INSTITUTIONEN FÖR MEDICIN
SAMHÄLLSMEDICIN OCH FOLKHÄLSA
ARBETS- OCH MILJÖMEDICIN

Informationssäkerhetskultur i praktiken – delstudie om arbetsorganisatoriska och psykosociala faktorers betydelse för informationssäkerheten

Populärvetenskaplig rapport

Juni 2022

Marianne Törner[1], Kristina Gyllensten[2], Anders Pousette[1,3]

[1]Arbets- och miljömedicin, Avdelningen för samhällsmedicin och folkhälsa, Institutionen för medicin, Göteborgs universitet

[2]Arbets- och miljömedicinska kliniken, Sahlgrenska universitetssjukhuset, Göteborg

[3]Psykologiska institutionen, Göteborgs universitet

Innehåll

1 Organisationers information – en viktig och skyddsvärd tillgång

Informationstillgångar är centrala för dagens organisationer – inom både den privata och den offentliga sektorn. En organisations hantering av informationssäkerheten kan påverka dess förmåga att följa lagkrav och att hantera risker och konkurrens (Dor & Elovici, 2016). Samhällets och dess organisationers integritet och pålitliga funktion förutsätter att beslut baseras på korrekt information. Det kräver att denna information är riktig och fullständig, vilket i sin tur kräver att den är tillgänglig endast för rätt användare vid rätt tillfälle. Informationssäkerhet definieras ofta genom CIA-akronymen, där C står för konfidentialitet (confidentiality) som tillförsäkrar att informationen är tillgänglig endast för auktoriserade användare; I står för integritet, vilket skyddar informationens riktighet och fullständighet; och A står för tillgänglighet (availability), som tillförsäkrar att informationen är tillgänglig på ett användbart sätt för auktoriserade användare när dessa behöver den. Andra definitioner av begreppet informationssäkerhet omfattar autenticitet, ansvarighet, omöjlighet att förkasta samt tillförlitlighet (ISO/IEC, 2013).

2 Människan en viktig del av informations-säkerheten

Informationssäkerheten kan utsättas för externa hot såsom hackare, företagsspionage och infrastrukturella haverier, men även av interna hot som icke tillåten datoranvändning eller brott mot regler och policyer (Chulkov, 2017). Tekniska och administrativa skyddssystem har stor betydelse för att skydda organisationers information, men för att uppnå hög informationssäkerhet kan man inte enbart förlita sig på tekniska och administrativa strukturer. Förmågan att hålla hög informationssäkerhet omfattar även psykologiska och organisatoriska aspekter (Wood, 2004). Det finns därför ett stort behov av att förstå hur anställda tänker kring informationssäkerhet och vad som har betydelse för ett informationssäkert förhållningssätt och beteende i arbetet. Med sådan kunskap kan organisationen förstärka sådana gynnsamma förhållanden och förutsättningar och därigenom på ett effektivt sätt stärka och utveckla informationssäkerheten.

För att på ett effektivt sätt skapa, upprätthålla och vidareutveckla en hög nivå på informationssäkerheten krävs inte bara hög teknisk kompetens utan även djup förståelse för hur arbetets organisering och psykosociala arbetsförhållanden påverkar anställdas förmåga och motivation att bidra till hög informationssäkerhet, och därmed

till samhällssäkerhet. Men forskningen har endast i liten omfattning inriktats mot organisatoriska faktorers betydelse för ledning och styrning av informationssäkerheten (Al-Darwish & Choe, 2019). Forskarna Khatib and Barki (2020) framhöll vikten av att beakta organisatoriska förhållanden, inte bara individburna faktorer, när man försöker förstå orsaker till bristande följsamhet till regler i IT-sammanhang. Andra forskare har framhållit betydelsen för anställdas informationssäkerhetsbeteende av användningen av sanktioner vid regelbrott, men även av organisationens säkerhetskultur och säkerhetsklimat (Alfawaz, Nelson, & Mohannak, 2010; Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy, Herath, & Shoss, 2014; Hooper & Blunt, 2019).

3 Informationssäkerhetskultur

Människor är sociala varelser och vår förmåga att samarbete utmärker oss som art. För att en organisation eller arbetsgrupp ska kunna samarbeta behöver man en gemensam 'världsbild' av organisationen och vad som är dess primära syfte. Denna världsbild baserar man på formellt, men inte minst informellt förmedlad information från viktiga företrädare för organisationen eller verksamheter i organisationen. Utifrån en sådan gemensam världsbild kan de anställda sedan informellt enas om hur man bäst koordinerar och organiserar sina arbetsinsatser för att på bästa sätt verka för verksamhetens grundläggande syfte. Den gemensamma världsbilden, gör tillvaron i organisationen ordnad, begriplig och meningsfull för dess medlemmar, vilket också är betydelsefullt för människors mentala hälsa (Antonovsky, 1987). Den gör även andra anställdas beteende förutsägbart och ger oss en referensram för vårt eget beteendet. Allt detta skapar en upplevelse av kontroll, som är viktigt för vår mentala välmåga, och samtidigt möjliggör det samarbete. Det har skapats en organisationskultur (Schneider, 1985). Begreppet organisationskultur har definierats på följande sätt av några av världens mest framstående organisationskulturforskare: organisationskulturen är de "gemensamma värden och grundläggande antaganden som förklarar varför organisationer gör vad de gör och fokuserar på det de gör; den existerar på en fundamental, kanske undermedveten, nivå, är grundad i historia och tradition och är en källa till kollektiv identitet och engagemang" (Schneider, González-Roma, Ostroff, & West, 2017). Organisationskulturen är inget lättrörligt fenomen, men den är heller inte statisk. Alla organisationer utsätts för förändrade krav genom exempelvis introduktion av ny teknologi, lagar och regler som kan påverka organisationskulturen.

Baserat på organisationskulturen skapas sociala normer kring vad som är 'rätt' sätt att värdera och agera i förhållande till en rad olika värden och målområden i organisationens liv. Ett sådant värde är informationssäkerheten. De aspekter av organisationskulturen som har betydelse för informationssäkerheten kan man kalla en informationssäkerhetskultur och har definierats på följande sätt: "de 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” (Hallberg et al., 2017, sid. 17). Denna definition av begreppet informationssäkerhetskultur är inte normativ i så måtto att en informationssäkerhetskultur alltid är bra. Den kan vara såväl bra som dålig, och är bra om den gynnar informationssäkerheten. Eftersom organisationskulturen inte är ett statiskt fenomen så är inte heller informationssäkerhetskulturen det. Förändringar i teknologi, lagar och regler, men även i förhållningssätt och agerande hos viktiga företrädare i organisationen, kan inverka på informationssäkerhetskulturen – till det bättre eller till det sämre. För att kunna understödja utvecklingen av en god informationssäkerhetskultur behövs arbetssätt och verktyg för att kunna identifiera förändringsbehov. Att förstå vilka faktorer i arbetet som har betydelse för informationssäkerhetskulturen och därmed de anställdas förhållningssätt och beteende i förhållande till informationssäkerhet är också en viktig förutsättning för effektivt utvecklingsarbete. Projektet Informationssäkerhetskultur i praktiken har som ambition att bidra till detta.

4 Värdekonflikter

Bristande följsamhet till informationssäkerhetsregler kan delvis bero på att de anställda upplever att det agerande som dessa regler kräver står i konflikt med agerande som krävs för att kunna uppnå andra centrala mål i verksamheten. Kraven kan alltså upplevas som paradoxala. Forskarna Smith och Lewis definierade organisatoriska paradoxer som ”motsägande men ändå interrelaterade element som existerar samtidigt och kvarstår över tid” (Smith & Lewis, 2011, sid. 382). De konstaterade att kraven i en paradox förefaller logiska och oproblematiska när man ser på dem vart och ett för sig, men motsägande eller till och med absurda när de ställs mot varandra. Anställda som ställs inför sådana paradoxala krav kan uppleva stressande målkonflikter. För att bättre kunna förstå varför anställda inte följer informationssäkerhetsregler, även om man med självklarhet ställer sig bakom de värden dessa regler ska värna, är det viktigt att undersöka vilka organisatoriska värden och krav som kan stå i konflikt med dessa regler. Det är samtidigt viktigt att utröna hur de anställda resonerar och agerar när de ställs inför sådana värdekonflikter.

5 Olika typer av informationssäkerhetsbeteende

Inom säkerhetsforskningen skiljer man ofta mellan två typer av säkerhetsbeteende. Som anställda kan man bidra till hög informationssäkerhet genom att nogsamt följa alla informationssäkerhetsregler och föreskrivna procedurer. Denna typ av säkerhetsbeteende brukar kallas regelföljande beteende. Delaktigt säkerhetsbeteende är den andra typen. Med detta menas ett slags organisatoriskt medborgerligt beteende (Organ, 1997), det vill säga ett beteende där man som anställd gör mer än det som explicit föreskrivs för ens roll och själv identifierar organisatoriska behov och tar egna

initiativ för att organisationen ska fungera så bra som möjligt. The European Union Agency for Network and Information Security (ENISA, 2018) konstaterade att båda dessa typer av beteenden är nödvändiga för att upprätthålla en hög nivå på informationssäkerheten.

En rad olika faktorer, såsom ledning och policyer, utbildning och träning, men också nationell kultur, har konstaterats ha betydelse för informationssäkerhetskulturen (da Veiga & Martins, 2017). Det finns dock ett behov av mer kontextualiserad kunskap om organisatoriska faktorer som påverkar anställdas förmåga och motivation till såväl regelföljande som delaktigt informationssäkerhetsbeteende.

6 Forskningsprojektet Informationssäkerhet i praktiken

Det övergripande syftet med projektet Informationssäkerhetskultur i praktiken är att utveckla arbetssätt och IT-stödda verktyg för att identifiera förändringsbehov i informationssäkerhets-kulturer och undersöka hur utbildning av medarbetare och chefer påverkar informations-säkerhetskultur och faktiska beteenden. Ett annat syfte är att utveckla kunskap avseende vilka faktorer som är betydelsefulla för anställdas bedömningar, beslut och beteenden med effekter på organisationers informationssäkerhet. Ytterligare ett syfte är att beskriva hur visselblåsning hanteras idag i olika organisationer och de problem som upplevs kopplade till det samt att ta fram etiskt robusta riktlinjer för att understödja visselblåsning.

Projektet, som är finansierat av MSB (dnr 2018-13755) genomförs under perioden 2019-2023. Det bygger vidare på resultat från ett tidigare forskningsprogram, Security Culture and Information Technology, SECURIT (Hallberg et al., 2017) och omfattar flera olika delstudier. Projektet koordineras av FOI. I projektgruppen för Informationssäkerhetskultur i praktiken ingår, liksom för det tidigare SECURIT, forskare från Totalförsvarets forskningsinstitut (FOI), Göteborgs universitet, Kungliga tekniska högskolan och Örebro universitet. Projektet är flervetenskapligt och forskarna arbetar inom ämnena informationssäkerhet, informatik och datavetenskap, arbets- och organisationspsykologi, filosofi, samt freds- och utvecklingsforskning.

7 Målgrupp för projektresultaten

Målgrupperna för projektet Informationssäkerhetskultur i praktiken är beslutsfattare i organisationer där informationssäkerhet är en viktig förutsättning för att värna organisationens funktion och integritet. Målgruppen omfattar också myndigheter som ansvarar för samhällsfunktioner där dessa organisationers funktion och integritet är av

avgörande betydelse, samt företag som konsulteras för att stödja myndigheter och organisationer i informationssäkerhetsarbetet. De arbetssätt, verktyg och den kunskap som är resultat av projektet kan användas för att utveckla anställdas vilja och förmåga att på ett effektivare sätt värna informationssäkerhet, samtidigt med andra organisatoriska och samhälleliga värderingar.

8 Projektets utgångspunkt i tidigare forskning

Forskning kring informationssäkerhetskultur har funnits på agendan sedan början av 2000-talet (Connolly, 2000; Von Solms, 2000). Ett antal översikter har gjorts under åren i syfte att sammanfatta existerande forskning (Chang & Lin, 2007; L. Connolly & Lang, 2013; F. Karlsson, Åström, & Karlsson, 2015; Malcolmson, 2009). Av dessa är (Karlsson et al., 2015) den mest aktuella och omfattande, med 72 analyserade studier publicerade mellan 2000 och 2013. Även om det är ett tag sedan översikten gjordes så är de mönster som identifierades där fortfarande aktuella. Översikten visar att den existerande forskningen spänner över en rad övergripande forskningsfrågor: vad informationssäkerhetskultur är och hur detta fenomen ska definieras (se t.ex. Harnesk & Lindström, 2011) och operationaliseras (se t.ex. Okere, van Niekerk, & Carroll, 2012); hur informationssäkerhetskulturer uppstår i organisationer (se t.ex. Dhillon, Syed, & Pedron, 2016; Knapp, Marshall, Rainer, & Ford, 2007); samt hur informationssäkerhetskulturer kan förändras (se t.ex. da Veiga & Martins, 2017; da Viega & Eloff, 2010). Av dessa tre områden har mest fokus lagts på hur informationssäkerhetskulturer uppstår. Forskning om effekter och konsekvenser av olika typer av informationssäkerhetskultur för informationssäkerheten i organisationer saknades helt i tidigare litteratur (Karlsson et al., 2015). Forskning inom det tidigare forskningsprogrammet SECURIT bidrog dock till att det under senare år har publicerats studier som adresserar denna fråga (Karlsson, Denk, & Åström, 2018; M. Karlsson, Karlsson, & Åström, 2017; Pousette & Törner, 2017b; Skyvell-Nilsson, Pousette, & Törner, 2018; Sommestad, 2018). Området får dock fortfarande anses relativt outforskat och det finns ett fortsatt behov av forskning som empiriskt prövar effekter och konsekvenser av olika typer av informationssäkerhetskultur och av initiativ till kulturella förändringar.

