Kompetensbehov och kompetensförsörjning inom informationssäkerhet från ett samhällsperspektiv

2015

Författare

Rose-Mharie Åhlfeldt, Högskolan i Skövde
Annelie Andersén, Högskolan i Skövde
Nomie Eriksson, Högskolan i Skövde
Marcus Nohlberg, Högskolan i Skövde
Erik Bergström, Högskolan i Skövde
Simone Fischer Hübner, Karlstads Universitet

Kontakt

Rose-Mharie Åhlfeldt
rose-mharie.ahlfeldt@his.se
0500 - 44 83 28

HS-IIT-TR-15-001

HÖGSKOLAN I SKÖVDE

KARLSTADS UNIVERSITET

MSB Myndigheten för samhällsskydd och beredskap

Sammanfattning

På uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) har en studie genomförts med syftet att komplettera resultatet från en tidigare genomförd förstudie (Åhlfeldt m.fl., 2014) med en analys av kompetensförsörjning och kompetensbehov på informationssäkerhetsområdet från ett samhällsperspektiv. Arbetet har genomförts av forskare från två lärosäten, Högskolan i Skövde och Karlstad Universitet, samt inom tre forskningsdiscipliner: pedagogik, informationssäkerhet och företagsekonomi.

Uppdraget har varit att besvara följande frågeställningar:

- Vilka är kompetensbehoven för att ha en god och balanserad informationssäkerhet som bidrar till samhällets informationssäkerhet?
    - Samtida kompetensbehov (nuläget)
    - Framtida kompetensbehov
- Hur ska nödvändig kompetens erhållas och på vem ligger ansvaret?
- Utifrån ovanstående frågeställningar, vilka är de viktigaste framgångsfaktorerna?

Arbetet har genomförts i form av fokusgrupper med representanter från myndigheter och företag som har en nära verksamhetskoppling till samhällets informationssäkerhet och som är viktiga för att samhällets informationssäkerhet ska fungera.

Resultatet visar att det finns stora brister avseende informationssäkerhetskompetens på alla nivåer i samhället. Tre tydliga områden pekas ut 1) nationellt - ökat behov av starkare styrning och ledning samt kravställning 2) organisation - ökat behov av kompetens från ledning till medarbetare men med starkt fokus på kompetenshöjande åtgärder på ledningsnivå samt vid upphandling och 3) medborgarperspektivet där framförallt skolområdet lyfts fram som ett viktigt insatsområde för kompetenshöjande åtgärder.

För att uppnå nödvändig kompetens krävs utbildningsinsatser på alla ovan angivna områden. Dels utbildningar på akademisk nivå för informationssäkerhetsexperter men även övriga utbildningar inom t ex juridik och ekonomi. Även yrkesverksamma på organisationsnivå behöver riktade kompetenshöjande åtgärder som sätter informationssäkerhet i fokus utifrån organisationens verksamhetsbehov, allt ifrån ledningsnivå till medarbetarnivå.

Resultatet visar även att ansvaret för samhällets kompetensförsörjning för informationssäkerhet ligger även den på alla ovan nämnda tre områden men med tydlig betoning på nationell nivå. Här betonas behovet av nationella krav för att medvetandegöra och lyfta informationssäkerheten i samhällsviktig verksamhet för att nå så många medborgare som möjligt.

Förslag på framtida arbete avseende utveckling av metoder för framtida studier av kompetensförsörjningen pekar främst på metoder för att angripa bristen på helhetssyn samt kompetensförsörjning för management och medborgare.

Skövde februari 2015

Innehållsförteckning

Sammanfattning 2

1 Inledning 4

1.1 Syfte 4

1.2 Begreppsbeskrivning 4

1.2.1 Samhälleligt perspektiv 4

1.2.2 Kompetens 5

1.2.3 Informationssäkerhet 5

2 Genomförande 7

2.1 Forskningsansats 7

2.1.1 Fokusgrupper 7

2.1.2 Innehållsanalys 8

2.2 Avgränsning 8

2.3 Projektsammansättning 8

3 Resultat 10

3.1 Vilka är kompetensbehoven för att ha en god och balanserad informationssäkerhet som bidrar till samhällets informationssäkerhet? 10

3.1.1 Samtida kompetensbehov 10

3.1.2 Framtida kompetensbehov 11

3.1.3 Vilka roller har kompetensbehov? 13

3.1.4 Hur ska nödvändig kompetens erhållas? 14

3.2 Vilka är framgångsfaktorerna? 17

4 Diskussion och jämförande forskning 22

4.1 Samtida och framtida kompetensbehovsområden 22

4.1.1 Nationell nivå 23

4.1.2 Organisation 24

4.1.3 Allmänheten – medborgaren 25

5 Förslag på framtida arbete 27

Referenser 29

1 Inledning

Under perioden november 2013 till mars 2014 har en förstudie genomförts på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) med syfte att sammanställa forskningsresultat om kompetenshöjande åtgärder inom informationssäkerhetsområdet. Detta för att få fram dels faktiska möjligheter att öka kompetensen genom utbildningsinsatser för yrkesverksamma, dels vilka effekter som kan förväntas av dessa utbildningsinsatser (Åhlfeldt m fl., 2014). Resultatet därifrån visar att det finns behov av ytterligare forskning avseende kompetensbehov och effekter av utbildningsinsatser i organisationer.

Med syfte att komplettera resultatet från den tidigare studien har MSB utformat ett nytt uppdrag i form av en analys av kompetensförsörjning och kompetensbehov på informationssäkerhetsområdet från ett samhällsperspektiv. Analysen utgår från en övergripande samhällelig nivå och innefattar även ansvarsfördelning mellan stat och näringsliv mot bakgrund av organisationsbehov, marknadsvillkor och samhällskrav.

1.1 Syfte

Syftet med uppdraget är att analysera och redovisa dels det samhälleliga perspektivet av kompetensbehov och kompetensförsörjning på informationssäkerhetsområdet, dels övergripande jämföra resultatet med den tidigare förstudien om kompetenshöjande åtgärder inom informationssäkerhetsområdet.

Resultatet ska ge underlag till kommande utveckling av vetenskapliga metoder för framtidsstudier av kompetensförsörjning på informationssäkerhetsområdet.

Tre övergripande frågeställningar har tagits fram:

- Vilka är kompetensbehoven för att ha en god och balanserad informationssäkerhet som bidrar till samhället informationssäkerhet?
    - Samtida kompetensbehov (nuläget)
    - Framtida kompetensbehov
- Hur ska nödvändig kompetens erhållas och på vem ligger ansvaret?
- Utifrån ovanstående frågeställningar, vilka är de viktigaste framgångsfaktorerna?

1.2 Begreppsbeskrivning

Tre ledord har funnits med genomgående i projektet. För att skapa en samsyn kring de tre ledorden *samhälleligt perspektiv*, *kompetens* och *informationssäkerhet,* har dessa beskrivits för deltagarna i fokusgrupperna enligt följande:

1.2.1 Samhälleligt perspektiv

Samhällsperspektivet inom informationssäkerhetsområdet är enligt MSBs handlingsplan (MSB, 2012) mycket väsentligt och angeläget för alla. ”Samtliga aktörer i samhället ska ha relevanta kunskaper om informationssäkerhet och kunna känna tillit till information och dess hantering på

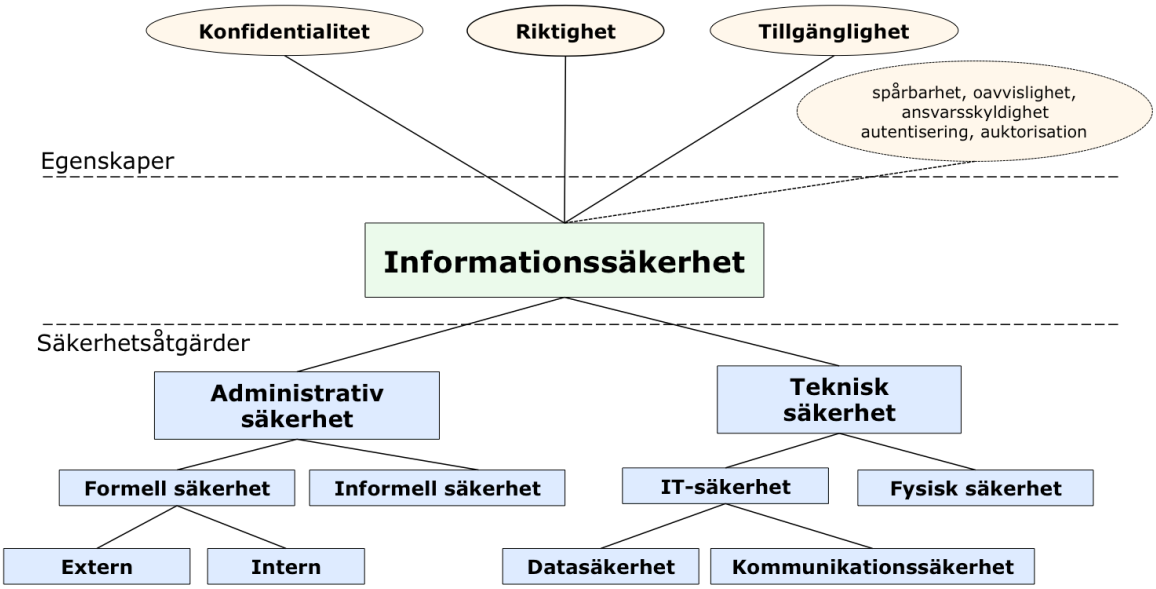
alla nivåer i samhället" (MSB, 2012). Föreliggande studie tar därför i beaktande aspekter av kompetensförsörjning inom informationssäkerhetsområdet på olika nivåer i samhället och fokuserar på de kompetenser som anses viktiga för samhällets informationssäkerhet som helhet och inte enbart en enskild organisations informationssäkerhet. Samhällsperspektivet anses viktigt att beakta då bortfall av information på olika nivåer kan leda till allvarliga samhällsstörningar. Utifrån ett samhällsperspektiv blir det därmed viktigt att öka riskmedvetenheten hos berörda.

