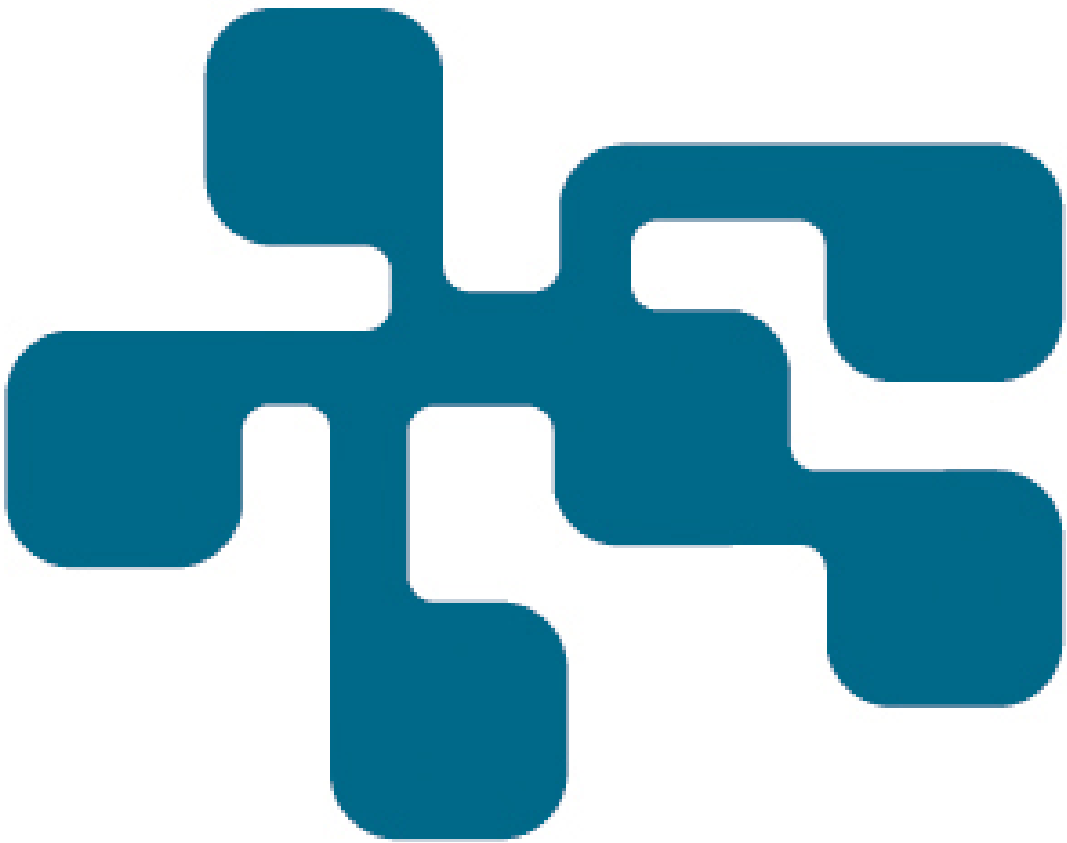
NCS3 - Effekten av kurser inom ICS-säkerhet

En studie av hur organisationers säkerhetsarbete påverkas av kursverksamhet inom området säkerhet i industriella informations- och styrsystem

ANN-SOFIE STENÉRUS DOVER & CAMILLA TRANÉ

FOI
MSB



FOI-R--4433--SE
MSB 2016-2331 Juni 2017
ISSN 1650-1942

Ann-Sofie Stenérus Dover & Camilla Trané

NCS3 – Effekten av kurser inom ICS-säkerhet

En studie av hur organisationers säkerhetsarbete påverkas av kursverksamhet inom området säkerhet i industriella informations- och styrsystem

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet

Titel	Effekten av kurser inom ICS-säkerhet
Title	The effect of awareness raising activities in ICS security
Rapportnr/Report no	FOI-R--4433--SE
Månad/Month	Juni
Utgivningsår/Year	2017
Antal sidor/Pages	64
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	6. Metod- och utredningsstöd
FoT-område	
Projektnr/Project no	E13551
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Genom programmet för ökad säkerhet inom ICS (Industrial Control Systems) arbetar MSB aktivt för att skapa en ökad nationell förmåga att förebygga och hantera IT-relaterade hot mot ICS. I MSB:s vägledningsdokument för området rekommenderas att organisationer regelbundet låter sina medarbetare delta vid utbildningar och övningar inom ICS-säkerhet. MSB finansierar också kurser inom området som NCS3[1] genomför, till vilka viktiga operatörer har möjlighet att skicka personal. Frågan är vilka effekter som utbildning och övning inom ICS i praktiken har. Tidigare kursdeltagare vid de av MSB finansierade NCS3-kurserna beskriver sammantaget flera exempel på att deras deltagande lett till ett förbättrat säkerhetsarbete inom respektive organisation. Även om effekterna till största del ligger på individnivå, som ökad medvetenhet, beskriver också ett antal av studiens respondenter att kurserna bidragit till faktiska förändringar på organisationsnivå, som exempelvis ökad separering av styrsystem från övriga system.

Utbildning som en metod för att öka säkerheten inom ICS, visar studien är en rekommendation som i princip genomgående återfinns i standarder och vägledningsdokument motsvarande den som MSB ger ut. Forskning inom utbildningsområdet bekräftar att deltagande i medvetandehöjande aktiviteter i allmänhet leder till förbättringar i verksamheten. Litteratur saknas dock som visar på hur utbildning och övningar inom ICS påverkar organisationers verksamhet. Rekommendationer om utbildning och övning för ökad säkerhet behöver därför förstås som att de i stort bygger på verksamhetsnära erfarenheter, på vad som har visat sig kunna ha effekt i respektive organisations sammanhang.

Nyckelord: industriella styrsystem, ICS, IT-säkerhet, kurseffekter, standarder

[1] Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet. Ett samarbete mellan MSB och FOI med syfte att bygga upp och sprida kunskap om cybersäkerhetsaspekter inom ICS.

Summary

Through its ICS security programme, the Swedish Civil Contingencies Agency (MSB) is working actively to create greater national capacity in the prevention and management of IT-related threats to ICS. In MSB's guidance document, the agency recommends that training and exercises focused on IT incidents affecting ICS should be held regularly. MSB also finances courses in the area of ICS security, held at NCS3[2], to which critical operators are offered to send their personnel. The question is what effect training and exercises in ICS have in practice. Previous course participants of the MSB financed NCS3-courses describe several examples of how their participation have led to improved security within their respective organisation. Even though most of the effects described are on an individual level, such as increased awareness or behavioural changes related to ICS security, a few of the respondents also describe that participation lead to concrete changes on an organisational level, such as increased separation of control systems from other organisational systems.

Awareness-raising measures as a method to increase security in ICS is a common recommendation in standards and guidance documents like the one MSB publishes. Research within the area confirms that the participation of personnel in awareness-raising measures in general leads to improvements in the operations of organisations. Specifically within the area of ICS there is however a lack of research on how awareness-raising measures affect organisations. Recommendations about awareness-raising measures could therefore generally be understood as being based on experience, on what has shown itself to be functional and useful in the practical activities.

Keywords: industrial control systems, ICS, IT security, course effects, standards

[2] National Centre for increased security in industrial information and control systems in vital societal functions and critical infrastructure. A collaboration between MSB and FOI.

Innehållsförteckning

1 Inledning

Genom programmet för industriella informations- och styrsystem (ICS[3]) arbetar Myndigheten för samhällsskydd och beredskap (MSB) aktivt för att ”*skapa en ökad nationell förmåga att förebygga och hantera IT-relaterade hot mot industriella informations- och styrsystem i samhällsviktiga verksamheter och i kritisk infrastruktur*”[4]. Som ett led i arbetet ger MSB ut ett vägledningsdokument med samlad information om hur organisationer kan öka säkerheten i dessa system[5]. I vägledningen rekommenderas att utbildningar och övningar av IT-incidenter genomförs. Även i andra standarder, rekommendationer och vägledningsdokument framhålls utbildning och övning som viktiga element för att utveckla organisationers säkerhetsarbete [se exempelvis CPNI 2015, DHS 2011, ISO/IEC 2010, NIST 2015, SS-ISO/IEC 2012].

För att stödja organisationer med utbildning har MSB genom NCS3:s[6] försorg sedan 2009 utvecklat kortare, unika, kurser inom området, till vilka viktiga operatörer har möjlighet att skicka personal. De två kurser som i dagsläget ges är SI3S[7], tidigare SIK, och I4S[8], tidigare ICS-CDX, vilka genomförs under två respektive tre och en halv dag i FOI:s lokaler i Linköping. Sammantaget har närmare 400 personer från nästan 100 olika organisationer deltagit vid kursverksamheten vid NCS3 sedan starten. Vissa organisationer är stora internationella företag medan andra är små och huvudsakligen verkar på den svenska marknaden. De flesta organisationer är privata men några tillhör den offentliga sektorn. En del är användare av industriella informations- och styrsystem medan andra är leverantörer av dessa system eller konsulter som arbetar med implementering och säkerhetsfrågor.

SI3S är en grundläggande IT-säkerhetskurs riktad till personer som arbetar med industriella informations- och styrsystem. Kursen varvar föreläsningar och laborationer. Målsättningen är att *”ge deltagarna en grund för att kunna arbeta med säkerhetshöjande åtgärder i IT- och OT[9]-system, samt att de ska få kännedom om verktyg och metoder för att identifiera sårbarheter i industriella informations-*

[3] Industrial Control Systems

[4] Från MSB:s hemsida om programmet, https://www.msb.se/sv/Forebyggande/Informationssakerhet/Stod-inom-informationssakerhet/IndustriSCADA/Nationellt-program/, 170529

[5] Vägledning för ökad säkerhet i industriella informations- och styrsystem [MSB 2014].

[6] Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet. Kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsaspekter inom industriella informations- och styrsystem. NCS3 är ett samarbete mellan Totalförsvarets forskningsinstitut (FOI) och MSB.

[7] Säkerhet i industriella informations- och styrsystem

[8] Praktisk incidenthantering i industriella informations- och styrsystem

[9] Operational Technology, teknisk utrustning som används i driftmiljöer, i motsats till kontorsmiljöer.

och styrsystem." [Lindahl 2016]. SI3S har sedan starten 2009 hållits vid sammantaget 24 tillfällen.

I4S är en IT-tekniskt mer avancerad kurs och riktar sig istället till IT-tekniker med syfte att öka deras processtekniska kunskaper. Jämfört med SI3S är I4S en scenariobaserad kurs. I4S har sedan starten 2014 hållits vid sammantaget fyra tillfällen.

Kurserna SI3S och I4S är båda mycket uppskattade bland deltagarna och får genomgående höga poäng i de utvärderingar som genomförs vid kurstillfällenas avslut[10]. Det har däremot inte gjorts någon uppföljning av vad som händer i organisationerna när kursdeltagarna kommer tillbaka till sin arbetsplats, dvs. hur deltagandet faktiskt påverkar säkerhetsarbetet hemma i organisationen.

Inför kommande utgåvor av MSB:s vägledningsdokument önskar myndigheten samla forskningsrelaterat och empiriskt underlag om hur utbildning och övning praktiskt påverkar säkerhetsarbetet inom olika organisationer. Ett sådant underlag kan användas för att underbygga de rekommendationer som MSB tillhandahåller organisationer och andra intresserade inom området säkerhet inom industriella informations- och styrsystem.

1.1 Syfte och mål

Den här studien syftar till att vidare utveckla MSB:s möjligheter och förmåga att sprida kunskap och ge rekommendationer om säkerhet i industriella informations- och styrsystem i kommande vägledningsdokument. Detta genom att tillhandahålla forskningsbaserad och empiriskt underbyggd kunskap om vad kurser och övningar kan leda till på organisatorisk nivå.

Målet med den här studien är tvådelat:

- Att om möjligt finna en teoretisk och forskningsbaserad grund till rekommendationer om kurser och övningar genom att scanna av forskningsreferenser och rekommendationer relaterade till kurser och övningar, i första hand inom området säkerhet inom industriella informations- och styrsystem, i andra hand inom andra mer eller mindre (tekniskt) relaterade områden.
- Att följa upp och visa på om de kurser som ges vid NCS3 inom området säkerhet i industriella informations- och styrsystem leder till organisatoriska effekter (dvs. om, och i så fall hur, personalens deltagande påverkar säkerhetsarbetet på organisationsnivå för olika aktörer).

[10] SI3S får genomgående omdömen över fem på en sexgradig skala [Lindahl 2016].

1.2 Avgränsningar

För den här studien har avgränsningen varit att fokusera på ett urval organisationer, dels de organisationer som sammantaget skickat många kursdeltagare vid upprepade tillfällen (stora organisationer), dels de organisationer som skickat ett fåtal deltagare vid ett enstaka tillfälle (företrädesvis mindre organisationer). Övriga organisationer som faller däremellan har således avgränsats bort.

Studien har avgränsat bort att undersöka organisationer vars medarbetare inte gått kurser. Avgränsningen innebär att studien inte utvärderat kursers effekt i strikt mening, dvs. att resultat i utfallsled av kursdeltagande jämförs med ett referensalternativ som visar vad utfallet hade blivit utan kursdeltagande.

1.3 Målgrupp

Målgruppen för föreliggande rapport är främst personer som på ett eller annat sätt är involverade i MSB:s program för ökad säkerhet i industriella informations- och styrsystem.

1.4 Begreppsförklaring

Vi beskriver här hur vi i rapporten kommer att använda nedan kursiverade begrepp, väl medvetna om att deras innehåll är föremål för olika synsätt:

Utbildning och *övning* är två aktiviteter som båda bidrar till *kompetensutveckling*. Utbildning kan ske i form av kurser som antingen främst kan vara av mer allmänorienterande karaktär eller mer inriktade mot att utveckla mer specifika kompetenser. Det senare, kursdeltagande för att utveckla mer specifik kunskaper och färdigheter, kallar vi *träning*[11].

Övning drivs av ett scenario. Övningar, skriver MSB, syftar främst till att utveckla förmågor hos organisationer[12]. I de fall där syftet främst är att individer/grupper utvecklar kunskaper och färdigheter genom scenariobaserade aktiviteter har vi i denna rapport dock kallat det för ”övning” eftersom det är i linje med hur studiens respondenter utryckt sig.

Ordet *effekt* är centralt i denna studie. Utvärdering av effekter är allmänt erkänt som svårt [Vedung 2009, s 215], och avgränsningen ovan innebär att studien inte utvärderar kursers effekt i strikt mening. Vi har istället i denna studie valt att se på effekter så som ordet effekt används i dess mer vardagliga betydelse, dvs. att effekt

[11] Fritt översatt från Wikipedia 16-06-03 ”Training is teaching, or developing in oneself or others, any skills and knowledge that relate to specific useful competencies.”

[12] Övning: Aktivitet som omfattar en eller flera aktörer och som främst syftar till att identifiera brister, pröva och/eller utveckla förmågor. (MSB 2014b)

innebär att det finns ett orsakssamband (kausalitet) mellan, för studiens del, kursdeltagande och förändringar i organisationernas säkerhetsarbete. Ordet påverkan kommer i denna rapport användas som en synonym med ordet effekt för att understryka rapportens mer alldagliga användning av ordet effekt.

1.5 Disposition

Efter detta inledande kapitel beskrivs i kapitel 2 våra metodval för genomförandet av studien. I kapitel 3 sammanfattas resultaten av både litteraturstudien och analysen av de organisatoriska effekterna av kursdeltagande vid SI3S och I4S. I bilaga A-D återfinns en fördjupad metodbeskrivning med intervju- och enkätunderlag samt mer utförliga resultatbeskrivningar.

2 Metod

I detta kapitel beskrivs den metod, med en kvalitativ ansats, efter vilken vi har arbetat med att samla in och bearbeta data för att kunna uppfylla målet med studien. Dels beskrivs vår metod för datainsamling, dels det ramverk som vi nyttjat för analys och bearbetning av insamlad data.

2.1 Datainsamling

Tillsammans med uppdragsgivaren kom vi fram till att datainsamlingen skulle ske genom en kombination av en litteraturstudie, intervjuer med personer från de organisationer som skickat sammantaget många deltagare vid flertalet kurstillfällen samt en enkät till de organisationer som skickat ett fåtal deltagare vid ett enstaka kurstillfälle. Valet att inte kontakta samtliga organisationer som skickat kursdeltagare var dels en resursfråga, dels en fråga om att undvika att belasta samtliga organisationer för den här studien. För de organisationer som skickat många deltagare prioriterades att genomföra intervjuer. Hypotesen var att vi med hjälp av intervjuer, med framför allt personer på chefsnivå i dessa organisationer, kunde få en sammantagen bild av uppnådda kurseffekter som representerade en stor mängd kursdeltagare. För de organisationer som skickat ett fåtal deltagare till kurserna valdes enkätutskick som datainsamlingsmetodik, ett mindre resurskrävande tillvägagångssätt som samtidigt bedömdes kunna generera relevant data.

2.1.1 Litteraturstudie av forskningsreferenser, standarder och rekommendationer

Genomgången av forskningsreferenser gjordes inte utifrån ambitionen att vara heltäckande, då studiens inte medgav en sådan allomfattande ansats[13]. Istället genomfördes den, under juli 2016, genom sökningar på internet och genom att via referenslistorna i funna artiklar söka sig vidare till ytterligare artiklar. Sökningen är avgränsad till tillgängliga[14] vetenskapliga artiklar på engelska. Scanningen av forskningsreferenser kopplade till utvecklade kunskaper och färdigheter genom kurser och övningar genomfördes för att i första hand hitta referenser inom området säkerhet inom industriella informations- och styrsystem, i andra hand inom andra mer eller mindre (tekniskt) relaterade områden. Resultaten av genomgången av forskningsartiklar återfinns i Bilaga B.

[13] Strukturerarad forskningslitteratursökning, som Systematic Litterature Review (SLR) [Kitchenham 2004], eller sökning i forskningsdatabaser som Scopus gjordes inte, då detta tillvägagångsätt bedömdes kräva avsevärt mer tid.

[14] Artiklar från forskningstidskrifter som FOI inte har tillgång till har införskaffats.

För att komplettera genomgången av forskningsreferenser genomfördes också en genomgång av 16 befintliga standarder, rekommendationer och vägledningar inom området industriella informations- och styrsystem från engelsk- och svenskspråkiga källor. Genomgången gjordes för att undersöka om och/eller hur dokumenten hanterar frågor relaterat till utbildning/övning och säkerhet samt om de refererar till forskning. Mer om urvalet av de 16 dokumenten återfinns i Bilaga C, som också beskriver resultaten av genomgången.

2.1.2 Intervjuer

Urvalet av personer att intervjua, förutom att de tillhör de organisationer som skickat flest deltagare till kurserna, var att vi ville ha en blandning av 1) chefer inom området med inflytande över kompetensutvecklings- och övningsfrågor, och 2) tidigare kursdeltagare som operativt arbetar med industriella informations- och styrsystem. Intervjuerna genomfördes semistrukturerat där de intervjuade på förhand fick en intervjuguide med frågor utifrån vilka intervjun sedan inriktades. Vi tog fram två olika varianter av intervjuguide, en som riktades mot chefer, och en mot tidigare kursdeltagare. Tre personer valde av tidsskäl att besvara frågorna skriftligt. Intervjuerna genomfördes under perioden augusti-oktober 2016. Frågeunderlaget återfinns i Bilaga A.