En majoritet av den tidigare forskningen är antingen empiriskt deskriptiv, problematiserande, eller teoretiserande (Karlsson et al., 2015). Teoriutvecklande empiriska studier, där teori och empirisk forskning kombineras, förekommer (se t.ex. Skyvell-Nilsson et al., 2018), men är mindre vanliga. Speciellt slående är att forskning kring ramverk för att förändra informationssäkerhetskulturer ofta saknar empirisk bas (se t.ex. Ngo, Zhou, & Warren, 2005; Thomson & van Niekerk, 2012). Dessa ramverk är fortfarande i mångt och mycket oprövade teoretiska produkter. Det finns således behov av forskning som utvecklar teoretiska modeller som är empiriskt grundade samt

att empiriskt testa och validera dessa. Det råder även brist på empiriska studier som klargör effekter och konsekvenser av olika informationssäkerhetskulturer för informationssäkerheten i organisationer. Med få undantag (da Veiga & Martins, 2017) saknas också interventionsstudier för att utveckla verktyg och arbetssätt som kan användas av praktiker för att förändra informationssäkerhetskulturen.

9 Delprojektet Arbetsorganisatoriska och psykosociala faktorers betydelse för informationssäkerheten

De följande kapitlen fokuserar specifikt på ett av de sex delprojekten inom projektet Informationssäkerhetskultur i praktiken, nämligen Arbetsorganisatoriska och psykosociala faktorers, och sociala processers, betydelse för informationssäkerheten.

9.1 Syfte

Syftet med delprojektet Arbetsorganisatoriska och psykosociala faktorers, och sociala processers, betydelse för informationssäkerheten var att undersöka betydelsen av arbetets kvantitativa och kognitiva krav, den psykosociala arbetsmiljön och informationssäkerhetsklimatet [1], för förhållningssätt och informationssäkerhetsbeteende bland anställda som hanterar digitaliserad information i organisationer med central betydelse för samhällets funktion och säkerhet. Ett specifikt fokus låg på att undersöka förekomst av arbetsrelaterade värdekonflikter som involverade informationssäkerhet, samt sådana konflikters relation till de anställdas informationssäkerhetsbeteende.

9.2 Delstudiens empiri i högriskverksamhet

Vi hämtade våra forskningsdata från två organisationer inom svensk kärnkraftsindustri och använde oss av såväl en enkätundersökning med två mätpunkter med ett års intervall, som djupintervjuer med chefer och deras medarbetare. Kärnkraftsproduktion och till denna industri relaterade verksamheter är av särskilt intresse när det gäller samhällssäkerhet. Verksamheten är av högriskkaraktär och måste vara rigoröst säkrad. Högriskindustri har definierats som verksamheter vars arbetsprocesser omfattar substantiell risk för människor och miljö, med hög potential antingen för

[1] Informationssäkerhetsklimat är ett fenomen besläktat med informationssäkerhetskulturen. Informationssäkerhetsklimatet definieras här, i analogi med annan organisationsklimatforskning (Neal & Griffin, 2002), som organisationsmedlemmarnas gemensamma perceptioner av policy, procedurer och praktik i relation till informationssäkerhet. För mer ingående begreppsförklaring, se (Törner, 2017).

omfattande olyckor, såsom i kärnkraftsindustri, kemisk industri eller flyg, eller för mindre omfattande händelser och arbetsolyckor (Grote, 2012). Processer och procedurer för drift och ledning i kärnkraftsindustri syftar alla till att minimera risken för olyckor. Denna typ av verksamhet genomgår utveckling som omfattar implementering av avancerad teknologi och ställer höga krav på informationssäkerheten för att värna verksamheten från externa hot såsom cyberattacker (Hamer, Waterson, & Jun, 2021). Kärnkraftverk samverkar också nära med andra typer av organisationer, som tillhandahåller material och tjänster och omhändertar och förvarar utbränt kärnbränsle. Kärnkraftsindustrins säkerhet är därför beroende av även dessa parters förmåga att säkerställa en hög nivå på säkerheten, inte minst informationssäkerheten.

9.3 Enkätundersökning

I enkätundersökningen vände vi oss till samtliga anställda i de två organisationerna, totalt 1073 personer. Vid det första mättillfället svarade 667 personer (62%) och vid det andra 589 av 999 personer (59%). Deltagarna vid mättillfälle 1 var i genomsnitt 48 år. De hade varit anställda i företaget i 15 år i genomsnitt och 7 år på den avdelning där de arbetade vid mättillfället. I medeltal hade de 10 års erfarenhet av nuvarande arbetsuppgifter. Sjuttio procent av de svarande var män och 34% hade en chefsposition.

Enkäten omfattade frågor om informationssäkerhetsklimat (Pousette & Törner, 2017a); kognitiva och kvantitativa krav i arbetet, utvecklingsmöjligheter i arbetet; inflytande; meningsfullhet; förutsägbarhet; rollklarhet; organisatorisk rättvisa; samt socialt stöd från överordnad (Pejtersen, Søndergård Kristensen, Borg, & Bue Bjorner, 2010). Enkäten omfattade även frågor om förekomsten av värdekonflikter i arbetet, mellan informationssäkerhet å ena sidan och å den andra a) att kunna utföra sina arbetsuppgifter; b) kunna arbeta tillräckligt snabbt; och c) kunna arbeta med tillräckligt hög kvalitet. Dessa frågor utvecklades av forskargruppen. Vidare ställde vi frågor om det egna regelföljande och delaktiga informationssäkerhetsbeteendet (frågor utvecklade av forskargruppen, delvis baserat på Neal & Griffin, 2002).

9.4 Djupintervjuer

Kvantitativa mått ses ofta som en gyllene standard vid undersökningen av mänskliga aspekter av informationssäkerhet. Man kan dock få en annan - och djupare - förståelse av relevanta fenomen om man även använder sig av kvalitativ metodik (ENISA, 2018). Kvalitativa studier kan ge rikhaltiga perspektiv och en djupare insyn i attityder, beteenden och sociala processer som påverkar informationssäkerheten. I den här studien eftersträvade vi en fördjupad förståelse kring organisatoriska och sociala förhållanden som påverkar regelföljande respektive delaktigt

informationssäkerhetsbeteende. Vi valde därför att komplettera den kvantitativa enkätstudien med kvalitativa intervjuer.
Djupintervjuerna genomfördes med 24 anställda i olika funktioner, 12 i var och en av de två deltagande organisationerna. Tre av informanterna i varje organisation var chefer och totalt intervjuades 14 män och 10 kvinnor. Medelåldern var 49 år.

I den första delen av intervjuerna var intervjumetoden baserad på så kallad Critical Incidence teknik (ungefär 'kritiska händelser') (Flanagan, 1954). Tekniken går ut på att man ber informanten själv beskriva en specificerad situation, utan att intervjuaren själv för in teman i beskrivningen. Genom Critical incident tekniken undviker intervjuaren alltså i hög grad oönskad påverkan på informanterna. Men tekniken har även andra fördelar. Genom att be informanten i minnet återkalla situationer hen upplevt understöder det informantens tillgång till sina kontextspecifika minnen och personliga upplevelser av relevanta situationer (Grill & Nielsen, 2019; Wheeler, Stuss, & Tulving, 1997). Man återupplever i någon mån händelsen och minns då känslor och omständigheter man lätt glömmer eller utelämnar när frågorna är mer generaliserade.

Vi inledde med att be informanten att så fullödigt och detaljerat som möjligt beskriva en situation då hen själv tagit initiativ för att värna eller förbättra informationssäkerheten på sin arbetsplats. Intervjuledarna ställde sedan följdfrågor för att fördjupa och tydliggöra de beskrivningar informanten själv gett, och utan att föra in nya, egna teman. Därefter ställdes frågor om huruvida man uppfattade att det fanns något i arbetssituationen (organisering, chefer, arbetskamrater) som motiverar respektive avmotiverar en själv att ta sådant personligt ansvar för informationssäkerheten. Vi efterfrågade också hur det initiativ man tagit hade tagits emot av ens chefer och arbetskamrater och hur man avsåg göra nästa gång man befann sig i en liknande situation.

När dessa frågor var uttömda bad vi informanten beskriva en situation hen kände väl till, då hen själv, eller någon annan på arbetsplatsen, underlåtit att till punkt och pricka följa föreskrivna procedurer eller regler som företaget har för att säkerställa hög informationssäkerhet.

Därefter ställdes en fråga om förekomst av värdekonflikter som involverade informationssäkerhet. Vi bad informanten beskriva en situation där hen upplevt att det varit svårt, för en själv eller för någon annan, att följa företagets informationssäkerhetsregler eller informationssäkerhetsprocedurer därför att det inneburit konflikt med andra för företagets verksamhet viktiga värden.

I intervjuns avslutande del bad vi informanten reflektera över hur det är i den egna arbetsgruppen, omfattande arbetskamrater och närmaste chef, och hur man där brukar prioritera när två olika typer av värdekonflikter förekommer. Vi bad dem på en skala 1-

5 skatta hur man brukar prioritera mellan att å ena sidan till varje pris följa informationssäkerhetsreglerna (5) och å andra sidan arbeta så effektivt som möjligt (1), respektive hålla så hög kvalitet som möjligt i arbetet (1). Intervjuerna, som bandades och transkriberades, analyserades sedan genom så kallad tematisk innehållsanalys (Braun & Clarke, 2006).

10 Resultat och diskussion

10.1 Organisatoriska och psykosociala förhållanden som påverkar informationssäkerhetsbeteendet

Som ett första steg i arbetet undersökte vi vilka organisatoriska och psykosociala förhållanden i arbetet som påverkade anställdas informationssäkerhetsbeteende, såväl det regelföljande som det delaktiga. Detta gjorde vi genom djupintervjuerna som beskrivits ovan. Analysen visade att dessa förhållanden kunde inordnas i tre övergripande kategorier, nämligen strukturella, sociala respektive individuella förhållanden. Dessa tre övergripande kategorier, deras sex huvudteman och respektive underteman presenteras översiktligt i Tabell 1, och mer ingående i följande text, där de olika temana illustreras med citat från intervjuerna.

10.1.1 Strukturella förhållanden

10.1.1.1 Tema 1: Väl anpassade och fullt accepterade regler

Undertema 1a: Reglernas mängd, systematisering och överblickbarhet

Intervjupersonerna rapporterade att det mycket stora antalet informationssäkerhetsregler gjorde dem svåra att överblicka. Förmågan att söka och förstå informationssäkerhetsregler skilde sig också mellan olika anställda och det kunde ibland vara en utmaning att hitta eftersökt information. God systematisering av reglerna ansågs därför fundamentalt, inte minst för att uppmuntra mindre erfaren personal att söka mer information om reglerna och därmed öka sannolikheten för regelefterlevnad.

Reglernas och föreskrivna procedurers detaljeringsgrad måste också vara väl balanserad och anpassad till den del av verksamheten de avser att reglera. Alltför generella regler skapar osäkerhet, medan alltför hög detaljeringsgrad ökar komplexiteten.

> *”Dom kan vara rätt omfattade dessa instruktioner och regler … Det är inte lätt att sätta sig ner och läsa igenom en av dessa instruktioner.”*

Tabell 1. Sammanställning av intervjuresultatens huvudteman och underteman avseende organisa-toriska och psykosociala förhållanden i arbetet som påverkade anställdas informationssäkerhets-beteende.