1.2.2 Kompetens

Ser man till hur kompetensbegreppet definieras i tidigare forskning står det klart att det finns olika sätt att definiera begreppet. Oftast handlar det dock om beskrivningar av vilka kunskaper och färdigheter som behövs för att vara kompetent istället för en tydlig definition av begreppet kompetens. Det som gör begreppet kompetens svårdefinierat är just att det är kontextbundet och därför alltid måste ses i sitt sammanhang. Kompetensen beror exempelvis på individens placering, d.v.s. inom vilken verksamhet eller vilken roll personen har i verksamheten eller sammanhanget samt vilket problem det är som ska lösas. En person som är kompetent i en roll behöver inte nödvändigtvis vara det i en annan roll, eller i samma roll men på en annan plats etc. Kompetens är något som utvecklas genom att man lär sig och att man utför något. Kompetens handlar om att ha vissa kunskaper och färdigheter (egenskaper). Med kunskap menas faktakunskap, att veta något om något specifikt, medan färdigheter är förmågan att kunna tillämpa dessa faktakunskaper i praktiken. Kompetens handlar också om att ha ett visst förhållningssätt, d.v.s. vilka intentioner man har med sin kunskap, hur individen handlar etiskt, moraliskt och vad som prioriteras liksom vilka attityder individen visar upp i relation till kontexten.

1.2.3 Informationssäkerhet

Informationssäkerhet handlar generellt om säker informationshantering. Information är fundamentet i vårt informationssamhälle och därför värdefull för både organisationer och samhälle men även på individ/medborgarnivå. Enligt ISO/IEC 27000 (2014) definieras informationssäkerhet som "bevarande av informationens konfidentialitet, riktighet och tillgänglighet". Dessutom kan även spårbarhet, autenticitet, ansvarsskyldighet, oavvislighet och auktorisation inkluderas i informationssäkerhet. För att kunna uppnå dessa egenskaper hos informationen och därmed informationssäkerhet behövs ett systematiskt informations–säkerhetsarbete och på sätt öka kvaliteten och förtroendet för verksamheten. Informationssäkerhet omfattar därför administrativa säkerhetsåtgärder som rutiner med policy, riktlinjer, utbildning och uppföljning men även tekniska säkerhetsåtgärder. Det handlar därmed om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge värdefull information det skydd den behöver. Nedan visas en bild över hur informationssäkerhet relaterar till dess egenskaper samt vilka säkerhetsåtgärder som behöver tas i beaktande för att uppnå informationssäkerhet.



Figur 1 Informationssäkerhetsmodellen, modifierad från Åhlfeldt, 2007

2 Genomförande

Projektet genomfördes under perioden oktober 2014 till februari 2015. Nedan beskrivs den använda forskningsansatsen samt projektsammansättningen.

2.1 Forskningsansats

Forskningsansatsen som används är så kallad praktikforskning (Goldkuhl, 2011; Pain, 2011) vilket innebär en verksamhetsinriktad typ av kunskapsutveckling. Kunskapsintresset är inriktat mot hur lokala verksamheter och dessa olika resurser fungerar, vad som fungerar bra, vad som fungerar mindre bra och varför det fungerar som det gör. I praktikforskning arbetar man mot olika målgrupper. I detta projekt med ett samhälleligt perspektiv har därför målgruppen varit deltagare från myndigheter och företag som har en nära verksamhetskoppling till samhällets informationssäkerhet och som är viktiga för att samhällets informationssäkerhet ska fungera. Fokusgrupper valdes som specifik datainsamlingsmetod med deltagare från nämnda typer av myndigheter och företag.

2.1.1 Fokusgrupper

Fokusgrupper är en kvalitativ forskningsmetod där en grupp individer intervjuas avseende uppfattningar, åsikter, kunskaper och attityder kring en frågeställning eller ett tema (Stewar & Shamdasani, 2014; Kitzinger, 1995). Fokusgrupper som ansats anses lämplig då det finns behov av både bred och djup information från en viss målgrupp. Frågor ställs till gruppen vilken uppmuntras till diskussion. Fokusgrupper har den fördelen att den bidrar till fördjupad diskussion då tankar från en deltagare genererar idéer hos övriga deltagare som då bidrar till den gemensamma diskussionen. Nackdelen kan dock vara att det är svårt att generalisera resultatet då deltagarna oftast är få samt att det kan finnas deltagare som inte kommer till tals. Metoden anses dock intressant och användbar i sammanhang där ett område behöver belysas kvalitativt och så brett som möjligt. Metoden ger också ett större och bredare underlag än vad vanliga intervjuer anses göra.

Deltagarna i fokusgrupperna valdes ut från projektdeltagarnas och MSBs kontaktnät. Valet av deltagare var ett sannolikhetsurval, d v s ett riktat urval, utifrån organisation och personernas bakgrund och möjlighet att kunna uttala sig i området. I vissa fall deltog två personer från samma organisation men då med olika roller och erfarenheter från informations-säkerhetsarbetet. Tre fokusgrupper genomfördes under november månad. Totalt deltog 33 personer i fokusgrupperna från följande organisationer:

Rikspolisen	Cybercom Sweden AB	Dataföreningen Kompetens
Trafikverket	Göteborgs Universitet	Inera
Karlskrona kommun	Canal Digital	Vattenfall
Stockholms läns landsting	Jordbruksverket	Sollefteå kommun
Swedish Standards Institute	Västra Götalandsregionen	Svenska Bankföreningen
Com Hem	Försvarets Radioanstalt	Safeside

Karlstad universitet	Livsmedelsverket	Skatteverket
KnowIt	SJ	Combitech
Sveriges Kommuner och Landsting	Borlänge kommun	

Dessutom genomfördes ett fokusseminarium i samarbete med säkerhetsnätverket SIG Security. Vid detta seminarium deltog 14 personer. Innehållet i diskussionerna tecknades ned av deltagande forskare. Detta material låg sedan till grund för den fortsatta analysen.

2.1.2 Innehållsanalys

För att analysera insamlat material har en innehållsanalys genomförts. Innehållsanalys är en analysmetod som enligt Greneheimm m fl. (2004) delas in i olika steg där först hela texten genomläsas ett antal gånger för att fånga helheten. Därefter plockas meningar och fraser som anses relevanta för frågeställningarna ut, så kallade meningsbärande enheter. Dessa kondenseras i syfte att korta ned texten men ändå försöka behålla hela innehållet. Därefter kodas och grupperas de meningsbärande enheterna i syfte att återspegla huvudbudskapet. Slutligen formuleras teman eller områden, där det relevanta innehållet framgår.

Då forskarna i projektet kommer från olika kunskapsdiscipliner genomfördes tre olika innehållsanalyser utifrån perspektiven; informationsteknologi, pedagogik och management. Genom en gemensam analys sammanställdes därefter resultaten. Kapitel 3 redovisar det sammantagna resultatet från analyserna och utifrån de tre övergripande frågeställningarna, se avsnitt 1.1. I kapitel 4 diskuteras det sammantagna resultatet och jämförs med tidigare forskning inom området. Förslag på fortsatt arbete redovisas i kapitel 5.

2.2 Avgränsning

Den övergripande avgränsningen har varit att begränsa deltagande organisationer till det samhälleliga perspektivet. Därför valdes, som tidigare nämnts, deltagare ut från myndigheter och företag som har en nära verksamhetskoppling till samhällets informationssäkerhet och är viktiga för att samhällets informationssäkerhet ska fungera. Avgränsning har också skett i antalet medverkande organisationer och dess representanter utifrån projektets tidsramar och resurser. Rollsammansättningen från organisationernas representanter avgränsades i huvudsak till informationssäkerhetsansvariga eller liknande roller med kompetens och erfarenheter inom informationssäkerhet, t ex CISO inom organisationer med verksamhetskoppling till samhällets informationssäkerhet.

2.3 Projektsammansättning

Projektdeltagarna kommer dels från Högskolan i Skövde inom ämnesområdena informationsteknologi, pedagogik och företagsekonomi, dels från Karlstad Universitet inom ämnesområdet datavetenskap. Projektet har letts av Högskolan i Skövde.

Rose-Mharie Åhlfeldt Dr Informationsteknologi	Högskolan i Skövde	Projektledare
Annelie Andersén Dr Pedagogik	Högskolan i Skövde	
Nomie Eriksson Dr Företagsekonomi	Högskolan i Skövde	
Marcus Nohlberg Dr Informationsteknologi	Högskolan i Skövde	
Simone Fischer Hübner Prof. Datavetenskap	Karlstad Universitet	
Erik Bergström Forskarstuderande Informationsteknologi	Högskolan i Skövde	

Projektet har genomförts i samarbete med en kontaktperson hos uppdragsgivaren, MSB. Kontaktperson har varit behjälplig med lokaler och kontaktnät. MSB har även bistått med inbjudan till deltagarna i fokusgrupperna.

