGRAM

Security culture and information technology SECURIT



Faktaruta

Security culture and information technology

2012-2017

Chalmers, Göteborgs universitet, FOI, Högskolan Väst, Karlstad universitet, KTH, Linköpings universitet och Örebro universitet

Jonas Hallberg, FOI

Syftet med Forskningsprogrammet Security Culture and Information Technology, SECURIT, har varit att förbättra organisationers förutsättningar att arbeta med sociala aspekter kopplade till informationssäkerhet.

MSB:s kontaktpersoner:
Johan Berglund, 010-240 41 61
Helena Andersson, 010-240 41 33

Bild: Logotyp Securit

Publikationsnummer MSB1222 - maj 2018
ISBN 978-91-7383-843-6

MSB har beställt och finansierat genomförandet av denna forskningsrapport (alt. studierapport). Författarna är ensamma ansvariga för rapportens innehåll.

Förord

Forskningsprogrammet Security Culture and Information Technology, SECURIT, har med finansiering av MSB genomförts under perioden juli 2012 till november 2017. Det övergripande syftet med forskningsprogrammet har varit att förbättra organisationers möjligheter att hantera sociala aspekter av informationssäkerhet.

Informationssäkerhetskultur är ett relativt nytt område och ett antal studier har genomförts inom SECURIT för att bidra till uppbyggnaden av kunskap inom området. Dessa studier har bland annat resulterat i 32 bidrag till vetenskapliga tidskrifter, konferenser och workshops samt sex stycken vetenskapliga rapporter.

Utöver de vetenskapliga resultaten har SECURIT haft som målsättning att sprida den kunskap som har byggts upp inom programmet till personer som är praktiskt verksamma med att utveckla informationssäkerhet i olika typer av organisationer, forskare inom andra ämnesområden och studenter. Med det syftet har SECURIT bland annat tagit fram antologin *Informationssäkerhet och organisationskultur*, som presenterar och diskuterar resultaten från 13 av de studier som har genomförts inom programmet.

SECURIT har genomförts av forskare vid Chalmers, Göteborgs universitet, FOI, Högskolan Väst, Karlstad universitet, KTH, Linköpings universitet och Örebro universitet. Mer information finns på SECURIT:s hemsida: www.foi.se/securit.

Innehåll

Sammanfattning

Informationssäkerhet är av vikt för hela vårt samhälle och den påverkas av såväl tekniska som sociala faktorer. Inom forskningsprogrammet SECURIT har ett antal forskare studerat sociala faktorer som påverkar organisationers informationssäkerhet. Arbetet har dels bedrivits inom nio stycken forskningsprojekt dels i form av gemensamma aktiviteter. I denna rapport presenteras resultaten från såväl de ingående forskningsprojekten som de gemensamma aktiviteterna.

1. Inledning

Det blir allt tydligare hur viktigt informationssäkerheten är för ett väl fungerande informationssamhälle. Under det senaste året har det i stort sett dagligen rapporterats om informationssäkerhetsincidenter som på något sätt har påverkat organisationer, enskilda individer och vårt samhälle. Ofta är dessa incidenter kopplade till tekniska system, men vid närmare beaktande så är det ofta mänskliga eller organisatoriska faktorer inblandade. Syftet med Forskningsprogrammet Security Culture and Information Technology, SECURIT, har varit att förbättra organisationers förutsättningar att arbeta med kulturella aspekter kopplade till informationssäkerhet. För att möjliggöra detta, formerades en tvärvetenskaplig forskargrupp med kompetenser inom bland annat psykologi, filosofi, informatik, statskunskap, informationssäkerhet och kognitionsvetenskap. De forskare som har arbetet inom SECURIT är verksamma vid Chalmers, Göteborgs universitet, FOI, Högskolan Väst, Karlstad universitet, KTH, Linköpings universitet och Örebro universitet.

Speciellt har SECURIT beaktat fenomenet informationssäkerhetskultur som tidigare inte har studerats i någon större omfattning. Inom SECURIT har följande definition tagits fram.

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[1]

Den huvudsakliga delen av arbetet inom SECURIT har genomförts inom de nio projekt som ingår i programmet. Dessa projekt och deras resultat presenteras i kapitel 2. En lista med de publikationer som har producerats återfinns i bilaga 1. Utöver projektens resultat har arbetet i SECURIT lett till flera programgemensamma resultat. Dessa resultat inkluderar en nationell enkät om informationssäkerhet och en populärvetenskaplig antologi, vilka presenteras i kapitel 3 respektive 4. Efter det egentliga avslutet av SECURIT i november 2017 fortsätter arbetet med ett specialnummer om värdekonflikter av tidskriften *Information Security Management*. Målsättningen är att specialnumret ska publiceras under 2018. Programmet har också presenterats och diskuterats vid ett antal seminarier och konferenser (bilaga 2).

---

[1] Hallberg, J. et al. (2015). *Definition of information security culture*. FOI Memo 5253. https://www.foi.se/rapportsammanfattning?reportNo=FOI%20MEMO%205253

2. Projektbeskrivningar

I detta kapitel beskrivs de nio projekt som har genomförts inom ramen för SECURIT.

2.1 Definition och användning av begrepp inom informationssäkerhet

Resultaten från projektet *Security culture* bekräftar att problematiken kring definitioner och användning av begrepp inom informationssäkerhet har praktiska konsekvenser. Resultaten visar exempelvis på behov av en ny definition av informationssäkerhet, istället för den traditionella som utgår från konfidentialitet, riktighet och tillgänglighet, och ett förslag till ny definition har presenterats. Den föreslagna definitionen är mer välanpassad för sociala, människliga och organisationskulturbundna säkerhetsutmaningar. Projektet bidrar även med en ny definition av personlig integritet. Ett värdefullt delresultat är de föreslagna definitionerna av säkerhet och personlig integritet som är väl anpassade för att analysera värdekonflikter mellan dessa värden. Projektet resultat bidrar även med analyser av begreppen information, anonymitet, samt kultur.