Huvudtema	**Undertema**
Strukturella förhållanden	
1. Väl anpassade och fullt accepterade regler	1a. Reglernas mängd, systematisering och överblickbarhet 1b. Reglernas legitimitet 1c. Regler väl anpassade till verksamheten 1d. Stödjande tekniska system och kontinuerlig anpassning mellan regler och teknologi
2. Kunskap, utbildning och väl anpassat kunskapsstöd	2a. Kunskap och förutseende 2b. Utbildning under hela anställningstiden
3. Resurser	3a. Informationssäkerhet tillåts ta tid 3b. Tillgänglighet till expertstöd 3c. Beroende av externa parters resurser
Sociala förhållanden	
4. Stödjande organisationskultur och empowerment[2]	4a. Hög riskmedvetenhet och säkerhetsprioritet 4b. Stödjande ledarskap 4c. Stöd från kolleger 4d. Stödjande experter
5. Samverkan och samordning	5a. Intern samverkan och samordning 5b. Extern samverkan
Individuella förhållanden	
6. Individuellt ansvarstagande och personlighet	6a. Ansvarstagande för organisationens mål 6b. Balans mellan systemstöd och individuellt ansvar och autonomi 6c. Personlighet

[2] Det finns ingen riktigt bra motsvarighet i svenskan till engelskans *empowerment.* Ibland används begreppet *bemyndigande*. Det handlar om att ledningen ger de anställda möjlighet att på olika sätt använda och utveckla sin kompetens. På ett informellt sätt delegerar ledningen på så sätt makt till de anställda, vilket är ett bra sätt att visa att man känner tillit till de anställdas förmåga och motivation att självständigt agera för organisationens bästa. Detta i sin tur stärker den anställdes upplevelse av mandat och tillit till den egna förmågan att bedöma och agera i arbetets olika situationer. Man känner sig bemyndigad.

10.1.1.2

Undertema 1.b: Reglernas legitimitet

Informationssäkerhetsreglerna ansågs vanligen hjälpsamma för att guida olika aspekter av arbetet, men kunskap om varför specifika regler och policyer finns och vilka risker de är avsedda att kontrollera är viktigt för att skapa legitimitet för dem, och därmed regelefterlevnad. Kontinuerlig säkerhetsträning ansågs viktigt för att upprätthålla reglernas legitimitet.

Det kunde föreligga konflikt mellan behovet att skapa regellegitimitet genom att dela bakgrundsinformation om hotbilden för verksamheten å ena sidan, och å andra sidan hålla vetskapen om sådana hot konfidentiell.

> *"Där finns också ett dilemma med potentiella hot som också är konfidentiella, så det finns ett pedagogiskt problem att förklara för folk, "Varför är detta viktigt?" … Det är svårt att motivera någon att skydda sig mot något som man inte får tala om."*

Ansvaret för att skaffa kunskap om säkerhetsreglerna låg i hög grad på den enskilda anställda. Det kunde ibland vara svårt att tolka hur regelverket skulle appliceras, och uppföljningen från ledningen för att tillförsäkra att de anställda hade fått tillräcklig kunskap om och förståelse för regler och procedurer ansågs otillräcklig.

Undertema 1c: Regler väl anpassade till verksamheten

Generella informationssäkerhetsregler fungerade bra för de flesta anställda men för vissa grupper och situationer var sådana generella regler inte kompatibla med arbetsuppgifterna. Detta blev ett problem när det fanns brist på resurser, förmåga eller vilja att hitta kontextuellt verksamma anpassningar. Då ansågs vissa regler omöjliga att följa. Vid andra tillfällen upplevdes reglerna som besvärliga och det togs genvägar för att öka effektiviteten.

> *"Man får inte använda USB-minnen för detta. Men många gånger fanns det inga andra möjligheter och då gjorde vi det i alla fall, vilket innebar regelbrott."*

Eftersom informationssäkerhetsreglerna i hög grad inverkade på de anställdas förmåga att utföra arbetet väl och effektivt, kontaktade de ofta säkerhetsavdelningen angående behov av bättre anpassningar. Sådant engagemang upplevdes inspirerande av de anställda på säkerhetsavdelningen, men bidrog samtidigt till deras arbetsbelastning.

Temat, *Väl anpassade och fullt accepterade regler*, belyser att väl systematiserade och legitima regler som är väl anpassade till verksamheten är viktiga för regelefterlevnaden. Detaljeringsgraden i reglerna måste vara väl balanserad och

anpassad till den kontext där de ska användas. För hög detaljeringsgrad ökar komplexiteten, medan alltför generella regler skapar osäkerhet. Forskaren Grote framhöll att säkerheten ibland kan ökas genom flexibla regler som kan anpassas efter sammanhanget och argumenterade för en god balans mellan flexibla och fasta regler som är anpassade till den specifika organisationen (Grote, 2015). Våra resultat står också i samklang med dem som presenterades i en forskningsöversikt (ENISA, 2018). Där konkluderades att bristande säkerhetsbeteende oftast berodde på att sådant beteende var alltför ansträngande eller komplext och att regler måste byggas på insikten att mänsklig uppmärksamhet och ansträngning är en värdefull resurs som huvudsakligen är inriktad på effektivitet. Det är därför viktigt, menar man, att informationssäkerheten passas väl in i arbetsprocesserna istället för att störa dem.

Undertema 1d: Stödjande tekniska system och kontinuerlig anpassning mellan regler och teknologi

Ett IT-system med inbyggda kontrollmekanismer som stödde och vägledde regelföljandet med avseende på informationssäkerhet ansågs vara ett bra stöd. Detta gällde särskilt i utförandet av arbetsuppgifter som förekom sällan. Sådana kontrollmekanismer minskade risken för vissa misstag och genvägar, och man önskade mer sådant stöd.

> *“Det man måste göra när man inför denna typ av regler, anser jag, är att noggrant tänka igenom… ”Hur är det med stödet i IT-systemet? Kan folk som arbetar med detta göra sitt jobb utan att bli fullständigt frustrerade?” För om man inte gör det, kommer folk att hitta genvägar jättesnabbt.”*

10.1.1.3 Tema 2: Kunskap, utbildning och väl anpassat kunskapsstöd

Undertema 2a: Kunskap och förutseende

Ibland, i ett tidigt skede av ett projekt eller en arbetsuppgift, var kunskapen otillräcklig för att välja rätt nivå på säkerhetsklassningen. Detta, i kombination med att proceduren för att i ett senare skede ändra säkerhetsklassningen var omständlig, uppmuntrade till ”översäkring”. En hög nivå på säkerhetsklassningen sattes då ”för säkerhets skull”, vilket ibland i onödigt hög grad begränsade möjligheterna att dela dokument relaterade till projektet eller arbetsuppgiften. Detta bidrog till ineffektivitet och frustration.

Undertema 2b: Utbildning under hela anställningstiden

Behovet av utbildning och träning, för att lära och minnas informationssäkerhetsreglerna, lyftes fram av många intervjupersoner. I den här aktuella typen av industri måste de anställda vara kunniga inom ett brett spektrum av säkerhetsområden. Det innebär att man måste genomgå en rad olika typer av säkerhetsutbildningar. Hur goda utbildningsprogrammen än är innebar detta ett dilemma, särskilt för nyanställda. Dels utgör tiden en begränsning, då det tar tid att

genomgå alla utbildningar samtidigt som man också måste komma igång med arbetet i någon mån. Dels är det en mycket hög kognitiv utmaning att integrera all information man får under de olika kurserna till kunskap som man kan tillämpa i arbetet. Vikten av hög kvalitet på introduktionsprogrammen, att tillräcklig tid gavs för att genomgå utbildningarna, samt att man erbjöds bra mentorer, framhölls i intervjuerna. Man menade också att det var viktigt att pilottesta alla nya kurser, så att de kunde utvärderas och förbättras innan de implementerades fullt ut.

För att säkerställa att informationssäkerhet ständigt hölls högaktuellt och för att säkerställa relevans och effektivitet i utbildningarna så att kunskapen var väl kopplad till konkreta arbetsuppgifter, var det viktigt att anställda genomgick upprepade utbildningar kontinuerligt under anställningstiden, oavsett erfarenhetsgrad. Vissa aspekter av informationssäkerhet är mycket komplexa och kräver mycket tid och träning att lära sig. Genom kontinuerlig utbildning och träning kunde man bättre upprätthålla medvetenheten om informationssäkerhetsreglernas betydelse och upprätthålla en ständig diskussion om dessa frågor.

> *”Vi är kanske noga med att utbilda de nyanställda, men alla dessa ”gamla rävar” som har jobbat här i många, många år, dom arbetar förmodligen så som de alltid har gjort och jag tror att det är lätt att glömma bort dem.”*

Temat *Kunskap, utbildning och väl anpassat kunskapsstöd* understryker att informationssäkerhetsregler och -procedurer kan vara mycket komplexa och kräva mycket tid att lära sig. Informanterna framhöll därför vikten av kontinuerligt utbildning och träning för att lära och minnas. Man framhöll samtidigt ett viktigt dilemma. I högriskindustri behöver en nyanställd omgående kunskap om ett brett spektrum av säkerhetsfrågor. Vid detta stadium i karriären är man också särskilt beroende av formella regler och procedurer eftersom man har ringa egen erfarenhet som kan guida en i svåra situationer. Samtidigt är tiden som kan ägnas åt utbildning och träning begränsad eftersom man också har arbetsuppgifter som måste skötas. Vidare är lärande av nya arbetsuppgifter en omfattande kognitiv uppgift vilket begränsar förmågan att därutöver ta till sig information om en mängd säkerhetsrelaterade områden i detta skede, samtidigt som det då behövs som allra mest. Detta dilemma tydliggör vikten av fortsatt pedagogisk utveckling och komplementära former för lärande i denna typ av industri.

10.1.1.4 Tema 3: Resurser

Undertema 3a: Informationssäkerhet tillåts ta tid

Att följa informationssäkerhetsreglerna krävde ofta mer tid än att bryta dem och ta genvägar, men informanterna uttryckte att det fanns en allmän acceptans för sådana tidskrav. Man gavs den tid som behövdes för att skydda informationssäkerheten.

Intervjupersoner angav att det inte förekom sanktioner när ett projekt på grund av informationssäkerhetskrav tog längre tid än beräknat.

> *”Man tar informationssäkerheten för givet… det är en förutsättning för att göra jobbet, så man kan aldrig säga ’jag struntar i den’. Snarare är informationssäkerheten en regel vi måste följa. Och under förutsättning att man följer den regeln arbetar man så effektivt man kan. I det dagliga arbetet på min avdelning pratar vi inte så mycket om informationssäkerhet, vi talar mycket om effektivitet. Men detta är alltid med förståelsen att informationssäkerhetsreglerna ska följas.”*

Undertema 3b: Tillgänglighet till expertstöd

Det ansågs viktigt att avdelningen som ansvarade för informationssäkerheten hade tillräckligt med tid och andra resurser för att besvara frågor och ta sig an ärenden som uppstod ute i verksamheterna. När detta saknades blev säkerhetsavdelningarna flaskhalsar. Problem som inte reddes ut i tid skapade frustration bland personal i operativ verksamhet.

Undertema 3c: Beroende av externa parters resurser

Externa partners resurser påverkade förmågan att arbeta enligt informationssäkerhetsreglerna. Ett exempel på sådan begränsning var att krypteringssystem i andra organisationer, exempelvis myndigheter, inte var kompatibla med dem som används i kärnkraftsindustrin. Ett annat exempel på beroendet av externa parters resurser var den säkerhetsgranskning som görs av all personal i kärnkraftsindustrin. Detta utvecklas i citatet nedan.

> *”Ibland sätter samhället upp vissa regler som omfattar någon form av myndighetsadministration. Och ibland klarar myndighetsadministrationen inte av att utföra den administration som krävs. Och det innebär väldigt höga kostnader och väldigt stora problem för oss i industrin. Ett exempel på det, om du jobbar i en högsäkerhetsorganisation, är bakgrundskontroller där säkerhetspolisen är inblandad. Och när den regeln infördes var väntetiden två veckor. Nu plötsligt är väntetiden sex till åtta veckor. Det betyder extremt mycket besvär och extremt höga kostnader. Ju vanligare sådana problem är, desto större är drivkraften att ignorera reglerna. Om reglerna uppfattas som alltför byråkratiska, svåra att följa, ineffektiva och så vidare, så tenderar man att inte följa dem.”*

Det gavs exempel där fördröjningar i bakgrundskontrollen av personer som sökt en tjänst tagit så lång tid att sökande hade valt annan anställning.

I temat *resurser* framkom vikten av acceptans i organisationen för den extra tid som informationssäkerhetsprocedurerna krävde. Sådana procedurer kan innebära extra arbetsbelastning och att den anställda måste hantera komplex teknologi.
Begränsningar i externa parters resurser orsakade ibland fördröjningar. Exempelvis innebar fördröjning i säkerhetsgranskningen av ny personal att sökande valde andra jobberbjudanden. Detta innebär ett hot mot företagens kompetensförsörjning.

10.1.2 Sociala förhållanden

10.1.2.1 Tema 4: Stödjande organisationskultur och empowerment

Undertema 4a: Hög riskmedvetenhet och säkerhetsprioritet
Informationssäkerhet var en fråga som var mycket aktuell i det dagliga arbetet och många intervjupersoner beskrev en hög medvetenhet i organisationen om detta område.

> *"Det känns som att det ligger i kulturen på något sätt …att ha det i bakhuvudet 'Är detta OK att visa någon annan?' Och det känns som att vi tänker så hela tiden, eller åtminstone gör jag det. Och jag tror att de flesta på min avdelning skulle svara på liknande sätt också."*

Undertema 4b: Stödjande ledarskap
Cheferna på alla nivåer ansågs vara starka förebilder i arbetet med informationssäkerhet, och det var viktigt att de föregick med gott exempel. Så ansågs också genomgående vara fallet. Den högre företagsledningen ansågs vara genuin och trovärdig i sina krav på säkerhetsprioritering. Dessa chefer signalerade att informationssäkerhet är viktigt, såväl genom att leda utbildningar i ämnet och genom att backa upp anställda som framhärdade i att följa informationssäkerhetsprocedurerna i situationer då det uppstått konflikt kring detta med personer inom andra (icke kärnkraftsproducerande) delar av koncernen eller externa parter.