3 Resultat

Nedan beskrivs resultatet utifrån de tre huvudfrågeställningarna som presenterats i avsnitt 1.1. Identifierade teman/områden från den gemensamma innehållsanalysen är markerade i fet stil.

3.1 Vilka är kompetensbehoven för att ha en god och balanserad informationssäkerhet som bidrar till samhällets informations-säkerhet?

3.1.1 Samtida kompetensbehov

Utifrån dagens (samtida) situation framkommer enligt deltagarna att det finns ett tydligt generellt behov av ett **helhetstänk** kring informationssäkerhet i samhället. Därmed finns ett stort behov av kompetens på nationell nivå för att kunna styra informationssäkerheten. Detta saknas idag och många av deltagarna menar att det är en viktig faktor till den rådande situationen avseende brister i samhällets informationssäkerhet. För närvarande är ansvaret för informationssäkerhet nationellt fragmenterad och ansvaret ligger hos ett antal olika myndigheter och organisationer. Detta leder enligt deltagarna till att ingen har den övergripande bilden av informationssäkerhetsläget från ett samhällsperspektiv. I detta sammanhang nämns också behovet av ett centralt stödorgan som kan ge underlag och hjälpa till vid bedömningar, t ex en baseline för informationssäkerhet som skulle kunna användas för jämförelser. Deltagarna menar att det behövs kompetens på bred nivå, inte enbart informationssäkerhetsexperter med specialistkunskap utan det finns även andra roller i samhället som behöver ha informationssäkerhetskompetens utöver sin professionskompetens. I sammanhanget nämns även behovet av beroendekunskap d.v.s. kunskap kring vilka beroenden som existerar mellan olika tjänster och system både inom organisationen men framförallt mellan organisationen och det omgivande samhället. Det är viktigt att kunna förstå vad ett beslut kan innebära i kommande steg avseende informationssäkerhet internt (inom organisationen) och externt (mellan organisationer och samhället i stort).

Vidare menar deltagarna att det finns en risk med att dela upp ansvaret för informationssäkerhet på flera personer/roller, som ofta sker i mindre organisationer där det inte finns resurser för en heltidstjänst med informationssäkerhetsansvar. När ansvaret delas tonas prioriteringen ner efter som tiden för uppdragen oftast blir en mindre del i tjänsten.

En annan generell uppfattning i fokusgrupperna var att informationssäkerhet måste bli mer **verksamhetsdrivet** istället för att som idag till stor del vara incidentdrivet. När något inträffar lyfts informationssäkerhet direkt upp på agendan men när effekterna av incidenten lagt sig återgår allt till det vanliga igen utan några långsiktiga förbättringar i informations-säkerhetsarbetet. Det finns dessutom ett generellt behov hos organisationerna att förstå att det är informationen i sig som är det väsentliga när informationssäkerhet omnämns. Säker informationshantering måste följaktligen bli en naturlig del i den dagliga verksamheten. Därför behövs kompetens på strategisk, taktisk och operativ nivå i verksamheten. Kopplat till detta

framkommer även behovet av att visa på nyttoeffekterna av ett strukturerat informationssäkerhetsarbete.

Informationsklassificering, riskhantering och kontinuitetsplanering är några specifika områden inom informationssäkerhet där deltagarna ser ett stort behov av kompetens. För att bedöma och klassa sin information måste det finnas kunskaps om vilken information som hanteras i verksamheten. Därför måste det finnas kompetens och resurser för att hantera och förvalta processer i verksamheten. Dessutom saknas **nyckeltal** för att kunna jämföra informationssäkerheten i den egna verksamheten mot någon annan verksamhet eller mätnorm. Flera deltagare menar att man svävar i stor okunnighet om såväl vilken säkerhetsnivå den egna verksamheten befinner sig på som vilken säkerhetsnivå den bör befinna sig på för att klassas som tillräckligt informationssäker.

Det är allmänt känt att **säkerhetsmedvetenhet** hos individer alltid varit ett kritiskt område. Att informationssäkerhetskompetens ofta saknas är något som framkommer även i fokusgrupperna. Deltagarna påpekar att naiviteten hos individer generellt kring informationssäkerhetsfrågor är uppenbar. Därför behövs medvetenhet om informationssäkerhet och dess betydelse i verksamheten på alla nivåer, såväl inom organisationer som i samhället i stort. Här omnämns inte minst managementnivån. Det finns stora brister hos verksamhetsledningen om vad informationssäkerhet är, dess betydelse för att uppnå verksamhetsmålen, konsekvensen av bristande informationssäkerhetsarbete etc. Andra grupper som omnämns som särskilt viktiga då det gäller säkerhetsmedvetenheten är yngre och nyanställda. Medarbetare som anställs har direkt ett stort behov av kompetenshöjning menar deltagarna. Att medarbetarna behöver öka sin säkerhetsmedvetenhet är ett behov som funnits länge, men det är också viktigt, ur ett samhällsperspektiv, att förstå att bristen på medvetenhet hos medarbetarna är kopplat till bristen på kompetens inom området hos samhällets medborgare. Därför betonas även medborgarens behov av informationssäkerhetskompetens. Då det gäller medarbetarnas ålder är informationens betydelse i en verksamhet och dess konsekvens för verksamheten om skyddet av information missköts, inte uppenbart för unga människor. Detta gäller även om de i många avseenden kan ha en större datamognad än äldre medborgare menar deltagarna.

3.1.2 Framtida kompetensbehov

Med framtida kompetensbehov menas i detta sammanhang en tidsperiod på 10-15 år. Det visar sig vara svårt för deltagarna att se någon direkt skillnad på vad som är dagens behov och det framtida behovet eftersom dagens behov speglar även framtida behov. Att förstå vilka trender som kommer och konsekvenserna av detta inom en nära framtid är och förblir hypotetiskt. Fokusgrupperna gjorde dock ett försök att dels försöka sig på en trendspaning inom området samt försöka identifiera gapet mellan nuvarande och framtida behov. Nedan ges en beskrivning av trender och uppfattat gap avseende framtida kompetensbehov.

Kommande trender inom informationssäkerhetsområdet som omnämns av deltagarna är följande:

- **Organisatoriskt** kommer förhoppningsvis informationssäkerhet att lyftas till ledningsnivå istället för att som idag vanligtvis vara underordnat på IT-avdelningen.

- **Molntjänster, Internet of Things, Bring your own device (BYOD)** blir vanligare fenomen i organisationer och kommer ingå som en naturlig del i verksamheten vilket innebär att organisationerna i framtiden inte är bärare och ägare av den egna informationen på samma sätt som tidigare.

- **Komplexiteten** ökar, inte minst på grund av att informationen finns på så många olika platser enligt ovanstående punkt, vilket i sin tur innebär att det blir ännu svårare att fånga helheten framöver. Beroenden till andra tjänster och system ökar.

- **Cyberkrigsföring** blir mer aktuellt även i Sverige. Det finns en naivitet kring dessa frågor för närvarande och de tas inte riktigt på allvar. Detta gäller även i organisationer med samhällsviktig verksamhet.

Som en följd av ovan redovisade trender ser deltagarna följande kompetensbehov i framtiden.

- **Top management -** Störst behov ansåg deltagarna var att fylla gapet på ledningsnivå. Chefer har ofta en lätt undfallande attityd till informationssäkerhetsfrågor och antar att det rör sig mest om tekniska frågor.

- **Nationellt stöd** - Det måste till en kravställning nationellt kring informationssäkerhet. Deltagarna var tydliga med att betona behovet av ett tydligt mandat nationellt för att det ska få genomslag i organisationerna. Därför menar deltagarna - ställ krav!!! De nämner även att MSB som myndighet behöver få ett större mandat för att både föreskriva krav avseende informationssäkerhet men även att göra tillsyn och kontrollera efterlevnad. Även behovet av en informationssäkerhetsminister lyftes fram.

- **Upphandling** – Det behöver ställas högre kompetenskrav på de som ansvarar för upphandlingar och gör beställningarna. I lagen om upphandling (LOU) finns idag inga krav vad gäller informationssäkerhet. Det framkommer även brister avseende beställarkompetens på nationell nivå hos exempelvis kammarkollegiet.

- **Rekrytering** – De som ansvarar för rekryteringen anses också behöva ökad kompetens då de måste förstå organisationens informationssäkerhetsbehov för att kunna rekrytera rätt kompetens.

- **Risk- och verksamhetsutveckling** - Det är viktigt att vidga vyerna och våga titta på andra branschområden t ex försäkringsbranschen som har lång erfarenhet av riskhantering. Det finns också behov av beroendekunskap.

- **Informationsklassificering och kontinuitetsplanering** – Två betydelsefulla områden för informationssäkerhetsområdet enligt deltagarna där bristen på kompetens är tydlig men där även avsaknaden av metoder för att utföra informationsklassificering samt kontinuitetsplanering saknas eller är bristfällig.

- **Barn och ungdom** – Barn och ungdomar är i många avseende är väldigt naiva med sin hantering information menar deltagarna. Eftersom denna gruppering är morgondagens medarbetare finns det många fördelar med att satsa på kompetenshöjande åtgärder för denna målgrupp.