Vilka begrepp man använder för att beskriva och tala om något påverkar hur vi tänker om olika fenomen. Hur vi tänker påverkar i sin tur både forskning och praktisk verksamhet. I projektet Security Culture har vi fokuserat på flera av de centrala begrepp rörande informationssäkerhet som används både inom de praktiska verksamheterna och i forskningen. Att utveckla nya eller förbättra tidigare definitioner av viktiga begrepp är en viktig del i att skapa bättre verktyg för praktiker och forskare. I projektet har vi arbetat med begreppsliga utredningar av såväl grundläggande som tillämpad natur. Många av utredningarna har sökt svaret på frågan om vilka begrepp vi behöver och hur dessa bäst ska förstås.

De insikter som projektets begreppsliga utredningar lett fram till kan användas för praktisk analys men har också en självklar användning i vidare forskning. Där skulle man bland annat kunna fortsätta utveckla de enskilda bidragen – var för sig eller gemensamt – i syfte att uppnå en mer enhetlig begreppsapparat. Ett intressant exempel är att utreda om exempelvis definitionen av säker information kan förstås i ett bredare säkerhetssammanhang: finns det, till exempel, ett enhetligt säkerhetsbegrepp? Ett annat sätt att ta projektets resultat vidare är att testa hur delar av bidragen fungerar i praktiken. Ett tredje sätt är att undersöka, och argumentera för/emot, mer konkreta ståndpunkter i tillämpade etiska frågeställningar inom säkerhetsområdet.

2.2 Bedömningar som påverkar informationssäkerheten

Attityd, uppfattade normer, uppfattad egen förmåga, om man tror att man kommer att ångra sig och vana är de faktorer som i högst utsträckning bidrar till att förklara användares intention att följa informationssäkerhetsbestämmelser. Det visar resultaten från projektet *User acceptance of information security policies*. Andra resultat från projektet visare att motsättningar mellan verksamhets- och informationssäkerhetsmål i en miljö leder till att medarbetare själva tvingas göra avvägningar och improvisera för att hantera dessa.

Gällande bedömningar av risker kopplade till informationssäkerhet visar erhållna resultat att bedömningar av risk är starkt beroende av uppfattad konsekvens, snarare än en kombination av sannolikhet och konsekvens. Det tyder på att deltagarna i studien bedömer informationssäkerhetsrisker på ett sätt som liknar de bedömningar som gör att personer ser större risker med att flyga än att åka bil.

Vidare visar resultaten att skillnaderna mellan olika personers bedömningar av informationssäkerhetsrisker är för stora för att bedömningarna ska utgöra en bra grund för organisationers informationssäkerhetsarbete. Denna slutsats är problematisk eftersom informationssäkerhetsarbetet, enligt etablerade standarder, ska utgå från aktuella informationssäkerhetsrisker. I praktiken får dock de anställdas uppfattning och bedömning av dessa risker och det beteende dessa bedömningar leder till en avgörande betydelse för om informationssäkerheten upprätthålls eller inte. Därför inför många organisationer informationssäkerhetsbestämmelser, som syftar till att styra beteenden på ett sätt som gynnar informationssäkerheten. Ibland kan dock målen för en organisations informationssäkerhet och målen för verksamheten i sig vara motstridiga. Hur dessa målkonflikter hanteras är avgörande bland annat för möjligheterna att samtidigt upprätthålla hög informationssäkerhet och hög effektivitet i organisationen.

Det övergripande syftet med projektet har varit att skapa förståelse för och kunskap om beteenden som påverkar informationssäkerhet, för att därigenom bidra till att organisationer och dess medarbetare ska kunna fatta mer välgrundade informationssäkerhetsrelaterade beslut. De forskningsfrågor projektet har utgått från är:

- Vilka faktorer påverkar användares intention att följa informationssäkerhetsbestämmelser?
- Hur görs avvägningar mellan verksamhets- och informationssäkerhetsmål i en organisation?
- Hur görs bedömningar av informationssäkerhetsrisker?

För att besvara frågorna har hypoteser formulerats och sedan testats med statistiska metoder. För att kunna nyttja så stora dataunderlag som möjligt har projektet sammanställt resultat från tidigare studier och kompletterat dessa med egna enkätstudier.

Fler studier behövs för att öka kunskapen kring mänskligt beteende och informationssäkerhet. Det behöver genomföras experiment kopplat till bestämmelser för att studera faktiska beteenden snarare än individers intention när det gäller att följa reglerna. Avseende bedömning av risker behövs det studier av vilka möjligheter som finns att stödja processen med att göra bedömningar, så att dessa blir användbara som grund för beslut kopplade till informationssäkerhet.

2.3 Professionell kultur, informationssäkerhet och vårdkvalitet

Digitala informationssystem i sjukvården medför nya krav på vårdpersonalen, inte minst i fråga om att upprätthålla och garantera informationssäkerheten. Syftet med projektet *Attitude, culture, and information security* var att belysa och beskriva hur läkare och sjuksköterskor inom sjukvården resonerar i relation till de värdekonflikter som kan uppstå i deras yrkesvardag i samband med användning av digitala informationshanteringssystem. På detta sätt ville vi synliggöra hur normer och värden knutna till vårdprofessionerna påverkar såväl informationssäkerhet som vårdkvalitet.

De frågor som ligger till grund för forskningsprojektet är:

- Hur resonerar vårdpersonalen i relation till värdekonflikter som involverar användning av elektroniska patientjournaler i det dagliga vårdarbetet?
- Vilka professionskulturella element synliggörs genom personalens sätt att resonera kring hur de hanterar dessa värdekonflikter?
- Hur kan ovan nämnda aspekter påverka informationssäkerhet respektive vårdkvalitet?