Intervjuer genomfördes med sammantaget nio personer, vilket motsvarar representation från sju organisationer. För fem av organisationerna intervjuades personer på chefsnivå.

2.1.3 Enkät

Närmare 70 av de nästan 100 organisationer som skickat deltagare till kursverksamheten vid NCS3 har skickat 1-2 deltagare genom åren. Till tidigare kursdeltagare från 35 av dessa nästan 70 organisationer skickade vi i september 2016 en mailenkät med sammanlagt tre frågor. I Bilaga A återfinns både urvalskriterier för enkätutskicket och enkätfrågorna i sin helhet. I enkäten ombad vi inte mottagarna att ange sin yrkesroll, men utifrån kurslistor och mailsignaturer kunde vi utläsa att de som besvarade enkäten utgjorde en blandning av chefer samt automationsingenjörer och IT-tekniker.

Efter påminnelse inkom sammanlagt tio svar vilket innebär en svarsfrekvens på knappt 30 procent. Vi kan bara spekulera i motiven bakom vilka som valt att besvara enkäten och vilka som valt att avstå. Svaren ger ändå indikationer på organisatorisk påverkan av kursdeltagande även om det är långt ifrån heltäckande.

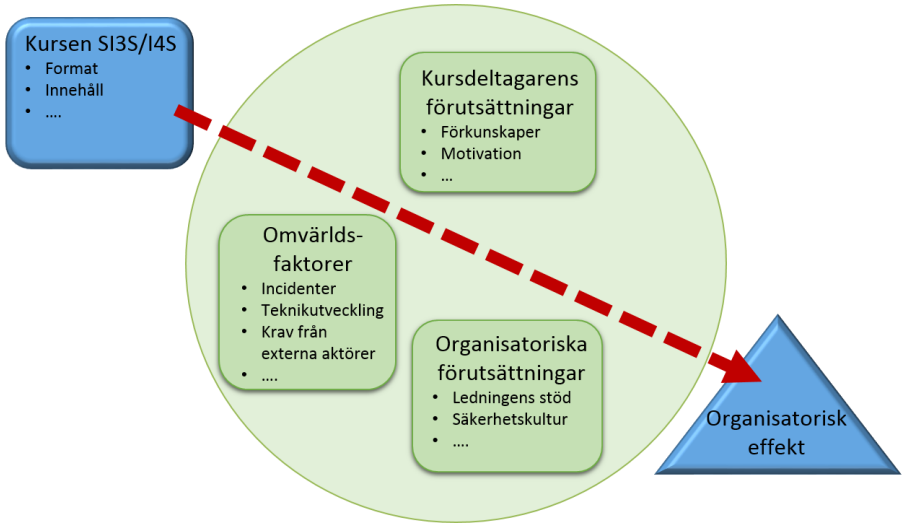
2.2 Ramverk för analys/bearbetning

Det ramverk som presenteras i detta avsnitt har fungerat som stöd i vårt tankearbete och beskriver vårt förhållningssätt till uppgiften och insamlad data. Vad är det vi kan observera? Vad kan vi uttala oss om, och vad har vi inte möjlighet att kontrollera för? Hur kan vi tolka dataunderlaget? Ramverket syftar också till att ge den som tar del av våra resultat ett stöd i att förstå hur vi har förhållit oss till uppgiften.

2.2.1 Påverkan av en kurs på verksamheten

Ett av delmålen med denna studie är att följa upp och visa på om de kurser som ges vid NCS3 inom området säkerhet i industriella informations- och styrsystem leder till organisatoriska effekter. Tillvägagångssättet för studien har varit att låta forna kursdeltagare, och deras chefer, med deras egna ord beskriva den eventuella påverkan som kursdeltagandet haft på deras egen organisation. Resultatet ska därmed tolkas som indicier på hur kursdeltagande kan ha påverkat organisationer.

Att härleda orsak-verkanssamband, påverkan av en enskild kurs på den organisatoriska nivån, är komplext. Vi har inte tagit hänsyn till alla faktorer som kan påverka orsaks-verkanssambandet, som kursen i sig, kursdeltagarens förutsättningar, organisationens förutsättningar och andra externa omvärldsfaktorer. Det innebär att kunskap om vad som ligger till grund för kursdeltagandets eventuella påverkan inte är i fokus för studien. Sannolikt beror den organisatoriska påverkan inte bara på kursen i sig, utan i hög grad även på kursdeltagarnas förutsättningar, organisationernas förutsättningar och andra omvärldsfaktorer, vilket vi illustrerar i Figur 1. Därtill finns det en tidsaspekt innan organisatorisk påverkan kan uppnås.



Figur 1: Vårt ramverk för hur vi ser på den organisatoriska effekten som ett resultat av dels själva kursen och dess innehåll, och dels en uppsättning interna och externa påverkansfaktorer (som kursdeltagarens förutsättningar, organisatoriska förutsättningar och andra omvärldsfaktorer). En analys av vilken explicit roll som dessa påverkansfaktorer haft på den organisatoriska effekten av kursdeltagande har inte inkluderats i studien, även om de högst sannolikt har avsevärd inverkan på effekten. Påverkansfaktorerna är inspirerade av [Robson 2011] och valda för att exemplifiera vad påverkansfaktorer kan vara och ska inte tolkas som de enda eller de viktigaste påverkansfaktorerna.

2.2.2 Nivåer av kurseffekter

I samband med genomgången av forskningsartiklar stod det klart att en ofta använd modell om effektutvärderingsnivåer också i vårt arbete kunde vara meningsfull för att tolka och kategorisera det empiriska resultat som framkom i intervju- och enkätsvaren. Modellen ifråga är den så kallade Kirkpatrickmodellen [Kirkpatrick 1994] som i fyra olika nivåer beskriver vilka olika typer av effekter av kursdeltagande som kan uppnås och utvärderas, se Figur 2. Modellen ger en bild av komplexiteten, och svårigheten, i uppgiften att undersöka de eventuella effekter för verksamheten som kursdeltagande ger.

Figur 2: Illustration av Kirkpatrickmodellens fyra effektutvärderingsnivåer. Nivå 1 handlar om kursdeltagarnas reaktion på kursen, nivå 2 om vad kursdeltagarna lärt sig av kursen, nivå 3 om kursdeltagarnas beteende förändras av kursen och slutligen nivå 4 som handlar om vad kursen har gett för resultat i verksamheten.

Kirkpatrickmodellen innehåller fyra utvärderingsnivåer[15] som handlar om *vad* som uppnåtts, inte *hur* detta uppnåtts:

- Nivå 1 Intryck/reaktion – handlar om vad kursdeltagarna upplevde
- Nivå 2 Lärande – handlar om vad kursdeltagarna lärt sig
- Nivå 3 Beteende/tillämpning – handlar om kursens påverkan på beteenden och arbetssätt hos kursdeltagarna
- Nivå 4 Utfall/resultat – handlar om vad kursen lett till för resultat i verksamheten

Nedan presenteras kortfattat samtliga nivåer för att ge en närmre inblick i hur kurser kan utvärderas. Notera att gränsdragningen mellan de olika nivåerna och de frågor som ställs vid kursutvärdering i någon mån kan skilja sig åt mellan olika källor. Värt att lyfta fram är också att modellen ibland tolkas som att nivåerna logiskt bygger på varandra, bl.a. av Kirkpatrick själv. Denna tolkning innebär att en positiv reaktion (nivå 1) krävs för lärande (nivå 2) osv. Logiken i den tolkningen har ifrågasatts.

Beskrivningen av Kirkpatrickmodellen som följer nedan bygger på [Wilson 2005].

[15] På engelska ”reactions, learning, behavior, and results”.

Nivå 1 – intryck/reaktion

Nivå 1 är det enklaste steget i att utvärdera en kurs och är det som oftast utvärderas. Utvärderingen syftar till att fånga deltagarnas direkta inryck av kursen och kan ställa frågor kring deltagarnas upplevelse av de olika kursmomenten, uppfattningar om allt från kursledarens kunskaper till lokalens lämplighet, och frågor om deltagarna upplevt sig ha lärt sig något. Utvärdering kan ge ett värdefullt underlag för att förändra kursen. Den kursutvärdering som görs i direkt anslutning till SI3S/I4S-kurserna är en nivå 1-kursutvärdering [Se Lindahl 2016 för kursutvärderingsfrågor].

Nivå 2 – lärande

Nivå 2 handlar om att undersöka lärande hos kursdeltagaren t.ex. genom mätning via färdighetstest eller kunskapstest. Till skillnad från nivå 1 görs utvärderingen inte genom att kursdeltagarna själva uppskattar förändringen, utan genom att kunskapsnivån bedöms före respektive efter träningen. Bedömningen efter kan ske i nära anslutning till kursen eller en tid senare. Bedömningsförfarandet kan vara enkelt när det finns färdigheter och kunskaper som är enkla att mäta eller bedöma, exempelvis via ett skriftligt prov om säkerhetsrutiner. Utvärderingen är mer utmanande när det gäller lärande som inte är så påtagligt mätbart, som t.ex. kunskap syftande till riskmedvetenhet eller andra förhållningsätt till säkerhetsarbete.

Nivå 3 – beteende/tillämpning

Nivå 3 handlar om att undersöka om utbildningen gett effekt gällande beteende/tillämpning hos kursdeltagaren och görs en tid efter att kursen genomförts, eller följs upp flera gånger över tid. På nivå 3 handlar utvärderingen om att se om arbetssätt har förändrats, om de lärdomar som kursen gav tillämpas i praktiken. Datainsamlingen kan göras genom observationer på arbetsplatsen och/eller genom att fråga chefer, medarbetare och kunder. Även här kan utvärderingsförfarandet vara enkelt om det finns konkreta mätetal (t.ex. key performance indicators) som t.ex. antal avvikelserapporter kopplat till säkerhetsrutiner före och efter genomförd kurs. Oavsett förekomst av mätmöjligheter eller om utvärderingen förlitar sig på mer kvalitativa data, behöver utvärderingsförfarandet ofta mer nogsamt på nivå 3 beakta om förändringen i individens beteende orsakats av kursdeltagandet eller har andra orsaker.

Nivå 4 – utfall/resultat

Nivå 4 handlar inte längre om enskilda kursdeltagare, utan vad kursen lett till för förändringar, utfall, resultat och åtgärder, i verksamheten. Utvärderingen görs en tid efter att kursen genomförts eller följs upp över tid vid flera tillfällen. Även här kan utvärderingen vara ”lätt” att göra. Dock anses effektutvärderingar på organisatorisk nivå oftast vara mycket utmanande då många faktorer förutom

kursen i sig påverkar resultatet. Utvärderingsresultaten på nivå 4 kommer i praktiken ofta handla om möjliga eller på sin höjd troliga effekter av en kurs.

2.2.3 Bearbetning av data

Vår utgångspunkt har varit att den information som intervju- och enkätrespondenterna har delgivit oss är korrekt. Några av de kursdeltagare som intervjuats eller besvarat enkäten gick SI3S redan 2009. Vi har vid både intervjuer och enkäter varit medvetna om utmaningarna i att återge vad kursdeltagandet har föranlett, speciellt när kursdeltagandet skedde för flera år sedan.

Intervjuerna har inte spelats in och transkriberats. Bedömt relevant innehåll har nedtecknats under intervjun, renskrivits i princip i direkt anslutning till intervjun och innehållet kategoriserats enligt intervjuguiden av den som hade ansvar för att dokumentera intervjun. Därefter har renskrivet intervjumaterial granskats och justerats av den som hade ansvar för att genomföra intervjun. Renskrivna intervjuanteckningar har inte delgivits intervjupersonerna för justeringar. Vi har vid bearbetningen av data sökt efter både mönster och meningsskiljaktigheter. Vi har haft som ambition att i största möjliga utsträckning försöka bibehålla de ord och uttryck om förmedlats till oss i skrift och tal.

Vi har under bearbetningen av materialet från intervjuer och enkäter inte gått vidare och studerat några dokument hos de kontaktade organisationerna som skulle kunna användas för att styrka, alternativt motsäga, den information som tillhandahållits oss. Insamlingen av data från de organisationer som representerats vid NCS3:s kursverksamhet har uteslutande skett muntligt och skriftligt genom intervjuer och enkät.

Kirkpatrickmodellen och dess effektutvärderingsnivåer har vi använt som stöd i tolkningen och kategoriseringen av det empiriska resultat som samlats in genom intervjuer och enkät. Den kursutvärdering som görs i direkt anslutning till SI3S och I4S är en klassisk nivå 1-utvärdering där en del handlar om kursupplägget med lokaler, måltider, kursanmälan och kursmaterialet och en del om deltagarnas upplevelse av kursinnehållet, föreläsningarna, laborationerna och lärarna. Fokus för den här studien ligger dock på vilken påverkan som kursdeltagande har på ett organisatoriskt säkerhetsarbete, vilket motsvaras av nivå 4 i modellen.

3 Sammanfattande resultat

För att stödja organisationer med utbildning har MSB genom NCS3:s försorg sedan 2009 utvecklat kortare unika kurser inom området säkerhet i industriella informations- och styrsystem. Målet för den här studien var att följa upp och visa på om kurserna SI3S och I4S som ges vid NCS3 leder till organisatoriska effekter (dvs. om, och i så fall hur, kursdeltagande påverkar säkerhetsarbetet på organisationsnivå för olika aktörer) samt om möjligt finna forskningsresultat som visar på effekter av kursverksamhet. Ett sådant empiriskt och teoretiskt underlag kan bl.a. användas för att underbygga MSB:s rekommendationer i kommande utgåvor av myndighetens *Vägledning till ökad säkerhet i industriella informations- och styrsystem*.

Studien bygger på data dels från genomförda intervjuer och enkäter med ett mindre urval organisationer vars medarbetare deltagit vid kursverksamheten vid NCS3, dels på forskningslitteratur och standarder/rekommendationer för industriella informations- och styrsystem relaterat till utbildningars och övningars påverkan på säkerhetsarbete.

Effekter av utbildningar kan spänna över ett brett område, från individbaserade effekter, som förvärvade kunskaper och förändrade beteenden, till organisatoriska effekter, som konkreta åtgärder i verksamheten. Om deltagandet i utbildningsverksamhet orsakar effekt på en organisatorisk nivå beror på en rad faktorer, som utbildningstillfället i sig, deltagarens förutsättningar, organisationens förutsättningar och andra omvärldsfaktorer.

Att genom utbildning förvärva kunskaper och färdigheter framhålls genomgående både av studiens respondenter och den undersökta forskningslitteraturen som en väldigt viktig och nödvändig del i arbetet med att stärka säkerheten inom industriella informations- och styrsystem. Studiens empiriska resultat vittnar om att kursverksamheten vid NCS3 har en påverkan, kanske framför allt på individnivå men också på en organisatorisk nivå.

3.1 Vad säger forskning och rekommendationer om betydelsen av utbildning och övning?

Liksom i MSB:s *Vägledning till ökad säkerhet i industriella informations- och styrsystem* framhålls utbildning genomgående i standarder, rekommendationer och vägledningar som en central del för utveckling av organisationers säkerhetsarbete[16]. Perspektivet att människor både är den viktigaste resursen och det potentiellt största hotet mot säkerheten är ett genomgående tema i det som

[16] Se exempelvis CPNI 2015, ISO/IEC 2010, DHS 2011, SS-ISO/IEC 2012 och NIST 2015.

skrivs. Att medarbetarnas kursdeltagande i allmänhet också leder till förbättringar för organisationers verksamhet bekräftas om och om igen av forskningsresultat[17], även om det självklart inte kan tas för givet i enskilda fall. Många faktorer som är viktiga för att kursdeltagandet ska ge ökad effekt lyfts fram inom forskningslitteraturen, men vilka som är mest väsentliga råder ingen samsyn kring.

Specifikt inom området industriella informations- och styrsystem har inga vetenskapliga studier som undersökt effekter på organisatorisk nivå av att låta medarbetare gå kurser påträffats vid genomgången av forskningslitteratur. Avsaknaden av effektutvärderingar innebär bland annat en avsaknad av riktmärke för vad kursverksamheten vid NCS3 kan förväntas uppnå. Inom angränsande områden finns några fall där samband mellan kursdeltagande och effekt på organisationsnivå undersökts kopplat till säkerhet. Exemplen handlar ofta om samband mellan utbildning och arbetsskador.

Avsaknaden av forskningsresultat innebär också att de standarder, rekommendationer och vägledningar som finns i stort behöver förstås som att deras innehåll bygger på erfarenheter, på vad som har visat sig fungerande och nyttigt i den praktiska verksamheten. Kopplat till att visa på vad som är fungerande återfinns i en dryg tredjedel av de studerade dokumenten skrivningar om att följa upp utbildningsinsatser för att undersöka vad de förändrat. När det gäller kompetensutveckling genom metoden övning så lyfts övningsdeltagande fram i mindre utsträckning än kursdeltagande i standarder, rekommendationer och vägledningar.

3.2 Vad visar empirin om de organisatoriska effekterna av kursverksamheten vid NCS3?

Intervju- och enkätsvar bekräftar bilden från de kursutvärderingar som genomförs i samband med kursavslut för SI3S och I4S, det vill säga att kurserna upplevs som omtyckta. De forna kursdeltagarna beskriver att kurserna skapar medvetenhet på ett attraktivt sätt och att det finns en efterfrågan inom organisationerna att delta. Utöver medvetenhet beskrivs kursdeltagandet leda till en upplevd bekräftelse på att området är viktigt, att det ger en teknisk inblick samt fungerar som en ”övergripande väckarklocka”, en ögonöppnare för säkerhetsrisker inom området industriella informations- och styrsystem. Dessa följder har det gemensamt att de beskriver upplevelser eller kunskapsutveckling hos *individer*, något som inte nödvändigtvis behöver leda till effekter inom organisationen. På en något högre nivå beskrivs kursdeltagandet också leda till påverkan på beteenden och arbetssätt hos kursdeltagarna i form av attitydförändringar uttryckt i ett ökat intresse för, och efterfrågan av, information och kompetens kring säkerhetsfrågor. Här har

[17] Se exempelvis Arthur 2003, Tharenou 2007 och Salas 2012.

upplevelser och kunskaper uttryckts i handling, handling som i förlängningen kan bidra till att utveckla säkerheten hos organisationen.