- **Äldre medborgare** – Äldre medborgare är en grupp som har och kommer fortsätta ha kompetensbehov framöver. Deltagarna menar att det är en demokratifråga att även inkludera äldre medborgare i kompetenshöjande åtgärder eftersom det är en viktig samhällelig aspekt.

3.1.3 Vilka roller har kompetensbehov?

Det är nästan omöjligt att diskutera behovet av informationssäkerhetskompetens utan att komma in på vilka roller i en verksamhet som berörs. Managementrollen har nämnts tidigare och den betonas starkt hos deltagarna. Ledningen måste ha en övergripande förståelse vad informationssäkerhet är. Många deltagare menar att ledningen fortfarande ser informationssäkerhet som en IT-fråga och är inte medvetna om sitt eget ansvarsområde avseende styrning och ledning. Det betyder dock inte att högsta ledningen måste förstå allt. Ekonomiområdet lyfts här fram som en jämförelse. Chefer har inte alltid kompetens inom ekonomi helt och fullt utan tar hjälp av medarbetare med ekonomikompetens, t ex controllers. Deltagarna menar att det borde kunna fungera på samma sätt inom informationssäkerhetsområdet.

Tabell 1 Roller och kompetensbehov

Roller	Behov av kompetens
Högsta ledning och övrig management	ansvarsskyldigheten, ökad medvetenhet kring informationssäkerhet och vad det står för, kunna visa med "hela handen", ledning och styrning av informationssäkerhet, säkerhetskultur
CIO, CISO, säkerhetschefer, informationssäkerhetsexperter	riskhantering, kunna koppla ihop ledning och teknik, verksamhetskunskap och teknikkunskap, pedagogik, uppföljning, kommunikation
IT-säkerhetsspecialister, tekniker	verksamhetskompetens, kravhantering, forensik, följa upp incidenter
Mellanchefer, verksamhetschefer	praktisk tillämpning av ledningssystem och hur man tillämpar föreskrifter etc. i sin egen verksamhet, ansvarsskyldighet
HR, personalansvariga	informationssäkerhet generellt, måste finnas med som en del i rekryteringen av personal
Jurister	informationssäkerhet generellt, beställarkompetens, verksamhetskompetens
Inköpsansvariga, kravställare	informationssäkerhet generellt, kravhantering avseende informationssäkerhet
Informationsägare, processägare, systemägare, systemförvaltare	ska kunna göra informationsklassificering

Roller	Behov av kompetens
Medarbetare, användare	värdet av information generellt (vad är skyddsvärt?), informationsklassificering, verksamhetens regelverk, säkerhetsmedvetenhet (attityd, säkerhetskultur)
Leverantörer	informationssäkerhet generellt, kravhantering
Journalister	informationssäkerhet generellt
Lärare	informationssäkerhet generellt, värdet av information, kunna förmedla informationssäkerhet till andra grupper
Medborgarna	säkerhetsmedvetenhet, ansvarsskyldighet, riskmedvetenhet

3.1.4 Hur ska nödvändig kompetens erhållas?

I fokusgrupperna gavs både exempel på kompetensutvecklingsinsatser och kompetens-överföringsstrategier i dag samt tänkbara kompetensutvecklingsstrategier i framtiden. De strategier som lyftes var såväl i form av formella och icke-formella utbildningsinsatser som mer svårfångat informellt lärande och kompetensöverföring. Nedan följer en redogörelse för de insatser som diskuterades under fokusgrupperna uppdelade i insatser på en samhällelig nivå och insatser på en organisatorisk nivå. Kompetensutveckling behöver dock inte bara vara att utbilda eller utveckla kompetensen hos en grupp medborgare eller anställda. Förutom kompetensutvecklingsinsatser pratas det på organisatorisk nivå om att rekrytera rätt kompetens är viktigt. Sett ur ett samhällsperspektiv är det dock svårt, för att inte säga omöjligt att rekrytera medborgare.

Formell nivå

Formell utbildning är standardiserade och jämförbara utbildningar, med antagningskrav, nivåer och formella mål och intyg/betyg på måluppfyllnad.

Samhällelig nivå

Den mesta av de formella kompetensutvecklingsinsatserna som föreslås och diskuteras i fokusgrupperna ligger på samhällsnivå eftersom det är utbildningar som vänder sig till eller är öppna för alla samhällsmedborgare såsom förskola, grundskola, gymnasium och olika högskoleutbildningar såsom utbildningar till lärare, systemvetare, polis och jurist. Det nämns som viktigt att informationssäkerhet kommer in i alla utbildningar, eller åtminstone fler utbildningar än enbart de inom teknikområdet. Framförallt betonas förskollärar- och lärarutbildningen eftersom förskola och skola är institutioner som når alla eller så gott som alla medborgare tidigt. Dessutom behöver förskollärare och lärare enligt fokusgruppsdeltagarna förstå varför barnen behöver lära sig informationssäkerhet och kritiskt tänkande i ett tidigt skede.

Även om deltagarna i fokusgrupperna är överens om att det är **viktigt med utbildning på en bred front och tidiga utbildningsinsatser** framkommer det inte så många konkreta förslag på

hur utbildningen ska utformas. I flera av fokusgrupperna jämförs dock lärandet av informationssäkerhet med lärandet av trafiksäkerhet. Att det i båda fallen är viktigt att starta med utbildning i informationssäkerhet tidigt, helst redan i förskolan och sedan öka kraven succesivt genom grund och gymnasieskolan. På så vis menar deltagarna att säkerhetsmedvetenheten kan öka långsiktigt och en medborgerlig säkerhetskultur skapas. Ett ytterligare exempel gällande hur informationssäkerhet kan komma in i skolan och som nämndes i flera av fokusgrupperna var att istället för sy- och träslöjd inrätta någon form av ”dataslöjd”.

Förutom att utbilda förskollärare och lärare så att de kan utbilda barn och unga nämns också att det är viktigt att utbilda de som tar fram skolmaterial så att informationssäkerhet finns med även här.

Organisatorisk nivå

Formella kompetensutvecklingsinsatser på organisatorisk nivå handlar om olika former av arbetsplatsutbildningar riktade till olika roller. Här pratas mycket vilken kompetens olika roller behöver (se 3.1.3), och mindre om hur denna kompetens ska erhållas. Till exempel nämns att cheferna behöver förståelse för informationssäkerheten, att det saknas informations-säkerhetskultur i ledningen, men inte så mycket om hur förståelsen ska skapas och informationssäkerhetskulturen byggas. Vad som dock nämns som viktigt är att utbildningarna inte ska vara generella, utan att de ska vara riktade just till de specifika rollerna. Här diskuteras också att det är viktigt att utbildningarna ligger på rätt nivå så att det varken blir för lätt eller för tungt och svårt, liksom att det finns tydliga kopplingar till arbetsuppgifter och att utbildningsmaterialet är anpassat till såväl arbetsuppgifter som ansvar. Att koppla utbildningen till någon form av krisövning är också något som nämns som ett förslag för att göra den mer **verklighetsförankrad.**

Icke-formell nivå

Det mesta av den kompetensutveckling som diskuteras under fokusgrupperna kan klassificeras som icke-formell. Icke-formellt lärande är medvetet lärande som äger rum vid sidan av de gängse systemen för allmän och yrkesinriktad utbildning och leder inte till något formaliserat utbildningsbevis (även om exempelvis intyg på genomgången kurs kan erhållas). Till skillnad från den formella nivån så sker den mesta kompetensutvecklingen på den icke-formella nivån på en organisatorisk nivå. Även om det också diskuteras hur sådana insatser skulle kunna göras mer allmänna och på ett sätt så att de når ut till alla i samhället. Ett exempel på detta är att man även här bör börja med barnen och att biblioteken kan vara en källa då det gäller att nå ut med kunskapen om informationssäkerhet.

Samhällelig nivå

Det framkommer i fokusgrupperna att det inte bara är specialister som behöver kompetens på informationssäkerhetsområdet, utan det är något som rör **alla medborgare**. En fråga som lyfts är dock hur man ska gå tillväga för att brygga över från specialist till medborgare så att alla får del av nödvändig kompetens. Här framkommer att en bristande kompetens hos många av dagens specialister är **kompetensen att lära ut och förmedla sina kunskaper.** Här saknas såväl pedagogik som drivande förebilder på området. **TV och annan media** nämns som möjliga

kanaler att nå ut och kommunicera informationssäkerhet till samhällsmedborgarna. Att använda sig av best practice/stimulerande målbilder och/eller skräckexempel eller iscensatta kriser nämns i flera fokusgrupper som möjliga sätt att förmedla budskapet. Det är viktigt att ha ett förhållningssätt som alla i samhället begriper och förstår.

Organisatorisk nivå

Förutom att lyfta fram utbildningar och workshops för olika roller inom organisationen som sätt att nå ut med kunskap om informationssäkerhet till medarbetarna diskuteras även ”**best practice”/stimulerande målbilder och/eller skräckexempel eller iscensatta kriser** som sätt att nå ut med budskapet om hur man bör handla informationssäkert i organisationen. Då det gäller kommunikationen nämns att det behövs utbildning av dem som jobbar på kommunikationsavdelningen både då det gäller informationssäkerhet men också hur de kan nå ut med information om informationssäkerhet till hela verksamheten. Speciellt nämns intranät och hur man kan använda detta som kanal för att **nå ut med information** när det gäller incidenthantering likväl som att förmedla ”best practice”.

