



Enheten för systematiskt informationssäkerhetsarbete

Nyckelroller inom informationssäkerhet

- CISO:s vänner

Innehållsförteckning

1. Introduktion.....	3
2. Kommunikatörens värld.....	4
2.1 Gemensamma intressen	4
2.2 Motsättningar och svårigheter i samarbete	4
2.3 Samarbete kring olika intressen	4
3. Dataskyddsombudets värld	5
3.1 Gemensamma intressen	5
3.2 Motsättningar och svårigheter i samarbete	5
3.3 Samarbete kring olika intressen	5
4. Beredskapssamordnarens värld	6
4.1 Gemensamma intressen	6
4.2 Motsättningar och svårigheter i samarbete	6
4.3 Samarbete mellan olika intressenter.....	6
5. Verksamhetsutvecklarens värld.....	7
5.1 Gemensamma intressen	7
5.2 Motsättningar och svårigheter i samarbete	7
5.3 Samarbete kring olika intressen	7
6. Säkerhetsskydds- och beredskapshandläggarens värld.....	8
6.1 Gemensamma intressen	8
6.2 Motsättningar och svårigheter i samarbete	8
6.3 Samarbete kring olika intressen	8
7. Verksamhetscontrollerns värld	9
7.1 Gemensamma intressen	9
7.2 Motsättningar och svårigheter i samarbete	9
7.3 Samarbete mellan olika intressen	9
8. It-samordnarens värld.....	10
8.1 Gemensamma intressen	10
8.2 Motsättningar och svårigheter i samarbete	10
8.3 Samarbete kring olika intressen	10

1. Introduktion

Informationshantering är centralt för de flesta av dagens organisationer. Information lagras, kommuniceras och bearbetas i olika utsträckning och behöver samtidigt skyddas på ett ändamålsenligt sätt utifrån exempelvis verksamhetens behov och externa krav. Flera olika roller i en organisation har intressen avseende informationshantering och informationssäkerhet. De tips och råd som beskrivs i detta dokument är resultatet av intervjuer med olika roller som tidigare identifierats som intressenter inom informationssäkerhetsområdet. Till de intervjuade ställdes följande frågor:

- Hur ser din "värld" ut – vad arbetar du med och vad är viktigt gällande informationshantering och informationssäkerhet för dig i din roll?
- I vilka delar har din roll gemensamma intressen med din CISO, Infossäkerhetssamordnare eller motsvarande (senare i texten informationssäkerhetssamordnare)?
- I vilka delar (om några) ser du motsättningar mellan de intressen du i din roll har gällande informationshantering och informationssäkerhet vilka kan leda till svårigheter för samarbetet med informationssäkerhetssamordnare?
- Hur kan du i din roll samarbeta med informationssäkerhetssamordnare kring era intressen – och hur kan ni få draghjälp av varandra?

Svaren är inkomna från medarbetare inom antingen kommun, länsstyrelse eller myndighet och är berättelser utifrån de olika rollerna. Svaren har anonymiserats.

Vi tar tacksamt emot berättelser från andra nyckelroller som kan stärka informationssäkerhetsarbetet!

Skicka in dina svar på frågorna ovan till:

informationssakerhet@informationssakerhet.se

2. Kommunikatörens värld

I arbetet med kommunikation är det viktigt att *rätt information* når *rätt målgrupp* i *rätt tid* via *rätt kanal*. Informationen ska vara tydlig och inte gå att missförstå. Det är viktigt att det finns en tydlig avsändare och en tydlig tänkt mottagare eller grupp av mottagare. Även *hantering av information* är viktigt. *Vem* som har tillgång till informationen, *var* den lagras och *hur länge* den är aktuell samt hur länge den kommer att finnas kvar på olika sätt är viktigt. Det är även viktigt med *källkritik* och att rätt avsändare delar sin information även om budskapet kan vara samma från flera olika avsändare.

2.1 Gemensamma intressen

Kommunikatören och informationssäkerhetssamordnaren har gemensamma intressen för att information behöver vara tillgänglig och riktig men också för att information inte tillgängliggörs förrän den ska tillgängliggöras. De har också gemensamma intressen gällande att uppmärksamma läsare eller medarbetare på behovet av källkritik dvs. vilken källa informationen kommer ifrån och om den är trovärdig. Både en kommunikator och en informationssäkerhetssamordnare är intresserad av aggregerad anonymiserad information. Det är skillnad på att säga att ”*män i 30-årsåldern gillar fotboll*” och ”*Anders, Andersson, från Axby i Västmanland, 32 år och gillar Ajax*”.