Resultaten visar att vårdpersonalens vardag kräver fortlöpande, komplexa avvägningar mellan olika värden. Efterlevnad av informationssäkerhetsregler, som syftar till att garantera hög vårdkvalitet och patienternas integritet, kan stå i konflikt med andra professionella behov för att kunna säkerställa exempelvis vårdkvalitet, patientsäkerhet, effektivitet och samarbete. Av de genomförda intervjuerna framgick att vårdpersonalen alltid hanterade informationssäkerhet i förhållande till ett tydligt överordnat och gemensamt professionskulturellt antagande. Detta antagande var att vårdens primära mål är att patientens fysiska hälsa och välbefinnande ska värnas. I värdekonflikter vägdes detta antagande samt andra professionella och organisatoriska värden dynamiskt mot informationssäkerhetsreglernas legitimitet och mot risken för sanktioner vid överträdelser av desamma. Resultaten visar på behovet av fortsatt forskning dels om hur IT-system och regelverk kan utformas, men också om hur organisation och ledning kan utvecklas för att minska förekomsten av värdekonflikter i vårdarbetet och för att underlätta för vårdpersonalen att hantera sådana konflikter.

2.4 Samhälleliga värden och informationssäkerhet

Informationssäkerhetsarbete har oftast ett inåtblickande perspektiv. Det innebär att det är den enskilda organisations egenintresse som står i fokus vid utveckling av informationssäkerhetskulturer. I projektet *Discourse and Security Practice* har vi närmat oss frågan ur ett bredare perspektiv och undersökt hur samhälleliga värden beaktas och uppfattas i relation till informationssäkerhet.

Projektet bestod av två delstudier, vilka fokuserade på värden som personlig integritet och jämlik hälsa respektive visselblåsning och meddelarfrihet. Den första delstudien visar att det ofta uppstår värdekonflikter vid utvecklingen av e-hälsoteknologi, där personlig integritet uppfattas som ett hinder för att uppnå mål som bättre vård och resurseffektivitet. Vidare framgår det att mer komplexa frågor – såsom vad personlig integritet innebär i specifika situationer, eller hur utvecklingen av ny välfärdsteknologi påverkar möjligheterna att uppnå jämlik hälsa – ofta faller mellan stolarna och inte beaktas i utvecklingen av nya system.

Den andra delstudien visar att det finns en hög acceptans för visselblåsning inom den egna organisationen. Däremot är acceptansen för att anställda går till media för att avslöja allvarliga missförhållanden i organisationen (det vill säga utövar meddelarfrihet) låg. Trots detta är stödet för meddelarfriheten som ett samhälleligt värde högt. Vidare visar studien att det finns ett stöd för att interna visselblåsarfunktioner bör ingå som en del av organisationers informationssäkerhetskultur.

Inom ramen för den första delstudien intervjuade vi sexton personer från elva olika aktörer på policynivå, aktiva i utvecklingen av e-hälsosektorn i Sverige. Det personliga e-hälsokontot Hälsa för mig användes som utgångspunkt för att diskutera frågor som är relevanta för utvecklingen inom hela e-hälsosektorn. Den andra delstudien var en enkätstudie där vi ställde frågor till svenska tjänstepersoner om visselblåsande och meddelarfrihet i relation till informationssäkerhetsarbete.

Projektets resultat pekar på ett behov av att utveckla riktlinjer och policys för utvecklingen inom områden där informationssäkerhet står i fokus, så att fundamentala demokratiska värden, såsom personlig integritet och visselblåsning, beaktas bättre. Vidare behövs forskning som fokuserar på strukturer och föreställningar inom informationssäkerhetssektorn samt hur dessa strukturer och föreställningar förhåller sig till demokrati och mänskliga rättigheter.

2.5 Balanserad informationssäkerhet

Resultaten från projektet *Balanced IT-based organizational development* visar att det ofta finns en konflikt mellan att lösa de omedelbara och akuta uppgifter som verksamheten ställs inför och samtidigt leva upp till existerande regler för informationssäkerhet. De individer som arbetar i verksamheter med operativt ansvar för hantering av samhällsstörningar har ofta en mycket god förmåga till

improvisation i sitt arbete. I många fall visade sig en sådan improvisation innebära tydliga avsteg från verksamhetens IT-säkerhetsregler, men också att man kunde hantera de uppgifter och akuta problem som krävde omedelbart agerande.

Genomförda studier visar att bland annat användning av kommersiella molntjänster varit vanligt förekommande för att lösa omedelbara problem kring att samla in, bearbeta och distribuera information. Medvetenheten kring hur sådan användning harmonierar med gällande rutiner för informationssäkerhet kan ifrågasättas.

De omständigheter som råder under insatsarbete vid allvarliga samhällsstörningar, såsom bränder eller epidemiutbrott, är ofta mycket pressade. Att i sådana situationer hitta en balans i arbetet mellan att samtidigt skydda verksamhetens information och underlätta för medarbetarna att göra sitt jobb är svårt. Projektet syftade till att studera hur verksamheter med stort beroende av IT-användning åstadkommer en balanserad informationssäkerhet. Med ’balanserad informationssäkerhet’ avses i detta sammanhang de organisatoriska och tekniska arrangemang som tillhandahålls för att man ska kunna möta verksamhetens krav både på hög säkerhet och effektivt utförande.

Frågeställningen ”Hur upprätthålls informationssäkerhet i operativa verksamheter vid hantering av samhällsstörningar?” har varit vägledande i de fältstudier som har genomförts. Fältstudierna har omfattat observation och intervjuer vid stabsarbete hos räddningstjänst, sjukvård, polis, länsstyrelse, SOS-alarm samt Myndigheten för samhällsskydd och beredskap.