> *"Vår företagsledning försöker verkligen sprida budskapet att dessa frågor är viktiga. Vi har en grundläggande säkerhetsutbildning som alla ska genomgå… Och dom har nu sett över strukturen på den kursen, uppdaterat den för alla anställda, och någon i högsta ledningen har lett kursen varje gång."*

Några intervjupersoner påpekade att företagets VD signalerade vikten av att lyfta fram misstag eller praktik som skulle kunna leda till brister i säkerheten, bland annat informationssäkerheten.

> *"Vi har en tydligt uttalad mentalitet i det här företaget, skulle jag säga, att säkerhet kommer först, och att det gäller i alla situationer oavsett om det relaterar till personsäkerhet, informationssäkerhet eller något annat. Alla anställda här har*

rätt att säga ”Stopp, det här är inte OK”, utan att man ses som ett svart får. Och det är väldigt tydligt kommunicerat hela vägen från VD att han förväntar sig detta också.”

Undertema 4c: Stöd från kolleger

Vikten av stöd från arbetskamraterna var ett framträdande område i de flesta intervjuerna. Det spelade en viktig roll för medvetenhet om och gemensam förståelse och tolkning av informationssäkerhetsreglerna.

“Det är kunskapen i gruppen, anser jag. Vi har ett projektteam… och det känns som att teamet har kunskap om det här, så det här blir naturligt… Man måste alltid ta reda på och dubbelkolla vad som är OK och inte OK att skicka. Och att visa. Men det känns som att vi löser detta rätt bra tillsammans.”

Diskussion mellan kolleger om olika aspekter av informationssäkerhet och hur reglerna ska tolkas är ett viktigt sätt att lära sig och öka medvetenheten, och det efterfrågades mer möjligheter till sådana diskussioner. Grupper av kolleger samlades spontant för att försöka lösa problem tillsammans, eller för att utveckla en gemensam tolkning av komplexa regler. Ibland var reglerna inte helt entydiga och diskussion med kolleger hjälpte till för att komma fram till gemensamma strategier för hur sådana situationer skulle hanteras. Arbetskamraterna erbjöd även stöd i bedömningen när olika viktiga värden skulle vägas mot varandra, såsom informationssäkerhet och effektivitet. Återkommande kollegiala samtal och diskussioner skapade en normativ konsensus avseende hur regler skulle tolkas och implementeras, vilket minskade risken att enskilda personers säkerhetsbeteende drev i en oönskad riktning. Samtal om informationssäkerhet ökade reflektionen och knöt detta ämne närmare den dagliga verksamheten.

Intervjupersonerna beskrev en öppen icke-skuldbeläggande kultur, där det var acceptabelt att begå misstag och att sådana sällan resulterade i sanktioner, men där det var socialt oacceptabelt att försöka sopa misstag under mattan. Det ansågs också socialt accepterat att påpeka andras misstag så länge detta gjordes respektfullt och konstruktivt. Flera informanter uttryckte att även socialt mycket utmanande agerande var accepterat, som att korrigera personer i högre organisationspositioner som agerat på ett regelvidrigt sätt.

[En informants reaktion på att ha blivit korrigerad av en mer junior kollega]: *”Vad sa jag? Tja, jag tackade honom, liksom, ‘Ha,ha!’ Och jag sa ’Bra gjort!” för det var en rätt ny kille som sa det, så det var rätt.”*

Nyanställda handleddes och socialiserades på ett aktivt sätt in i en kultur av personligt ansvarstagande. Detta skapade inte bara gruppsammanhållning och

rollklarhet utan också kollegial kontroll, då ett avvikande beteende spiller över negativt även på arbetskamraterna i teamet och påverkar hur hela teamet uppfattas av andra.

Undertema 4d: Stödjande experter

Experter på informationssäkerhet erbjöd stöd till de anställda och intervjupersonerna rapporterade att dessa experter vanligen hade en välkomnande och öppen attityd som uppmuntrade de anställda att ställa frågor. Det ansågs viktigt att kunna komma i kontakt med en expert snabbt och enkelt, men personalen på säkerhetsenheten kunde vara överbelastad vilket fördröjde svar på frågor som inte hade högsta prioritet. Anställda som upplevde att informationssäkerhetsreglerna i hög utsträckning begränsade deras möjlighet att utföra sitt arbete efterfrågade betydligt mer dialog med och engagemang från säkerhetsexperterna än vad som för närvarande erbjöds, för att kunna utveckla lösningar som var acceptabla för båda parter.

Temat *Stödjande organisationskultur och empowerment* pekar på betydelsen av ett stödjande ledarskap och stöd från kolleger och experter. Vikten av ledningens prioritering av säkerhet som en primär förutsättning för ett bra säkerhetsklimat är tydligt visat i annan säkerhetsforskning (Beus, Payne, Bergman, & Arthur, 2010; Christian, Bradley, Wallace, & Burke, 2009).

Organisationskulturen, liksom därmed säkerhetskulturen, omfattar också sociala normer bland arbetskamraterna och forskaren Jackson konstaterade att socialt stöd från och tillit mellan arbetskamraterna var viktigt för att individen skulle internalisera gruppens säkerhetsprioritering och validera hens upplevelse av kompetens. Denna upplevelse av egen kompetens var viktig för att kunna hantera oklara arbetssituationer (Jackson, 2017). Andra forskare har också funnit att anställda vänder sig till arbetskamraterna för social verifiering när situationen är oklar (Festinger, 1964; Weick, 1995). Förbättring av informationssäkerheten har också visat sig kräva innovativa sätt att uppmuntra kunskapsdelning mellan kolleger (Pérez-González, Preciado, & Solana-Gonzalez, 2019). I vår studie underströk informanterna vikten av frekventa och spontana kollegiala diskussioner om olika aspekter av informationssäkerhet och hur reglerna skulle tolkas och implementeras i specifika situationer. Detta var ett sätt att lära och att höja medvetenheten, men inte minst att utveckla en gemensam tolkning av regler och komma fram till gemensamma strategier för hur dessa skulle tillämpas i oklara situationer. Det har tidigare framhållits att cybersäkerhet kräver ”heroiskt agerande” när nya hot ska hanteras, och sådant agerande kan bara åstadkommas av anställda som är kunniga, engagerade, betrodda och känner tydligt stöd från organisationen (Pfleeger, Sasse, & Furnham, 2014). I vår studie uttryckte intervjupersonerna att stöd och feedback från kolleger och ledning ökade upplevelsen av empowerment och motivation att ta initiativ för att förbättra informationssäkerheten. Man framhöll betydelsen av ett arbetsklimat där det är socialt accepterat att respektfullt

och konstruktivt ifrågasätta och kritisera kollegers och överordnades beteende. Att göra detta kräver en hög grad empowerment och ömsesidig tillit.

10.1.2.2 Tema 5: Samverkan och samordning

Undertema 5a: Intern samverkan och samordning

God samverkan mellan olika enheter och team inom organisationen var viktigt för att dela och utveckla arbetssätt i enlighet med informationssäkerhetsreglerna. Organisering baserad på olika arbetsuppgiftsområden skapade god rollklarhet men också skarpa rollgränser. Olika funktionella enheter hade sina egna organisationslogiker. Detta bidrog till ’stuprör’ och motverkade koordinering mellan olika delar av organisationen. Det fanns också en tendens till ’vi och dom-mentalitet’ mellan olika geografiska organisationsetableringar. Många möten kunde hållas genom elektroniska medier, men ibland behövdes fysiska mötena för att överbrygga sådana hinder.

> *“Utmaningen är att kommunicera så att vi förstår varandra. Det kan gälla både dom och oss… men vi måste fortfarande försöka få dem att förstå. Men vi bör också försöka förstå dom… Och då, om man är på samma plats, fungerar det… och då verkar det som att vi förstår varandra.”*

Mer och bättre kommunikation mellan informationssäkerhetsavdelningarna och specialistavdelningar efterfrågades, för att kunna hitta lösningar som var acceptabla för båda parter. Det framhölls att IT-systemen var designade för att passa standardanvändaren, vilket fungerade bra i de flesta fall. Men det ansågs viktigt att mer tid och resurser las på att utveckla lösningar för de mer specialiserade användarna, för att möjliggöra bättre effektivitet i deras arbete.
Det framhölls också att experternas kunskap behövde utvecklas om projektadministratörernas tidsbehov för sina informationssäkerhetsrelaterade arbetsuppgifter. Sådan ökad kunskap skulle underlätta koordinering och därmed kvaliteten i arbetet, och reducera belastningen och stressen på båda parter.

Undertema 5b: Extern samverkan

Informationssäkerhetsreglerna kunde orsaka störningar i samarbetet med externa parter och göra sådana processer svårmanövrerade.

> *“Och vi sa, ‘Nej, men detta är säkerhetsklassade dokument, så ni kan inte få dem. I så fall måste de skickas på papper.’ Dom ville att vi skulle scanna dom och maila dom. ’Nej, det kan vi inte göra.’ Dom pratade med vår VD för dom var så upprörda för att vi följde… Självklart kan vi inte säga att vi ska göra ett undantag [skratt] från våra informationssäkerhetsregler. Så det är olika kulturer.”*

Användningen av allmänt förekommande datorprogramvara, som underlättade arbetets utförande men som inte erbjöd tillräcklig informationssäkerhet, var restrikterad. Detta orsakade kontroverser mellan olika parter och minskade effektiviteten i samarbetet. Man förutsåg att ökad digitalisering skulle komma att öka dessa konflikter i samarbetet med parter såväl inom som utanför koncernen, och att det även skulle komma att öka mängden hot mot säkerheten. Det är lättare att kontrollera spridningen av pappersdokument än elektroniska dokument. Även användningen av elektroniska konferensmedier begränsar möjligheten att kontrollera vem som deltar i ett möte.

Kommunikationen med myndigheter kunde ibland vara problematisk. Ett exempel var olika lagverk som stod i konflikt med varandra, där ett föreskrev konfidentialitet och ett annat öppenhet. Svensk lag föreskriver en hög grad av allmän tillgänglighet till myndigheters information. Det ansågs därför att det fanns en risk att hemliga dokument som sändes till myndigheter oavsiktligt skulle komma att spridas.

Etablerad internationell samverkan kring kärnkraftssäkerhet, där informationssäkerhet är en del, framhölls som viktigt och bra.

Det socialt relaterade temat *Samverkan och samordning* omfattade således såväl interna som externa samarbeten. I dessa organisationer, liksom de flesta andra, kan organisationslogiken skilja sig mellan olika avdelningar. När denna skillnad är stor, vilket ibland var fallet i de aktuella organisationerna, uppstår lätt misstro och omfattande problem i koordinationen mellan olika avdelningar. Andra forskare har rapporterat liknande problem. Samarbetet mellan säkerhetsexperter och andra anställda kan ibland vara bristfälligt med envägskommunikation från säkerhetsspecialisterna och anställda som undviker att rådgöra med dessa (Ashenden & Sasse, 2013). Även ENISA har påpekat behovet av att förbättra samarbetet mellan säkerhetsexperter och andra organisatoriska funktioner (ENISA, 2018).

10.1.3 Individuella förhållanden

10.1.3.1 Tema 6: Individuellt ansvarstagande och personlighet

Undertema 6a: Ansvarstagande för organisationens mål

Många intervjupersoner uttryckte ett starkt personligt ansvar för att arbeta i enlighet med informationssäkerhetsreglerna, och aktivt bidra till att utveckla informationssäkerheten. Att ta personligt ansvar ansågs vara en viktig del av jobbet för alla anställda.

> *"Individuellt ansvar är en viktig del av att upprätthålla säkerheten. Så det handlar om att ta mycket initiativ, så jag försöker leda på det sättet."*

Undertema 6b: Balans mellan systemstöd och individuellt ansvar och autonomi

Det ansågs viktigt att ha en balans mellan å ena sidan styrande systemstöd och detaljeringsgrad i regler och procedurer, och å den andra individuell uppmärksamhet och ansvar. Kritisk reflektion som utmanade befintlig praktik, och att vara öppen för fortsatt utveckling nämndes som viktigt. Det framhölls att det finns risker med ett system som är alltför specificerande och kontrollerande. Ett sådant system kan frånta individen känslan av personligt ansvar och därigenom minska observans, kritisk reflektion och drivkraften att agera på ett delaktigt sätt.

> *"Man kan bygga det ideala systemet, där alla dokument, all mail, allt hanteras, men då alienerar man människan; med andra ord, han eller hon känner att man saknar kontroll – jag är bevakad och kan sluta tänka på säkerheten."*

Emellertid, samtidigt som viss autonomi och utrymme för tolkningar ansågs viktigt så underströks det som nödvändigt att ta konservativa beslut i tveksamma situationer.