Ytterligare ett exempel på en icke-formell kompetensutvecklingsinsats inom organisationen är **introduktion för nyanställda.** Inte heller här framkommer några direkta konkreta förslag på hur den ska gå till mer än att det är viktigt att informationssäkerhet förmedlas i dessa utbildningar och att man här kan gå runt på arbetsplatsen och se vad andra gör. Något som även nämns i andra sammanhang då det gäller kompetensöverföring såväl inom som mellan olika organisationer. Då det gäller nyrekrytering nämns det också vid en av fokusgrupperna att det är vanligt att rekrytera seniorer som redan har kompetens, men att det också är viktigt att kunna ta hand om dem som är nyexaminerade och att det borde finnas någon form av program för dem.

Deltagarna i fokusgrupperna betonar vikten av att lyfta fram och kommunicera befintliga **framgångsexempel.** Detta gäller både inom organisationer och nationellt. Tyvärr menar deltagarna att det saknas framgångsexempel där man kan visa rent praktiskt hur man gör i olika steg och stadier. Det framkommer också att det behövs tas fram råd och tips på hur man som organisation kan arbeta med att sprida informationssäkerhet inom organisationen. Här efterfrågas stöd i form av standardmallar som enkelt går att anpassa efter de egna regelverken och på ett sätt så att de egna medarbetarna förstår dem. Av fokusgrupperna framkommer också att det finns ett stort behov av **incitament** för säkerhet. Deltagarna menar att det måste kosta att ha dålig säkerhet och löna sig med god säkerhet.

För att avgöra vad som är god respektive dålig säkerhet nämns betydelsen av olika standarder, ratings och klassningar. Deltagarna menar att säkerhetsarbetet måste **standardiseras** så att det blir transparent för verksamheten. Det betyder inte att det enbart måste vara globala standarder som används utan standardisering kan ske på olika nivåer. Ledningssystem för informationssäkerhet (LIS) och standarderna ISO/IEC 27001 och 27002 omnämns dock som grundläggande standarder att utgå ifrån. Det behövs också olika listor för **rating och klassning** av exempelvis myndigheter och kommuner. Dessa listor driver enligt deltagarna på utvecklingen eftersom ingen vill vara ”sämst i klassen”.

Det anses också viktigt, oavsett utbildningsform, att ta fram material som lärare och andra utbildare kan använda sig av, liksom att utbildningarna ska bygga på **verksamhetsexempel eller liknande** som medarbetarna känner till. Genom att integrera informationssäkerheten i det dagliga arbetet blir det en naturlig del i verksamheten.

Informell nivå

Informellt lärande är en naturlig del av vardagslivet. I motsats till formellt och icke-formellt lärande är informellt lärande inte nödvändigtvis avsiktligt lärande och därför erkänns det ofta inte ens av individerna själva som något som bidrar till deras kunskaper och färdigheter. Informell kompetensutveckling är förmodligen den vanligaste formen av kompetensutveckling. Dock är informellt lärande svår att mäta eller ens uppfatta och således är det inget som diskuteras explicit i fokusgrupperna även om det ändå alltid finns närvarande i diskussionerna. Många av de exempel på insatser som redogjorts för på den icke-formella nivån (ovan) innehåller tankar om att individerna också ska lära sig informellt genom att exempelvis ta del av andra personers erfarenheter.

Annat som kommit upp under fokusgrupperna och som kan anses höra hemma på den informella nivån är bland annat vikten av **helhetstänk**, att det finns någon form av **informationssäkerhetskultur** i organisationen, eller för den delen samhället som helhet. Här handlar det inte bara om att förmedla och lära ut om risker och konsekvenser utan också att förmedla en **attityd**. Här betonas vikten av att ”prata säkerhet” och att ta fram nyttoeffekter för att långsiktigt förändra attityden till säker informationshantering. Ytterligare ett exempel är det faktum som flera personer nämner i samband med vikten av att lyfta skräckexempel och att dela med sig av andras misslyckanden är att det kan behövas en katastrof för att lyfta upp informationssäkerhet på agendan då informationssäkerheten inte är något man normalt tänker på så länge den fungerar.

Som nämnts innan framkommer det i flera av fokusgrupperna att det är viktigt att börja tidigt, reda i förskolan eller den tidiga skolåldern. En sådan formell utbildningsinsats tar dock tid innan den har nått ut till alla medborgare eftersom de flesta av oss lämnat skolåldern bakom oss. Dock kan en sådan insats om den görs på rätt sätt nå ut (informellt) till en bredare grupp i form av **barnens föräldrar** genom att dessa engageras i skolarbetet genom läxor och annat. Även TV och annan media där föräldrarna tittar tillsammans med sina barn nämns som vägar att nå flera samhällsgrupper på en gång. Deltagarna betonar också att för att kunna fånga helheten och beroenden till andra samhällstjänster måste **samverkan** mellan olika parter på alla nivåer förbättras.

3.2 Vilka är framgångsfaktorerna?

Nedanstående framgångsfaktorer har ordnats utifrån hur många av fokusgrupperna som har betonat framgångsfaktorn samt att några av framgångsområdena bygger på att det finns ett föregående område att bygga vidare på. Dessa framgångsfaktorer är inte beprövade utan ska ses mer som rekommendationer på vad som kan komma att bli framgångsfaktorer.

- **Bygg informationssäkerhet långsiktigt och hållbart - att förstå behovet av informationssäkerhet** - Kompetens inom informationssäkerhet måste byggas långsiktigt

och hållbart för att erhålla god säkerhetskultur. Här handlar det om att bygga upp en förståelse för informationssäkerhet allt från nybörjaren till experten, från medarbetaren till chefen etc. Alla som hanterar information på något sätt har ett ansvar och för alla med ansvar är det väsentligt att förstå informationssäkerheten. Principen att "någon annan" tar ansvar för detta fungerar inte.

Ett led i att bygga informationssäkerhet långsiktigt är vikten av att informationssäkerhetsfrågor kommer upp på olika mötens agenda och kontinuerligt diskuteras vad gäller ansvar och lösningar på uppkomna problem. Ett haveri är inte önskvärt men det är tydligt att när något kraftfullt inträffar i organisationen kommer informationssäkerheten direkt upp på agendan och informationssäkerheten skärps väsentligt. Därför måste det finnas en förståelse för hur informationssäkerhet finnas med som en naturlig del vid möten, internutbildningar eller liknande aktiviteter i den ordinarie verksamheten.

- **Inrikta och anpassa kompetensförsörjningen till olika målgrupper -** Informationssäkerhetsfrågor behöver komma i rätt "hierarkisk" ordning. Medarbetarna har visserligen ett stort behov av att förstå och ta till sig tänkandet kring informationssäkerhet men det saknas bärkraft om inte förståelsen först finns i chefsleden. När chefer förstår att de har ansvar för organisationens informationssäkerhet då ger det ringar på vattnet till övriga grupperingar i organisationen att känna tillit och ha förståelse för framtagna beslut och riktlinjer avseende skydd av säkerhet. Därefter behövs riktade insatser inom organisationen för respektive verksamhetsinriktning och roll för att få förståelse för hur en säker informationshantering ska uppnås.

- **Tänk risk -** Risktänkandet måste få ett större fokus genom att informationens behov av skydd måste kartläggas och beslutas samt att nivån på osäkerhet blir tydlig. Att inte alls tänka risk kan ses som ett "öppet mål". Risktänkandet behöver dock ske utifrån den nivå som informationens skydd ska prioriteras. Ett högt risktänkande blir kostsamt. Varje organisation måste därför själv välja vad som ska prioriteras när det gäller risk och hur mycket det får kosta i utbildning, olika säkerhetsåtgärder m.m. För en liten organisation kan det innebära inköp av vissa externa tjänster och utbildning av personal efter att ledningen gjort prioriteringar av vad som ska skyddas. För större organisationer kan det innebära att sätta upp hela avdelningar för att arbeta med riskhantering.

- **Ställ krav på informationssäkerhet i upphandlingar – kravspecifikationer -** Kompetens inom och krav på informationssäkerhet behövs vid upphandling av varor och tjänster. Ansvariga för upphandlingar av olika slag kan inte frikoppla frågorna om informationssäkerhet. Det måste framgå i kravspecifikationerna att informationssäkerhet har en framträdande position och ska drivas av ansvariga för upphandlingen. Därför behöver även de som är ansvariga för upphandling utbildning inom informationssäkerhet. Vid framtagandet av kravspecifikationen ska även ledningen vara med och definiera informationssäkerhetsnivån. Detta kan ske genom att antingen fastlägga informationssäkerhetskrav i form av regelverk eller att vara en aktiv deltagare.

- **Mät informationssäkerhet där så är möjligt -** Det som går att mäta bör mätas. Deltagarna menar att det man inte mäter det ser ingen. Det går lättare att diskutera informationssäkerhetsfrågor om man kan visa på mätetal. Det är ekonomin som styr trots allt. Kontinuerliga mätningar av ett och samma fenomen ger bra underlag. Vad som ska mätas varierar beroende på vad organisationer har för uppdrag och på informationens risknivå. I flera av de standarder och kvalitetssystem m.m. som erbjuds finns mätmetoder angivna och kan användas av organisationer i de fall där dessa mätpunkter är relevanta.