Studierna visar också att det finns ett behov av att säkerställa tillgång till kompetens inom informationssäkerhet i det operativa arbetet med att hantera samhällsstörningar. På en generell nivå pekar resultaten på att det i fråga om hur informationssäkerhetsfrågor prioriteras finns en betydande skillnad mellan å ena sidan kärnverksamhet och å andra sidan de expertfunktioner som ansvarar för informationssäkerhet. Detta påverkar den informationssäkerhetskultur som utvecklas i organisationen.

Utifrån de resultat som framkommit i studierna finns det anledning att fundera kring behovet av interventionsstudier i verksamheter med bristande informationssäkerhet. Sådana studier skulle dels kunna indikera vilken typ av åtgärder som fungerar men kanske än viktigare, identifiera vilka oväntade och kanske oönskade effekter avseende förstärkt informationssäkerhet som dessa åtgärder kan resultera i.

2.6 Organisationskultur och informationssäkerhet

Resultaten från projektet *Attitude* visar att organisationskulturen har en viss betydelse för informationssäkerheten. Att påverka organisationskulturen i en viss riktning kan således vara ett effektivt sätt att öka informationssäkerheten i en organisation. Vidare visar resultaten att det har betydelse om regelföljande kring informationssäkerhet mäts som en integrerad del av en arbetssituation

eller inte. Detta resultat bör ha betydelse för utformning av mätningar kring anställdas regelföljande, även när studier genomförs av praktiker.

En organisationskultur utgörs av medarbetarnas gemensamma grundläggande värderingar och antaganden om omvärlden. Dessa värderingar och antaganden styr de anställdas handlande. Organisationskulturen beskrivs ofta som en central del i styrningen av en organisation och många studier kring kultur och informationssäkerhet ser ofta organisationer som ett rationellt instrument där ledningen kan forma anställdas agerande. Mer sällan görs det i dessa studier ansatser till att förstå hur olika mönster av attityder och värderingar, och därigenom prioriteringar, kan variera mellan olika sammanhang.

I forskningsprojektet Attitude undersökte vi sambandet mellan organisationskulturer och anställdas attityder och beteenden kring informationssäkerhet i olika branscher. Vi var även intresserade av en metodmässig fråga som rör hur man i enkätbaserade studier går till väga för att mäta regelföljande kring informationssäkerhet. Dessa studier är ofta utformade utan hänsyn till i vilken utsträckning det uppstår situationer där de anställda behöver prioritera mellan att antingen följa reglerna för informationssäkerhet eller utföra sina arbetsuppgifter. Gör det någon skillnad om man istället för att bara låta respondenten svara ja eller nej utifrån påståendet ”Jag följer informationssäkerhetspolicyn på min arbetsplats” ställer frågan ”Hur ofta bortser du från informationssäkerhetspolicyn för att den försämrar kvaliteten i ditt arbete?”?

2.7 Design och kommunikation av informationssäkerhetspolicyer

Projektet *Congruence* resulterade i en metod för att analysera informationssäkerhet och riktlinjer för hur informationssäkerhetspolicyer bör designas. Vid brott mot informationssäkerhetsreglerna gör metoden det möjligt att identifiera om sinsemellan motstridiga budskap och mål kring informationssäkerhet kommunicerats. Metoden kan användas för att ta reda om olika ledningssystem i organisationen kommunicerar oförenliga saker till de anställda. Riktlinjerna ger stöd för hur informationssäkerhetspolicyer kan designas för att kommunicera informationssäkerhetspolicyer på ett mer sammanhållet sätt.

Organisationer använder en rad olika åtgärder för att kommunicera hur information ska hanteras på ett säkert sätt. Exempel på åtgärder är informationssäkerhetspolicyer, regler, riktlinjer och utbildningsmaterial. För att maximera utfallet av dessa åtgärder är det viktigt att de kommunicerar ett gemensamt och sammanhållet budskap. Om de tillvägagångssätt och målsättningar som kommuniceras innehåller mål som är sinsemellan motstridiga, blir det svårt för den anställde att veta hur hen förväntas agera.

Syftet med projektet var att bidra med verktyg för hur man kan kommunicera informationssäkerhet på ett gemensamt och sammanhållet sätt. Projektet utgick från två forskningsfrågor:

- Hur kan man identifiera när olika budskap och mål kring informationssäkerhet kommunicerats?
- Hur kan ett gemensamt och sammanhållet sätt att kommunicera informationssäkerhet understödjas?

Frågorna har undersökts genom fallstudier som inkluderat intervjuer, observationer och innehållsmässiga analyser av informationssäkerhetspolicyer och -regelverk inom svensk sjukvård.

En framtida forskningsfråga är hur väl de utvecklade riktlinjerna för design av informationssäkerhetspolicyer fungerar i andra miljöer än sjukvård, som är den miljö de skapades för. Det är även intressant att studera om riktlinjerna kan användas vid design av annat informationssäkerhetsmaterial, såsom utbildningsmaterial.

2.8 Konflikter som uppstår när olika informationssäkerhetskulturer möts

Projektet *Interorg* har resulterat i två modeller som kan användas av praktiker respektive forskare för att analysera informationsutbyte mellan offentliga organisationer. Den första modellen är ett analysverktyg för att utvärdera den existerande interorganisatoriska informationssäkerhetskulturen vid olika tidpunkter. Modellen gör det möjligt att identifiera hur väl kulturen fungerar för att finna kompromisser avseende informationssäkerhetsrelaterade frågor och att för lösa de arbetsuppgifter som samarbetet berör. Den andra modellen beskriver vilka faktorer som bidrar till/hindrar interorganisatoriskt informationsutbyte och kan användas för att mer detaljerat identifiera faktorer som spelat roll i ett specifikt samarbete och hur dessa utvecklats över tid.