Undertema 6c: personlighet

Individuella skillnader och personlighet påverkar om en anställd tar ansvar för att följa och utveckla det pågående informationssäkerhetsarbetet. En del av intervjupersonerna uttryckte tydligt att risktagare, eller personer som saknar tålamod med ibland svårarbetade procedurer, inte är lämpade att arbeta i denna typ av verksamhet.

I temat, *Individuellt ansvarstagande och personlighet,* framhålls, liksom i tidigare forskning, att organisationer behöver anställda som är empowered och kan agera för att hantera snabbt uppkomna hot mot informationssäkerheten (Kirlappos, Parkin, & Sasse, 2015). I vår studie uttryckte informanterna tydligt att de tog personligt ansvar för informationssäkerheten och såg sig själva som viktiga aktörer för att skydda organisationens säkerhet. Vidare framhölls vikten av att balansera individuellt ansvar och tvingande tekniska systemstöd. Ett alltför kontrollerande system kan beröva de anställda känslan av ansvar. Forskaren Grote menade att säkerheten i vissa situationer kan stärkas genom flexibla regler som kan anpassas enligt de specifika förutsättningar som är aktuella (Grote, 2015). Grote menade att individen måste uppmuntras att tänka fritt och säga ifrån när hen ser problem. Övertro på säkerhetssystemen kan leda till falsk trygghet, något som har framhållits som en viktig bakomliggande orsak till stora olyckor (Årstad & Aven, 2017).

Personlighetens betydelse för informationssäkerhetsinsikt har tidigare studerats och man har funnit att personlighetsegenskaperna samvetsgrannhet, tillmötesgående, och emotionell stabilitet kan vara gynnsamma, medan en risktagande personlighet kan vara negativt (McCormac et al., 2017). ENISA (2018) menade dock att personlighet sällan kan kopplas till informationssäkerhet på ett konsistent sätt. I vår studie påpekade

intervjupersoner att en risktagande personlighet inte hör hemma i kärnkraftsindustrin. Några påpekade också att eftersom högriskverksamhet alltid kommer att vara strikt reglerad, med en stor mängd regler och procedurer så krävs det anställda som har tillräckligt med tålamod att utstå och upprätthålla ett sådant omständligt arbetssätt.

10.2 Krav och resurser i arbetet i relation till informations-säkerheten

Syftet med denna del av studien var att undersöka vilken betydelse arbetskrav och arbetsresurser hade på självskattat regelföljande och delaktigt informationssäkerhetsbeteende. Våra grundantaganden var att god tillgång till arbetsresurser skulle vara förknippat med en hög grad av såväl regelföljande som delaktigt informationssäkerhetsbeteende, medan höga arbetskrav skulle vara förknippade med lägre förekomst av informationssäkerhetsbeteende bland de anställda.

Forskarna Bakker och Demerouti utvecklade ett ramverk för hur olika arbetsförhållanden kan få önskade eller oönskade effekter i en organisation, den så kallade krav-resursteorin. Teorin definierar arbetskrav som “sådana fysiska, psykologiska, sociala eller organisatoriska aspekter av arbetet som kräver ihållande fysisk och/eller psykologisk (kognitiv eller känslomässig) ansträngning eller förmåga och därför är förknippade med vissa fysiologiska eller psykologiska kostnader” (Bakker & Demerouti, 2007, sid. 312). Arbetsresurser definieras av samma forskare som motsvarande organisatoriska aspekter som istället är stimulerande och minskar fysiologiska och psykologiska kostnader.

I denna undersökning använde vi oss av såväl tvärsnittsdata som longitudinella enkätdata. Vi undersökte hur vanligt förekommande enkätrespondenterna ansåg att olika arbetskrav och arbetsresurser var i deras arbete med hjälp av enkätskalor hämtade från Copenhagen Psychosocial Questionnaire (COPSOQ-II), version två (Pejtersen et al., 2010).

Vi mätte fyra dimensioner av *arbetskrav: kvantitativa krav* (exempelfråga: Är din arbetsbörda ojämnt fördelad så att arbete samlas på hög?); *arbetstakt* (exempelfråga: Är du tvungen att arbeta väldigt snabbt?); *kognitiva krav* (exempelfråga: Måste du överblicka många saker samtidigt i ditt arbete?); samt *rollkonflikt* (exempelfråga: Måste du ibland göra något som egentligen borde ha gjorts annorlunda?).

Vi mätte sju dimensioner av *arbetsresurser*: *inflytande* (exempelfråga: Har du möjlighet att påverka väsentliga beslut som gäller ditt arbete?); *utvecklingsmöjligheter* (exempelfråga: Har du möjlighet att lära dig något nytt genom ditt arbete?);

meningsfullhet (exempelfråga: Känner du dig motiverad och engagerad i ditt arbete?); *förutsägbarhet* (exempelfråga: Får du information i god tid på din arbetsplats, t.ex. när det gäller viktiga beslut, förändringar och framtidsplaner?); *rollklarhet* (exempelfråga: Vet du exakt vilka som är dina ansvarsområden?); rättvisa (exempelfråga: Löses konflikter på ett rättvist sätt?); samt *socialt stöd* (exempelfråga: Om du behöver, är din närmaste chef beredd att lyssna på problem som rör ditt arbete?).

Inledningsvis kunde vi konstatera att stabiliteten över tid i de olika mätvariablerna varierade en del. Medan arbetskrav och tillgången till arbetsresurser var tämligen stabilt från mättillfälle ett till mättillfälle två, så var det större variation över mättiden i skattningarna av de två typerna av informationssäkerhetsbeteende.

När vi studerade sambanden i tvärsnittsdata fann vi, för det första, att regelföljande och delaktigt informationssäkerhetsbeteende hade tydligt samband med varandra. Vi fann vidare, som förväntat, att god tillgång till arbetsresurser hade ett positivt samband med såväl regelföljande som delaktigt informationssäkerhetsbeteende. Höga arbetskrav hade, som vi också förväntat, ett negativt samband med sådant regelföljande informationssäkerhetsbeteende. Däremot fanns inget samband alls mellan arbetskrav och delaktigt beteende.

De longitudinella analyserna visade en del resultat som styrkte våra antaganden. God tillgång till arbetsresurser vid mättillfälle ett ledde till högre delaktigt informationssäkerhetsbeteende vid mättillfälle två. Detta var i enlighet med vårt antagande. Däremot hade tillgång till arbetsresurser ingen direkt effekt på det regelföljande informationssäkerhetsbeteendet.

Analyserna visade även några delvis oväntade och därför särskilt intressanta resultat. Höga arbetskrav hade en positiv effekt på det delaktiga informationssäkerhetsbeteendet. Här menar vi att resultaten bör ses i ett lite vidare perspektiv. När kraven är höga så ökar behovet av ett delaktigt säkerhetsbeteende för att kunna lösa komplexa situationer och problem. Om arbetsförutsättningarna för övrigt är tillfredsställande så ökar då också motivationen att bete sig delaktigt. Detta resonemang styrks ytterligare av de effekter vi fann att höga krav hade på ett regelföljande beteende. Där kunde vi konstatera att även här fanns en positiv effekt av krav på beteende, men endast under förutsättning att den svarande också upplevde sig ha god tillgång till arbetsresurser. Sådan tillgång till arbetsresurser var alltså ett ramvillkor för att höga krav skulle leda till mer regelföljande informationssäkerhetsbeteende. Om tillgången till arbetsresurser inte var hög hade höga krav ingen effekt på det regelföljande beteendet. Det är också viktigt att inse att sambandet mellan krav och delaktigt säkerhetsbeteende sannolikt inte är rätlinjigt utan snarade invert U-format. Höga krav leder till högre delaktigt säkerhetsbeteende upp till

en viss nivå av krav. Ökar kraven ytterligare blir de sannolikt snarast avmotiverande och man kan förvänta att det delaktiga beteendet istället minskar.

En annan sak som är viktig att beakta i tolkningen av det positiva sambandet mellan krav och delaktigt säkerhetsbeteende är att det kan föreligga en gemensam bakomliggande faktor. Höga krav och högt delaktigt beteende kan båda bero på ett tredje fenomen som vi inte mäter. I detta fall menar vi att yrkesroll kan vara en viktig sådan gemensam bakomliggande faktor. Att exempelvis inneha en chefsroll innebär i sig högre såväl kvantitativa som kognitiva krav. Man kan även förvänta att personer i en chefsbefattning befinner sig på den övre delen av skalan när det gäller motivation för och faktiskt delaktigt beteende. Det är sannolikt att sådant beteende har varit ett av urvalskriterierna utifrån vilka man fick sin chefsbefattning.

I kapitel 9.8 nedan tar vi upp Informationssäkerhetsklimatets betydelse för informationssäkerheten. Här kan vi nämna att våra longitudinella analyser visade att informationssäkerhetsklimatet stärktes av såväl höga krav som god tillgång till arbetsresurser.
Det finns alltså anledning att studera sambandet mellan höga arbetskrav och informationssäkerhetsbeteende och informationssäkerhetsklimat ytterligare i framtida longitudinell forskning.

10.3 Värdekonflikter i arbetet och deras betydelse för informationssäkerheten

Här ville vi med hjälp av intervjuer kvalitativt undersöka hur värdekonflikter som omfattar informationssäkerhet påverkar informationssäkerhetsbeteendet och vilken betydelse kontextuella faktorer har i sammanhanget. Vi ville även med enkäter studera hur vanligt förekommande sådana värdekonflikter var i den här aktuella typen av industriell verksamhet och vilken effekt de befanns ha på informationssäkerhetsbeteendet.

10.3.1 Intervjuer

I intervjuerna identifierade vi fem olika typer av värdekonflikter. Informationssäkerhetsregler visade sig kunna stå i konflikt med a) effektivitet; b) öppenhet och transparens; c) kvalitet; och d) lärande. Dessutom visade sig e) olika aspekter av informationssäkerhetsvärden kunna stå i konflikt med varandra.

10.3.1.1 Effektivitet kontra informationssäkerhet

Den värdekonflikt som oftast togs upp av informanterna var mellan informationssäkerhet och effektivitet i arbetet. Effektivitet avsåg här såväl möjligheten att utföra arbetsuppgifterna som den tid som krävdes för att göra detta.

Högriskverksamhet är kraftfullt reglerat och att arbeta i enlighet med alla informationssäkerhetsregler uppfattades ofta som tidskrävande.

> *”För mig är det att uppnå en… där jag kan vara både effektiv på samma gång som jag följer våra regler. Det är den optimala situationen, men jag tror inte vi är där idag … informationssäkerhet trumfar effektivitet som det är nu.”*

Många informanter framhöll att det var en generell acceptans i organisationen att arbetet i enlighet med informationssäkerhetsreglerna fick ta den tid som krävdes och att det inte fanns något tryck att arbeta snabbare genom att kompromissa med säkerheten. Denna acceptans bidrog till säkerhetsreglernas och -procedurernas legitimitet. Somliga menade dock att samtidigt som denna acceptans var viktig så kunde den missbrukas. Att kunna balansera olika kärnvärden var en viktig kompetens och en del av att ta ansvar för hela spektrat av organisatoriska mål, där kostnadseffektiviteten var ett. Vissa informanter uttryckte åsikten att för att undgå sådant ansvarstagande hade vissa anställda en tendens att ”gömma sig” bakom informationssäkerhetsreglerna. Hävdade man säkerhet kunde man aldrig ifrågasättas.

> *“Relationen mellan att få saker gjorda och inte gjorda, man måste gå försiktigt fram, det är inte svart eller vitt. Det blir en gråzon… Som nyanställda, dom tar en “taliban-approach”, ursäkta uttrycket. ’Om jag bara följer reglerna så gör jag inga misstag.’ Men då blir väldigt lite gjort. Så det är en balansakt.”*

> *“För mig handlar det om att hitta en effektiv väg. För det är ofta jobbigt när det är [informationssäkerhets-]krav… och man ska göra det med minsta möjliga krångel men fortfarande följa reglerna. Jag tycker det är viktigt. Och just nu, tja jag undrar om vi inte kunde göra det lite mer effektivt inom ett visst område. Istället för att ta reda på exakt hur det fungerar så översäkrar en del, gör det extra svårt och lägger till extra bara för att vara på säkra sidan, för dom vågar inte utmana. Ibland tycker jag vi borde fråga oss ’Måste det verkligen vara på det här sättet’?”*

Tidspress förekom ibland på grund av att överordnade saknade en holistisk syn på de anställdas arbetssituation. Även om varje arbetsuppgift i sig tilläts ta tillräckligt med tid och med adekvata deadlines så kunde den sammanlagda mängden sådana uppgifter leda till tidspress. För att kunna leverera även sina andra arbetsuppgifter tvingades de anställda då leverera resultaten av varje enskild uppgift långt innan deadline. När de överordnade saknade ett holistiskt perspektiv kunde de uppfatta sådana tidiga leveranser som av den anställda självinducerad och onödig brådska.