2.2 Motsättningar och svårigheter i samarbete

Svårigheter för samarbete mellan en kommunikator och en informationssäkerhetssamordnare kan uppstå när information ska delas utifrån konfidentialitet. Ett exempel är när information ska delas utan en tydlig målgrupp och/eller kanal. En informationssäkerhetssamordnare vill begränsa spridning av information till endast de mottagare som är behöriga och via utvalda kanaler medan en kommunikator gärna vill nå ut till många i en eller flera målgrupper och via flera kanaler samtidigt. Ett annat exempel är synen på statistik. Det är i kommunikatörens intresse att ha så mycket kunskap som möjligt om sina målgrupper. En kommunikator mäter resultat antingen i antal klick på en annons eller i hur länge en läsare stannat på ett inlägg. En informationssäkerhetssamordnare vill ofta minimera insamling av information till ett förutbestämt ändamål och syfte.

2.3 Samarbete kring olika intressen

Genom att inkludera varandra tidigt i respektive arbeten blir det enklare att samarbeta. Om en kommunikator identifierar ett kommunikationsbehov kan en informationssäkerhetssamordnare stödja så att informationens värde och behov av säkerhetsåtgärder och skydd tydliggörs. Likadant kan en kommunikator hjälpa till att formulera tydliga budskap som en informationssäkerhetssamordnare vill förmedla. Tillsammans kan de identifiera relevanta målgrupper och lämpliga kanaler och tidpunkter att nå dessa målgrupper på.

3. Dataskyddsombudets värld

Som dataskyddsombud (DPO) går arbetet hand i hand med informations-säkerhetssamordnarens arbete i stort. ”Jag är lyckligt lottad eftersom mina kollegor inom arkivfunktionen, registraturen och säkerhetsorganisationen har god säkerhetsmedvetenhet” säger en DPO. Ett nära samarbete med informationssäkerhetssamordnaren och att medarbetare har rätt kompetens gällande informationshantering är en förutsättning för att kunna göra ett bra arbete som DPO.

3.1 Gemensamma intressen

Tillräckliga säkerhetsåtgärder, både tekniska och organisatoriska, är en del av dataskyddsregleringen, och inom detta område behövs en gemensam syn och ett gemensamt arbete mellan DPO, informationssäkerhetssamordnare och it-ansvariga. Rollerna har även gemensamma intressen inom risk- och konsekvensanalyserna som görs utifrån GDPR men som i stort är de samma som görs utifrån informationssäkerhetsperspektivet. Det arbete som utförs som DPO är väldigt beroende av det arbete som utförs inom informationssäkerhetsarbetet och it-enheten eftersom dataskyddet är beroende av dessa. Arbetet med informationshantering bör ske tillsammans på övergripande nivå eftersom informationssäkerhet är en del av informationshanteringen och det finns ett gemensamt intresse av att säkerställa att ansvar för informationshanteringen i organisationen är tydligt.

3.2 Motsättningar och svårigheter i samarbete

Det finns inga direkta motsättningar mellan DPO och informationssäkerhetssamordnaren. Däremot är det viktigt att arbeta för att skyddet ska vara kostnadseffektivt och att det inte blir för omständligt för verksamheten. För att få till en sån avvägning mellan rätt skydd och verksamhetens effektivitet behöver alla som arbetar med informationssäkerhetsfrågor och personuppgiftsbehandling förstå verksamhetens behov och krav på effektivitet samtidigt som information ska hanteras korrekt. Som DPO kan man bistå med vad som är rimliga krav att ställa på medarbetarna, vad man kan överlämna till medarbetarna att själva bestämma hur de ska göra och samtidigt ha tillräcklig kontroll för hur vi hanterar information. Det gäller att man förstår varandra och kan ha en dialog.

3.3 Samarbete kring olika intressen

Samarbetet med informationssäkerhetssamordnaren måste fungera, dvs. denna och DPO har ofta samma avsikt med de krav vi ställer. Exempelvis kan man samverka när det gäller nätverk för medarbetare som behöver samverka inom personuppgiftshantering. Informationssäkerhetssamordnaren har också behov av närmare samarbete med samma målgrupp så då kan det vara ett gemensamt nätverk.

4. Beredskapssamordnarens värld

Kommunens beredskaps- och säkerhetssamordnare handlägger och samordnar övergripande säkerhets- och krisberedskapsfrågor inklusive frågor som rör höjd beredskap, civilt försvar och totalförsvarsfrågor. Beredskaps- och säkerhetssamordnaren ansvarar för att aktörer inom kommunens geografiska område samverkar och samordnar sitt arbete före och vid särskilda händelser, samt samordnar information om en sådan händelse till allmänheten.

Kommunens beredskaps- och säkerhetssamordnare ansvarar bl.a. för att upprätta planering för krisberedskap som en del i kommunens plan för extraordinära händelser enligt lagen om extraordinära händelser (LEH) och att upprätta planering för kommunens del i det brottsförebyggande arbetet. Ansvaret för kommunens arbete för den så kallade risk- och sårbarhetsanalysen (RSA) ligger också på beredskaps- och säkerhetssamordnaren.