Av de studier som tidigare gjorts kring informationssäkerhetskultur och informationssäkerhet fokuserar i princip samtliga på arbetet inom enskilda organisationer, inte på arbetet som sker mellan organisationerna. Detta trots att dagens organisationer ofta ingår i nätverk av aktörer. Samarbete för att uppnå gemensamma resultat innebär att olika organisationers kulturer och föreställningar kring informationssäkerhet möts och potentiellt kolliderar med varandra.

Syftet med projektet Interorg var att utveckla kunskap om konflikter som uppstår när flera informationssäkerhetskulturer möts i en interorganisatorisk kontext. Forskningsfrågorna som ställs är följande:

- Vilka faktorer påverkar informationsdelning mellan organisationer och hur förändras de över tid?
- Hur kan utvecklingen av en interorganisatorisk informationssäkerhetskultur förstås?

Projektet har rekonstruerat hur information delades mellan tre organisationer, som ingick i en svensk referensgrupp kring kopparkorrosion och svensk kärnbränsleförvaring. Referensgruppen etablerades 2010 på initiativ av Svensk Kärnbränslehantering AB och upphörde 2014. I arbetet deltog ett flertal

organisationer, varav de tre mest aktiva ingick i studien: Svensk Kärnbränslehantering AB, Kungliga tekniska högskolan och Miljöorganisationernas kärnavfallsgranskning. De tre organisationerna företrädde olika åsikter kring sakfrågan, men hade också olika syn på hur information hanterades. Rekonstruktionen av referensgruppens arbete gjordes genom intervjuer och dokumentstudier.

Intressanta framtida forskningsuppgifter är att utvärdera hur dessa modeller fungerar i andra sammanhang och att med stöd i modellerna identifiera framgångsrika och mindre framgångsrika samarbeten. Det skulle kunna leda till möjligheter att förutsäga framgång kring informationsdelning i interorganisatoriska sammanhang.

2.9 Kulturella aspekter vid utveckling av informationssäkerhetstandarder

Standardiseringsarbete beskrivs av SIS, den standardiseringsorganisation som projektet har följt, som ett arbete grundat i konsensus mellan många olika intressenter. Den genomförda studien visar dock något delvis annat resultat. Projektets resultat visar att arbetet med att ta fram standarder visserligen har tydliga inslag av konsensus, men också att det aktiva deltagandet i arbetet är lågt. Detta innebär i praktiken att de få aktörer som är med och fattar besluten om informationssäkerhetsstandarder får stor makt. Projektet har också funnit att utvecklingsarbetet har ytterligare en struktur, präglad av strategi, politik och konkurrens – speciellt kring det arbete som bedrivs internationellt. Denna struktur är mer dold för utomstående än den första.

Informationssäkerhetsstandarder är ”best practices” som utvecklas globalt av informationssäkerhetsexperter. Dessa standarder har indirekt ett inflytande på hur informationssäkerhet utvecklas i olika organisationer, då de ofta används som utgångspunkt för det lokala informationssäkerhetsarbetet. Exempelvis så ska svenska myndigheter följa standarden ISO-27000 när de inför ledningssystem för informationssäkerhet.

Trots det stora genomslag som internationella informationssäkerhets-standarder får är kunskapen om hur arbetet med att utveckla dem går till relativt liten. Forskningsfrågan som projektet arbetat med är: Vilka strukturer påverkar arbetet med att utveckla informationssäkerhetsstandarder?

Syftet med projektet Kulturella aspekter vid utveckling av informationssäkerhetstandarder var att kartlägga vilken kultur, i form av strukturer, som präglar arbetet med att utveckla informationssäkerhetsstandarder. Ökad kunskap om detta arbete är betydelsefullt då det ger ökad förståelse för dels varför standarder får en viss utformning, dels i vilka sammanhang de kan betraktas som ”best practices”.

Kartläggningen av vilka strukturer som finns i arbetet med att ta fram informationssäkerhetsstandarder gjordes genom en etnografisk studie där forskarna deltog som medlemmar i en så kallad teknisk kommitté. Medlemskapet innebar att forskarna under flera år var närvarande i arbetet

med att ta fram standarder inom informationssäkerhet, vilket gav en detaljerad inblick i hur arbetet går till.

3. Enkätstudie om informationssäkerhet i mer än 100 organisationer

Hur ser svenska tjänstepersoner på informationssäkerhet och hur kan man förstå deras beteende i relation till fenomenet? Brist på kunskap om dessa frågor föranledde att man inom ramarna forskningsprogrammet SECURIT lät genomföra en omfattande enkätundersökning riktad till svenska tjänstepersoner. Undersökningen genomfördes våren 2016 av Statistiska centralbyrån (SCB) på uppdrag av forskarna.

Enkätundersökningen var ett samarbete mellan flera av de projekt som ingick i programmet. Frågeställningarna rörde bland annat följande:

- Hur kan beteenden relaterade till informationssäkerhetsbestämmelser förklaras?
- Vilka samband finns mellan organisationskultur och anställdas attityder och beteenden kring informationssäkerhet?
- Vilka effekter har informationssäkerhetsklimat?
- Vilka attityder har anställda till visselblåsande och meddelarfrihet?

Urvalet till undersökningen gjordes dels som ett representativt urval av 2000 av tjänstepersoner i Sverige (riksurvalet), dels som ett organisationsurval av cirka 9000 tjänstepersoner i sex olika branscher (branschurvalet). Branscherna var valda för att omfatta såväl privat som offentlig verksamhet, som hanterar skyddsvärd information. De tre privata branscherna var kemisk tillverkningsindustri, IT-sektorn och banksektorn. De tre offentliga branscherna var högskola och universitet (stat), sjukvård (landsting) och socialtjänst (kommun). 3681 personer besvarade enkäten (svarsfrekvens: 34 procent), 674 i riksurvalet (svarsfrekvens: 34 procent) och 3007 i branschurvalet (svarsfrekvens: 31 procent till 34 procent i de olika branscherna).