- **Ställ krav på utbildning -** Utbildning inom informationssäkerhet är självklart för experter inom området. Här handlar det inte enbart om tekniska utbildningar utan här måste akademin även ta ansvar för att se till att det finns möjlighet till utbildning för informationssäkerhetsansvariga på bred nivå. Det handlar då även om kompetenser inte enbart inom fackområdet utan även kompetenser som kommunikationsförmåga, verksamhetskunskaps, ledningsförmåga, etc. Som tidigare nämnts (se 3.1.4) måste informationssäkerhet även in i andra utbildningar som jurist-, ekonomiutbildningar etc. Utbildningsinsatserna kan antingen erbjudas som enstaka kurser i informationssäkerhet inom utbildningsprogram eller som genomgående strimmor i befintliga kurser. För att utbilda framtidens medarbetare i företag och organisationer behöver informationssäkerhetsfrågorna få plats i utbildningar på förskole-, grund- och gymnasienivå (se 3.1.4). Dessutom behövs kortare kurser till den bredare allmänheten eller som internutbildning till anställda i företag och organisationer. För att ovanstående ska kunna genomföras behövs en kravställning från nationell nivå t ex genom att skriva in kraven i föreskrifter, läroplaner etc.

- **Satsa på medborgaren – från barn till morgondagens anställda -** För att öka kompetensen för samhällets informationssäkerhet måste fokus riktas mot medborgaren. För att bygga hållbart och långsiktigt måste därför informationssäkerhet aktualiseras tidigt och då förslagsvis redan i förskolan och därefter på grund- och gymnasienivå med åldersanspassad utbildning. Även mycket unga använder idag nätbaserad information, sociala medier och liknande. Därför är det enligt deltagarna viktigt att redan tidigt bygga upp en medvetenhet kring värdet av både egen och andras information och hur den kan skyddas och hanteras på ett säkert sätt.

  Avseende de unga handlar problemen mer om att hantera information i sociala medier etc. Har skolan redan tidigt lärt de unga hur informationssäkerhet alltid måste vara med i hantering av information, blir det en naturlig progression i utbildningen att mer fördjupat lära ungdomar hur man handskas med information på ett säkert sätt och vad som kan hända om man inte gör detta.

  För den “vuxne” medborgaren som inte fått den tänkt kompetens i informationssäkerhet genom skolan krävs ytterligare utbildning i form av riktade insatser inom specifika områden. Det finns goda initiativ från t ex MSB men ytterligare kompetenshöjande åtgärder behövs. Detta måste vara ett långsiktigt arbete för att få till en mognad avseende informationssäkerhet för medborgaren.

- **Visa på framgångsrika exempel -** Ta fram lyckade exempel i form av positiva målbilder för att visa på hur man kan arbeta med kompetenshöjande åtgärder inom informationssäkerhet i en organisation. En av de deltagande myndigheterna lyfte fram ett sådant framgångsrikt exempel. Genom att använda en ISO-standard hade de arbetat igenom hela organisationen, från chefsleden via säkerhetspersonal till alla anställda. Informationssäkerhetsfrågor diskuterades på kontinuerliga internutbildningar och varje anställd, inkl. nyanställda, fick skriftligen ta del av vad som gällde för en säker informationshantering. Resultatet blev att en organisation som sedan flera år väl förtrogen med organisationens säkerhetsnivå och som bibehållits över tid.

  Positiva målbilder ska vara så enkla att de kan gälla för så många företag och organisationer som möjligt.

- **Använd social och kommunikativ kompetens för att sälja in informationssäkerhet -** Informationssäkerhet kan aldrig tvingas in bland medarbetarna i en organisation även om en organisation kan fatta beslut om vilken säkerhet och vilket skydd som måste finnas för informationen. Det handlar dock om att den enskilde medarbetaren måste förstå sin del i informationssäkerhetsarbetet, ta sitt ansvar och att hitta motivation att hantera informationen på ett säkert sätt. För att bygga upp en sådan säkerhetskultur i en organisation krävs enligt deltagarna att de som håller i informations-säkerhetsfrågorna har förmåga att kommunicera och motivera medarbetarna.

  I större organisationer finns även kommunikationsavdelningar eller kommunikatörer. Dessa avdelningar/personer kan användas för att vara behjälpliga i att paketera informationssäkerhetsfrågor på ett sätt så att det både attraherar och är lättillgängligt för de flesta. En kommunikationsavdelning kan med sin kompetens få fram korta och kärnfulla dokument med ett lättförståeligt språk till skillnad från den ofta fackspråkliga information som ofta kommer från informationssäkerhets- och/eller teknikpersonal.

- **Utarbeta förenklade standarder och regelverk -** Någon myndighet behöver utarbeta förenklingar av standarder och ett mer genomarbetat regelverk som också ger möjlighet till uppföljning. För att informationssäkerheten ska genomsyra organisationer behövs ett standardiserat sätt att arbeta. Istället för att organisationer ska utarbeta sina egna standarder, vilket är mycket tidskrävande, borde detta kunna göras mer effektivt genom att någon lämplig myndighet tar sig an detta arbete.

- **Ställ hårdare krav på kommuner -** Sveriges kommuner behöver få hårdare krav på sig för att upprätthålla en hög informationssäkerhet. Kommuner hanterar både värdefull och känslig information och informationssäkerhet är därför väsentlig för kommunerna själva men också ur ett samhällsperspektiv.

- **Samordna överlappande krav från myndigheter –** För att samordna alla överlappande krav behövs en instans som samordnar kraven som kommer från olika myndigheter i syfte att undvika dubbelhanteringen inte genererar någon nytta.

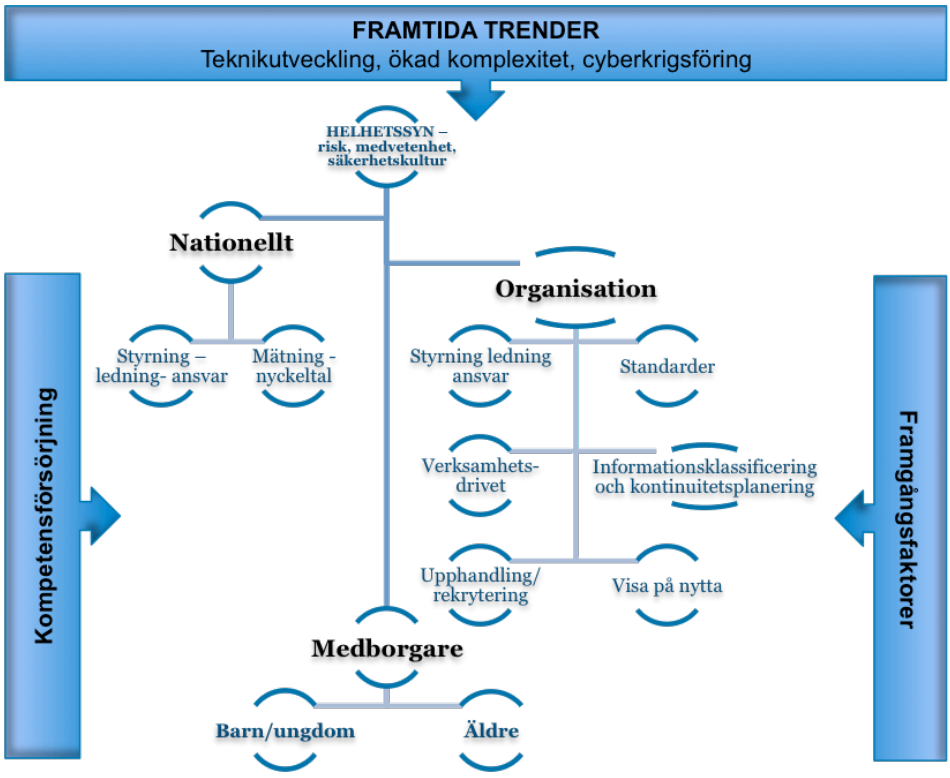
- **Tillsätt en informationssäkerhetsminister -** Tillsätt en informationssäkerhetsminister för att få en central instans som kan arbeta med frågorna övergripande. Detta tror deltagarna skulle leda till framgång för informationssäkerhetsområdet samt höja statusen på informationssäkerhetsfrågorna.

4 Diskussion och jämförande forskning

Nedan sammanfattas och diskuteras ovanstående resultatet samt jämförs i de delar som har bäring mot tidigare förstudie avseende effekter av utbildningsinsatser i forskningen.

4.1 Samtida och framtida kompetensbehovsområden

När ovanstående resultat analyseras framkommer vissa specifika områden tydligare än andra. Eftersom studien har ett samhällsperspektiv lyfts såväl det **nationella,** det **organisatoriska** som det **medborgerliga** behovet fram**.** Förutom att resultaten visar på generella kompetensbehov av allmänheten nämns också vikten av att höja kompetensen av informationssäkerhet för vissa specifika målgrupper i samhället som barn och ungdom samt den äldre generationen. Över detta finns en övergripande brist på **helhetssyn** och samordning av informationssäkerhet från ett samhällsperspektiv. Denna brist genomsyrar alla nivåer i samhället; nationellt, organisation och medborgare, se figur 2 som visar en översikt över framträdande teman från resultatet.



Figur 2: Översikt över framträdande teman från resultatet uppdelat i områden med utgångspunkt från de samtida och framtida kompetensbehoven.