Informationssäkerhetsreglerna kunde hindra de anställda att arbeta flexibelt, hemifrån eller under resor. Detta påverkade deras effektivitet, men även deras balans mellan arbete och fritid. Problemet var mest framträdande för anställda som reste mycket i

tjänsten. Det förstärkte också konflikten mellan säkerhetsavdelningen och anställda i vissa specialistfunktioner som upplevde att informationssäkerhetsreglerna avsevärt begränsade deras möjligheter att utföra sitt arbete. Detta kunde orsaka att man tog genvägar med säkerheten.

> *”Man känner att informationssäkerheten bara är jobbig. Arbetet tar en viss tid och sen ska informationssäkerheten läggas på det…. ”Du måste kryptera det”… och då blir det som vattnet i en bäck, minsta motståndets väg… Man försöker hitta genvägar när man har sådana höga krav på informationssäkerheten och då kan fusk bli en enkel utväg.”*

10.3.1.2 Öppenhet och transparens kontra informationssäkerhet

Somliga informanter uttryckte att det är ett kärnvärde för organisationen att dela information med allmänheten, eftersom transparens är grundläggande för att bygga tillit till organisationen och dess verksamhet. Samtidigt stod transparens ofta i konflikt med informationssäkerhetspolicyer vars syfte var att skydda inte bara organisationen utan även allmänheten och hela samhället. Att balansera kärnvärdena informationssäkerhet och transparens beskrevs som en delikat fråga. För att upprätthålla allmänhetens tillit måste den externa kommunikationen även komma vid rätt tid. Ibland fördröjdes den då tillåtelsen att kommunicera budskapet inte gavs tillräckligt snabbt på grund av hög arbetsbelastning på den enhet som fattade sådana beslut.

> *“Men det är mer den här reflektionen kring informationssäkerhet och vad vi kan prata om kontra transparens, öppenhet och att bygga tillit… Ja, kanske vi inte kan säga allt på grund av sekretess… men samtidigt vill vi vara så öppna och transparenta som möjligt.”*

Det var således en komplex uppgift att hitta den rätta balansen mellan öppenhet och att skydda information. Det uttrycktes klart att i sådana dilemman, till syvende och sist, hade informationssäkerheten företräde. Men att inte kunna kommunicera positiv information kunde ibland vara frustrerande.

> *”Man har olika mål … och tänker att ’det här är fina grejer vi har utvecklat’… Kommunikation och säkerhet passar inte alltid ihop.”*

Värdekonflikten mellan öppenhet och informationssäkerhet var särskilt problematisk för funktioner som var beroende av att kunna dela information med externa parter. De tvingande restriktiva informationssäkerhetspolicyerna upplevdes, ibland allvarligt, hämma de anställdas i dessa funktioner förmåga att utföra sitt arbete och det fanns olika uppfattningar om vilket material som borde vara konfidentiellt.

”Där har du dilemmat att man kan ha olika uppfattningar om vad som är känsligt, så detta är en viktig aspekt att det finns olika uppfattningar om vad som bör vara konfidentiellt, eller vad som är känslig information och vad som inte är det. För en forskare kan hävda att dessa data är tillgängliga på Internet medan andra personer kan hävda att det fortfarande är känsliga uppgifter att sända åtminstone till det landet. Så det kan vara en konflikt kring hur vi värderar informationen.”

10.3.1.3 Kvalitet kontra informationssäkerhet

Att göra ett bra jobb var viktigt för intervjudeltagarna och de flesta uttryckte att informationssäkerheten inte stod i konflikt med kvalitet i arbetet utan snarare var en viktig aspekt av kvaliteten. Ibland utmanades dock kvaliteten av informationssäkerhetsreglerna. Intern och extern kommunikation i text och bild måste alltid presenteras i enlighet med informationssäkerhetsreglerna trots att detta kunde göra presentationerna mindre intressanta och spektakulära. Extern information måste ofta urvattnas vilket kunde minska värdet av innehållet. Detta dilemma accepterades dock som en del av jobbet. Deltagarna uttryckte en förståelse för detta och att det kunde finnas en stimulans att hitta en acceptabel lösning.

”Nej, men då måste den [kommunikationen] bli mer beige… så man måste vara lite speciell för att arbeta här. Man vill alltid ha den där lilla gnistan kvar förstås…’Men det här då? Om jag hittar något som är OK?’ … Man gör den perfekta bilden från ett informationssäkerhetsperspektiv.”

En annan aspekt av värdekonflikt mellan kvalitet och informationssäkerhet relaterade till resurser. Att få tillgång till dokumentation för att förbereda sig för möten kunde ta lång tid på grund av procedurer för att skydda informationen. Detta betydde att man ibland deltog i möten mindre förberedd än man hade önskat.

10.3.1.4 Lärande kontra informationssäkerhet

Några informanter beskrev att strikta informationssäkerhetsregler kunde hindra lärande. Det kunde handla om situationer där en incident inträffat och där det fanns lärdomar att dra från detta men på grund av informationssäkerhetsreglerna kunde informationen inte delas.

”Det skulle vara bättre kvalitet om vi kunde lära från sekretessbelagda situationer… Men detta får man lösa på annat sätt.”

10.3.1.5 Konflikt mellan olika aspekter av informationssäkerhet

Det fanns ibland en konflikt mellan olika aspekter av informationssäkerheten. En informationssäkerhetsaspekt föreskriver att informationen ska vara tillgänglig för auktoriserade användare. En annan aspekt är att informationen ska vara fullständig och riktig. Det senare kräver att informationen är noggrant kvalitetsgranskad före

användning. Informationen i rapporter och dess källor måste dubbelkontrolleras. Detta är mycket tidskrävande och ibland behövs informationen innan det är klart. Detta betydde att viktiga beslut kan försenas då all erforderlig information inte är tillgänglig. Om ett beslut inte kunde vänta måste ibland viktig information lyftas ut ur en rapport tills kvalitetskontrollen slutförts och beslut kunde därför komma att fattas på basis av ofullständig information.

Konflikt mellan olika aspekter av informationssäkerheten visade sig även som en konflikt mellan konfidentialitet och fullständighet/riktighet. Vissa effektiva sätt att dokumentera möten, såsom inspelning eller foto, i syfte att fullständigt kunna relatera eller använda informationen från mötet var inte tillåtna. Detta innebar en risk att viktig information utelämnades eller att informationen förvanskades.

10.3.2 Enkätundersökning

Baserat på tidigare forskning förväntade vi oss att hög förekomst av värdekonflikter skulle medföra en lägre grad av såväl regelföljande som delaktigt informationssäkerhetsbeteende. I enkäten mätte vi förekomsten av värdekonflikter i arbetet genom att fråga hur vanligt förekommande det var i de svarandes arbetsvardag att informationssäkerhetsreglerna stod i konflikt med andra centrala värden i arbetet, nämligen a) möjligheten att utföra sina arbetsuppgifter; b) möjligheten att arbeta tillräckligt snabbt; c) möjligheten att utföra ett arbete med hög kvalitet; d) egen eller andras personliga integritet; samt e) legala aspekter.

De inledande tvärsnittsanalyserna av data från mättillfälle ett visade att värdekonflikter i arbetet var tämligen lite till måttligt vanligt förekommande. På en sexgradig svarsskala (från ”förekommer aldrig” (1) till ”förekommer alltid” (6)) skattades i genomsnitt förekomsten av konflikt med möjligheten att arbeta tillräckligt snabbt till 3,07. Konflikt med möjligheten att utföra sina arbetsuppgifter skattades till 2,95; med att arbeta med hög kvalitet till 2,37; konflikt med personlig integritet till 1,78 och förekomst av konflikt mellan informationssäkerhetsreglerna och legala aspekter skattades i genomsnitt till 1,74.

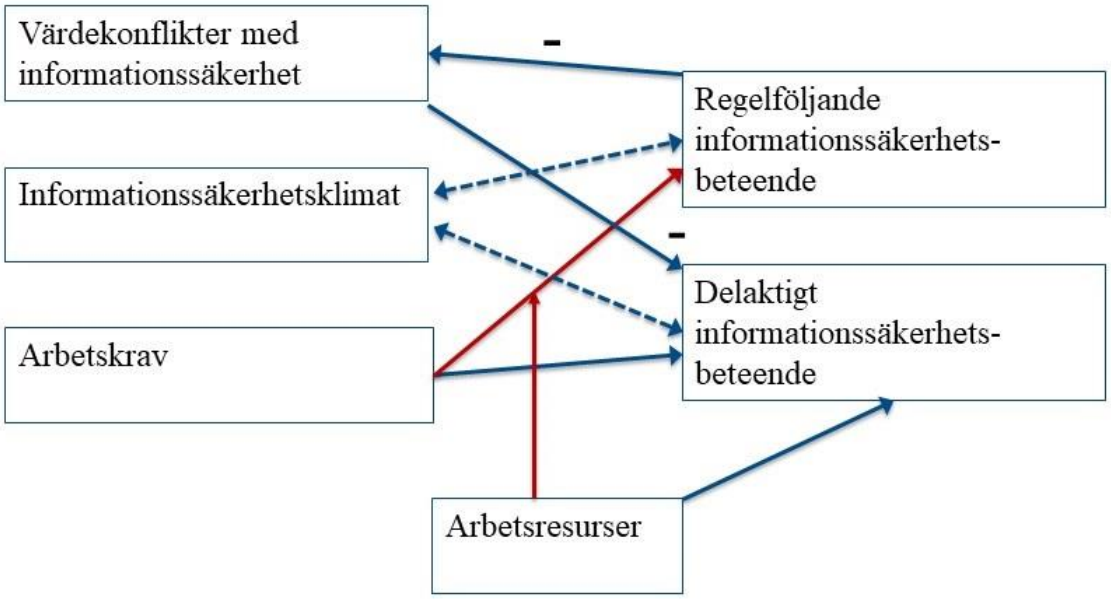
Dessa resultat avviker en del från tidigare forskning. Karlsson, Denk, and Åström (2018) fann exempelvis, att värdekonflikter med informationssäkerhet var vanligt förekommande bland tjänstepersoner, särskilt i organisationer som hanterade mycket känslig information. Det är möjligen så att ju mer informationssäkerhet uppfattas vara en del av kärnverksamheten, desto högre prioritet ges det framför andra värden, såsom effektivitet. I sådana organisationer kan de anställda uppfatta det som mindre krävande att skydda informationen och konflikterna med andra värden kan därför uppfattas som färre. Kärnkraftsrelaterad verksamhet är helt och hållet beroende av en hög nivå av säkerhet. I denna typ av verksamhet är informationssäkerheten ett kärnvärde och en förutsättning för att arbetet ska utföras med hög kvalitet. Detta är

också något som uttrycktes av intervjupersonerna vid produktionsenheterna, som generellt upplevde färre värdekonflikter mellan informationssäkerhet och att arbeta med hög kvalitet. Intervjupersoner, huvudsakligen från dessa enheter, fann det också svårt att ställa informationssäkerhet i motsats till att kunna arbeta med hög kvalitet. Informationssäkerhet sågs av dessa informanter istället som en aspekt av hög kvalitet. Å andra sidan upplevde intervjupersoner som arbetade inom delar av verksamheten som inte var direkt produktionsinriktade, och där informationssäkerhet var mindre av ett kärnvärde, ofta värdekonflikter mellan informationssäkerhetsregler och kvalitet i arbetet.

I analyserna av tvärsnittsdata från enkätundersökningen var, som förväntat, hög förekomst av värdekonflikter negativt relaterat till såväl regelföljande som delaktigt informationssäkerhetsbeteende. Det vill säga, ju vanligare det var med värdekonflikter, desto lägre var båda typerna av informationssäkerhetsbeteende.

De longitudinella analyserna visade, som tidigare angetts, att stabilitet över tid var måttlig för såväl regelföljande som delaktigt informationssäkerhetsbeteende. Detsamma visade sig gälla förekomsten av värdekonflikter i arbetet. Samtliga dessa variabler varierade således en del mellan mättillfälle ett och två. Resultaten av enkätresultaten presenteras i Figur 1.

De longitudinella analyserna visade också att hög förekomst av värdekonflikter vid mättillfälle ett ledde till lägre delaktigt informationssäkerhetsbeteende vid mättillfälle två. Värdekonflikterna tycktes således försvåra, eller minska motivationen till, ett delaktigt beteende. Detta var inte oväntat, men även här ska man förstås vara lite försiktig med tolkningen eftersom det, liksom beskrivits i avsnittet om effekten av höga arbetskrav ovan, kan finnas gemensamma bakomliggande faktorer. Även i detta fall kan exempelvis yrkesrollen vara en sådan faktor. Det är inte omöjligt att tänka sig att chefer generellt är lite mer motiverade att agera delaktigt än andra anställda, samtidigt som de i den roll de innehar upplever färre värdekonflikter.



Figur 1. Resultat av enkätundersökningarna. Streckad, dubbelriktade pilar representerar korrelationer i tvärsnittsdata. De heldragna pilarna anger kausala, longitudinella relationer. De röda pilarna anger att det positiva sambandet mellan arbetskrav och regelföljande informationssäkerhetsbeteende endast förelåg om man även hade god tillgång till arbetsresurser.