Enkätresultaten gav en representativ bild av anställdas uppfattning om informationssäkerhet i svenska privata och offentliga organisationer. De visade vidare att det fanns betydande skillnader mellan olika organisationer och branscher gällande de aspekter av informationssäkerhet som enkäten undersökte. Baserat på resultat från enkätundersökningen utvecklades ett verktyg för att göra det möjligt att mäta informationssäkerhetsklimat i organisationer. Detta verktyg kan användas för att undersöka standarden i den egna organisationen jämfört med andra organisationer. Enkäten kan också användas i vidare forskning genom att det nu finns ett jämförelsematerial som möjliggör undersökningar av hur informationssäkerhet utvecklas över tid. En annan möjlighet till att utnyttja materialet är att olika delar av enkäten

användas i utvärdering av förändringsprojekt som avser att utveckla informationssäkerhet i organisationer.

4. Informationssäkerhet och organisationskultur – en populärvetenskaplig antologi

Frågor om informationssäkerhet behöver idag hanteras av såväl enskilda individer som inom organisationer och på en mer övergripande samhällsnivå. Det blir också allt tydligare att tekniska lösningar inte alltid räcker till för att lösa problemen. Syftet med antologin Informationssäkerhet och organisationskultur var att på ett populärvetenskapligt sätt ge ett brett perspektiv på organisationskulturers betydelse för informationssäkerheten i olika delar av samhället, baserat på den forskning som bedrivits inom ramen för programmet Security culture and information technology (SECURIT).

I antologin medverkar ett tjugotal forskare från olika discipliner, alla verksamma i SECURIT. Forskarna presenterar och diskuterar resultaten av 13 olika studier som genomförts inom ramen för forskningsprogrammet. De flesta kapitlen presenterar empiriska studier, där forskarna alltså baserar sina resultat på observationer av verkligheten.

Boken är indelad i fyra delar, där de första tre innehåller kapitel som resonerar om informationssäkerhetskultur dels utifrån breda samhällsperspektiv, dels på en mer verksamhetsnära nivå. Den fjärde delen innehåller kritisk reflektion kring ett antal centrala begrepp och förutsättningar för informationssäkerhetsarbete.

Genom det mångfacetterade anslaget belyser antologin fenomenet informationssäkerhet ur många olika perspektiv. Förhoppningen är att detta ska bidra till att fördjupa läsarens förståelse för informationssäkerhet såväl i ett organisatoriskt som i ett bredare samhälleligt sammanhang. Antologin avser göra resultaten från SECURIT-programmet tillgängliga och tillämpbara för personer som är praktiskt verksamma med att utveckla informationssäkerhet i olika typer av organisationer. Boken är även avsedd att kunna användas som introduktion till ämnet för forskare och för studenter i grundutbildning.

Bilaga 1: Publikationer

I denna bilaga återfinns tabeller med de publikationer som har tagits fram inom SECURIT. Den första tabellen innehåller de publikation som har publicerats vid programmets avslutande (2017-11-15). Den andra tabellen innehåller de publikationer som har blivit accepterade för publicering respektive är under granskning för publicering.

Publikation	**Partner**	**År**
Hallberg et al. SECURIT poster, 5th Resilience Engineering Association Symposium (REA5).	FOI	2013
Sommestad et al. Variables influencing information security policy compliance: a systematic review of quantitative studies. In Information management and computer security.	FOI	2013
Sommestad et al. A review of the theory of planned behaviour in the context of information security policy compliance. Proc. of the 28th IFIP TC-11 SEC. Auckland, New Zealand.	FOI	2013
Hallberg et al. User Acceptance of Information Security Policies, poster and abstract at the National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC).	FOI	2013
Kvalitativ delstudie: SECURIT– vård, GU and HV.	GU	2013
Information security climate survey, Draft version, GU.	GU	2013
Räisänen. Standard-making in Information Security – A Literature Review. 7th Workshop on Information Security and Privacy. AIS Electronic Library (AISeL), Paper 31.	ORU	2013
Sommestad et al. The Sufficiency of the TPB for Information Security Policy Compliance, Information Management and Computer Security.	FOI	2014
Sommestad et al. A Meta-Analysis of Studies on PMT and Information Security Behavior. Presented at the Dewald Roode Information Security Workshop.	FOI	2014
Franc. Vårdanställdas efterlevnad av informationssäkerhetspolicys – faktorer som påverkar efterlevnaden, M.Sc. LiU.	FOI	2014
Pousette. (working paper) Bortfallsanalys SECURIT-piloten.	GU	2014
Skyvell-Nilsson et al. Safety or Security? Formation of Information Security Culture in Health Care. Poster for NSQH conference in Stavanger.	GU	2014
Karlsson et al. Practice-Based Discourse Analysis of Information Security Policy in Health Care. Presented at the 11th Scandinavian Workshop on E-government (SWEG), Linköping.	ORU	2014
Hallberg et al., Definition of information security culture, FOI Memo 5253, FOI.	(Joint)	2015
Sommestad. Social groupings and information security obedience subcultures within organizations. The 30th International Information Security and Privacy Conference, Hamburg.	FOI	2015