4.1.1 Nationell nivå

Ansvarsområdet för informationssäkerhet är uppdelat nationellt vilket får till följd att brister inte bara noteras i samband med revisioner (Riksrevisionen, 2014) utan det påverkar även organisationer med en samhällsviktig verksamhet. Bristen på helhetssyn har en nära koppling till behovet av förbättrad styrning och ledning av informationssäkerhet. Detta gäller både inom organisationen vilket deltagarna ger uttryck för men från ett samhälleligt perspektiv även på nationell nivå. Avsaknaden av styrning och ledning på nationell nivå får konsekvenser i organisationerna vilket genererar osäkerhet för ledare i samhällsviktig verksamhet om vad som egentligen gäller. Kraven på nationell nivå upplevs spretiga och inte samstämmiga. Bristen på helhetssyn samt ledning och styrning stämmer även väl överens med Riksrevisionens rapport (Riksrevision, 2014) vars samlade slutsats är att arbetet med informationssäkerhet på en nationell nivå inte är ändamålsenlig och att det finns brister i styrning av informationssäkerhet nationellt. Orsaker till detta kan diskuteras men vad som framgår av resultaten i denna studie och som även bekräftas av både Riksrevisionen (2014) samt tidigare forskning är just bristen på kompetens inom informationssäkerhetsområdet och då framförallt med bäring på de som har ledningsansvar (Dutta och McCrohan, 2002).

Ett annat område som betonats starkt av deltagarna är vikten av nationell kravställning på informationssäkerhet för samhällsviktig verksamhet. Kraven på nationell nivå upplevs spretiga och inte samstämmiga. Dessutom anges kommuner som ett exempel på att kraven inte är jämställda. Kommunerna finns inte med i t.ex. föreskrifter där ett strukturerat säkerhetsarbete är ett krav. Anledningen till detta är att föreskrifterna ofta enbart riktar sig mot statliga myndigheter där nationella krav kan ställas. Kommunerna måste dock anses vara en viktig aktör i den samhällsviktiga verksamheten och därför bör nationella krav även gälla kommuner. Om kraven ställs kommer bristen på kompetens inom området framträda tydligare och därmed menar flera deltagare kommer medvetenheten kring behovet av informationssäkerhets-kompetens öka inom berörda discipliner och verksamhetsområden. Värt att notera i detta sammanhang är att deltagare från hälso- och sjukvårdsområdet betonade att trots att det finns tydliga krav inom hälso- och sjukvårdssektorn har inte informationssäkerheten fått önskat genomslag i större omfattning. Detta betyder dock inte att kravställningen är oviktig utan hjälper till att aktualisera och medvetandegöra informationssäkerheten.

Resultatet visar på en medvetenhet hos deltagarna avseende komplexiteten och svårigheterna med mätning. Trots detta utrycker de behov av olika former av nyckeltal. Det behövs ta fram nyckeltal på nationell nivå som sätter nivåer för informationssäkerhet. På det sättet skulle det gå att mäta säkerhetsnivåerna och även jämföra organisationer mellan varandra menar deltagarna. Ett exempel var att visa nyckeltalen i årsredovisningen. Frågan behöver ställas hur detta ska genomföras och vilka kompetenser som behövs för att ta fram mätetal som är relevanta för att jämföra informationssäkerheten på en generell nivå men som ändå är relevant för olika verksamhetsområden? Deltagarna menar att man kan börja med “redan lågt hängande frukter” vilket betyder att där det finns exempel på nyckeltal att börja med, så börja, och bygg sedan ut metoderna efter hand. Det behövs mer forskning kring metodutveckling avseende mätning om den ska ha någon legitimitet i längden.

Sett ur ett samhällsperspektiv framkommer att stort ansvar ligger på den nationella nivån för framtida kompetensförsörjning. Det handlar om att sätta ramarna för samhällets informationssäkerhet i stort.

4.1.2 Organisation

Även på organisationsnivå betonas bristen på kompetens avseende ledning, styrning och ansvar. Flera av dessa brister har nära koppling till det som diskuterats på den nationella nivån. Vad gäller ansvarsfrågan betonas att förståelsen för informationssäkerhet innebär att alla inom organisationen har ansvar för sin information, d.v.s. alla som hanterar information, kan inte lämna över ansvaret till någon mer teknisk inriktad funktion, utan behöver förstå det egna ansvaret för informationen. Här nämns exempel på chefer som ju längre ifrån den operativa verksamheten de befann sig, lämnar över informationssäkerhetsfrågor till andra funktioner.

Vikten av att chefer på olika nivåer bör vara väl insatta i och kompetenta när det gäller informationssäkerhetsfrågor är helt i enlighet med den forsknings som finns inom området där exempelvis Bojanc och Jerman-Blažič (2008) analyserar informationssäkerhet utifrån ett ekonomiskt perspektiv. Brist på kompetens men också svagt intresse för dessa frågor hos framför allt högsta ledningen i flera organisationer stämmer väl överens med forskningen som visar på chefers något svala attityd till behovet av egen kompetens för informationssäkerhetsfrågorna (Hyeun m.fl., 2012). Deltagarna var tydliga med att betona förståelsen och attityden kring informationssäkerhet först måste börja på övergripande chefsnivå för att så småningom nå alla medarbetare i organisationer som hanterar information, vilket också stämmer väl med tidigare forskning (Dutta och McCrohan, 2002). Van Niekerk och von Solms (2010) visar i sammanhanget på att kunskapsbrist bland anställda är ett av de större hoten mot informationssäkerhet. Det blir därmed tydligt vilket både fokusgruppsdeltagarna och Waly m.fl. (2012) påpekar, att användarnas beteende och attityder till informationssäkerhetsfrågor är framgångsfaktorer när informationssäkerhet ska införas i organisationer.

Förutom bristen på kompetens avseende ledning, styrning och ansvar på organisationsnivå, betonas vikten av att driva informationssäkerhetsfrågorna från ett verksamhetshåll. Detta har påtalats från praktik och forskning tidigare men fortfarande upplevs det som att informationssäkerhetsfrågorna drivs från ett mer tekniskt håll. Att informationssäkerhet bör vara verksamhetsdrivet har även en koppling till kompetensbristen på ledningsnivå då ansvaret kring var och hur informationssäkerhetsfrågorna ska hanteras ute i organisationerna ligger hos ledningen. Det har även koppling till den kritik som i viss mån framkommer från informationssäkerhetsexperterna själva då betoningen på att ”visa nyttan” med informationssäkerhet saknas. Eftersom ledningsnivån anses mer välvillig att se till nyttoeffekter och därmed också lyssna till hur dessa nyttoeffekter kan åstadkommas bör frågan ställas varför detta inte har gjorts långt tidigare. En förklaring som framkommer i tidigare forskning på området är att informationssäkerhetsexperter, när vissa säkerhetsåtgärder inte införs och efterlevs, är mer benägna att måla upp krissituationer och skräckscenarier istället för att visa på vardagliga nyttoeffekter med att ha ordning och reda på informationen och därmed en god informationshantering (Armstrong, 2013; Futcher m.fl., 2010).

Upphandlings- och rekryteringsområdet är två intressanta områden som lyfts fram i denna studie. Riksrevisionen (2014) nämner också upphandlingsområdet som ett viktigt förbättringsområde avseende informationssäkerhet. Det de inte nämner och som inte i någon större utsträckning har tagits upp i tidigare forskning är behovet av kompetens inom informationssäkerhet hos de personer som hanterar rekryteringsprocessen. Thompson (1999) betonar dock behovet av informationssäkerhetskompetens hos olika roller inom organisationer vilket också resultatet från denna studie visar.

Kompetenshöjande insatser för yrkesverksamma behöver vara praktiknära och ha riktade utbildningar för att få störst effekt (Albrechtsen & Hovden, 2010) vilket också passar väl in med vad praktiken visar på i denna studie.

I avsnitt 4.1.1 framkommer att ett stort ansvar för att sätta ramarna för informationssäkerheten ligger på den nationella nivån. Dock har organisationer med samhällsviktig verksamhet också själva ett stort ansvar i att se till att informationssäkerhetsarbetet och kulturen i verksamheten finns och förbättras. Viktiga områden för att förbättra säkerhetskulturen i en organisation handlar om strukturerat arbete avseende bl a ledningens engagemang, säkerhetsmedvetenhet, utbildning inom informationssäkerhet, riskhantering och efterlevnad. Det behöver också finnas ett ansvarstagande hos medarbetarna själva att ta del av utbildningar och andra kompetenshöjande insatser som erbjuds såväl internt som externt.

4.1.3 Allmänheten – medborgaren

Ett intressant område som tydligt betonades under diskussionerna och särskilt behöver lyftas fram är medborgarens kompetensbehov. För att öka kompetensen hos medborgaren långsiktigt krävs enligt deltagarna att medvetenheten för informationssäkerhetsområdet påbörjas tidigt. Därför blir skolområdet en viktig aktör för att öka kompetensen hos medborgaren i samhället men också ur perspektivet den framtida medarbetaren i organisationerna.