Den longitudinella analysen gav dock även här ett oväntat och därmed särskilt intressant resultat. Vi fann en omvänd kausal ordning mellan värdekonflikter och regelföljande beteende, där en högre grad av regelföljande beteende vid mättillfälle ett ledde till att man upplevde färre värdekonflikter vid mättillfälle två. Det tycks således inte vara så att om man upplever mycket värdekonflikter så blir man mindre regelföljande. Istället förefaller det vara så att om man är i hög grad regelföljande så upplever man färre värdekonflikter. ”Lösningen” på detta är alltså inte, som kan förordas baserat på egna och andras tvärsnittsresultat, att om man minskar de anställdas värdekonflikter så ökar deras regelföljande beteende. Istället tycks hög grad av regelföljande innebära en förenkling. Den anställda har bestämt sig för att i varje situation prioritera att följa informationssäkerhetsreglerna och nedprioritera andra organisatoriska värden. I detta sammanhang blir det intressant att relatera enkätresultaten till de kvalitativa resultat som presenterats ovan. Där framhålls vikten för organisationen i sin helhet av att de anställda kan inta ett holistiskt perspektiv och balansera olika organisatoriska värden, snarare än att vara fundamentalistiskt regelföljande och ”gömma sig” bakom informationssäkerhetsreglerna. Ett sådant förhållningssätt har också stöd i tidigare forskning om paradoxer i organisationer, där det ömsesidiga beroendet mellan olika konflikterande värden framhålls (Johnson, 2014), liksom vikten av att stödja de anställda i att på ett funktionellt sätt hantera

värdekonflikter, snarare än att eliminera dem (Lewis, 2000; Lewis & Smith, 2014). I vår egen tidigare forskning (Skyvell-Nilsson et al., 2018) kunde vi belysa hur läkare och sjuksköterskor baserade sina beslut att agera i situationer där informationssäkerhetskrav stod i konflikt med andra viktiga värden på noggranna överväganden där en rad olika situationsspecifika aspekter beaktades. Dessa aspekter omfattade exempelvis en bedömning av hur akut behovet var att tillfredsställa olika krav, i vad mån värden som inte omedelbart prioriterades kunde säkras långsiktigt genom senare åtgärder, liksom av egen kompetens och kompetensen hos andra personer som var involverade i den aktuella situationen.

Hur organisationen kan stödja personalen att funktionellt balansera konflikterande värden framstår som en viktig fråga att samtala om i den praktiska verksamheten i industriell högriskverksamhet.

10.4 Informationssäkerhetsklimatets betydelse för informationssäkerheten

Informationssäkerhetsklimatet mättes genom de sju dimensionerna i enkätverktyget Information Security Climate Questionnaire (INSECQ) (Pousette & Törner, 2017a): a) Ledningens prioritet av informationssäkerhet (exempelfråga: På den här arbetsplatsen visar ledningen uppskattning om man är noga med informationssäkerheten, även om det innebär att arbetet fördröjs); b) ledningens involvering av medarbetare i informationssäkerhetsarbetet (exempelfråga: Ledningen uppmuntrar medarbetarna att delta i utformningen av informationssäkerhetsbestämmelser.); c) ledningens rättvisa i hantering av avvikelser (exempelfråga: Ledningen söker orsaker i rutiner och system, inte skyldiga personer, när en informationssäkerhetsavvikelse inträffar); d) arbetsgruppens engagemang i informationssäkerhet (exempelfråga: I den här arbetsgruppen tar man gemensamt ansvar för att informationssäkerhets-bestämmelserna upprätthålls); e) arbetsgruppens lärande om informationssäkerhet (exempelfråga: I den här arbetsgruppen lär man av sina erfarenheter för att förebygga informationssäkerhetsavvikelser); f) regellegitimitet i arbetsgruppen (exempelfråga: I den här arbetsgruppen anser man att det bästa sättet att skapa hög informationssäkerhet är genom tydliga informationssäkerhetsbestämmelser); och g) arbetsgruppens hotbild (exempelfråga: I den här arbetsgruppen är man överens om att det finns en verklig hotbild mot våra IT-system).

Tvärsnittsanalyserna visade att informationssäkerhetsklimatet var starkt positivt relaterat till såväl regelföljande som delaktigt informationssäkerhetsbeteende. Ju starkare informationssäkerhetsklimatet var, desto vanligare var båda typerna av informationssäkerhets-beteende. Hade vi endast haft tvärsnittsdata hade en näraliggande slutsats varit att ett bra informationssäkerhetsklimat leder till ett högt

informationssäkerhetsbeteende. När vi analyserar longitudinella data framträder dock en bild som tvingar oss att fundera en vända till över tvärsnittsresultaten Den longitudinella analysen gav inget stöd för att ett högt informationssäkerhetsklimat vid mättillfälle ett ledde till högre informationssäkerhetsbeteende ett år senare. Vi fann heller inte att den kausala ordningen gick i andra riktningen, dvs att beteendet vid tillfälle ett påverkade klimatet vid tillfälle två. Dessa resultat visar på vikten av att inte välja antingen tvärsnittsanalyser eller longitudinella analyser, utan att dessa olika analyser kan komplettera varandra. Utifrån bara longitudinella resultat skulle slutsatsen lätt kunna dras att informationssäkerhetsklimatet inte har någon betydelse för informationssäkerheten. Tvärsnittsanalysen, liksom tidigare resultat från ett representativt nationellt urval svenska tjänstepersoner i olika branscher (Pousette & Törner, 2017a), visar att fenomenen har ett samband. En möjlig förklaring kan förstås även här vara, att båda fenomenen bestäms av en gemensam bakomliggande variabel, som vi inte mätte. Men här kan vi se även en annan möjlig förklaring. Tittar vi återigen på de statistiska stabilitetsanalyserna så finner vi att såväl de två typerna av informationssäkerhetsbeteende som informationssäkerhetsklimatet var måttligt stabilt över tid. Det visar att förändringar skett i alla dessa fenomen över mätperioden på ett år. En rimlig tolkning är att de processer som kopplar klimat och beteende till varandra har kortare tidscykler än ett år. Klimatet kan ha förändrats under året och detta kan ha följts av en ändring i beteendet men denna process kan inte uppfångas med det långa tidsintervallet. För att undersöka detta närmare krävs longitudinell forskning med fler och tätare mätpunkter.

Ett annat intressant resultat rör informationssäkerhetsklimatets roll för relationen mellan informationssäkerhetsbeteende och värdekonflikter i arbetet. Vi konstaterade ju i de longitudinella resultat vi redovisade ovan (kapitel 9.7.2) att anställda som hade en hög grad av regelföljande informationssäkerhetsbeteende generellt sett upplevde färre värdekonflikter med informationssäkerhetskraven i sitt arbete. Vi tolkade detta som att mycket högt regelföljande innebär en slags förenkling när man väljer beteende i situationer då informationssäkerhetskraven står i konflikt med andra organisatoriska värden. Nu fann vi även att informationssäkerhetsklimatet hade en modererande effekt på sambandet mellan regelföljande beteende och värdekonflikter. Detta innebär att bland anställda som upplevde ett högt informationssäkerhetsklimat, det vill säga ett arbetsklimat där informationssäkerheten är högt värderad, var det negativa sambandet mellan regelföljande informationssäkerhetsbeteendet och värdekonflikter svagare än bland anställda där informationssäkerhetsklimatet var lågt. Här är vår tolkning att om säkerhetsklimatet är högt så upplever de som har en hög grad av regelföljande informationssäkerhetsbeteende fler värdekonflikter i sitt arbete än om säkerhetsklimatet på arbetsplatsen är lågt. Det kan alltså vara så att ett högt informationssäkerhetsklimat inte medger den förenkling som vissa informanter beskriver, där vissa anställda ”gömmer sig” bakom informationssäkerhetsreglerna och

prioriterar regelföljande i alla lägen, snarare än att balansera hela spektrat av organisatoriska värden.

11 Framtida forskningsbehov

Tvärsnittsstudierna gav genomgående stöd för de hypoteser vi uppställde om samband mellan olika organisatoriska stöd och hinder å ena sidan och informationssäkerhetsbeteende å den andra. När sådana samband får stöd tolkar man det lätt som ett stöd för en viss antagen kausal ordning. Longitudinella enkätundersökningar inom informationssäkerhetsområdet är synnerligen få och den här studien visade med all tydlighet vikten av att i fortsatt forskning i högre grad fokusera intresse och resurser mot longitudinella studier för att kunna bidra till teoretisk (och därmed praktisk) utveckling inom området. Våra longitudinella resultat visade i några fall på en omvänd kausal ordning mot den som kunnat antas baserat på tidigare tvärsnittsstudier. Kombinationen av starka tvärsnittssamband men avsaknad av longitudinell effekt pekar på att tidsaspekten för vissa förändringsprocesser måste beaktas noga.

Kombinationen av kvantitativa och kvalitativa studier är också en stor styrka i det här projektet och förordas i framtida forskning. De kvantitativa metoderna kan visa på robusta samband (eller avsaknad därav) i större undersökningsgrupper. De kan också användas för att undersöka likheter och skillnader mellan gruppen. De kvalitativa resultaten kan hjälpa till att förklara och fördjupa de kvantitativa resultaten. Kvalitativ metodik kan exempelvis hjälpa till i tolkningen av oklara kvantitativa resultat.

12 Studiens begränsningar

När man studerar känsliga frågor som säkerhetsattityder och säkerhetsbeteende kan resultatens riktighet och fullständighet hotas av att forskningspersonerna inte vågar vara öppna och uppriktiga, dels för att skydda sig själva, men också dels för att skydda känslig information. Detta problem kan dessutom vara extra uttalat när forskningen avser just informationssäkerhet och genomförs i högriskindustri. I samband med intervjuerna diskuterades därför inledningsvis detta noga med informanterna. Såväl enkätrespondenter som intervjupersoner informerades också om studien av såväl forskarna som av företagens ledning innan deltagandet. Deltagarna i intervjuerna valdes ut och kontaktades av företagens säkerhetsavdelningar med en inbjudan att delta. De informerades om att deltagandet var frivilligt och alla valde att delta. Vi klargjorde också att syftet med studien vare sig var att komma åt skyddad information eller att identifiera individer med mindre önskvärt säkerhetsbeteende, utan att belysa organisatoriska fenomen som kunde klargöra vilka förhållanden som understöder

respektive hämmar hög informationssäkerhet. Intervjuledarnas upplevelse var att informanterna fritt och öppet reflekterade kring och besvarade våra frågor. Det klargjordes också för alla forskningspersoner hur data behandlades för att tillförsäkra att inga andra än forskarna hade tillgång till dem, och att resultaten skulle redovisas på ett sätt så att enskilda individer inte kunde identifieras.

En annan begränsning avser urvalet av organisationer. Vi kan inte uttala oss om i vad mån resultaten är relevanta i annan typ av högriskverksamhet än den vi här studerat. Flera av resultaten resonerade väl med tidigare forskning i andra branscher och avseende andra typer av säkerhet, men ytterligare forskning i andra branscher är befogad.

Studien omfattade endast två organisationer inom den aktuella branschen i Sverige, varför fler studier även i andra organisationer och andra länder behövs för att säkra extern validitet och transferabilitet av resultaten. Inom de två deltagande organisationerna gjordes ett totalurval för enkätundersökningen och svarsfrekvensen var god varför vi bedömer att enkätresultaten väl representerar dessa organisationer. Intervjuundersökningen omfattade ett adekvat antal informanter och dessa rekryterades strategiskt för att representera olika arbetsenheter, roller och hierarkiska nivåer i företagen. I rekryteringen eftersträvades också god spridning på olika erfarenhetsgrad och kön. Detta säkrade att vi fick bredd i de olika arbetssituationer som beskrevs och ur olika perspektiv. Användandet av Critical incident metodiken begränsade också påverkan på resultaten av intervjuarnas förförståelse. Validiteten i projektresultaten stärktes genom att vi återrapporterades samtliga resultat till säkerhetsansvariga i de deltagande företagen och resultaten gav genklang i deras erfarenheter.

13 Sammanfattning

Informationstillgångar är centrala för dagens organisationer – inom både den privata och den offentliga sektorn. En organisations hantering av informationssäkerheten kan påverka dess förmåga att följa lagkrav och att hantera risker och konkurrens. Samhällets och dess organisationers integritet och pålitliga funktion förutsätter att beslut baseras på korrekt information. Det kräver att denna information är riktig och fullständig, vilket i sin tur kräver att den är tillgänglig endast för rätt användare vid rätt tillfälle.

Tekniska och administrativa skyddssystem har stor betydelse för att skydda organisationers information, men för att uppnå hög informationssäkerhet kan man inte enbart förlita sig på tekniska och administrativa strukturer. Förmågan att hålla hög informationssäkerhet omfattar även psykologiska och organisatoriska aspekter. Det

finns därför ett stort behov av att förstå hur anställda tänker kring informationssäkerhet och vad som har betydelse för ett informationssäkert förhållningssätt och beteende i arbetet.