Publikation	Partner	År
Sommestad, Karlzén, Nilsson and Hallberg. Perceived information security risk as a function of probability and severity. International Symposium on Human Aspects of Information Security & Assurance (HAISA), edited by Steven Furnell and Nathan Clarke. Plymouth University.	FOI	2015
Sommestad, Karlzén, Nilsson and Hallberg. An empirical test of the perceived relationship between risk and the constituents severity and probability, in special issue of Information and Computer Security, Vol. 24 Iss: 2.	FOI	2015
Sommestad, Karlzén, and Hallberg. A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy 9 (1): 26–46.	FOI	2015
Johansson and Hellberg. Health, Privacy and (Information) Security: Competing Discourses in eHealth Programmes and Genome Data Regulations. Conference paper presented at the International Studies Association Annual Convention in New Orleans, USA.	GU	2015
Karlsson, Åström and Karlsson. Information security culture – state-of-the-art review between 2000 and 2013. Information and Computer Security, Vol. 23, Iss. 3, pp. 246-285.	ORU	2015
Löfstedt. Exploring integrated management systems – challenges and potentials in relation to IT governance, 38th Information Systems Research Seminar in Scandinavia (IRIS38), Oulu, Finland.	ORU	2015
Karlsson, Kolkowska, Hedström and Frostenson. Inter-organisational information sharing – between a rock and a hard place. In Proceedings of the 9th International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), Lesvos, Greece, July 1-3 July, 2015.	ORU	2015
Karlsson, Goldkuhl and Hedström. Practice-based Discourse Analysis of InfoSec Policies. In Federatth, H. and Gollmann, D. (Eds.) ICT Systems Security and Privacy Protection - 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany. Springer, Heidelberg, pp. 297-310.	ORU	2015
Uhr, Frykmer, Koelega, Cedergårdh, Ekman, Fredholm and Landgren. Att åstadkomma inriktning och samordning – 7 analyser utifrån hanteringen av skogsbranden i Västmanland 2014. Centrum för samhällets resiliens, Lund University.	CTH	2015
Lundgren. The Information Liar Paradox: A Problem for Floridi's RSDI Definition. Philosophy and Technology 28(2): 323-327.	KTH	2015
Lundgren. Information Security and Resilience: The Right Definition. Poster Session, Third Deans Forum Workshop on Resilience Engineering, Tokyo University, Tokyo, Japan.	KTH	2015
Karlsson, Kolkowska and Prenkert. Inter-organisational information security: a systematic literature review. Information & Computer Security, Volume 24, Issue 5. 418-451.	ORU	2016
Bergstrand and Stenmark. Leveraging Bystander Reports in Emergency Response Work: Framing Emergency Managers Social Media Use. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 162-171). IEEE.	CTH/GU	2016

Publikation	Partner	År
Uhr, Johansson, Landgren, Holmberg, Bynander, Koelega and Trnka. Once upon a time in Västmanland - the power of narratives or how the "truth" unfolds. In proceedings of ISCRAM16, Rio de Janerio, Brazil.	CTH	2016
Woltjer. *Workarounds and Trade-offs in Information Security – an Exploratory Study*. Information and Computer Security 25(4), pp. 402–420. Emerald.	FOI	2017
Sommestad, Karlzén and Hallberg. The Theory of Planned Behavior and Information Security Policy Compliance. Journal of Computer Information Systems.	FOI	2017
Hallberg, Bengtsson, Hallberg, Karlzén, Sommestad. *The Significance of Information Security Risk Assessments Exploring the Consensus of Raters' Perceptions of Probability and Severity*. International conference on Security and Management, pp. 131–137.	FOI	2017
Sommestad, Karlzén, Hallberg. *The Theory of Planned Behavior and Information Security Policy Compliance*. Journal of Computer Information Systems. Taylor & Francis, pp. 1–10.	FOI	2017
Hellberg and Johansson. eHealth strategies and platforms - the issue of health equity in Sweden. Health Policy and Technology. Volume 6, Issue 1, Pages 26–32.	GU	2017
Karlsson, Hedström and Goldkuhl. Practice-Based Discourse Analysis of Information Security Policies. Computers & Security. Volume 67 Issue C.	ORU	2017
Kolkowska, Karlsson and Hedström. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. Journal of Strategic Information Systems.	ORU	2017
Karlsson, Karlsson and Åström. Measuring employees' compliance – the importance of value pluralism. Information & Computer Security	ORU	2017
Lundgren. Conceptualising the Values of Anonymity in the 21st Century and Beyond. IACAP (International Association of Computing and Philosophy), Stanford University, June 26-28, Stanford, USA.	KTH	2017

Publikation	Partner	Status
Karlsson, Frostenson, Prenkert, Kolkowska and Helin. (accepted) Inter-organisational information sharing in the public sector: a longitudinal case study on the reshaping of success factors. Government Information Quarterly.	ORU	Accep-terad
Lundgren. Need Semantic Information be Truthful? Accepted for publication in Synthese.	KTH	Accep-terad
Lundgren, Möller. Defining Information Security Accepted for publication in Science and Engineering Ethics.	KTH	Accep-terad
Lundgren. The Concept of Anonymity: What is really at Stake?. Under contract to be published in Macnish and Galliot, Big Data and the Democratic Process.	KTH	Accep-terad

Sommestad, T. The Theory of Planned Behavior and Information Security Policy Compliance: a Multilevel Analysis of the Role of Social Background Factors.	FOI	Under gransk-ning
Skyvell-Nilsson, Pousette and Törner. Professional culture, information security and healthcare quality - physicians' and nurses' perspective on value conflicts in the use of electronic medical records.	GU	Under gransk-ning
Johansson and Berndtsson. (under review). Whistleblowing and Freedom of Communication in Swedish Organizations. Information and Computer Security.	GU	Under gransk-ning
Karlsson, Denk and Åström. Organizational culture and value conflicts in information security management. Special Issue in Information & Computer Security (submitted).	ORU	Under gransk-ning
Hedström and Dhillon. Reconciling Value-based Objectives for Security and Identity Management. Special Issue in Information & Computer Security (submitted).	ORU	Under gransk-ning
Andersson, Karlsson and Hedström. Consensus versus Control – Unveiling Discourses in De Jure Information Systems Standardisation Work. MIS Quarterly (submitted).	ORU	Under gransk-ning
Bergstrand. Caring over the distance.	CTH/GU	Under gransk-ning
Lundgren. Privacy as a Relational Concept Currently under review.	KTH	Under gransk-ning
Lundgren. A Dilemma for Privacy as Control and Why the Context Matters. Currently under review.	KTH	Under gransk-ning

Bilaga 2: Presentationer av SECURIT

Denna bilaga innehåller en lista med de presentationer som har genomförts inom ramen för SECURIT.