När vi ser till den påverkan på *organisationsnivå* som beskrivs av respondenterna noterar vi en skillnad mellan intervjuer, vilka genomförts med individer från stora organisationer, och enkäter, som företrädesvis besvarats av kursdeltagare från mindre organisationer. Svaren indikerar att kursdeltagande haft praktisk genomslagskraft bland enkätrespondenterna till skillnad mot den påverkan som framkommit i intervjuunderlaget. Enkätsvaren ger exempel på efterverkningar på organisatorisk nivå av SI3S, som att geografiskt skilja på huvudsystem och backupsystem, att göra en analys av sin sårbarhet med särskild uppmärksamhet på driftstödsystem eller ökad separering av styrsystem från övriga servrar. Svaren är samtidigt också tydliga med att de bakomliggande orsakerna inte enbart kan isoleras till kursdeltagande, utan att händelseförloppet efter kursdeltagandet i stor utsträckning också beror på andra faktorer. Kurspåverkan beskrivs i intervjuerna istället i mer generella termer kopplade till lägre effektnivåer, som ökad medvetenhet och attitydförändringar. Flera av respondenterna från stora organisationer uttrycker dock att kursen bidragit med att uppdatera deras kunskaper, samtidigt som flera också uttrycker att deras motiv för kursdeltagande var att sondera vad kursen handlade om snarare än att inhämta ny kunskap.

Från intervjusvaren ges en bild av skillnader organisationerna emellan i hur de arbetar med utbildningar och övningar inom området industriella informations- och styrsystem, från strukturerade utbildningsprogram till mer ad hoc-lösningar eller individstyrda lösningar. Det betyder också att motiven bland kursdeltagarna för att medverka vid en av NCS3:s kurser spretar. I en del fall har det skett på uppmaning av chefen, i andra att det skett efter eget val att söka upp utbildningstillfället för sin egen kompetensutveckling alternativt som utbildare för att se hur FOI/MSB håller kurser. Samtidigt är det få av de intervjuade som uttrycker vad kursdeltagande kan förväntas leda till för den egna organisationen.

Både intervju- och enkätrespondenterna vittnar om att medvetenheten om risker och säkerhetsaspekter kopplade till industriella informations- och styrsystem generellt har förändrats de senaste åren, både bland medarbetare, på chefsnivå inom organisationerna och i samhället som helhet. Ökad medierapportering om inträffade händelser beskrivs som en av orsakerna. Även om medvetenheten ökat så anses det fortfarande finnas ett glapp mellan nuvarande och önskvärd kunskapsnivå, en utsaga som motiveras av att funktionella krav ofta prioriteras framför säkerhetskrav. Samtidigt lyfts avsaknaden av kunskapsunderlag som visar det ekonomiska värdet av säkerhetsrelaterade investeringar. I det avseendet lyfts krav från externa aktörer fram som en viktig faktor för förändringsbeslut, vilket i förlängningen innebär att kompetensnivån hos kravställande funktioner och organisationer är central.

4 Referenser

Abrahamson Löfström, C. & Larsen, T. (2013), Hållbara strukturer för organisatoriskt lärande organisatoriskt lärande Slutrapport för GRo-projektet, FoU i Väst/GR Göteborgsregionens kommunalförbund, Februari 2013 Tryckeri: Sandstens, Göteborg, ISBN: 978-91-89558-77-9

Alliger, G.M., Scott I., Tannenbaum, S.I., Bennett Jr, W., Traver, H. & Shotland, A. (1997), Personnel Psychology, Volume 50, Issue 2 June 1997 Pages 341–358

Arthur, W., Bennett, W., Edens, P.S. & Bell, S.T. (2003), 'Effectiveness of training in organizations: a meta-analysis of design and evaluation features', Journal of Applied Psychology, 88, 234–45

Blume, B.D., Ford, J.K., Baldwin, T.T. & Huang, J.L. (2010), Transfer of training: a meta-analytic review, Journal of Management, 39, 1065–105

Cheng, E.W.L. & Hampson, I. (2008), Transfer of training: a review and new insights, International Journal of Management Reviews, 10, 327–41

Cohen, A. & Colligan, M.J. (1998), Assessing Occupational Safety and Health Training A Literature Review, June 1998, DHHS (NIOSH) Publication No. 98-145

Dong X., Entzel, P., Men, Y., Chowdhury, R. & Schneider S. (2004) Effects of safety and health training on work-related injury among construction laborers. J Occup Environ Med. 2004 Dec;46(12):1222-8

FHS 2016 på internet 16-06-30 Effektutvärdering UGL och UL
http://www.fhs.se/sv/utbildning/uppdragsutbildningar/ledarskap/ugl/ugl/

Grossman, R. & Salas, E. (2011), The transfer of training: what really matters, International Journal of Training and Development, Volume 15, Issue 2 June 2011 Pages 103–120

HP/ Ponemon Institute, (2010), Security Effectiveness Framework Study, Ponemon Institute sponsored by HP Information Security and Check Point Software Technologies Ltd, July 2010

Kinn, S., Khuder, S.A., Bisesi, M.S. & Woolley, S. (2000), Evaluation of safety orientation and training programs for reducing injuries in the plumbing and pipefitting industry. J Occup Environ Med. 2000 Dec;42(12):1142-7

Kirkpatrick, D.L. (1994), Evaluating Training Programs: The Four Levels. San Francisco, CA: Berrett-Koehler.

Kitchenham, B. (2004), Procedures for Performing Systematic Reviews, NICTA Technical Report 0400011T.1

Lindahl, D. (2016), Grundläggande kurs Säkerhet i industriella informations- och styrsystem, FOI Memo 5632

MSB (2012), Att lära stort från små incidenter: en handling med fokus på att utvärdera effektiviteten i lärandet MSB430 - juli 2012

MSB (2014), Vägledning till ökad säkerhet i industriella informations och styrsystem MSB718 - juli 2014

MSB (2014b), Övningsvägledning Grundbok, MSB602 - aug 2014

Reid, B (2004), A critical analysis of evaluation practice: the Kirkpatrick model and the principle of beneficence Evaluation and Program Planning 27 (2004), 341–347

Robson, L., Stephenson, C., Schulte, P., Amick, B., Chan S., Bielecky A., Wang, A., Heidotting, T., Irvin, E., Eggerth, D., Peters, R., Clarke, J., Cullen, K., Boldt, L., Rotunda, C. & Grubb, P. (2010), A systematic review of the effectiveness of training & education for the protection of workers. Toronto: Institute for Work & Health. Cincinnati: National Institute for Occupational Safety and Health

Sokas, R.K., Jorgensen, E., Nickels, L., Gao, E. & Gittleman, J.L. (2009), An Intervention Effectiveness Study of Hazard Awareness Training in the Construction Building Trades Public Health Reports / 2009 Supplement 1 / Volume 124

Salas, E., Tannenbaum, S.I., Kraiger, K. & Smith-Jentsch, K.A. (2012), The Science of Training and Development in Organizations: What Matters in Practice Psychological Science in the Public Interest 13(2), 2012, 74–101

Tharenou, P., Saksb, A.M. & Moorec, C. (2007) A review and critique of research on training and organizational-level outcomes Human Resource Management Review Volume 17, Issue 3, September 2007, Pages 251–273

Vedung, E. (2009) Utvärdering i politik och förvaltning.

Vignolia, M., Punnettb, L. & Depoloa Vignoli, M. (2014) How to Measure Safety Training Effectiveness? Towards a More Reliable Model to Overcome Evaluation Issues in Safety Training, Chemical Engineering Transactions Vol. 36, 2014

Wilson, D. (2004), Internet 16-02-28
http://research.elearnity.com/A555F3/research/research.nsf/1645538ed5011e3680256ac500571ff2/eac5d5b9518406bf80257037005feca3/$FILE/Measuring%20the%20effectiveness%20of%20Training.pdf

Wilson, J.P. (2005), Human Resource Development: Learning & Training for Individuals & Organizations Kogan Page Publishers, 2005

Standarder, rekommendationer och vägledningar

BSI (2012), Recommendations for security-related trainings, Bundesamt für Sicherheit in der Informationstechnik, 2012

CPNI (2008), Good Practice Guide Process Control and SCADA Security, Centre for the Protection of National Infrastructure (CPNI), Storbritannien 2008, http://www.cpni.gov.uk/documents/publications/2008/2008031-gpg_scada_security_good_practice.pdf

CPNI (2015), Security for industrial control systems - improve awareness and skills - a good practice guide, Centre for the Protection of National Infrastructure (CPNI), Storbritannien, Maj 2015, https://www.cpni.gov.uk/Documents/Publications/2015/12-May-2015-4.%20Improve%20Awareness%20and%20Skills%20Final%20v1.0.pdf

DHS (2009), Cyber Security Procurement Language for Control Systems, Idaho National Laboratory and Department of Homeland Security (USA), 2009, https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

DHS (2011), Catalog of control systems security: Recommendations for Standards Developers, Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT. April 2011, https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf

DOE (2002), 21 Steps to Improve Cyber Security of SCADA Networks, Department of Energy (DOE), USA, September 2002, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

ENISA (2011), Protecting Industrial Control Systems Recommendations for Europe and Member States, Deliverable – 2011-12-09, https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

IAEA (2011), Nuclear security series #17 (Computer Security at Nuclear Facilities), International atomic energy agency, 2011, http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf

ISO/IEC 2005 62264 (ANSI/ISA-95) — Manufacturing Enterprise Systems Standards and User Resources, International Electrotechnical Commission (IEC), 2005–2012 beroende på dokument

ISO/IEC 62443-2-1 (ISA-99) — Industrial Communication Networks — Network and system security International Electrotechnical Commission (IEC), 2010

ISO/IEC Draft ISA 62443-2-1 (f.d. ISA-99) — Industrial Communication Networks — Network and system security, International Electrotechnical

Commission (IEC), Draft version, 2016, http://isa99.isa.org/Public/Documents/ISA-62443-2-1-WD.pdf

NERC 2014, CIP-002-4 till 009-4, StandardNorth American Electric Reliability Council (NERC), USA, Version 4, 2011-01-24, www.nerc.com

NIST (2015), SP 800-82 — Guide to Industrial Control Systems (ICS) Security, National Institute for Standards and Technology (NIST), USA, Revision 2 – maj 2015, http://dx.doi.org/10.6028/NIST.SP.800-82r2

OLF (2009), Information security baseline requirements for process control, safety and support ICT systems, Oljeindustrins Landsförening (OLF), Norwegian Oil and Gas Association, Norge 2009, Revision no: 05
https://www.norskoljeoggass.no/Global/Retningslinjer/Integrerte%20operasjoner/104%20-%20Recommended%20guidelines%20for%20information%20security%20baseline%20requirements%20for%20process%20control%20safety%20and%20support%20ICT%20systems.pdf

PSC (2012), Industrial Control System (ICS) Cyber Security: Recommended Best Practices Number: TR12-002, Public Safety Canada, December 2012
http://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-en.aspx

SS-ISO/IEC 27000-serien - 27002 (kap 7.2.2), Swedish standard institute, Sverige. Feb 2014

SS-ISO/IEC 27000-serien – 27035 Standard, Swedish standard institute, Sverige. Mar 2012

TNO (2015), Eric Luiijf, Bert Jante Paske, Cyber Security of Industrial Control Systems - Good Practices, 2015,
https://www.thehaguesecuritydelta.com/media/com_hsd/report/39/document/Cyber-Security-of-Industrial-Control-Systems-GCCS2015.pdf

Bilaga A Metod – intervjuer och enkät

A.1 Intervjuguide

Intervjuguiden som vi utformade bestod av ett antal semistrukturerade intervjufrågor och fungerade som en översikt över vilka ämnen och frågor vi tänkte behandla under intervjun. Intervjuguiden utformades primärt utifrån våra frågeställningar om hur man ser på kurser och övningar och arbetar med detta inom organisationer. Samtalet inleddes med bredare frågor om den intervjuades roll och organisation för att sedan smalna av med mer fokuserade frågor.

Intervjuguide för kursdeltagare

1. Hur arbetar ni med utbildning och övningar vid din arbetsplats inom området industriella informations- och styrsystem?
2. Hur kom det sig att du gick kursen SI3S/I4S i Linköping? Var t.ex. initiativet ditt eller var kursen en del av ett obligatoriskt utbildningspaket?
3. Vad tycker du att kursen SI3S/I4S gav dig?
4. Efter att du hade gått kursen SI3S/I4S tänkte du kring något ”Det här borde vi förändra hos oss”?
5. Finns det något med kursen SI3S/I4S som kan utformas annorlunda för att skapa bättre förutsättningar att påverka arbetet med säkerhet på din arbetsplats?
6. Vilka andra utbildningar och övningar kopplat till säkerhet i industriella informations- och styrsystem har du deltagit i? Vad bidrar i så fall dessa med för det interna säkerhetsarbetet?
7. Vilka externa faktorer ser du som viktigast för utvecklingen av säkerhetsarbetet vid din arbetsplats? (som exempelvis incidenter, förändrad hot- och riskbild, teknikutveckling, förändrade krav från externa aktörer, samverkan med tjänsteleverantörer eller kompetenshöjande insatser som utbildningar och övningar)

Intervjuguide för chefer

1. Hur arbetar ni med utbildning och övningar vid din arbetsplats inom området industriella informations- och styrsystem?
2. Vad ser du för nytta med utbildningar och övningar inom området industriella informations- och styrsystem? (Varför är det viktigt? / Är det viktigt?)
3. Ingår kursen SI3S/I4S i Linköping i ett utbildningspaket för anställda vid din arbetsplats?

4. De erfarenheter som medarbetare tog med sig från kursen (SIS3/I4S) har de påverkat (förändrat eller upprätthållit) det interna säkerhetsarbetet på något sätt?
5. Tycker du att *antalet* kursdeltagare från en och samma organisation spelar roll för vilken påverkan som det har på det interna säkerhetsarbetet? (gäller både i de fall som flera medarbetare deltar vid ett och samma kurstillfälle eller om organisationen skickar ett mindre antal medarbetare men kontinuerligt över tid)
6. Vilka andra utbildningar och övningar kopplat till säkerhet i industriella informations- och styrsystem deltar din organisation i? Vad bidrar i så fall dessa med för det interna säkerhetsarbetet?
7. Vilka externa faktorer ser du som viktigast för utvecklingen av säkerhetsarbetet vid din arbetsplats? (som exempelvis incidenter, förändrad hot- och riskbild, teknikutveckling, förändrade krav från externa aktörer, samverkan med tjänsteleverantörer eller kompetenshöjande insatser som utbildningar och övningar)
8. Ser du att det stöd som MSB erbjuder i form av utbildning kan vidareutvecklas/förändras för att ännu bättre möta de behov som du ser finns för 1) din arbetsplats samt 2) området säkerhet industriella informations- och styrsystem i stort?
9. I MSB:s *Vägledning för ökad säkerhet i industriella informations- och styrsystem* beskrivs rekommendation 15 ”*Genomför utbildning och övning av it-incidenter i industriella informations- och styrsystem*”. I denna rekommendation ges fem riktmärken för säkerhetsarbetet (se nedan). Tycker du att dessa riktmärken är de mest relevanta kopplat till utbildning och övning, eller kan/bör dessa förändras på något sätt?

A.2 Urval för mailutskick

Aktuella för mailutskick var samtliga organisationer där en till två medarbetare deltagit vid kursen. 68 organisationer har skickat 1-2 medarbetare till kursen sedan kursstarten 2009. 29 aktörer har skickat tre eller flera medarbetare till kursen.

Kursdeltagande under 2016 (slutet på maj) bedömdes ligga alltför nära i tiden, varvid de 12 aktörer som skickat kursdeltagare enkom under 2016 valdes bort. Ett antal medarbetares mailadresser var i deltagarlistan noterade som inte giltiga vid tidigare utskick till kursdeltagarna (2015-04-29), dessa valdes också bort, vilket föranledda att 47 aktörer kvarstod. Från dessa valde vi bort organisationer som vi bedömde mindre intressanta då deras verksamhet inte involverar praktiskt arbete med industriella informations- och styrsystem (såsom myndigheter) eller aktörer med en eller ett fåtal medarbetare. Efter detta urval kvarstod 36 organisationer som vi antingen kategoriserade som användare, leverantörer eller konsulter. En aktör,

som var belastade med frågor i andra projekt inom området, togs bort från urvalet efter diskussion med uppdragsgivaren. Till de 35 organisationer som kvarstod skickades ett mailutskick till en av medarbetarna som gått kursen. Påminnelse om svar skickades tre veckor senare.

A.3 Frågor för mailutskick

Följande frågor mailades ut till ett urval av kursdeltagare via den e-post adress som fanns i kursens deltagarlista. Totalt gick utskicket till 35 kursdeltagare varav 23 användare, 8 konsulter samt 4 leverantörer. Av dessa visade sig sju mailadresser inte vara funktionella (5 användare, 1 konsult, 1 leverantör). Totalt inkom 10 enkätsvar, vilket vi anser är en för låg siffra för att analysera data utifrån kategorierna användare, konsulter och leverantörer.

Frågor: (Du kan skriva dina svar direkt i mailet)

Har ditt kursdeltagande påverkat ert arbete med säkerhet på din arbetsplats? Om ja, beskriv gärna på vilket sätt och varför. Om nej, beskriv gärna varför. För exempel på områden som kan påverkas (anläggning och utrustning, personal och procedurer) se nedan punkter**.** **Svar:**
Finns det något med kursen som kan utformas annorlunda för att skapa bättre förutsättningar att påverka arbetet med säkerhet på din arbetsplats? Om ja, beskriv vad. **Svar:**
Vilka externa faktorer ser du som viktigast för utvecklingen av säkerhetsarbetet vid din arbetsplats? (som exempelvis incidenter, förändrad hot- och riskbild, teknikutveckling, förändrade krav från externa aktörer, samverkan med tjänsteleverantörer eller kompetenshöjande insatser som utbildningar eller övningar). **Svar:**

Områden från MSB:s Att lära stort från små incidenter (2012).

Anläggning och utrustning (inklusive teknisk dokumentation)

- Grundläggande designspecifikationer och konstruktionsstandarder
- Verksamhets-/processbeskrivning
- Hård- och mjukvara
- Annan anläggningsutrustning

Personal

- System för ansvar och befogenheter (befattningsbeskrivningar, delegeringshandlingar mm.)
- Utbildningsprogram/-material
- Kompetens hos personal på alla nivåer

Procedurer

- Ledningssystem
- Instruktioner för drift och underhåll eller motsvarande
- Program för förebyggande underhåll, inspektion med tillhörande arkiv
- Loggar och loggböcker
- Incidenthantering
- Upphandling

Bilaga B Forskningsreferenser om kurseffekter

I denna bilaga redovisas en sammanställning av den genomgång av forskningslitteratur som genomförts inom studien. Litteraturgenomgången gav både en förförståelse för utmaningarna i att göra en effektuppföljning och kunskap som vi tog med oss vid genomförandet av datainsamlingsfasen och vid sammanställning av resultaten. Notera att genom hela Bilaga B används termen ”effekt” i den vetenskapligt strikta meningen, dvs. att resultat i utfallsled av kursdeltagande jämförs med ett referensalternativ som visar vad utfallet hade blivit utan kursdeltagande.

B.1 Forskning för generaliserbara resultat om kurseffekter

Vad visar egentligen forskningen att kurser i allmänhet har för effekt på verksamheter, dvs. vad visar effektutvärderingar av nivå 4 i Kirkpatrickmodellen (se Kapitel 2 Metod)? Till att börja med framstår forskningsresultaten som eniga i att kurser sammantaget ger effekt, både på nivå 1, 2, 3 och 4. [Arthur 2003, Salas 2012]. Forskningsresultaten är dock spretiga när det gäller t.ex. 1) vilka studier som anses vara tillräckligt kvalificerade för att underbygga generella resultat kring kursers effekter, särskilt på nivå 4, och 2) omfattningen av kursers effekter [Arthur 2003, Blume 2010, Burke 2006, Cheng 2008, Robson 2010, Tharenou 2007].