Denna rapport fokuserar på projektet Arbetsorganisatoriska och psykosociala faktorers, och sociala processers, betydelse för informationssäkerheten som är ett delprojekt inom forskningsprogrammet Informationssäkerhet i praktiken. Det här aktuella delprojektets syfte var att undersöka betydelsen av arbetets kvantitativa och kognitiva krav, den psykosociala arbetsmiljön och informationssäkerhetsklimatet, för förhållningssätt och informations-säkerhetsbeteende bland anställda som hanterar digitaliserad information i organisationer med central betydelse för samhällets funktion och säkerhet. Ett specifikt fokus låg på att undersöka förekomst av arbetsrelaterade värdekonflikter som involverade informationssäkerhet, samt sådana konflikters relation till de anställdas informationssäkerhetsbeteende.

Projektet genomfördes i två organisationer inom svensk kärnkraftsindustri och omfattade en enkätundersökning med två mätpunkter med ett års intervall, och djupintervjuer med chefer och deras medarbetare.

De kvalitativa resultaten pekade på betydelsen av organisationsstrukturella, sociala och individuella faktorer för en hög grad av såväl regelföljande som delaktigt informationssäkerhetsbeteende bland de anställda. Det handlade framför allt om väl anpassade regler och kunskapsstöd, adekvata interna och externa resurser, en stödjande organisationskultur, god intern och extern koordinering och samarbete, samt individuellt ansvarstagande. Intervjuerna identifierade även fem typer av värdekonflikter med informationssäkerhetskraven, som påverkade de anställdas informationssäkerhetsbeteende. De främsta konfliktområdena var med effektivitet, öppenhet och transparens, kvalitet i arbetet, lärande, samt mellan olika aspekter av informationssäkerhetskraven sinsemellan.

De kvantitativa resultaten visade att en hög förekomst av värdekonflikter som involverade informationssäkerhetskrav minskade det delaktiga informationssäkerhetsbeteendet bland de anställda, medan god tillgång till psykosociala arbetsresurser och höga arbetskrav båda hade en positiv effekt på sådant beteende.

Enkätresultaten visade också att en hög grad av regelföljande informationssäkerhetsbeteende ledde till att man upplevde färre värdekonflikter med informationssäkerhetskraven. När man hade god tillgång till arbetsresurser hade höga arbetskrav även en positiv effekt på regelföljande informationssäkerhetsbeteende.

Vidare fann vi i enkätresultatens tvärsnittsdata att ett högt informationssäkerhetsklimat hade ett starkt positivt samband med båda typerna av informationssäkerhetsbeteende, men något kausalt samband över tid kunde inte konstateras mellan dessa två parametrar, i någondera riktning. Dessa resultat antyder att tidsintervallet på ett år mellan enkätmätningarna kan ha varit för långt för att registrera de kausala processerna i detta fall.

Projektet är ett av mycket få inom informationssäkerhetsområdet med en kombination av kvalitativ och kvantitativ metodik och med en longitudinell design. Detta möjliggör en bättre förståelse för de psykosociala och organisatoriska fenomen och processer som har betydelse för informationssäkerheten, och studien pekar ut nya, viktiga forskningsinriktningar inom detta fält.

Resultaten av delprojektet Arbetsorganisatoriska och psykosociala faktorers betydelse för informationssäkerheten har även presenterats i två vetenskapliga publikationer (Gyllensten, & Törner, 2021; Gyllensten, Pousette, & Törner, 2021), samt i ett artikelmanus (Gyllensten, Törner & Pousette. The impact of psychosocial working conditions on information security behaviour in the nuclear industry).

14 Uppmärksammanden

Projektet finansierades av Myndigheten för samhällsskydd och beredskap (MSB), vilket härmed tacksamt uppmärksammas. Vi vill även framföra vårt tack till Evelina Larsson, teknikkonsult vid Säkerhetsenheten Atea AB för värdefull medverkan i referensgruppen till delprojektet Arbetsorganisatoriska och psykosociala faktorers betydelse för informationssäkerheten.

15 Referenser

Al-Darwish, A. I., & Choe, P. (2019). *A framework of information security integrated with human factors.* Paper presented at the Lecture Notes in Computer Science, HCI for Cybersecurity, Privacy and Trust.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010). *Information security culture: a behaviour compliance conceptual framework*. Paper presented at the 8th Australasian Information Security Conference, Brisbane, Australia.

Antonovsky, A. (1987). *Unraveling the mystery of health*. San Francisco: Jossey-Bass.

Ashenden, D., & Sasse, M. A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security, 39*, 396–405.

Bakker, A. B., & Demerouti, E. (2007). The Job Demand-Resources model: state of the art. *Journal of Managerial Psychology, 22*(3), 309-328.

Beus, J., Payne, S., Bergman, M., & Arthur, W. (2010). Safety climate and injuries: an examination of theoretical and empirical relationships. *Journal of Applied Psychology, 95*(4), 713-727.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*, 77–101.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*, 523-548.

Chang, S. E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107* (3), 438-458.

Christian, M., Bradley, J., Wallace, C., & Burke, M. (2009). Workplace safety: a meta-analysis of the roles of person and situation factors. *Journal of Applied Psychology, 94*(5), 1103-1127.

Chulkov, D. V. (2017). Escalation of commitment and information security: Theories and implications. *Information and Computer Security, 25*, 580–592.

Connolly, L., & Lang, M. (2013). *Information systems security: the role of cultural aspects in organisational settings*. Paper presented at the Workshop on Information Security and Privacy (WISP'13), Milano.

Connolly, P. J. (2000). Security starts from within. *InfoWorld, 22,* 39-40.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems, 31*, 285-318.

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70* (September 2017), 72-94.

da Viega, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computer & Security, 29* (2), 196-207.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56* (February 2016), 63-69.

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers and Security, 63*, 1–13.

ENISA. (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Retrieved from www.enisa.europe.eu website:

Festinger, L. (1964). *Conflict, Decision, and Dissonance*: Stanford University Press, Stanford, California.

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), 327-357.

Grill, M., & Nielsen, K. (2019). Promoting and impeding safety – A qualitative study into direct and indirect safety leadership practices of constructions site managers. *Safety Science, 114*, 148-159.

Grote, G. (2012). Safety management in different high-risk domains – all the same? *Safety Science 21, 93-111., 50*, 1983-1992.

Grote, G. (2015). Promoting safety by increasing uncertainty - Implications for risk management. *Safety Science, 71*, 71-79.

Gyllensten, K., Pousette, A., & Törner, M. (2021).Value conflicts and information security – a mixed-methods study in nuclear power industry. *International Journal of Information and Computer Security*; 30(3), pp. 346-363. https://doi.org/10.1108/ICS-09-2021-0139

Gyllensten, K., & Törner, M. (2021). Prerequisites for information security in a nuclear power industry – the role of organizational and social factors. Organizational Cybersecurity Journal: Practice, Process and People, DOI 10.1108/OCJ-04-2021-0012.

Hallberg, J., Johansson, P., Karlsson, F., Lundberg, F., Lundgren, B., & Törner, M. (Eds.). (2017). *Informationssäkerhet och organisationskultur*. Lund: Studentlitteratur.

Hamer, R., Waterson, P., & Jun, T. (2021). Human factors and nuclear safety since 1970 – a critical review of the past, present and future. *Safety Science 21, . 133*, 93-111.

Harnesk, D., & Lindström, J. (2011). Shaping security behaviour through discipline and agility – implications for information security management. *Information Management & Computer Security, 19* (4), 262-276.

Hooper, V., & Blunt, C. (2019). Factors influencing the information security behaviour of IT employees. *Behaviour and Information Technology, 39*, 862-874.

ISO/IEC. (2013). Information technology Security techniques Code of practice for information security management. http://docplayer.net/668061-Information-technology-security-techniques-code-of-practicefor-information-security-controls.html

Jackson, J. (2017). *Coworker influence upon individual internalization of safety.* Carleton University, Ottawa, Ontario, Ontario.

Johnson, B. (2014). Reflections: A perspective on paradox and its application to modern management. *Journal of Applied Behavioral Science, 50*(2), 206-212.

Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. *Information & Computer Security, 23*(3), 246-285.

Karlsson, M., Denk, T., & Åström, J. (2018). Perceptions of organizational culture and value conflicts in information security management. *Information and Computer Security, 26*(2), 213-229. doi:10.1108/ICS-08-2017-0058

Karlsson, M., Karlsson, F., & Åström, J. (2017). Organisationskulturens påverkan på informationssäkerhetsarbetet. In J. Hallberg, P. Johansson, F. Karlsson, F. Lundberg, B. Lundgren, & M. Törner (Eds.), *Informationssäkerhet och organisationskultur*: Studentlitteratur.

Khatib, R., & Barki, H. (2020). An activity theory approach to information security non-compliance. *Information and Computer Security, 28*, 485-501.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). "Shadow security" as a tool for the learning organization. *Computers and Society, 45*, 29–37.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2007). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14* (1), 24-36.

Lewis, M. (2000). Exploring paradox: toward a more comprehensive guide. *Academy of Management review, 25*(4), 760-776.

Lewis, M., & Smith, W. (2014). Paradox as a metatheoretical perspective: sharpening the focus and widenimg the scope. *Journal of Applied Behavioral Science, 50*(2), 127-149.

Malcolmson, J. (2009). *What is security culture? Does it differ in content from general organisational culture?* Paper presented at the 43rd Annual International Carnahan Conference on Security Technology, 5-8 October, Zurich.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Malcolm Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behaviour, 69*, 151–156.

Neal, A., & Griffin, M. A. (2002). Safety climate and safety behaviour. *Australian Journal of Management, 27*(Special Issue), 67-76.

Ngo, L., Zhou, W., & Warren, M. (2005). *Understanding transition towards information security culture change*. Paper presented at the 3rd Australian Information Security Management Conference, Edith Cowan University, Perth.

Okere, I., van Niekerk, J., & Carroll, M. (2012). *Assessing information security culture: a critical analysis of current approaches*. Paper presented at the ISSA 2012.

Organ, W. D. (1997). Organizational Citizenship Behavior: It's construct clean-up time. *Human Performance, 10*(2), 85-97.

Pejtersen, J. H., Søndergård Kristensen, T., Borg, V., & Bue Bjorner, J. (2010). The second version of the Copenhagen Psychosocial Questionnaire. *Scandinavian Journal of Public Health, 38,* 8-24.

Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology & People, 32* (5), 1262-1275. doi:https://doi.org/10.1108/ITP-06-2018-0261.

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behaviour. *Journal of Homeland Security and Emergency Management, 11*, 489–510.

Pousette, A., & Törner, M. (2017a). Kunskap om informationssäkerhetsklimat ger verktyg för förändring. In J. Hallberg, P. Johansson, F. Karlsson, F. Lundberg, B. Lundgren, & M. Törner (Eds.), *Informationssäkerhet och organisationskultur*. Lund: Studentlitteratur.

Pousette, A., & Törner, M. (2017b). Organisationsklimatets betydelse för informationssäkerhet. In J. Hallberg, P. Johansson, F. Karlsson, F. Lundberg, B. Lundgren, & M. Törner (Eds.), *Informationssäkerhet och säkerhetskultur*. Manuskript: Studentlitteratur.

Schneider, B. (1985). Organizational behaviour. *Annual Review of Psychology, 36*, 573-611.

Schneider, B., González-Roma, V., Ostroff, C., & West, M. A. (2017). Organizational climate and culture: reflections on the history of the construct in JAP. *Journal of Applied Psychology, 102*(3), 468–482. doi:10.1037/ap10000090

Skyvell-Nilsson, M., Pousette, A., & Törner, M. (2018). Professional culture, information security and healthcare quality - physicians' and nurses' perspective on value conflicts in the use of electronic information systems. *Safety in Health, 4*(11). doi:https://doi.org/10.1186/s40886-018-0078-9

Smith, W., & Lewis, M. (2011). Toward a theory of paradox: a dynamic equilibrioummodel of organizing. *Academy of Management review, 36*(2), 381-403.

Sommestad, T. (2018). Work-related groups and information security policy compliance. *Information & Computer Security, 26*(5).

Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security, 20*, 39-46.

Törner, M. (2017). Förklaring av några centrala begrepp. In J. Hallberg, P. Johansson, F. Karlsson, F. Lundberg, B. Lundgren, & M. Törner (Eds.), Informationssäkerhet och organisatonskultur (pp. 20-22). Lund: Studentlitteratur.

Von Solms, B. (2000). Information security – the third wave? *Computers & Security, 19*, 615-620.

Weick, K. (1995). *Sensmaking in organizations*. Thousand Oaks, California, USA: sage.

Wheeler, M. A., Stuss, D. T., & Tulving, E. (1997). Toward a theory of episodic memory: The frontal lobes and autonoetic consciousness. *Psychological Bulletin, 121*(3), 331-354.

Wood, C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security, 1*, 16–17.

Årstad, I., & Aven, T. (2017). Managing major accident risk: Concerns about complacency and complexity in practice. *Safety Science 21, . 91*, 114–121.