Presentation	**Ort**	**Datum**
Karlsson F. An international research seminar on Information security was organized by SECURIT. The seminar included participants from research organizations in Sweden, Norway, the UK, and the US.	Örebro	2013-05-15
Landgren J. Presentation at Svenska Laboratorieresponsnätverket on information sharing and information security in emergency response work.	Göteborg	2013-05-28
Hallberg J. An overview of SECURIT and some of the specific results were presented at the annual seminar of the Swedish IT Security Network for PhD Students (SWITS).	Malmö	2013-06-04
Hallberg J. SECURIT was presented as part of a presentation at the National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC).	Stockholm	2013-11-13
Hallberg J., Sommestad T. SECURIT was presented at a seminar with the organization Säkerhetskulturnätverket (www.säkerhetskultur.se).	Stockholm	2013-12-10
Räisänen K., Seminar on Standard making in Information Security.	Örebro	
Hallberg J., Sommestad T., Karlsson M., Lundgren B., Doug Maughan from DHS visited Sweden and SECURIT and discussed possible collaboration.	Linköping	2014-03-31
Axelsson K., Hallberg J., Karlsson F., Pousette A., Sommestad T., Törner, M. SECURIT participated in a panel discussion in the conference Informationssäkerhet för offentlig sektor.	Stockholm	2014-08-26
Karlsson F., Presentation on Attityder till informationssäkerhet	Örebro	2014-10-07
Karlsson F., Seminar on ATTITUDE: survey on organisational culture and information security	Örebro	2014-11-14
Lundgren B. Presentation at Security Link, LiU.	Linköping	2014-11-20
Hallberg J. An overview of SECURIT was presented at the NordForsk joint Nordic Conference on New trends in societal security research in the Nordic countries.	Stockholm	2014-11-27
Sommestad T. SECURIT was presented and discussed during a Collaboration session at the DHS Cyber Security Division R&D Showcase and Technical Workshop.	Washington DC, USA	2014-12-17

Presentation	Ort	Datum
Johansson P., Berndtsson J. SECURIT participated at the open seminar presentation Whistleblowers, Information Security, and the Freedom to Disclose Information at Urban Safety and Societal Security - URBSEC seminar series.	Göteborg	2015-02-04
Johansson P., Hellberg S. SECURIT participated in the International Conference Panel Health, Privacy and (Information) Security: Competing Discourses in eHealth Programmes and Genome Data Regulations at the International Studies Association's (ISA) 56th Annual Convention.	New Orleans, USA	2015-02-21
Landgren J. Presentation at Västra Götalandsregionens Information Security Education.	Skövde	2015-03-06
Hallberg, J. SECURIT participated in the workshop on Society, integrity and cyber-security arranged by NordForsk, The Economic and Social Research Council in United Kingdom (ESRC) and The Netherlands Organisation for Scientific Research (NWO).	London, UK	2015-05-12–13
Lundgren, B. (2015). Presented at The Swedish Philosophy Conference, Linköping as "Why semantic information is only meaningful data". Previous working-title: "A Minimalistic Definition of Semantic Information".	Linköping	2015-06
Johansson P, Hellberg S. presented the Discourse project at an open seminar organised in conjunction with MSB: Perspectives on values and value conflicts among actors in e-health. Törner M., Skyvell-Nilsson M presented the Attitude, culture, and information security project: formation of information security culture in healthcare: Health care professionals' perspective on values and value conflicts, at the same seminar.	Stockholm	2015-09-17
Sommestad T. The User acceptance project was presented to stakeholders at an open seminar organised in conjunction with MSB: Information security policies: Who follows it and when are they followed?.	Stockholm	2015-09-18
Hallberg J. SECURIT participated in and was presented at the MSB Researcher Day (sv. MSB forskardag).	Stockholm	2015-11-12
Hallberg J.; Lundgren B.; Landgren J.; Åström J., Karlsson F., Karlsson M.; Prenkert F., Frostensson M., Karlsson F. SECURIT and MSB arranged the one day conference Information Security Culture within and between Organizations (sv. Informationssäkerhetskultur inom och mellan organisationer) with five seminars on information security culture.	Stockholm	2016-03-11
Hallberg J. SECURIT was presented at the annual seminar of the Swedish IT Security Network for PhD Students (SWITS).	Linköping	2016-06-09–10

Presentation	Ort	Datum
Hallberg J. SECURIT participated in and was presented at MSB's National information security conference for the public sector. Landgren J. presented the project Balanced IT-based Organizational development as a keynote in the closing session of the same conference.	Stockholm	2016-09-15
Hallberg J. SECURIT was presented at the annual seminar called the IT security day (sv. IT-säkerhetsdagen) arranged by FOI.	Stockholm	2016-11-02
Lundgren B. A presentation on the concept of Privacy, which argues for a relational definition on privacy: The Definition of Privacy: Privacy as a Relational Concept. Invited talk at Turku University.	Turku, Finland	2017-05-16
Lundgren B. Presentation on the concept of culture, arguing that cultures are constituted by the context: "What is Culture?", Filosofidagarna, Uppsala University.	Uppsala	2017-08-25–27
Johansson P. Presentation titled Discourse and Security Practice, Department of History at Lund University.	Lund	2017-03
Hallberg J and Karlzén H. Bildspel i monter vid konferensen Informationssäkerhet för offentlig sektor.	Stockholm	2017-09-05—06

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1222 - maj 2018 ISBN 978-91-7383-843-6