Effektmätningar av enskilda interventioners (kursers) effekter är självklart inte tillräckligt för att göra generaliserbara utsagor om kursers effekt i allmänhet. För att uttala sig generellt om kursers effekt krävs populationsdata som visar på signifikanta skillnader. En komplikation i analysen av populationsdata är att effekter i olika studier inte enkelt kan kategoriseras t.ex. som nivå 1-4-effekter, utan ofta går på tvären igenom flera nivåer och även fokuserar på olika mer specifika delar inom nivåerna. En annan komplikation som försvårar jämförbarheten mellan kursutvärderingar är att kursverksamheter, det vill säga ingångsvärdena i utvärderingarna, i sig är heterogena. I det här sammanhanget lyfts t.ex. begreppet träning i distinktion till mer allmänorienterande utbildning fram och att det inte finns en enhetlig uppfattning om vad skillnaderna mellan dem är [Robson 2010]. I engelskspråkig litteratur är träning ett eget begrepp som inte är synonymt med mer allmän utbildning[18]. Vi har valt att avgränsa denna genomgång

[18] Som ett exempel på hur begreppet ”training” används på olika sätt i standarder om IT-säkerhet i industriella informations- och styrsystem så beskrivs det som att ”Training should be in two phases: 1) general training for all personnel and 2) role-based training aimed at specific duties and

kring effektutvärdering till forskningslitteratur om träning snarare än allmän utbildning. Detta innebär att mer generell utbildning som ofta syftar till att höja ”awareness”, dvs. medvetenhet, inte är i fokus för scanningen. Vi valde att fokusera på träning framför mer generell utbildning utifrån vårt antagande att effekten av träning skulle vara enklare att studera eller ”mäta” i termer av organisatoriska förändringar. SI3S/I4S-kurserna har vi tolkat som att de har inslag både av att vara en mer allmän utbildning med mål att bidra till generell förståelse, men att kurserna även rymmer inslag som betraktas som träning, inslag syftandes till att förvärva mer specifika kompetenser som kan nyttjas i verksamheten.

Som en förutsättning för genomgången av forskningslitteraturen finns alltså komplikationerna med brokiga ingångsvärden, där vi valt att fokusera på kurser av träningskaraktär, och utfall som rör effekter alltifrån nivå 1 till nivå 4, samtidigt som många faktorer kan påverka sambandet mellan ingångsvärden och utfall. En reviewartikel som spänner över området påpekade också att inkonsekventa och oväntade fynd ofta har gjort forskare och utbildningspraktiker besvikna trots att intresset för forskning inom träningsområdet spridits under de senaste decennierna [Cheng 2008]. En annan, ännu nyare, artikel beskriver forskningsfältet som att det har förblivit präglat av blandade fynd och brist på empirisk syntes [Blume 2010].

Samtidigt har många vetenskapliga försök gjorts för att statistiskt säkerställa vilken effekt kurser har. I en ofta citerad metaanalys av 165 vetenskapliga publiceringar visar resultaten på positiva effekter oavsett om effekterna av träningen mäts på nivå 1, 2, 3 eller 4 [Arthur 2003]. Artikeln visar också på att i studier som samtidigt tittar på effekter på olika nivåer, t.ex. där nivå 2 jämförs med nivå 3 och/eller nivå 4, där sjunker i allmänhet effekten substantiellt vid en jämförelse mellan nivå 2 och nivå 3-4. Artikelförfattarna framför som hypotes att detta kan bero på miljön där de nyvunna lärdomarna ska manifesteras i verksamheten.

Forskningsartikeln undersöker också när i tid effekterna mäts. Nivå 1, upplevelse, mäts direkt efter kursen. Nivå 2, lärande, studeras i snitt efter 26 dagar efter kursen. Nivå 3, beteende, efter 134 dagar efter och nivå 4, resultat för verksamheten, efter 159 dagar [Arthur 2003].

I en annan metaanalys av 67 studier som fokuserar specifikt på effekter på nivå 4 visar resultaten att träning har effekt på uppfyllnadsgraden av organisationens mål, men i metaanalysen skrivs däremot att träning inte verkar vara relaterad till det finansiella resultatet [Tharenou 2007]. Att notera är dock att det endast är 18 av de 67 studierna som har använts som underlag för metastudiens resultat kopplat till ekonomi och att enskilda studier visar på att träning ger effekt på det ekonomiska utfallet. Utan att dra för stora växlar av metastudiens resultat i sig, kan det noteras att det inom nivå 4 kan finnas olika ”nivåer”. Detta har också föreslagit ett tillägg

responsibilities.” [ISO/IEC 2010] medan det i en senare utkastversion av dokumentet istället för att fokus ligger på ”training” istället skrivs om ”education and training” [ISO/IEC 2016].

till Kirkpatrickmodellen som generellt attribueras till Hamblin (1974) som skrev om en femte nivå, ”the ultimate level”, som handlar om avkastning på investering.

Forskningen om effekter av träning framstår i huvudsak röra sig inom två områden, som ofta går in i varandra. Dels spåret som ägnar sig åt om träningen får effekt, utan att ställa frågan om vad i processen som medierade eller hindrade detta, och dels spåret som ägnar sig åt orsak-verkan-samband mellan hur träningen bedrivs, hur individen lär sig och hur organisationen lär sig [Robson 2010]. Det senare, dvs. vilka faktorer som är viktigast för att nå effekt, kommer inte beröras mer än på ytan i den här studien. De två artiklarna nedan, som handlar om forskningsstudier inom skyddsområdet[19], berör dock både om och hur kurser ger effekt på organisatorisk nivå.

I en forskningsartikel, som bygger på 95 enskilda studier, undersöks skyddsfrågor ur perspektivet hur utformningen av träning ger effekt kopplat till incidenter, skador och sjukdom på arbetsplatsen (nivå 4), samt även hur träning påverkar nivå 2 och 3 [Burke 2006]. Studien utgår alltså ifrån att träning generellt, på alla nivåer, ger effekt. Resultaten visar att effekten av träningen generellt är beroende av i vilken utsträckning den involverar kursdeltagarna, varvid slutsatsen är att utformningen av träningen är en viktig faktor för vilken effekt den får. Slutsatsen är dock mindre väl underbyggd för nivå 4 och anledningen till detta är att antalet nivå 4-utvärderingar inte är tillräckligt omfattande.

En liknande metaanalys inom arbetsmiljöskyddsområdet har gjorts av forskningsinstitut i USA och Kanada[20], som samlats kring att göra en systematisk genomgång av de mest rigoröst designade studierna av enskilda effektutvärderingar under 1996-2005 [Robson 2010]. Metaanalysen tog också sitt avstamp i ett ofta citerat liknande arbete från 1998 som bl.a. lyfte fram ledningens stöd som en viktig faktor i att nå effekt med träning inom säkerhetsområdet [Cohen 1998]. Utifrån studiens databassökning, som gav 7 892 kandidater, kvarstod endast 14 artiklar som mötte kriteriet att vara tillräckligt rigoröst designade (dvs. inte bara kollegialt bedömda artiklar som i t.ex. Arthur 2003 and Burke 2006, vilket i sig är en hög tröskel). Detta ger en fingervisningen om utmaningen i att designa rigorösa effektutvärderingar, oavsett om de är på nivå 2, 3 eller 4. De återstående 14 artiklarna handlar om alltifrån brandskyddsutbildning, till ergonomi, till skydd mot blodburna patogener. Studiens analys av de kvarstående artiklarna visar att träning har en positiv påverkan på beteende hos de som genomgått träningen (vilket, vår

[19] Notera att vi i nedan stycken skiljer på begreppen skydd och säkerhet. Skydd (safety) ses som vidtagandet av förbyggande åtgärder för att undvika olyckor, vilket i USA ofta associeras med Occupational Safety and Health och handlar om arbetsmiljöfrågor. Säkerhet (security) ses som vidtagandet av förbyggande åtgärder för att undvika incidenter, vilka avsiktligt genomförs av individer, vilket i USA ofta associeras med Department of Homeland Security. I Sverige har MSB ansvar för delar inom både skydd och säkerhet.

[20] National Institute for Occupational Safety and Health (NIOSH) i USA och Institute for Work & Health (IWH) i Canada.

tolkning, motsvarar nivå 3). Kvalitén på grundmaterialet medger, enligt studien, inte mer långtgående slutsatser än så.

I den senaste större studie om träning för utvecklad säkerhet (dock inom arbetsmiljöskyddsområdet) som vi hittat medger grundmaterialet alltså inga generaliserande slutsatser om träningens effekt på säkerheten inom organisationers verksamhet (nivå 4) eller slutsatser om vilka träningsmetoder som är mest effektiva. Studien menar att fortsatt arbete kring vilken effekt träning ger behövs för att identifiera de viktigaste variablerna som påverkar lärandeprocessen. Vanligtvis, skriver studien, påverkar förutsättningarna på arbetsplatsen, som ledningens engagemang, resurser, organisationens säkerhetsklimat, systematisk övervakning och återkoppling, kursdeltagarnas möjlighet att praktisera kursens innehåll, effekten av träning [Robson 2010]. Likaså påverkar kursdeltagarnas försättningar. Dessutom, som Burke (2003) skriver, visade sig träningens utformning påverka dess effekt. Till detta tillkommer att vare sig kursdeltagare eller organisationen lever i ett vakuum, utan även influeras av omvärldsfaktorer. Studien formulerar också det som framstår som det rådande paradigmet kring vilka faktorer som egentligen är viktigast för att nå effekt med träning – de kan variera med situationen [Robson 2010].

B.2 Forskning om organisatoriska effekter av enstaka kurser

Som vi såg i ovan avsnitt finns det både resultat som visar att kurser i allmänhet påverkar nivå 4, men också resultat som visar att det inte finns effektutvärderingar av tillräcklig kvalitet för att dra så generella slutsatser inom säkerhetsområdet. Vi kommer nu att övergå från det generella populationsperspektivet till att undersöka vad enskilda studier visar.

Men innan vi lämnar det generella vill vi nämna resultat som visar på vilka nivåer av effekter utvärderingar av kurser generellt tittar på. När det gäller forskningspublikationer visar det sig att relativt få studier handlar om nivå 4 [Arthur 2003, Burke 2006, Robson 2010]. I t.ex. Arthur (2003), som bygger på 165 publikationer, handlar fyra procent om nivå 1, 59 procent om nivå 2, 31 procent om nivå 3 och 7 procent om nivå 4. En i viss mån motsvarande undersökning inom näringslivet som gjorts i American Society for Training and Development 2002[21], som alltså bygger på att fråga företag om deras effektutvärderingar, ger, enligt Arthur et. al., att 78 procent av företagen använder nivå 1-utvärdering, 32 procent nivå 2, 19 procent nivå 3, and 7 procent nivå 4. En annan forskningsstudie från ett privat konsultföretag som gjorts vid sju multinationella företag, däribland Coca Cola Europe, BP och Vodafone, visade,

[21] Van Buren & Erskine, 2002, American Society for Traning and Development 2002 State-of-the-industry report.

enligt konsultföretaget, att analysen av nivå 2-3 var begränsad och att nivå 4 ofta ignorerades helt [Wilson 2004]. En fem år äldre studie från American Society for Training and Development, som även den beskrivs av en sekundärkälla [Alliger 1997], visar att företag överlag anser sig använda utvärdering på nivå 1, 80 till 90 procent av företagen använder nivå 2, cirka 60 till 80 procent nivå 3 och cirka 30 till 45 procent gör nivå 4-utvärderingar. Samma data visar dock att andelen kurser som utvärderas specifikt är lägre: över 90 procent av kurserna utvärderas på nivå 1, en tredjedel på nivå 2, ca 10 procent på nivå 3 och en nästan försvinnande procentandel på nivå fyra [Alliger 1997].

Även om resultaten ovan visar på att kursers effekt på organisationens verksamhet utvärderas i skiftande omfattning, från liten till försvinnande liten, så visar resultaten också att det finns utvärderingsinsatser som handlat om detta.

Inom skyddsområdet finns exempelvis en del enskilda studier som genom att t.ex. mäta förändring i arbetsrelaterade skador som fallolyckor visar på att interventioner i form av träning/kurser leder till förbättrad säkerhet [Dong 2004, Kinn 2000, Sokas 2009]. De flesta forskningsstudierna för effektutvärdering använder sig just av ett kvantitativt tillvägagångsätt [Vignoli 2014].

Inom området säkerhet inom industriella informations- och styrsystem hittar vi inga vetenskapliga studier om effekt av träning (eller kurser) på någon av nivåerna 1-4. Vi hittar heller ingen information kopplat till säkerhet inom andra närliggande områden, så som informationssäkerhet eller arbetsmiljösäkerhet inom processindustrin.

Sökningar har gjorts både utifrån relevanta sökord på google.com samt genom att gå igenom rubrikerna på artiklarna som använts i ovan nämnda metastudier med säkerhetsanknytning. Det utesluter självklart inte att vetenskapligt publicerade studier inom industriella informations- och styrsystem eller angränsande områden har gjorts. Och mot bakgrund av att det inom näringslivet åtminstone i någon mån genomförs nivå 4-utvärderingar kan man tänka sig att effektutvärderingar av kursers påverkan på organisatorisk nivå gjorts eller görs även av företag som har eller arbetar med industriella informations- och styrsystem. Detta uppdrag har även ostrukturerat sökt efter studier utanför forskningslitteraturen på google.com som relaterar till säkerhet och industriella informations- och styrsystem, men sökandet har varken resulterat i fynd från den offentliga sfären eller näringslivet. Såvida det inte handlar om t.ex. marknadsföring av kurser eller utvärderingstjänster kan man tänka sig att företag är sparsamma kring att publicera resultat kring detta på sina hemsidor. Dock har även marknadsföring kring kurser eller utvärderingars förtjänster i princip inte framkommit. I en tidningsartikel har vi hittat exempel på

en berättelse om hur kurser kopplade till phishingattacker, enligt artikeln, visat sig ge hög avkastning på nivå 4[22].

I en rapport från HP Information Security ställdes frågor till mer än 100 chefer inom IT-säkerhetsområdet i USA och Storbritannien i syfte att undersöka vad de anser vara kritiska komponenter för ett framgångsrikt säkerhetsarbete. Tillvägagångsättet för undersökningen var att använda ett omfattande batteri av frågor kopplat till det av HP utvecklade ” Security Effectiveness Rating” [HP 2010]. Sammanställningen av frågorna visade vilka cheferna ansåg vara de främsta faktorerna som bidrar till informationssäkerhet. Bland dessa fem främsta faktorer för ett framgångsrikt säkerhetsarbete återfanns träning[23].

När det gäller information på svenska hittar vi heller inga publikationer som utvärderar effekter av kurser kopplat till industriella informations- och styrsystem eller vetenskapliga publikationer om effektutvärdering av nivå 4 inom andra områden. Det finns exempel på rapporter från forskningsprojekt inom andra områden som tangerar nivå 4 [Abrahamson Lövström 2013] och även en utfästelse om en forskningspublikation på Försvarshögskolans hemsida om nivå 4-effekt av kursen Utveckling av Grupp och Ledare [FHS 2016]. Övriga publikationer som vi hittat är på motsvarande masteruppsatsnivå.

[22] På internet 16-07-01. http://www.csoonline.com/article/2987822/data-protection/does-security-awareness-training-even-work.html.

[23] De fem faktorerna som lyftes fram var:

- Utnämning av en organisatorisk ledare för informationssäkerheten.
- Träning och program kopplat till säkerhetsmedvetenhet om dataskydd och säkerhet för slutanvändarna
- En organisationskultur som respekterar integritet och dataskydd
- Ledningens stöd kring informationssäkerhet
- Starka slutpunkts kontroller

Faktorerna är översatta från “Top 5 drivers to a good Security Effectiveness Rating: a) Appointment of a CISO or organizational leader for information security. B) Training and awareness programs on data protection and security for end-users. C) An organisational culture that respects privacy and data protection. D) Executive-level support for security. E) Strong endpoint controls.” s. 6 [HP 2010].

Bilaga C Rekommendationer, standarder och vägledningar

I denna bilaga redovisar vi resultaten från en genomgång av 16 standarder, rekommendationer och vägledningar inom området industriella informations- och styrsystem. Samtliga befintliga referenser som finns i MSB:s *Vägledning till ökad säkerhet i industriella informations- och styrsystem* ingick i urvalet av dokument. I flera fall finns det uppdaterade versioner av dessa referenser [CPNI 2015, NIST 2015], och i två fall har referensarena inte varit fritt tillgängliga för oss [IEC 2005, NERC 2011]. Till referenserna i MSB:s vägledning har dokument på engelska tillfogats som varit tillgängliga vid sökningar på internet under september 2016 [BSI 2012, DHS 2011, ENISA 2011, PSC 2012, TNO 2015]. I urvalet av dokument har skrivningar relaterat till utbildningsprogram, medvetenhetshöjande åtgärder, utbildning (”training”), kunskapsutbyte mellan organisationer, utvärdering av utbildning samt lednings involvering sökts.

Genomläsningen av de 16 dokumenten visar till att börja med att det i inga av dessa dokument återfinns hänvisningar till vetenskapliga publiceringar som handlar om effekt av utbildning och övning inom området. I många fall finns utförliga referenser i dokumenten, men dessa hänvisar till andra standarder och rekommendationer. Det är självklart positivt att beakta erfarenheter i andras standard- och rekommendationsverk, men detta behöver göras med en medvetenhet om risken för att med tiden mer referera i cirklar än till kunskapskällor baserat på vetenskaplig empiri snarare än individers upplevelser (erfarenheter). Ett dokument skriver i klartext att rekommendationerna som ges är baserade på erfarenheter och tumregler [BSI 2012]. I ett dokument skrivs att erfarenheter visar att majoriteten av de IT-säkerhetsincidenter som sker i stor utsträckning beror på användarnas beteende[24] [IAEA 2011]. I en av rekommendationerna hänvisas till enkätundersökningar som visar att felaktig användning av ICS-utrustning och applikationer ligger bakom de flesta datorrelaterade problem[25] [OLF 2009].

Den generella bilden efter genomläsning är att trots avsaknaden av vetenskapliga publiceringar kring effekter som kurser har på organisationers verksamhet inom området säkerhet inom industriella informations- och styrsystem, framstår det som helt självklart att träning är en viktig och självklar del i att utveckla säkerheten. I Figur 3 nedan, redovisas vilka av dokumenten som tar upp något relaterat till utbildningsprogram, medvetenhetshöjande åtgärder (”awareness”), utbildning

[24] Experience has demonstrated that the majority of computer security incidents are human related and the security of any computer system depends largely on the behaviour of all its users.

[25] Surveys have shown that incorrect use of ICT equipment and applications cater for most of the computer related problems.

(”training”), kunskapsutbyte mellan organisationer, utvärdering av utbildning samt lednings involvering.