Av resultatet framkommer att informationssäkerhet rör alla medborgare och att det därför behövs riktade kompetenshöjande insatser mot olika grupper av medborgare. Förutom att nå barn och unga genom förskola och skola nämns det som viktigt att nå samhällets äldre medborgare, de som inte längre är aktiva i arbetslivet. Att ha kompetens i informationssäkerhet blir i framtiden mer eller mindre en fråga om allmänbildning och om den äldre generationen inte får denna kompetensökning finns det risk att de inte kommer ha samma möjligheter som övriga medborgare att skydda sin information.

Biblioteken diskuterades också som en tänkbar kanal för att nå ut och förmedla kompetens till samhällsmedborgarna. Det finns en del forskning gjord inom civilsamhällsområdet om hur man kan nå ut med information till samhällsmedborgare (Ghernouti-Helie, 2010), men det behövs ytterligare forskning avseende både kartläggning och metodutveckling då det gäller att nå ut med komptensåtgärder inom informationssäkerhet. Överhuvud taget behövs forskning på kompetenshöjande åtgärder riktade till samhällets medborgare då den tidigare forskning som finns inom kompetensutveckling på informationssäkerhetsområdet mestadels handlar om formell utbildning inom det formella utbildningsväsendet eller på arbetsplatsen (Åhlfeldt m.fl., 2014).

Förutom det nationella ansvaret (se 4.1.1) och det organisatoriska ansvaret (se 4.1.2) framkommer det i studien att det också behövs ett ansvarstagande från medborgarna själva att ta del av det som samhället erbjuder i form av utbildningar och andra kompetenshöjande insatser.

5 Förslag på framtida arbete

Förutom att analysera kompetensbehov och kompetensförsörjningen på informationssäkerhetsområdet, var syftet med denna studie att även ge underlag för kommande utveckling av metoder för framtida studier av kompetensförsörjningen. Nedan följer några förslag på framtida arbete. Dessa ska dock ses i första hand som ett diskussionsunderlag.

- **Metoder för att angripa bristen på helhetssyn** - De trender som deltagarna lyfter fram med ökad komplexitet kring exempelvis molntjänster, Internet of Things och ökade beroenden mellan samhällstjänster, organisationer etc., innebär stora utmaningar avseende framtida kompetensförsörjningen. Dessutom visar resultatet övergripande på bristen av helhetssyn avseende informationssäkerhet i samhället. Kompetensen behöver höjas på alla nivåer och metoder för att göra detta på ett effektivt sätt saknas. Här behövs mer forskning kring dels vilka utbildningsinsatser för olika områden som ger effekt (Åhlfeldt m.fl., 2014) dels kring utveckling av kompetensanalysmetoder för att kartlägga befintlig och framtida områden för kompetensutveckling. Denna studie har fångat en del av dessa områden/sammanhang men ytterligare studier behövs för att utarbeta strategier för hur analyser av dessa sammanhang ska gå till, t ex. ”job and task analysis”. En annan intressant fråga är hur säkerhetskulturen kan spela roll för helheten? Hur bygger vi upp en hållbar säkerhetskultur på lång sikt som täcker in kompetensbehovet för olika roller och individer i samhället? Forskningen tar ofta avstånd från stora och breda forskningsområden och studerar istället fenomenen i detalj. Därför är det även bristfälligt med metoder som kan vara till stöd för att fånga helheten. Det systemteoretiska perspektivet är ett intressant angreppssätt att använda sig av för att utveckla metoder för kompetensförsörjning utifrån ett helhetsperspektiv.

- **Kompetensförsörjning på managementnivå** – Det är viktigt för den framtida kompetensförsörjningen att forskningen får möjlighet att undersöka såväl kompetens på olika nivåer och grupper i samhället som organisering av informationssäkerhet. Men det stora fokus som visats både från praktik och forskning, på organisationer och dess lednings svaga utveckling av kompetens och kultur för informationssäkerhetsfrågor blir det ett fortsatt viktigt forskningsområde. Utan ledningens engagemang och kunskap kommer inte övriga medarbetare att förstå vikten av kunskap eller att få ta del av denna kunskap. Det blir därmed viktigt att kompetensutveckla såväl ledning som medarbetare inom en organisation. Kompetensutvecklingsinsatserna behöver vara verklighets-anknutna eftersom kunskap som inhämtas verksamhetsnära och evidensbaserat ger såväl lättillgänglig som bestående kompetenser. Hur kan kompetensen avseende informationssäkerhet förbättras hos ledningsfunktionerna så att den får genomslag i hela organisationen samt blir mer verksamhetsdriven?

- **Kompetensförsörjning till medborgaren** - Sett ur ett samhällsperspektiv handlar det om att gemene man behöver få förståelse för behovet av informationssäkerhet och varför det är viktigt att ha kompetens på informationssäkerhetsområdet. I detta avseende

behövs kompetens allt ifrån barn till de äldre. I den tidigare förstudien var medborgarperspektivet avgränsat vilket gör att underlaget för att se vilka utbildningsinsatser som görs till medborgare saknas. Vid en snabb sökning kan det dock konstateras att forskningen kring utbildningsinsatser och dess effekter av kompetensutveckling för medborgare är sparsam samtidigt som behovet av ny kunskap är påtagligt. Då det finns lite forskning på området vore det intressant att följa sådana breda kompetensförsörjningsarbeten från utformning till genomförande och resultat/utvärdering.

Enligt resultat av både tidigare förstudie och detta arbete är det tydligt att kompetensbristen inom informationssäkerhetsområdet är omfattande. Det kommer att krävas en långsiktig och hållbar planering för att täcka kompetensförsörjningen i framtiden från ett samhällsperspektiv. Det kommer krävas insatser både top down och bottom up för att om möjligt täcka in behovet av helhet och långsiktigt bygga upp en hållbar säkerhetskultur i samhället. Rapporten kan ses som en förstudie och underlag till fortsatt konkretisering. Denna konkretisering kan utgöras av en handlingsplan med förslag på konkreta metoder och åtgärder på nationell, organisatorisk och medborgerlig nivå.

Referenser

Albrechtsen, E. & Hovden, J. (2010). *Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study*. Computers & Security, 29(4), 432-445

Armstrong, C. J. (2013). *An Approach to Visualising Information Security Knowledge*. In R. Dodge, Jr. & L. Futcher (Eds.), Information Assurance and Security Education and Training (Vol. 406, pp. 148-155): Springer Berlin Heidelberg.

Bojanc, R. & Jerman-Blažič, B. (2008). *An economic modelling approach to information security risk management."* International Journal of Information Management, Vol. 28, No 5, pp: 413–422.

Dutta, A. & McCrohan, K. (2002). "*Management's role in information security in a cyber economy."* California Management review, Vol. 45, No. 1, pp: 67-87.

Futcher, L., Schroder, C., och von Solms, R. (2010). *Information security education in South Africa*. Information Management & Computer Security, 18(5), 366-374. Arthur, W Brian (1994). Increasing Returns and Path Dependence in the Economy. Michigan: The University Michigan Press.

Ghernouti-Helie, S. (2010). *A national strategy for an effective cybersecurity approach and culture. Availability, Reliability, and Security*, 2010. ARES'10 International Conference on, IEEE.

Goldkuhl, G. (2008). *Practical inquiry as action research and beyond.* Paper presented at the European Conference on Information Systems, 2008.

Graneheim, Hällgren, U. & Lundman, B., (2004). *"Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness."* Nurse education today 24.2 (2004): 105-112.

Hyeun-Suk, R., Ryu, Young U. & Cheong-Tag K., (2012). *Unrealistic optimism on information security management.* Computers & Security, Vol.31, No. 2, pp: 221-232.

Kitzinger, J. (1995). *Qualitative research: introducing focus groups*. Bmj, 311(7000), 299-302.

MSB (2012). Samhällets informationssäkerhet. Nationell handlingsplan. Myndigheten för samhällsskydd och beredskap (MSB). ISBN 978-91-7383-254-0.

Pain, H. (2011) *Practice research: what it is and its place in the social work profession*, European Journal of Social Work, Vol 14 (4), p 545-562

Riksrevisionen (2014) Informationssäkerhet i den civila statsförvaltningen. RIR 2014:23. ISBN 978 91 7086 361 5.

Stewart, D. W., & Shamdasani, P. N. (2014). *Focus groups: Theory and practice* (Vol. 20): SagePublications.

Thomson, M. (1999). *Making information security awareness and training more effective.* Paper presented at the Proceedings of the IFIP TC11 WG11. 3 First World Conference on Information Security Education (WISE1), Kista, Sweden.

van Niekerk, J.F. & von Solms R. (2010). "*Information security culture*: A management perspective", Computers & Security, Vol. 29, No. 4, pp: 476-486.

Waly, N., Tassabehji, R., & Kamala, M. (2012). *Measures for improving information security management in organisations: the impact of training and awareness programmes*.

Åhlfeldt R-M., Fischer Hübner S., Carlén U., Andersén A., Eriksson N., Björck F, and Nohlberg M. (2014) Förstudie kompetensbehov informationssäkerhet. Slutrapport i uppdragsprojekt till Myndigheten för samhällsskydd och beredskap. Mars 2014. HS-IIT-TR-14-001.

Åhlfeldt, R-M., Spagnoletti, P. and Sindre, G. (2007). *Improving the Information Security Model by using TFI.* In Proceedings of the 22tn IFIP TC-11 International Information Security Conference (SEC 2007). Sandton, South Africa, May 14-16, 2007. pp 73-84. ISBN: 13:978-0-387-72366-2, eISBN: 13:9780-387-72367-9, ISSN: 1571-5736