Som Figur 3 visar täcker dokumenten i huvudsak in likande områden trots att de är inriktade mot olika målgrupper. Målgrupper kan vara t.ex. till de som tar fram standarder, till ansvarig(a) myndighet(er) på nationell nivå eller direkt till industrin. Vad inom respektive område som tas upp i dokumenten återges översiktligt nedan. Noterbart är dock att endast ungefär en tredjedel av dokumenten tar upp någon form av utvärdering av utbildningsinsatserna. Likaså tar endast en tredjedel upp övning (dvs. kunskaps-/förmågehöjande åtgärder utifrån ett spelat scenario) som en del i säkerhetsarbetet.

Att människor både är den viktigaste resursen och det potentiellt största hotet mot säkerheten är ett genomgående tema i det som skrivs kopplat till kurser och övning.

Något som också konstateras frekvent i dokumenten är behovet av att länka ihop IT och OT. Det skulle underlätta kunskapsöverföring, bygga arbetsrelationer och lyfta fram skillnader och likheter mellan IT-system och ICS.

	Namn	Typ av dokument	Land	Publicerad	Program-verksamhet	Medvetenhet (awareness)	Utbildning (training)	Utanför egen organisation	Utvärdering av utbildning	Ledningens involvering
Återfinns i 2014 års version av Vägledningen	NIST SP 800-82 — Guide to Industrial Control Systems (ICS) Security	Rekommendation	USA	2015	Ja	Ja	Ja	Nej	Ja	Ja
	CPNI Good Practice Guide Process Control and SCADA Security	Rekommendation	GB	2008	Ja	Ja	Ja	Ja	Nej	Ja
	21 Steps to Improve Cyber Security of SCADA Networks	Rekommendation	USA	2002	Ja	Ja	Ja	Nej	Nej	Nej
	Information security baseline requirements for process control, safety and support ICT systems	Rekommendation	Norge	2009	Ja	Ja	Ja	Nej	Nej	Nej
	Cyber Security Procurement Language for Control Systems	Rekommendation	USA	2009	Nej	Nej	Ja	Nej	Nej	Nej
	IAEA Nuclear security series #17 (Computer Security at Nuclear Facilities)	Teknisk vägledning	Internationell	2011	Ja	Ja	Ja	Ja	Ja	Ja
	SS-ISO/IEC 27000-serien - 27002 (kap 7.2.2)	Standard	Internationell	2014	Ja	Ja	Ja	Ja	Ja	Ja
	SS-ISO/IEC 27000-serien - 27035	Standard	Internationell	2012	Ja	Ja	Ja	Ja	Ja	Ja
	ISO/IEC 62443-2-1 (ISA-99) — Industrial Communication Networks — Network and system security	Standard	Internationell	2010	Ja	Ja	Ja	Ja	Ja	Ja
	ISA−62443−2−1 Draft 7, Edit 5, Security for industrial automation and control systems Part 2-1: Industrial automation and control system security management system	Standard	Internationell	2015	Ja	Ja	Ja	Ja	Ja	Ja
Återfinns ej i 2014 års version av Vägledningen	Catalog of control systems security: Recommendations for Standards Developers	Rekommendation	USA	2011	Ja	Ja	Ja	Ja	Ja	Ja
	Security for industrial control systems - improve awareness and skills - a good practice guide	Vägledning	GB	2015	Ja	Ja	Ja	Ja	Nej	Ja
	Cyber Security of Industrial Control Systems - Good Practices	Vägledning	Holland	2015	Ja	Ja	Ja	Ja	Nej	Ja
	Protecting Industrial Control Systems Recommendations for Europe and Member States	Rekommendation	EU	2011	Ja	Ja	Ja	Ja	Nej	Ja
	Industrial Control System (ICS) Cyber Security: Recommended Best Practices Number: TR12-002	Rekommendation	Kanada	2012	Ja	Ja	Ja	Ja	Nej	Nej
	Recommendations for security-related trainings	Rekommendation	Tyskland	2012	Nej	Ja	Ja	Nej	Nej	Ja
	ICS-CERT Recommended pratices	Rekommendation	USA	2016/2007	Nej	Ja	Ja	Nej	Nej	Nej

Figur 3: Dokumenten som bland annat skriver om träning och övning inom industriella informations- och styrsystem. Referenserna på vit botten är referenser som finns i MSB:s Vägledning till ökad säkerhet i industriella informations och styrsystem med utgivningsår 2014.

C.1 Utbildningsprogram

Både en utbildningspolicy och mer handfasta utbildningsprogram specifika för ICS föreslås i princip genomgående i dokumenten. Utbildningsprogrammen beskrivs bl.a. som ett sätt att visa att ledningen står bakom utbildningsinsatserna.

Utbildningsprogram beskrivs genomgående som att de bör upprepas regelbundet och omfatta en grundlig introduktion till informationssäkerhet. Bland de saker som lyfts fram för att säkerhetsprogram ska lyckas är engagemang från högsta ledningen, att ett informationsprogram bör inrättas samt att det innehåller stödjande business case.

Enligt den internationella standarden ISO/IEC 27002:2013, för vilken Swedish Standards Institutet (SIS) ger ut en svensk version, rekommenderas att ett utbildningsprogram ”*bör ha som målsättning att göra anställda och i tillämpliga fall leverantörer medvetna om sitt ansvar för informationssäkerhet och hur detta ansvar kan uppfyllas*”, att det ”*bör fastställas i enlighet med organisationens informationssäkerhetspolicy, tillhörande regelverk och relevanta rutiner*”, och att det ”*bör planeras med beaktande av de anställdas roller i organisationen och i tillämpliga fall organisationens förväntan på medvetenhet hos entreprenörer* (se 7.2.2) [SS-ISO/IEC 2014]. Här liksom i ISO/IEC 62443-2-1 betonas också att ”*Vid skapandet av ett utbildningsprogram är det viktigt att inte bara fokusera på “vad” och “hur” men också “varför”. Det är viktigt att medarbetarna förstår syftet med informationssäkerhet och de potentiella konsekvenserna, positiva som negativa, på organisationen av sitt eget beteende*. (se 7.2.2).” [ISO/IEC 2010, SS-ISO/IEC 2014].

C.2 Medvetenhetshöjande åtgärder

Som det skrivs i ISO/IEC 27002:2013 ”*Alla organisationens anställda och i förekommande fall leverantörer bör erhålla lämplig utbildning och fortbildning för ökad medvetenhet och regelbundna uppdateringar vad gäller organisationens policy, regelverk och rutiner i den omfattning som är relevant för deras befattning*.” Det lyfts också fram att ökad medvetenhet inte är något som skapas genom en engångsinsats, utan att det är ett pågående arbete.

Något som lyfts fram avseende medvetenhetshöjande åtgärder är hot i form av social ingenjörskonst, att manipulera människor till att ge bort privat information som lösenord.

De medvetandehöjande åtgärderna ligger på varje enskild organisation att genomföra och föreslås kunna genomföras genom t.ex. affischering, genom e-nyhetsbrev/meddelanden från högre organisations tjänstemän, meddelanden på inloggningsskärmen och genom att genomföra säkerhetsmedvetenhetshöjande

evenemang. Tillvägagångssättet för hur dessa medvetandehöjande åtgärder görs kommer variera från en organisation till en annan.

Enligt den internationella standarden ISO/IEC 27002:2013 rekommenderas att *”Informationssäkerhetsutbildningen bör också omfatta allmänna aspekter såsom:*

a) ledningens engagemang för informationssäkerhet inom hela organisationen;

b) behovet av att bekanta sig med och följa gällande informationssäkerhetsregler och skyldigheter som är definierade i policy, standarder, författningar, avtal och överenskommelser;

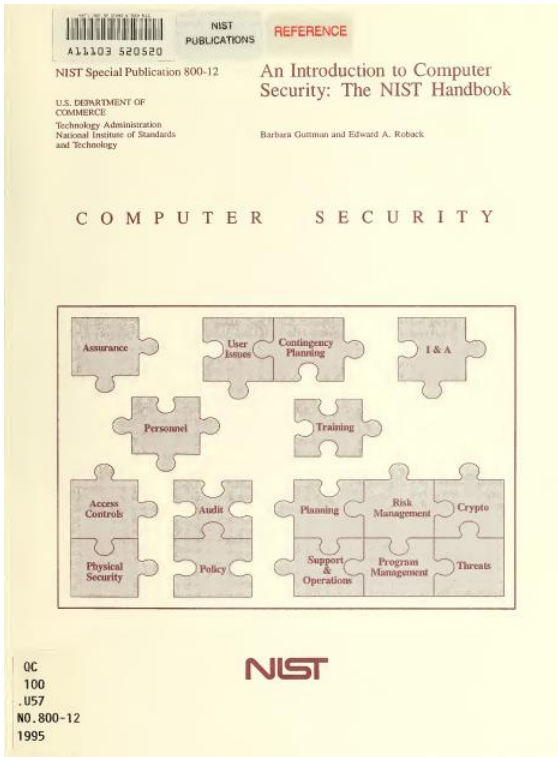
c) personligt ansvar för sina egna handlingar och passivitet samt allmänna skyldigheter mot att säkra eller skydda information som tillhör organisationen och externa parter;

d) grundläggande informationssäkerhetsrutiner (t.ex. rapportering av informationssäkerhets-incidenter) och grundläggande säkerhetsåtgärder (såsom lösenordsskydd, skydd för skadliga program och renstädat skrivbord);

e) *kontaktpunkter och resurser för ytterligare information och råd i frågor gällande informations-säkerhet, inbegripande ytterligare informations-säkerhetsutbildning och utbildningsmaterial*.” [SS-ISO/IEC 2014, avsnitt 7.2.2.]

C.3 Utbildning (training)

I jämförelse med medvetenhet handlar training om mer specifik utbildning, färdighetsträning, anpassad för olika roller och som Figur 3 visar är träning det som inkluderas i samtliga av de 16 studerade dokumenten. Föreställningen eller övertygelsen om träningens centrala roll är ingen modefluga. I NIST:s handbok om IT-säkerhet från 1995 återfinns träning som en central pusselbit, Figur 4.



Figur 4: Träning återfinns som en central pusselbit i NISTs handbok om IT-säkerhet från 1995[26].

Men vad ska den mer specifika utbildningen, träningen, handla om och hur ska den genomföras? Vad utbildningarna ska innehålla på en mer generell nivå samt hur dessa ska genomföras varierar från övergripande skrivningar i dokumenten om att träningen kan handla om t.ex. sårbarheter och incidenttrender till att vara konkret exempel på kursupplägg [BSI 2012]. Det lyfts fram att organisationen bestämmer innehållet i utbildningen utifrån de specifika kraven i organisationen och de system som personalen arbetar med. Också när det gäller formerna för träningen, om den t.ex. sker på jobbet eller i ett klassrum eller kring hur interaktiv den är, så lämnas inga specifika inriktningar, utan de 16 dokumenten lyfter snarare fram alla de former som träning kan ske på.

[26] Från NIST 1995, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

C.4 Kunskapsutbyte mellan organisationer

Något som också tas upp i de flesta av de 16 lästa dokumenten är vikten av att även arbeta utanför sin enskilda organisations väggar med utbildning. Vikten av att inte enbart utbilda anställda, utan även utbilda entreprenörer och leverantörer lyfts fram [t.ex. DHS 2011, IAEA 2011, ISO/IEC 2010]. Alla kontrollsystemanvändare (inklusive chefer, ledande befattningshavare och entreprenörer) ska genomgå grundläggande utbildning om säkerhetsfrågor innan de ges tillträde till systemet [DHS 2011].

Något som det också skrivs om är att organisationen etablerar och upprätthåller kontakt med säkerhetsgrupper och föreningar för att hålla sig a jour med de senaste inom området och dela aktuell säkerhetsrelaterad information, inklusive hot, sårbarheter och incidenter [DHS 2011].

C.5 Utvärdering av utbildning

En dryg tredjedel av dokument tar inte bara upp att de kompetenshöjande aktiviteterna som görs t.ex. ska följas och dokumenteras över tid, utan även att ansatser för att säkerställa att utbildningsinsatserna gett önskad effekt ska göras [DHS 2011, IAEA 2011, ISO/IEC 2010, NIST 2014, SS-ISO/IEC 2014][27]. Önskade effekt relaterar oftast till medarbetarnas upplevelse och kunskap, t.ex. ”*En utvärdering av medarbetarnas förståelse kan genomföras i slutet av en medvetenhetsutbildning för att testa kunskapsöverföringen.*” [SS-ISO/IEC 2014] eller tar ett större perspektiv på så vis att det är träningsprogrammen som kontinuerligt ska utvärderas för att säkerställa att medarbetare får tillräcklig träning. [28]

Det finns även inriktningar som pekar mot att utvärdera nivå 4, dvs. organisatorisk effekt. I USA skriver Department of Homeland Security 2011 i sina rekommendationer till dem som tar fram rekommendationer för standarder inom

[27] När det gäller färdighetsträning framstår rekommendationerna sikta lägre, här finns inte rekommendationen att utvärdera nivå 4, det är tillräckligt att dokumentera, upprätthålla och monitorera träningen. Om träning, “The organization documents, maintains, and monitors individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization’s records retention policy. The organization maintains a record of training requirements for each user in accordance with the provisions of the organization training and records retention policy.” [DHS 2011].”
”En utvärdering av medarbetarnas förståelse kan genomföras i slutet av en medvetenhetsutbildning för att testa kunskapsöverföringen.” [ISO/IEC 2014]
”The training programme should include metrics to evaluate computer security awareness, training effectiveness, and processes for continuous improvement or retraining.” [IAEA 2011]

[28] Fritt översatt från “The training program should be validated on an on-going basis to ensure that personnel understand the security program and that they are receiving the proper training.” [ISO/IEC 2010]

industriella informations- och styrsystem att effektivitet på organisationsnivå, kopplat till träning kring säkerhetsmedvetenhet, behöver ses över minst en gång per år[29] [DHS 2011]. När det gäller färdighetsträning framstår rekommendationerna sikta lägre, här finns inte rekommendationen att utvärdera nivå 4, det är tillräckligt att dokumentera, upprätthålla och monitorera träningen[30] [DHS 2011].

C.6 Övning

När det gäller övningar så är detta något som i mindre utsträckning än träning lyfts fram, både i antal standarder/rekommendationer som omnämner övning (fem av sexton), samt även i omfattningen av det som skrivs. I ett fåtal dokument står det att det ska planeras för att öva incident- eller krishanteringsplanen (”disaster recovery plan”) regelbundet och att de erfarenheter som övningarna ger ska leda till uppdaterade planer. Ett dokument lyfter fram (inter)nationella övningar [TNO 2015][31]. I två dokument lyfts mer ICS-specifik träning utifrån scenarier fram, dvs. det vi i denna rapport kallat övning som en metod att driva kunskap- och färdighetsutvecklingen [DHS 2011, SS-ISO/IEC 2012][32].

Att notera är dock att i den utkastversion som finns tillgänglig av ISA 62443-2-1 [ISO/IEC 2016] (som motsvarar [ISO/IEC 2010]) finns tidigt i stycket som handlar om ”Information security awareness, education and training” en skrivning om att organisationen skall träna sin personal i deras beredskapsroller och ansvar, vilket inkluderar att inkludera simulerade händelser i beredskapssyfte för att främja en effektiv krishantering[33]. Den synbara förstärkning av övning som metod för att

[29] Fritt översatt från ”The effectiveness of security awareness training, at the organization level, needs to be reviewed once a year at a minimum” [DHS 2011].

[30] Om träning, “The organization documents, maintains, and monitors individual control system security training activities, including basic security awareness training and specific information and control system security training in accordance with the organization’s records retention policy. The organization maintains a record of training requirements for each user in accordance with the provisions of the organization training and records retention policy.” [DHS 2011].

[31] Creating awareness by performing (inter)national exercises which include cyberattacks against critical infrastructure ICS. [TNO 2015]

[32] “The organization includes practical exercises in security awareness training that simulate actual cyber attacks.” [DHS 2011].
“Periodic tests should be organized to check processes/procedures and to verify how the ISIRT responds to severe complex incidents, through the simulation of realistic attacks, failures or faults. Particular attention should be paid to the creation of the simulated scenarios, which should be based on real new information security threats. Tests should involve not only the ISIRT, but all the internal and external organizations that are involved in the management of information security incidents. Organizations should ensure that any changes made as a result of post testing reviews are subject to thorough checking, including further testing, before the changed scheme goes live.” [ISO/IEC 2012].

[33] Fritt översatt från ”The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.” [ISO/IEC 2016].

främja säkerhetsarbetet som återfinns i utkastet till [ISO/IEC 2016] kan vara början på en spirande trend där övningar, dvs. agerande eller diskussioner utifrån simulerade händelser, ges ett större fokus.

C.7 Ledningens involvering

Flertalet av de 16 studerade dokumenten tar upp ledningens roll kopplat till säkerhet. I flera dokument framstår ledningens engagemang som hjulet som driver säkerhetsarbetet inom organisationen. I Protecting Industrial Control Systems Recommendations for Europe and Member States [ENISA 2011] skrivs att många säkerhetsexperter under arbetet med denna rekommendation signalerat att en av deras mest utmanande uppgifter var att göra sina överordnade medvetna om faktiska risker och hot. Experter uttryckte att högsta ledningen vanligtvis ser IT-säkerhet mer som en kostnad än en investering, och att de felaktigt tror att de redan gör tillräckligt [ENISA 2011]. Ledningen behöver motiveras och se hur viktig ICS-säkerhet är för verksamheten. Förslag som lyfts för att främja detta är ta fram ett ”business case” som visar fördelar och nackdelar med att ha ett säkerhetsprogram och/eller att få samarbeta med ledningen för att säkerställa att konsekvenserna för verksamheten av säkerhetsrisker förstås vilket skulle bidra till att ledningen vidtar åtgärder för att hanterar dessa risker. Det är oklart vem som har den motiverande rollen, om det t.ex. är en inomorganisatorisk eller utomorganisatorisk uppgift. Att ta fram business case och visa på konsekvenserna kan vara grannlaga uppgifter som i sig kräver att ledningen tillhandahåller resurser för detta arbete. Ett förslag på en utomorganisatorisk åtgärd är att tillhandahålla gratis workshops för chefer [TNO 2015]. Ett annat förslag är att det finns en särskild utbildning för ledningsnivån som inte bara syftar till att medvetandegöra ledningen om problemet utan också ge ytterligare förståelse för området [BSI 2012].

Bilaga D Uppföljning av de organisatoriska effekterna av de kurser som tillhandahålls av NCS3

I denna bilaga redovisar vi resultatet av den uppföljning av kursverksamheten vid NCS3 som genomförts baserat på en intervju- och enkätstudie med tidigare kursdeltagare och chefer med ansvarsområden inom området säkerhet inom industriella informations- och styrsystem. Utifrån de intervju- och enkätfrågor som ställdes beskrivs resultaten under rubrikerna 1) Nyttjande av utbildningar och övningar i sin verksamhet, 2) Organisatoriska effekter av kursdeltagande, 3) Externa påverkansfaktorer och 4) Förslag på vidareutveckling av kurskonceptet. Bilagan avslutas med ett avsnitt med slutsatser. För tydlighets skull redovisas intervju- och enkätsvaren var för sig.

D.1 Nyttjande av utbildningar och övningar i verksamheten

Bland de organisationer som de intervjuade respondenterna tillhör finns en stor variation i hur man arbetar med utbildningar och övningar inom området säkerhet inom industriella informations- och styrsystem, från strukturerade utbildningsprogram till ad hoc-lösningar eller individstyrda lösningar. De flesta organisationer beskrivs ha någon form av grundläggande (e-)kurs i informationssäkerhet, även om en respondent uttryckte att dessa kurser ofta är på en så pass grundläggande nivå att det snarare handlar om information än utbildning. Dessutom beskrivs dessa grundläggande säkerhetskurser som oftast inte innehålla särskilt mycket specifikt kring industriella informations- och styrsystem.

Bland de organisationer som strukturerat arbetar med utbildningar och övningar inom området verkar utbildningsstrategier/program/planer vara förankrade högt inom organisationerna, koncernövergripande och med avstämningar på chefsnivå. Informationssäkerhetschefen beskrivs här ha en central roll i organisationernas utbildningsprogram och beskrivs vara aktiv i arbetet med att prioritera mellan vilka personer eller funktioner som har utbildningsbehov, det vill säga inriktar platstilldelningen vid interna och externa utbildningar. Flera av respondenterna uppger att de organiserar interna kurser inom säkerhet och ICS. Fördelar som nämns är att det underlättar interna kontakter och etablerar organisationens arbetssätt. Interna kurser kan anpassas efter den egna verksamheten, efter den egna miljön och efter de egna rutinerna. Fördelar med externa kurser uppges å andra sidan vara möjligheten att lyssna till kunniga externa föreläsare, att knyta kontakter

med personer från andra organisationer som har likande utmaningar, och att man fysiskt reser bort från sin vardagliga arbetsplats.

Ingen av respondenterna uppgav att SI3S/I4S ingått eller ingår som ett obligatoriskt utbildningsmoment inom deras organisation. Platser för respektive organisation till SI3S/I4S fördelas centralt och är begränsade i antal. Att organisationer inte kan garanteras plats skulle kunna vara en bidragande orsak till att kurserna inte kan vara ett obligatorium. Samtidigt har vi inte i intervjuerna frågat om kurserna skulle införas som obligatoriska i utbildningsplanen om de kom med platsgaranti. SI3S och I4S ingår däremot, i förekommande fall, bland de kurser som rekommenderas i organisationerna utbildningsprogram.

I de organisationer där utbildningsplaner inte beskrivs som lika tydligt strukturerade och använda kan det istället vara upp till de enskilda individerna att identifiera och flagga för sina kunskapsluckor och hitta lämpliga kurser. Även om de personer som vi intervjuat oftast fått ett erbjudande från sin chef om att gå en av kurserna vid NCS3, så svarar också en att kursdeltagandet istället skedde på dennes eget initiativ.

I jämförelse med de insatser som vid intervjuerna beskrivs läggas av organisationen på kurser, framstår arbetet för ökad säkerhet inom industriella informations- och styrsystem i mindre utsträckning ske genom övningar. Inom två av de sju organisationerna används övningar som ett instrument för att arbeta med säkerhetsfrågor för industriella informations- och styrsystem. Både Red/Blue team-övningar och skrivbordsövningar nämns. En annan respondent uppger att det finns funderingar inom organisationen på att arbeta med övningar och ytterligare en att det fläckvist och sporadiskt visserligen genomförs övningar, men inte specifikt inom detta område. Det faktum att de tekniska system som de intervjuade organisationerna handhar måste vara i kontinuerlig drift gör det också svårt att utforma övningar som är något annat än seminarieövningar.

Utöver interna kurser och SI3S/I4S nämner flera av respondenterna att andra externa utbildningar, övningar och konferenser nyttjas för att höja medarbetarnas kunskap inom området, exempelvis kurser vid SvK och SANS Institute, Nationell informationssäkerhetsövning (NISÖ) samt konferensen 4SICS.

D.2 Organisatoriska effekter av kursdeltagande

Som nämns i inledningskapitlet har SI3S, tidigare SIK, getts vid betydligt fler tillfällen än I4S och fler personer har därmed också deltagit vid denna kurs. Enligt en beskrivning av SI3S är målet med kursen att deltagarna ska:

- få förståelse för betydelsen av och möjligheterna med att aktivt arbeta med säkerhetshöjande insatser i industriella informations- och styrsystem

- få kännedom om lämpliga verktyg och metoder för att identifiera sårbarheter i industriella informations- och styrsystem
- kunna delta i arbetet med att förbättra och utveckla säkerheten i en organisations industriella informations- och styrsystem
- utbyta erfarenheter med varandra [Lindahl 2016]

I detta avsnitt sammanställs resultaten av vad som framkommit i intervjuer och enkät relaterat till frågor om nyttan av utbildningar och övningar inom området säkerhet i industriella informations- och styrsystem och hur de erfarenheter som kursdeltagarna tagit med sig från kurserna eventuellt påverkat det interna säkerhetsarbetet i organisationerna. Frågan om ”nyttan” av utbildningar ställdes i samband med intervjuerna och syftade till att allmänt sondera respondenternas inställning till kompetensutveckling som medel för stärkt säkerhet.

D.2.1 Allmänt om nytta av utbildning och övning enligt intervjusvaren

Under informationsinhämtningen genom intervjuer har nyttan av utbildningar och övningar lyfts fram unisont. Utbildningar och övningars roll beskrivs som en väldigt viktig och nödvändig del i arbetet för att stärka säkerheten inom industriella informations- och styrsystem. Även om utbildning och övningar inte beskrivs som lösningen på allt, så är synsättet som genomsyrar intervjuerna att kompetenshöjande insatser i sig alltid är värdefullt. Att resurser och krav också har en stark påverkan på utveckling inom säkerhetsområdet har påtalats under intervjuerna, däremot har olika säkerhetsstärkande tillvägagångssätts relation till varandra, som regel-, ekonomi- eller kunskapsstyrning, får att nå effekt inte lyfts fram under intervjuerna. Både utbildningars och övningars nytta beskrivs också som nära förknippade med i vilken utsträckning dessa är en ledningsfråga eller inte inom organisationen.

D.2.1.1 Allmän nytta av utbildning och övning för individen

Den nytta som främst lyfts fram kopplad till utbildning och övning generellt är ökad medvetenhet, dvs. det som lyfts fram är individens ansvar och roll i helheten, att individen genom sin förvärvade medvetenhet kan bidra med en positiv påverkan. Individens roll i att inom sin organisation föra vidare kunskaper förvärvade vid utbildning och övning om hur problem kan lösas eller hur man kan agera vid händelser, omnämns i några fall. Däremot lyfts inget om generella etablerade strukturer, former, för hur detta bör eller kan ske inom organisationerna. En annan faktor som lyfts fram relaterat till just kurser, likt NSC3-kurserna, dvs. kurser som ger ”medvetande/uppvaknandet/aha-upplevelsen”, är att individer får ökad kraft (vågar) att arbeta vidare med frågorna inom organisationen.

Något som också lyfts fram är att nyttan av enskilda utbildningstillfällen är kopplad till individens förutsättningar. För *”[…] en del gav det större effekt, för att potentialen var mycket större.”* Att utbildning kan vara tvingande lyfts också fram vid flera tillfällen och att om det inte finns intresse eller om behovet av utbildningen inte ses eller förstås av medarbetaren för sin roll, då kommer kursdeltagandet inte leda till nytta. Kopplat till nyttan lyfts också vikten av att se utbildning i ett sammanhang. *”[…] då utbildning är i ett led i ett program, en del i en utveckling i ett företag, då är den ju otroligt värdefull*.”

D.2.1.2 Nyttan hos organisationer kopplat till utbildnings- och övningsplaner

Intervjuerna ger också exempel på när målet med att delta vid utbildning eller övning uttrycks som att det mer direkt knyter an till nytta på organisatorisk nivå. Att notera är att förekomsten av dessa exempel sammanfaller med användande av en strukturerad utbildningsplan/strategi/program inom organisationen. En strukturerad fastställd utbildningsplan beskrivs inrikta utbildningsinsatserna mot att möta organisationens behov t.ex. för att få genomslag där det finns problem med att få igenom lösningar, för att rikta utbildningen mot ny personal, mot incidenter eller händelser, mot respektive bolags/funktionens vikt inom organisationen etc. Dessutom beskrivs en fastställd utbildningsplan i sig vara en signal från ledningen att utbildning är viktigt.

Något som också lyfts fram som en underliggande tanke som kan genomsyra en utbildningsplan är att ett syfte är att få medarbetarna att vända sig till de kollegor som redan besitter expertkompetens och färdigheter. Utbildningsplanens aktiviteter kan helt enkelt syfta till att medarbetare inom organisationen får kompetens att upptäcka kunskapsbehov inom säkerhetsområdet och att de då, också genom utbildning och övning, har kännedom om och förtroende för organisationens experter inom området.

D.2.1.3 Den snabba utvecklingen inom området säkerhet inom ICS innebär att individer behöver förses med uppdaterad kunskap – men effekten av höjd kunskapsnivå visar sig flera år senare

Nyttan av utbildning och övning inom området säkerhet och industriella informations- och styrsystem specifikt betonas också särskilt mot bakgrund av att industriella informations- och styrsystem är ett område som förändras väldigt snabbt. Det beskrivs som viktigt att ha den senaste informationen och ökad medvetenhet och kompetens till exempel om hot och risker. En ökad kunskapsnivå om hur IT-baserade hot ser ut och vilka konsekvenser de har för anläggningarnas produktion beskrivs som oerhört viktigt för att skapa en tillräckligt stor generell medvetenhet för att få en positiv attityd till att införa skyddsåtgärder. I detta sammanhang beskrivs också den tröghet som finns i organisationen innan kompetenshöjande initiativ ger effekt. *”Vi har arbetat målmedvetet med detta*

inom […] sedan 2007 när vi höll den första internkonferensen i SCADA-säkerhet och det är först nu de senaste åren som det börjar ge effekt."

D.2.1.4 Skillnader i nytta mellan kurser och övningar

Få skillnader i nytta mellan kurser och övningar lyfts fram, förutom att övningar beskrivs som att de kan vara ett bra angreppssätt som kan ge mer medvetandehetsmässigt än kurser och att övningar kan vara underskattande i arbetet för att stärka säkerheten inom ICS. För att förstå frågeställningen kring övningar behöver det också uppmärksammas att det kan finnas en skiljelinje mellan vad som ses som kurs/träning och vad som är övning, beroende på hur man ser på ”övning”. Övning kan ses som en aktivitet som är scenariodriven som används för att utbilda och träna färdigheter hos individer. Övning kan också ses som en aktivitet som syftar till att utveckla förmåga hos organisationer i enlighet med MSB:s Övningsvägledningsterminologi där övningar ses som ”*Aktivitet som omfattar en eller flera aktörer och som främst syftar till att identifiera brister, pröva och/eller utveckla förmågor.*” [MSB 2014b] Både mer träningslikande övningar motsvarande de som görs vid I4S-kursen och övningar, likt Nationell Informationssäkerhetsövning (NISÖ) som syftar till att öva organisationers förmåga, lyfts fram som nyttiga och att det är viktigt att få öva på båda dessa sätt.

D.2.2 Effekter av kursverksamheten vid NCS3 enligt intervjusvaren

Att notera är att under intervjuerna lyfts inga exempel som vi tolkar som nivå 4-effekter fram. Däremot beskrivs många effekter på nivå 1-3.

D.2.2.1 SI3S beskrivs som en omtyckt och väldigt bra kurs som skapar medvetenhet på ett attraktivt sätt

Intervjuerna bekräftar den bild som kursutvärderingarna för SI3S visar [Lindahl 2016]. Kursen beskrivs som *”väldigt bra och omtyckte av våra medarbetare som gick den.”* Särskilt lyfts övningsmiljön fram, en fullt fungerande miljö där man får knappa och testa själv. *”Systemen som man gör övningarna i är fantastiska”*. Kursen beskrivs också som att den *”skapar medvetenhet på ett attraktivt sätt”*, med sitt blandade innehåll samt ”demo”. *”En riktigt bra kurs!”*

D.2.2.2 SI3S-kursen är efterfrågad

Ytterligare observationer som lyfts fram för att visa på att SI3S-kursen är en uppskattad kurs, bortom kursutvärderingarna och intervjupersonernas egen bild av sitt kursdeltagagande och den bild de förmedlar av medarbetares upplevelse, är att det inte beskrivs som ett problem att fylla kursplatserna. Tvärtom finns det en efterfrågan på fler platser. I ett fall framfördes på chefsnivå en önskan om att kontinuerligt kunna inkludera kursen i organisationens utbildningsplan. I ett annat fall framfördes att det som skulle skapa bättre förutsättningar för att påverka

arbetet med säkerhet kopplat till SI3S-kursen helt enkelt handlade om att fler medarbetare har genomgått utbildningen.

D.2.2.3 Effekter av kurserna beskrivs i generella snarare än specifika termer – inga exempel på verksamhetspåverkande åtgärder som direkt resultat av kurserna (dvs. effekter på nivå 4)

Intervjuerna gav inga exempel på direkta åtgärder som ett resultat av individers kursdeltagande. Intervjusvaren behöver förstås mot bakgrund av att de individer som intervjuades alla är verksamma inom stora organisationer. Få förändringar som sker inom organisationer, om ens några, kan förväntas kunna enskilt härledas till deltagande vid en enskild kurs. Däremot kan man från intervjusvaren utläsa en stark tilltro till att kursdeltagande verkligen är en av de viktiga byggstenarna som bidrar till effekt, som bidrar till verksamhetspåverkan. I ett svar på frågan om de erfarenheter som medarbetare tog med sig från kursen (SIS3/I4S) har påverkat (förändrat eller upprätthållit) det interna säkerhetsarbetet på något sätt anges uttryckligen *”Ja men det tar lång tid och man behöver komma upp i en kritisk massa.”*

D.2.2.4 Individer har skilda motiv för att gå kurserna vilket starkt påverkar vad de tar med sig därifrån

Bland de intervjuade som gått SI3S och/eller I4S kan det noteras att dessa individer deltagit vid kursen med väsentligt skilda motiv och att det självklart påverkar vad de tar med sig därifrån. Samtliga intervjuade är också verksamma sedan länge inom området och har en gedigen komptensbas. Vad de tog med sig från kursen beror också på vilken version av kursen de deltagit vid, vilket i huvudsak är I4S/SI3S under våren 2016, några fall en tidig omgång av SIK-kursen som getts mellan 2009-2014 och i några fall ISC-CDX, föregångaren till I4S.

En intervjuperson beskriver att deltagande i kursen SIK erbjöds och att intervjupersonen såg positivt på det. Upplevelsen under kursen var att den kunskapsmässigt låg på en alltför grundläggande nivå, den grund som kursen gav besitter redan de som arbetat med säkerhet i många år. Kursen var mer för dem som inte är så säkerhetskunniga. Intervjupersonens allmänna bild av kurser är att det som är mest intressant med kurser är att träffa andra individer från andra organisationer och diskutera med dem.

En individ ser sitt kursdeltagande (I4S) som en del att hålla sina egna kunskaper uppe inom området. Intervjupersonen tog initiativ till sitt kursdeltagande eftersom upplägget med red/blue/white team verkade intressant och deltagande i en tidig omgång av kursen även skulle främja individens roll, i vilken det ingår att fördela/prioritera kursplatser inom organisationen. Kursen gav dels en teknisk inblick i hur attacker mot denna miljö kan genomföras och upptäckas samt exempel på verktyg som kan användas för att bättre kunna kravställa förebyggande åtgärder och bättre kunna leda verksamheten i tillfälle av händelse. En annan viktig

aspekt som lyfts fram kopplat till kursdeltagande är att *”Deltagande i formella utbildningar är också ett sätt att skapa en egen trovärdighet när jag för dialog med ledningen kring vilka åtgärder som behövs. Så när jag säger vi behöver investera X för att skapa Y så vet mina chefer att jag är utbildad och har nära kontakt med expertmyndigheter vilket gör att jag blir mindre ifrågasatt.”*

En annan av de intervjuade blev tillfrågad/utvald att gå kursen. Individen arbetar med utbildning inom säkerhet och industriella informations- och styrsystem inom sin organisation och efter individens deltagande har organisationen skickat många ytterligare deltagare till kursen och intervjupersonen uttrycker att de är ”*på hugget*” för att skicka fler. SIK- kursen gav däremot inte individen något direkt nytt relaterat till medvetenhet.

En intervjuperson som är verksam inom utbildningsområdet gick kursen på eget initiativ *”för att se hur FOI/MSB sköter utbildningen”*, vilka verktyg som användes och hur kursen förhåller sig till andra kurser. Syftet med kursdeltagandet var alltså inte att få ny kunskap, och kursen beskrivs heller i princip inte ha bidragit kunskapsmässigt men att det var intressant att diskutera med andra kursdeltagare. *”Inte i form av en aha-upplevelse. Jag var redan övertygad om att man behöver ta tag i saker*” men att kursen ändå gav *”Lite bekräftelse att det är viktigt”*.

En annan intervjuperson, som är den enda av de intervjuade som deltagit i ett kurstillfälle dedikerat till en enskild organisation, dvs. som gått kursen samtidigt som många kollegor, lyfter i sammanhanget fram att ju längre och djupare man jobbat med systemen, desto mer bekväm blir man kanske i sitt sammanhang, och menar att de flesta av deltagarna har fått ett lite annat tänk efter kursen. Problem och störningar som man tror sig veta vad de är, som ger ett likande symptom, tänker man kring på ett lite annat sätt. Bakgrunden till kursdeltagandet var *”önskemål från vår chef, som fått det högre uppifrån att vi skulle gå kursen”*. För egen del menade den intervjuade att kursen *”Gav ganska mycket.” ”Jobbat en del med detta de senaste året, för min del gav det andra tankesätt, andra infallsvinklar och framförallt, något som man i och för sig redan visste, men nu fick svart på vitt, hur mycket elände det finns därute som man behöver hålla ögonen på.”*

En av de intervjuade deltog på anmodan av sin chef, vid ett av de första tillfällena då I4S (ICS-CDX) gavs. Denne menade att kursinnehållet presenterades som ”*säkerhet kring industriella kontrollsystem utifrån IT-säkerhet*” men att den snarare handlade om incidenthantering kring att hitta attacker. Att kursens målgrupp/innehåll inte var tillräckligt tydligt beskriven fick under kursen konsekvensen att beroende på vilka kursdeltagarna var och vilka förkunskaper de hade så tog kursens aktiviteter olika riktning. De erfarenheter som kursdeltagarna kunde dra från kursen var väldig olika och avhängiga de aktiviteter som deltagarna råkade ta del av, vilket beskrivs som negativt. Organisationen ser nu en viss fara med att låta t.ex. driftingenjörer inom underhåll gå kursen, då de inte bedöms ha den kompetensnivå som behövs för ett givande kursdeltagande. Den intervjuade framförde också att kursens scenario var rätt enkelt (en avgränsad fabrik) och att

en insikt från den incidentlikande övningen är att kursdeltagare från andra organisationer har olika syn på vad som är vad och hur man felsöker.

D.2.2.4 Många olika generella effekter av kurserna – mest återkommande framförs höjd medvetenhet, men även att de lett till attitydförändringar och fungerar som en länk mellan IT/OT (effekter på nivå 1-3)

Utifrån de intervjuades olika motiv att gå kursen leder deras eget kursdeltagande till olika påverkan, olika följdeffekter där vi inte har tolkat det som att någon effekt rör nivå 4, dvs. effekt på säkerhetsarbetet i organisationen.

- En effekt som beskrivs är kopplad till ”bilden av kursen i sig” som i ett nästa steg påverkar vilka medarbetare som organisationen vill skicka som kursdeltagare och även påverkar hur NCS3-kurserna ses och prioriteras i förhållande till andra kurser och kompetenshöjande aktiviteter.
- En effekt som beskrivs är att kurserna i sig är ett nätverkstillfälle som ger möjlighet till intressanta diskussioner.
- En effekt, även om kurserna av de intervjuade inte uppfattas som en ”aha-upplevelse”, är beskrivningen som att kurserna var ”*Lite bekräftelse att det är viktigt*”.
- En effekt som beskrivs, även om man arbetat inom området det senaste åren, är att kurserna kunna ge andra tankesätt, andra infallsvinklar och framförallt, något som man i och för sig redan visste, men nu fick svart på vitt, hur mycket elände det finns därute som man behöver hålla ögonen på.
- En effekt som också beskrivs är också att kurserna gav kunskap, att kurserna gav en teknisk inblick i hur attacker kan genomföras och upptäckas samt exempel på verktyg som kan användas för att bättre kunna kravställa förebyggande åtgärder och leda verksamheten i tillfälle av händelse.

Flera av de intervjuade är också chefer som, förutom att ha gått en eller flera av NSC3-kurserna själva, även skickat flera medarbetare till kurser. Så förutom sin egen bild av vad kursdeltagandet gav dem, kan intervjupersonen beskriva vilka resultat de tolkar att kursdeltagande gett deras medarbetare. Chefer kan också resonera om/hur utfallet av att skicka medarbetare på kurser förhåller sig till anledningen till att de skickade medarbetarna på kurser.

Cheferna berättar att för de medarbetare som de skickat på kursera har kurserna främst fungerat medvetandehöjande. *”Kursen skapar medvetenhet till de som kursen är riktad till.”* Det utrycks också en övertygelse om att denna ”medvetandehöjning” kommer ge genomslag. *”Kommer tänka på detta vid en*

upphandling, kommer tänka på detta kopplat till åtgärder. Åtgärder är dock slutligen en resursfråga, avhängigt budget och ledningsnivå."

Något som också lyfts fram är att kursdeltagandet föranlett vad som framstår som en korttidseffekt, att frågorna hamnat i fokus och att de anses viktigt, att de får attention, lyfts fram. Kopplat till detta lyfts även att kursdeltagande ger mer råg i ryggen att driva frågorna i den egna organisationen, ger en ytterligare bekräftelse på att området är viktigt. Korttidseffekt kan självklart vara nog så viktig för att driva på åtgärder, dock lyfts inga sådan direkta korttidseffekter fram under intervjuerna.

Ytterligare effekter av andra medarbetares kursdeltagande, som är mer eller mindre övergående, är exempel som vittar om att man som ansvarig inom säkerhetsområdet fått lite mer frågor och bemöts av mer intresse kopplat till sin roll. En intervjurespondent lyfter att medarbetares deltagande vid ett kurstillfälle föranledde gemensamma möten om säkerhetsfrågor efter kursen och intervjupersonen är inte helt säker på att detta annars blivit av. Samtidigt vittnar intervjupersonen om andra kollegors inställning efter kursdeltagandet: *"Det här var ju intressant, men vad har jag för nytta av det?"* och uttrycker att det är *"synd att man inte triggade mer på vilka otrevliga möjligheter det finns att komma in i systemen."* Intervjupersonen tangerar också en mer direkt effekt av kursen som möjligen är på nivå 4 *"Vi har försökt strama åt systemen ytterligare – mer än vad vi haft tanken på att göra innan kursen."* Vad denna åtstramning exakt innebar var inte en fråga som fördjupades under intervjun.

Även något som framstår som en mer långtidseffekt av andra medarbetares kursdeltagande lyfts fram, intervjupersonens observation av att medarbetarnas kursdeltagande innebar en märkbar attitydskillnad, vilket vi tolkar som en nivå 3-effekt, eftersom en medarbetares attitydförändring manifesteras i ett beteende om chefen kan observera det. Chefens observation beskrivs utifrån det arbete som gjorts inom organisationen med att trycka ut/pusha information om regelverk, krav i upphandlingar osv., brister som redan identifierats som utbildningsbehov av säkerhetsansvariga, men likväl inte var information som efterfrågades generellt ute i organisationen. Kursen beskrivs som att den medförde *"markant skillnad"* efter att medarbetare gått kursen. Efter kursdeltagandet *"efterfrågades instruktioner, rutiner, det etablerades en helt annan kontakt*" och att uppfattningen hos organisationens medarbetare som gått kursen var att *"det verkar som andra hade det, vi har det inte. Istället för att vi pushade ut, så blev det en efterfrågan på många saker."* Kursen beskrivs som att den *"slår mot målgruppen som jobbar praktiskt med dessa frågor, att organisationen inte ur ett beslutsperspektiv fick det lättare att fatta beslut, men att det efter kursen fanns medvetna personer i systemet som inte tillät vissa genvägar, inte tillät vissa passager."* Innan kursdeltagandet uppmärksammades inte konsekvenserna, medarbetarna var inte medvetna om sina handlingar på samma sätt tidigare.

Ett annat resultat, eller effekt, som lyfts fram är att kursen länkar samman två tidigare separata säkerhetsdiscipliner (IT och OT) och för att vara framgångsrik inom området behöver man förstå dem båda. Noterbart är att detta resultat av kursen endast lyfts fram från myndighetshåll i intervjuerna.

D.2.2.5 Kurserna bekräftade redan kända behov av åtgärder

Även om åtgärder som kan tolkas som att de har att göra med den organisatoriska nivån beskrivits i något fall under intervjuerna, *”Vi har försökt strama åt systemen ytterligare – mer än vad vi haft tanken på att göra innan kursen.”* är bilden från intervjuerna att kursen snarare bekräftade åtgärdsbehov som redan fanns på radarn. På kursen togs saker upp *”som vi saknade då och som vi saknar nu”*. Kursen bekräftade *”att vissa av våra åtgärdsplaner var väldigt rätt”*.

Återigen behöver uttalanden om att kursen redan bekräftade kända behov av åtgärder förstås mot bakgrund av att de intervjuade representerar stora organisationer som har funktioner dedikerade mot säkerhetsarbete inom industriella informations- och styrsystem.

D.2.2.6 Ledningsnivån uttrycker att det är en fördel för att nå påverkan på det interna säkerhetsarbetet att flera individer från en organisation går kurserna medan denna fördel inte alla gånger lyfts fram hos medarbetarna

Återigen behöver intervjusvaren förstås mot bakgrund av att de intervjuade personerna representerar stora organisationer, där det även internt inom organisationen kan finnas olika kulturer och även på många andra sätt olika förutsättningar. En intervjurespondent från en stor organisation där många medarbetare deltagit vid kursen uttryckte *”Har inte hör något från andra medarbetare […] kopplat till att de gått kursen.”* medan en annan intervjurespondent från samma organisation i sin roll upplevde ett större intresse från medarbetare som gått kursen.

Logiken kopplat till frågan ”Tycker du att antalet kursdeltagare från en och samma organisation spelar roll för vilken påverkan som det har på det interna säkerhetsarbetet?” motiveras med följande *”Ja när det varit 2-3 deltagare som därmed kan diskutera och stötta varandra så börjar det ha effekt. En ensam deltagare blir oftast inte tillräckligt uppmärksammad och stark för att genomdriva några större förändringar. Dock behöver de inte gå vid samma tillfälle.”* Det skrivs som *”Bra med minst två personer från samma organisation så man kan diskutera sin hemmamiljö med andra…”.* Det lyfts också fram som positivt med ett kurstillfälle som är dedikerat till en organisation – *” vi jobbade med samma system så vi kunde prata på ett annat sätt om potentiella faror just i våra system”* samtidigt som det lyfts fram att det är *”också viktigt att diskutera med andra organisationer.”*

D.2.3 Effekter av kursverksamheten vid NCS3 enligt enkätsvaren

Responsen om kursverksamheten som återges i enkätsvaren är översvallande positiv. Kurserna har otvivelaktigt upplevts som att den påverkade medvetenheten och väckt nya funderingar kring risker, hot och andra säkerhetsfrågor hos kursdeltagarna. Kursdeltagarna vittnar många år efter avslutat kursdeltagande om just detta. SIK-kursen beskrivs t.ex. som en ”*övergripande väckarklocka*”. Att kursdeltagarna minns och återger kursmoment i detalj kan också tolkas som att kurserna gav mer än information som bara fladdrade förbi.

Enkätsvaren ger exempel på effekter av kursdeltagande hos organisationer som skickat en eller två deltagare till kurserna. I enkätsvaren lyfts det tydligt fram att orsakerna till effekterna inte enbart kan isoleras till kursdeltagande, utan vad som händer efter en kurs beror i stor utsträckning på andra faktorer. I ett svar skrivs ”*Jag ska försöka återge vad detta [kursdeltagandet] givit dock finns många fler aspekter till varför vi gjort de förändringar vi har*.” Med vetskapen och förförståelsen om att kursen inte är den enda faktorn som ligger bakom förändringarna, anges dock i enkätsvaren flera exempel på specifika effekter som kurserna har fått inom organisationen, förutom att de allmänt påverkat medvetenheten och säkerhetstänket hos kursdeltagarna. Vi redovisar här de svar kring mer specifika effekter som enkätrespondenterna angett på frågan ”Har ditt kursdeltagande påverkat ert arbete med säkerhet på din arbetsplats? Om ja, beskriv gärna på vilket sätt och varför. Om nej, beskriv gärna varför.”

”Ja, vi tillåter inte vilka vidlyftiga kommunikationslösningar som helst.”

”Ja: Kursen belyste vissa risker man kanske tidigare missat att ha med i beräkningen. Försöker även geografiskt skilja på huvudsystem och backupsystem.”

”Vi har gjort en analys av vår sårbarhet med särskild uppmärksamhet på driftstödsystem.”

”Ja, jag upplever att förståelsen, för att stärka skyddet kring styrsystemen, har ökat. Det är sällan eller aldrig någon som ifrågasätter varför man måste ge avkall på funktionalitet till förmån för säkerhet. Jag får större trovärdighet i de ökade kraven, när jag kan hänvisa till denna kurs och inte minst att den hållits av FOI/MBS. Jag själv har fått en ökad/annorlunda uppfattning om hur hotet ser ut och framförallt vilka som utgör ett hot. Den största lärdomen för mej var att man inte behöver vara en avancerad hacker med genial kunskap om datorer och system för att vara ett hot, p.g.a. det faktum att verktyg och metoder finns färdiga på nätet.”

”Medvetenheten för hur vi skulle säkra upp nätverket med autentisering, utbildning i informationssäkerhet till hela personalgruppen, ökad separering av Scadan från övriga servrar, minskad åtkomst generellt sätt etc.”

”Internt gav kursen ledningen inspiration till ett säkerhetstänk och jag har fått hålla flera föredrag för våra anställda bland annat om det kursen handlade om. Detta har gjort att vi har infört specifik hårdvara för att säkra upp lagring”.

Enkätsvaren indikerar att kursen är en del i att orsaka efterdyningar bortom individens, kursdeltagares, ökade medvetenhet eller förändrade beteende.

Enkätsvaren visar också på exempel där kursdeltagandet inte gav effekt på kursdeltagarens arbetsplats, men däremot en spridningseffekt genom att kursdeltagaren i sitt arbete mot andra aktörer tagit med sig insikter från kursen. *”Systemens sårbarhet och vår egen naivitet i frågan är bra input i mitt säkerhetsarbete bland mina kunder (ej direkt med IT- eller scada säkerhet)”.*

Enkätsvaren ger också exempel på att en kursdeltagare sprider erfarenheter in house genom att strukturerat, genom föredrag, berätta för kollegor.

Ett annat exempel på en möjlig effekt på organisatorisk nivå anges i ett annat enkätsvar.

”Det har givit mig ett högre säkerhetsmedvetande, och dessutom en bättre förståelse kring uppsäkring av datornätverk både trådade och trådlösa. […] Samt även ha en förståelse när jag kommer i kontakt med it-avd hos kunder när de påpekar potentiella risker i lösningen vi presenterar. ”

Att de krav som användarna ställer kopplat till de risker som användarna ser möter en förståelse från leverantörshåll, skulle i förlängningen kunna ha spin-off effekten att leverantören i andra sammanhang för in/säljer som förslag motsvarande säkerhetslösningar till andra användare som från början hade en lägre medvetenhet om potentiella risker.

D.3 Externa påverkansfaktorer för arbetet med säkerhet

Både i intervjuerna och i enkäten efterfrågade vi vilka externa faktorer som respondenterna såg som viktigast för utvecklingen av säkerhetsarbetet vid sin arbetsplats. Som exempel på externa faktorer listade vi incidenter, förändrad hot- och riskbild, teknikutveckling, förändrade krav från externa aktörer, samverkan med tjänsteleverantörer och kompetenshöjande insatser som utbildningar och övningar[34]. I detta avsnitt redovisar vi hur respondenterna resonerade kring dessa påverkansfaktorer.

[34] Dessa faktorer utgör på ingalunda sätt någon komplett uppsättning påverkansfaktorer, utan är några exempel som vi fångat upp bland annat utifrån MSB:s Vägledning till ökad säkerhet i industriella informations- och styrsystem.

D.3.1 Intervjusvar

Vilka faktorer som de intervjuade väljer att lyft fram som viktigast för utvecklingen av säkerhetsarbetet kretsar i stort kring två områden, en ökad allmän medvetenhet om säkerhetsrisker i industriella informations- och styrsystem samt krav från externa aktörer. En ökad medvetenhet nämns av så gott som samtliga intervjuade. Ökad medvetenhet är dock ett brett begrepp och bygger på flera av de faktorer som vi listade som exempel, som kännedom om incidenter, förändrad hot- och riskbild, teknikutveckling mm. Flera av respondenterna påpekar att säkerhetsmedvetenheten på ledningsnivå har ökat de senaste åren. I en del fall kanske inte så mycket som man hoppats på. Som en av de intervjuade uttryckte *”Funktionella krav går fortfarande före säkerhetskrav. Förståelsen för att säkerhet inte är något som man kan lägga på som plåster efteråt, utan att det måste vara med från början, saknas fortfarande. Men fler har blivit medvetna om att det inte räcker.”* I andra organisationer verkar medvetenhetsökningen har varit större, som en annan av de intervjuade beskrev *”För fem år sedan pratade man inte alls om det inom organisationen. För tre år sedan pratade inte ledningen om IT-säkerhet. Numera är det uppe på bordet hos dem som styr pengarna”*. Relaterat till detta påpekar också två av de intervjuade att just pengar spelar en viktig roll för säkerhetsutvecklingen. Om inte ledningen kan se det ekonomiska värdet av säkerhetsrelaterade investeringar (i både personal och materiel) är det svårt att driva igenom någon förändring.

Utöver en ökad medvetenhet är det som ovan nämnts krav från externa aktörer som lyfts fram av nästan alla intervjuade som en viktig faktor för säkerhetsutveckling. Som en respondent beskriver *”Rätt formulerade regulativa krav ökar möjligheten att få igenom inköpsbeslut eftersom det finns sparbeting på allt som inte är krav.”* Som chef inom området får man helt enkelt bättre genomslag i organisationen när man har en reglering att luta sig mot. En respondent lyfter också en önskan om att MSB ska ställa hårdare krav inom området, framför allt när det handlar om samhällsviktiga funktioner. Samme respondent nämner också Tyskland som exempel som har en nationell lag för infrastrukturverksamheter som exempelvis deras transportsektor kan luta sig mot.

Andra faktorer som nämns av de intervjuade är teknikutveckling som clouding och outsourcing. Några respondenter tar upp betydelsen av inträffade incidenter. Dessa utgör bevis på att saker och ting faktiskt har inträffat och därmed också kan ske i framtiden. Problemet är att det är svårt att få underlag om verkliga händelser vilket gör att informella kontakter blir en viktig informationskälla.

D.3.2 Enkätsvar

Avseende de externa faktorer som lyfts fram som viktiga för utveckling av säkerhetsarbetet noterar enkätrespondenterna att dessa är väldigt många. Den röda tråden som dock går genom enkätsvaren är att i säkerhetsarbetet knyta an till

verkligheten, ta avstamp i faktiska händelser, risker och hot, vad andra har blivit utsatta för. Som en enkätrespondent skriver ”*Annars blir det lätt ”Det där händer ju inte här hos ”lilla” oss”*.”

En spaning som parallellt lyfts fram är att ”*den allmänna medvetandegraden för IP-säkerhet i industriella styrsystem har ökat på senare år. Detta sker bl.a. via media, med information om incidenter, även om väldigt mycket säkert mörkas. Det sker naturligtvis även p.g.a. den lokala organisationens enträgna arbete, där som sagt förståelsen är mycket lättare att få idag, än den var för 10-15 år sedan*.” Enkätsvaren visar på att även om medvetandegraden ökat så finns ett behov av ytterligare förståelse. Det finns med andra ord fortfarande ett glapp mellan nuvarande kunskapsnivå och den nivå som de insatta bedömer att andra internt inom organisationen och externt inom branschen bör ha. Fråga är dock vad är en rimlig medvetandenivå är? Och när påverkar det man vet det man gör?

Beställarkompetens är också en omvärldsfaktor som lyfts fram som viktig för utvecklingen av säkerhetsarbetet inom industriella informations- och styrsystem. Säkerhet har en prislapp, eller som en enkätrespondent uttrycker det, *”Som ni vet vinner alltid anbudsgivaren med lägst anbud, vilket gör att det inte finns utrymme för oss som leverantör att lägga extra krut på dessa delar om inte kravet specifikt ställs.”*

Statens roll som samordnande för kunskap, förutom en ren kravställande roll, lyfts också fram som en faktor bland externa faktorer. En respondent skriver *”Vi följer Cert väldigt nära och har byggt upp en modell som också har ett ISO-tänk med styrning, förebyggande insatser, avvikelsehantering etc. ”*

D.4 Förslag på vidareutveckling av kurskonceptet

Detta avsnitt presenterar förslag på vidareutveckling på kurskonceptet. Först presenteras förslag som framkommit under intervjuerna, därefter förslag från enkätsvaren och avslutningsvis följer rapportförfattarnas ytterligare förslag på förändringar utifrån helheten som vi uppfattat den under studien.

D.4.1 Intervjusvar

Medvetenhetshöjande kurs för ledningsnivå

Majoriteten av dem som vi intervjuat, både på chefs- och medarbetarnivå, uttrycker att det finns behov av att på högsta ledningsnivå öka medvetenheten kring IT-säkerhet generellt och säkerhetsfrågor kopplat till industriella informations- och styrsystem specifikt. Som en av respondenterna uttryckte det ”*ledningen är duktiga på sitt sätt men har inte förståelse för de problem och frågeställningar som vi har nere på golvet*”. En annan uttryckte på likande sätt att

”*om det saknas förståelse för att det krävs resurser och kompetens för informationssäkerhet generellt så går det inte heller att bedriva framgångsrikt arbete för att öka säkerheten i industriella informations- och styrsystem*”.

Ett sätt som lyfts fram i intervjuerna för att höja medvetenheten är att utforma någon form av kortare chefsutbildning. En sådan kurs måste vara betydligt kortare än nuvarande upplägg med SI3S och I4S, kanske maximalt tre timmar och gärna genomföras på plats ute i organisationerna. För att skapa intresse får de också likt SI3S och I4S gärna innehålla interaktiva moment.

Mer riktad inbjudan till kurstillfällen

En av de intervjuade, på chefsnivå, uttryckte en önskan om att inbjudan till kurserna skickades ut från MSB direkt till organisationerna, istället för via en annan aktör (i det här fallet SvK). En annan av de intervjuade menade att kursinbjudan ofta når informationssäkerhetsansvariga inom organisationer och att dessa också tar tillfället i akt att gå utbildningen. Informationssäkerhetsansvariga är, enligt respondenten, ofta redan kunniga inom området. Det är istället de som praktiskt arbetar med drift och underhåll av de industriella informations- och styrsystemen som behöver dessa grundläggande kurser om säkerhetsluckor i systemen, men den kategorin nås inte alltid av inbjudan.

Erbjud fler platser till SI3S och I4S

Det finns ett stort intresse inom organisationerna för att få en plats till SI3S och I4S samtidigt som platserna är starkt begränsat. Intresset överstiger med andra ord utbudet. Dessutom är utbudet av kommersiella motsvarigheter till dessa kurser få. Önskemålet från flera av de intervjuade är således att det erbjuds fler utbildningstillfällen.

Skippa sektorsindelning vid kurstillfällena

En av de intervjuade, på chefsnivå, ansåg att det finns fördelar med att bryta upp den sektorsindelning som ofta kurserna ofta har, det vill säga att ett kurstillfälle är riktat mot exempelvis enbart transportsektorn. Den största fördelen är möjligheten att dela erfarenheter mellan sektorer. Som den intervjuade uttryckte det är utmaningarna för dem som arbetar nära systemen ändå ”till 90 procent lika överallt”.

Gör kurserna mer verklighetsförankrade

Några av de intervjuade tog upp att kurserna, kanske framför allt I4S, inte är inriktad mot hur man arbetar med den tekniska driften i verkligheten. De exempel som används i kurserna anses exempelvis vara för akademiska, inte tillräckligt verklighetstrogna och därmed inte praktiskt tillämpbara i hemorganisationen. Dessutom använder inte alla samma tekniska utrustning i labbmiljön som i hemorganisationerna. Ett förslag som lyftes var möjligheten att, utanför ramarna

för kurserna, arbeta på distans mot IT-miljön vid FOI för att på så sätt skapa en bättre verklighetsförankring.

Modernisering av SI3S

SI3S haft ungefär samma innehåll sedan starten 2009 (då SIK) vilket innebär att vissa delar av kursen, som en av de intervjuade uttryckte det, kan moderniseras för att upplevas mer samtida. Exempelvis används incidentexempel som har flera år på nacken liksom mobiltelefoner som också kan kännas lite ålderstigna.

Målgruppsanpassa kursinnehållet avseende mediehantering

Många av deltagarna som går I4S kommer från stora organisationer med egna kommunikationsenheter. I händelse av en incident är det därför sällan som en enskild medarbetare behöver hantera media. En av de intervjuade uttryckte därför att kursmomentet om mediehantering tar fokus från de tekniska bitarna som är mer relevanta ur deltagarnas perspektiv. För mindre organisationer kan dock mediehanteringsavsnittet enligt respondenten vara givande.

Erbjud längre kurser för fördjupade kunskaper

Även om SI3S och I4S är tvådagarskurser lyfte en av de intervjuade kursdeltagarna önskemål om att, av pedagogiska skäl, göra SI3S något längre. Respondenten menade att det är mycket ny information att ta till sig och laborationerna handlade det mest om att utföra dessa genom att läsa instruktionerna innantill snarare än att sitta ner och ha möjlighet att själv fundera på olika lösningar. Man hann med andra ord inte ner på det djup som deltagaren hade önskat sig av kursen.

Stöd för att genomföra interna övningar

Som en av respondenterna på chefsnivå menade har övningar potential att ge mer än utbildningar då övningar handlar om att *göra* något, till skillnad mot en utbildning som ofta handlar mer om att sitta och ta emot. För att underlätta genomförandet av övningar skulle MSB kunna utarbeta scenarier som organisationerna kan använda sig av i genomförandet av interna övningar.

Erbjud lightversion av övning ute i organisationerna

Ett förslag som lyftes av en respondent på chefsnivå var möjligheten för NCS3 att erbjuda att genomföra en lightversion av en scenariobaseras kurs (övning) ute hos organisationer, exempelvis i samband med interna säkerhetsrelaterade event. På detta sätt kan övningen både göras mer verksamhetsnära och samtidigt nå fler deltagare inom organisationen.

D.4.2 Enkätsvar

Bättre balans mellan teori och praktik

Förslagen på hur kursen kan justeras för att öka dess effekt är fåtaliga, vilket kan tolkas som ett positivt omdöme kring kursens utformning och innehåll. I enkätsvaren lyfts dock exempel på hur kursen skulle kunna göras ännu mer skräddarsydd, förslag som kan vara viktiga att beakta. Förslagen rör balansen mellan teori och praktik under kursen, där de som inte arbetar praktiskt i vardagen efterfrågar en mer teoretisk kurs medan de som arbetar praktiskt efterfrågar mer praktik.

Kursmoment för att öka beställarkompetensen

Något som efterfrågas specifikt i enkätsvaren är kursmoment för att öka beställarkompetensen för att lättare kunna prata med konsulter och leverantörer.

D.4.3 Övriga förslag

Utöver det som respondenterna själva uttryckligen gett som förslag till vidareutveckling av kurskonceptet kan vi också utifrån det samlade intervju- och enkätunderlag se ett möjligt behov av följande:

- Inkludera ett pass mot slutet av kurserna som fångar upp tankar kring **vad** deltagarna kommer att ta med sig hem från kurserna till sina hemorganisationer. Ett sådant pass borde också inkludera förslag på **hur** deltagarna konkret kan arbeta för att förändra saker i sin hemorganisation. Ett sätt att överväga för att ytterligare tydliggöra målbilden med kursen, är att som kursmål inkludera överspridning av kunskaper och erfarenheter från kursdeltagande till sin egen organisation eller att helt enkelt införa ett kursmål som ännu tydligare handlar om att leda till utvecklad säkerhet i verksamheten. Ett av de fyra kursmålen för SIS3 är formulerade som ”kunna delta i arbetet med att förbättra och utveckla säkerheten i en organisations industriella informations- och styrsystem”. Kursmålet skulle kunna övervägas att ersättas t.ex. med ”förvärva förståelse och kännedom som bidrar till arbetet för förbättrad säkerhet i organisationers industriella informations- och styrsystem.
- Se över informationsmaterial om kurserna så att dessa är utformade på sådant sätt att organisationerna kan skicka de mest lämpade deltagarna och att deras förväntningar stämmer överens med kursinnehållet. För att kurserna ska uppnå avsedd verkan är det viktigt att det sker en bra matchning mellan kurs och deltagare, dvs. att deltagarna har en passande roll i organisationen och rätt förutsättningar att ta till sig de lärdomar som kurserna avser förmedla. Om kursdeltagarna inte har tillräckliga förkunskaper, eller inte ser nyttan med kursdeltagandet, kan de

organisatoriska effekterna naturligtvis utebli, oavsett hur väl utformad själva kursen än är. Samtidigt kan det vara så att också organisationerna ska kunna motivera sitt urval för kursdeltagande och uppmuntras eller uppmanas att vara tydligare kring vad de har för målbild med att skicka sina medarbetare på kurs.

- Flera av de intervjuade uttryckte att syftet med deras kursdeltagande var att ”kolla upp” hur kursen var. Om det är möjligt, kan ett förslag vara att samlade (några av) dessa engagerade individer vid tillfälle, för att omhänderta deras klokskap och erfarenheter samt djupare diskutera hur kursutbudet kan anpassas och utvecklas mot olika målgrupper.

- När det gäller antal deltagare som skickas per kurstillfälle uttrycker flera att det är bra/positivt att vara två eller fler deltagare från samma organisation så att kursdeltagarna kan diskutera med och stötta varandra efter kursen. Detta kan jämföras med att när organisationen skickar flera deltagare men vid olika tillfällen kan följden bli att medarbetarna inte är har kännedom om att även andra inom organisationen gått kursen. Vi förslår självfallet en fortsatt lyhördhet inför det behov kopplat till sitt kursdeltagande organisationerna uttrycker, men vill samtidigt lyfta fram att empirin pekar mot att konceptet att vara minst två personer från samma organisation vid ett kurstillfälle framhållits som uppskattat.

- Kursverksamhet är ett sätt att utveckla kompetensen inom området industriella informations- och styrsystem. Även om samtliga som intervjuats har tillhört ”de redan frälstas skara”, så visar enkäten som skickades till och besvarades av mindre organisationer att även icke-frälsa gått kursen, t.ex. mot bakgrund av att upplevelsen av kursen beskrivs som en ”övergripande väckarklocka”. Inriktningen för kursprogrammet som MSB tillhandahåller är central, där målet t.ex. främst kan vara att utgöra ett ”kunskapslyft” och nå effekt hos de organisationer där säkerhetstänket är mindre utvecklat eller främst kan vara att säkerställa att de samhällsviktiga verksamheter som bedöms högst prioriterade har en ”tillräcklig kunskapsnivå”. Det är viktiga övergripande diskussioner som inriktar vilka organisationer som får kursplatser, och på länge sikt är en del av instrumenten som styr utvecklingen av säkerhet inom industriella informations- och styrsystem.

D.6 Sammanfattande slutsatser om effekter på organisationsnivå

Intervju- och enkätsvaren vittnar om flera individrelaterade effekter av kursdeltagande

De svar som vi fått genom intervjuer och enkäter bekräftar bilden från de kursutvärderingar som genomförts i samband med kursavslut för SI3S och I4S, det vill säga att kurserna upplevs som omtyckta. Detta har tidigare beskrivits motsvara lägsta nivån, nivå 1, i Kirkpatricks modell för effektutvärdering av kurser. De forna kursdeltagarna beskriver att kurserna skapar medvetenhet på ett attraktivt sätt och att det finns en efterfrågan inom organisationerna att delta, kanske framför allt gällande SI3S som är den mer grundläggande kursen. SI3S beskrivs framför allt att den leder till höjd medvetenhet kring säkerhet inom industriella informations- och styrsystem, vilket vi tolkar motsvaras av nivå 2, dvs. att kunskap finns men inte uttrycks i handling. Andra följder av nivå 1- och 2-karaktär som kursdeltagande beskrivs leda till är att det varit en bekräftelse på att området är viktigt, gett en teknisk inblick samt även att kursdeltagandet fungerat som en ”övergripande väckarklocka”, en ögonöppnare för säkerhetsrisker inom området industriella informations- och styrsystem.

Det beskrivs också att kursdeltagandet lett till påverkan på beteenden och arbetssätt hos kursdeltagarna (motsvarande den näst högsta nivån, nivå 3) i form av attitydförändringar som tar sig uttryck i ett ökat intresse för, och efterfrågan av, information och kompetens kring säkerhetsfrågor.

Få indikationer på effekter på organisatorisk nivå

Studien har syftat till att undersöka motsvarande nivå 4 i Kirkpatrick modellen, dvs. vad kursen lett till för resultat i verksamheten. När vi ser till den påverkan på nivå 4 som beskrivs av respondenterna noterar vi en skillnad mellan intervjuer, vilka genomförts med individer från stora organisationer, och enkäter, som företrädesvis besvarats av kursdeltagare från mindre organisationer. Svaren indikerar att kursdeltagande haft praktisk genomslagskraft, motsvarande nivå 4, bland enkätrespondenterna till skillnad mot den påverkan som framkommit i intervjuunderlaget. Det är i sig inte förvånande då beslutsvägar generellt är kortare i en mindre organisation och att en enskild chef eller medarbetare kan förväntas få större genomslag i att omsätta sin kunskap till verkstad. Till del kan denna skillnad vara en konsekvens av att samtliga av de som intervjuats, dvs. representanterna för stora organisationer, arbetat inom området i många år och därför redan har en gedigen kunskap om säkerhet i industriella informations- och styrsystem. Flera av de intervjuade uttrycker dock att kursen bidragit med att uppdatera deras kunskaper (motsvarande nivå 2), samtidigt som flera också uttrycker att deras motiv för kursdeltagande var att sondera vad kursen handlar om snarare än att inhämta ny kunskap. Enkätsvaren ger exempel på specifik påverkan av SI3S för

nivå 4, som att geografiskt skilja på huvudsystem och backupsystem, att göra en analys av sin sårbarhet med särskild uppmärksamhet på driftstödsystem eller ökad separering av styrsystem från övriga servrar, samtidigt som svaren också är tydliga med att de bakomliggande orsakerna inte enbart kan isoleras till kursdeltagande, utan att händelseförloppet efter kursdeltagandet i stor utsträckning också beror på andra faktorer. Påverkan av SI3S beskrivs vid intervjuerna i generella termer kopplade till lägre effektnivåer, som ökad medvetenhet och attitydförändringar exempelvis. Komplexiteten i att härleda påverkan av en specifik kurs framstår också som mer invecklad för stora organisationer jämfört med mindre, men sammanfattningsvis, för större organisationer beskrivs alltså inga exempel på direkt verksamhetspåverkande åtgärder, nivå 4, kopplat till organisationens säkerhetsarbete som ett resultat av den kunskap och de erfarenheter som medarbetare tog med sig från kurser (SIS3/I4S).

Något som skulle kunna ses som effekt på nivå 4 är beskrivningen av att kursen fungerat som en länk mellan IT/OT. Vad detta innebär för konkreta effekter i praktiken har ingen av respondenterna uttryckt, och eftersom det handlar om ett synsätt är det kanske inte enkelt att klä i ord. Säkerhet inom industriella informations- och styrsystem länkar samman dessa tidigare separata säkerhetsdiscipliner och, som det beskrivs under en intervju, för att vara framgångsrik inom säkerhetsarbetet behövs en förståelse för dem båda finnas. Att förena två områden innebär kulturkrockar. NSC3-kurserna anses bidra till att överbrygga två olika synsätt på säkerhet. Respondenternas svar visar därmed också på en möjlig utmaning vid att ta fram en kurs som kopplar ihop IT/OT-området, eftersom det uttrycks väsentligt skilda uppfattningar av hur stort ansvar för säkerhetsarbetet som respektive område har.

Ett perspektiv från intervjuerna att lyfta fram är också att kunskap och erfarenheter från en kurs självfallet inte behöver manifesteras som nivå 4-effekter här och nu, utan kan ligga latent och gro för att nyttiggöras när ett möjligheternas fönster för att påverka verksamheten öppnas. Just perspektivet att det tar tid är tydligt hos de som arbetat under en längre period med en strukturerad utbildningsverksamhet och i det sammanhanget lyfts även att kunskapen behöver nå ”en kritisk” massa, att ett tillräckligt stort antal medarbetare är kunskapsbärare, för att påverka verksamheten (nivå 4).

Organisationernas olika förhållningssätt till kunskapsutveckling

Utifrån intervjusvaren har vi fått bilden av att det skiljer sig åt mellan organisationer i hur man arbetar med utbildningar och övningar inom ICS-området, från strukturerade utbildningsprogram till mer ad hoc-lösningar eller individstyrda lösningar. Det betyder också att motiven bland kursdeltagarna för att medverka vid en av NCS3:s kurser spretar, från att det sker på uppmaning av chefen att gå till att det sker efter eget val att söka upp utbildningstillfället för sin egen kompetensutveckling alternativt som utbildare för att se hur FOI/MSB håller kurser. Oavsett hur deltagarplatserna tillsätts vittnar intervjuerna om att kurserna

är eftertraktade och att efterfrågan upplevs som större än utbudet av kurstillfällen, detta samtidigt som de kommersiella kursalternativen är få.

Att utbildning och övning betraktas som centrala aktiviteter för att utveckla säkerhetsarbetet inom industriella informations- och styrsystem bekräftas av både intervju- och enkätsvar. Tilltron till att utbildning bidrar till bättre säkerhet är orubblig. NCS3:s kurser är efterfrågade. Samtidigt är det få av de intervjuade som uttrycker en klar vision, eller målbild, om vad kursdeltagande förväntas leda till för den egna organisationen. Det nämns vid något tillfälle att kursdeltagandet strukturerat har utvärderas och reflekteras kring. Intervjuerna indikerar att de organisationer där det finns en plan/struktur för utbildningsverksamheten med högre precision kan beskriva önskade effekter av kursen på organisatoriskt nivå jämfört med de organisationer där utbildningen sker mer ad hoc.

Ökad medvetenhet

Både intervju- och enkätrespondenterna vittnar också om att medvetenheten om risker och säkerhetsaspekter kopplade till industriella informations- och styrsystem generellt har förändrats de senaste åren, både bland medarbetare, på chefsnivå inom organisationerna och i samhället som helhet. Ökad medierapportering om inträffade händelser beskrivs som en av orsakerna. Även om medvetenheten ökat så anses det fortfarande finnas ett glapp mellan nuvarande och önskvärd kunskapsnivå, en utsaga som motiveras av att funktionella krav ofta prioriteras framför säkerhetskrav och följer logiken att med en annan kunskap (medvetenhet hos beslutsfattare) hade andra prioriteringar gjorts. Samtidigt lyfts avsaknaden av kunskapsunderlag som visar det ekonomiska värdet av säkerhetsrelaterade investeringar. I det avseendet lyfts krav från externa aktörer fram som en viktig faktor för förändringsbeslut, vilket i förlängningen innebär att kompetensnivån hos kravställande funktioner och organisationer är central.

Resultatens generaliserbarhet

De urval av organisationer som kontaktats, och från vilka dataunderlag samlats in genom intervjuer och enkäter, utgör bara en mindre andel av alla de organisationer som deltagit vid NCS3:s kursverksamhet. Vi kan med andra ord inte uttala oss om huruvida de effekter som beskrivits i intervjuer och enkäter även gäller för de organisationer som inte kontaktats. För att påstå att resultaten är generaliserbara hade studien behövt designas annorlunda. Resultaten visar dock på att kursverksamheten vid NCS3 har haft en påverkan inom området säkerhet i industriella informations- och styrsystem, både på individnivå och organisationsnivå för de organisationer som ingått i studien.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se