4.1 Gemensamma intressen

Inom ramen för säkerhetsskydd och då främst skyddet av information finns gemensamma intressen mellan beredskaps- och säkerhetssamordnaren och informationssäkerhetssamordnaren. Genom informationssäkerhetsarbetet och dess syfte att skydda all information ingår också att skydda den information som främst hanteras inom säkerhetsskyddet. Arbetet vid risk- och sårbarhetsanalyser av kommunens verksamhets- samt samhällskritiska system har också intresse hos båda rollerna. Det finns en teknisk del där IT är en naturlig del vid både normal verksamhet och vid beredskap där även informationssäkerhetsansvariga bistår för att bygga upp motståndskraft, resiliens, inom informationssäkerhetsområdet och höja medvetandet om säker informationshantering och de tekniska aspekter som finns. Alla medarbetare, oavsett om de arbetar med teknik eller i annan verksamhet måste känna till varandra och hitta organisationsövergripande forum och tankesätt där säkerhetsåtgärder kan hanteras utifrån helheten snarare än i silos, dvs. utifrån enskilda verksamheter.

4.2 Motsättningar och svårigheter i samarbete

Inga motsättningar, bara möjligheter att samordna.

4.3 Samarbete mellan olika intressenter

Den tekniska delen inom informationssäkerhetsområdet behöver samordnas. Utgångspunkten i arbetet skiljer sig genom att arbetet vid beredskap ofta blir mer personbaserat vilket är en utmaning och där arbetet måste ske utifrån vad den enskilda människan eller människor i grupp kan åstadkomma. Samarbetsmöjligheter finns genom att samordna kunskapsförmedling tillsammans med it-chef och informationssäkerhetssamordnare.

5. Verksamhetsutvecklarens värld

Började på myndigheten som arkivarie men har nu ett uppdrag som verksamhetsutvecklare inom arkivering och diarieföringsverksamheten. Som verksamhetsutvecklare med ansvar för det administrativa diariet och e-arkivet är jag även involverad i annan informationshantering som berör organisationens övriga administrativa arbetssätt. På myndigheten finns arkivredovisningen som inkluderar organisationens klassificeringsstruktur, vilka gallringsbeslut som finns och hur de ska tillämpas samt en generell beskrivning av arkivet och registerförteckningen. Som verksamhetsutvecklare sker arbetet verksamhetsnära avseende it-leveranser från leverantör och där kommer säkerhetsfrågor in då det går hand i hand med informationshantering.

5.1 Gemensamma intressen

Klassning av information är gemensamt med informationssäkerhetsstandarderna då myndigheten ska klassificera sin information utifrån sin verksamhet i enlighet med Riksarkivets föreskrifter (RA-FS 2008:4). Regleringen ställer krav på att organisationen ska klassificera sina olika informationsmängder och då kommer även informationens skyddsklassificering in i bilden. Personuppgiftsbehandling är också ett område där det finns gemensamma intressen och vi arbetar för att de olika klassningsstrukturerna, utifrån typ av information och värdet av informationen, dvs. skyddsklassificeringen båda ska fungera i våra it-system. Ett annat område där det finns gemensamma intressen är säker inhämtning av information och att information lämnar organisationen på ett säkert sätt t.ex. hur information får skickas över e-post och vilken kryptering vi bör använda.

5.2 Motsättningar och svårigheter i samarbete

Inom terminologiområdet behöver man reda ut vad man pratar om för att skapa gemensam förståelse. Informationsägarbegreppet är vanligt förekommande inom informationssäkerhet- och it-området men är inget juridiskt begrepp. Ett annat begrepp som behöver redas ut är vad information är i juridisk mening. Detta skiljer sig från arkivjuridiska begrepp och man behöver komma överens om varför medarbetarna behöver utföra vissa aktiviteter på vissa sätt och hur det ska förmedlas till medarbetarna i olika verksamheter för att undvika begreppsförvirring.

5.3 Samarbete kring olika intressen

Ett integrerat sätt för att arbeta med informationshantering är att rekommendera, ett tätt samarbete mellan olika intressenter och att sitta tillsammans i projekt där gemensamma frågor behöver hanteras. Samarbete sker också gällande exempelvis ansvarsmodeller. I mindre organisationer måste ibland samma person ha flera roller t.ex. kan det vara svårt att ha ett dataskyddsombud som bara har det som arbetsuppgift vilket kan bli problem om denna har andra roller där den t.ex. skulle kunna granska sig själv. Fördelen med en liten organisation är att det är lätt att få personlig kontakt med dem som man behöver samarbeta med.

6. Säkerhetsskydds- och beredskapshandläggarens värld

Säkerhetsskyddet omfattar ett systematiskt arbete med personsäkerhet, fysisk säkerhet och informationssäkerhet. Arbetet som säkerhetsskydds- och beredskapshandläggare handlar om att arbeta inom Länsstyrelsen och externt mot våra samverkande aktörer (samordnande, rådgivande, stödjande, kravställande). Det är särskilt viktigt att samverka med aktörerna fungerar på ett bra sätt för de verksamheter som ska samordnas och att alla arbetar för att hitta arbetssätt som ger synergier.

6.1 Gemensamma intressen

Informationssäkerhet med bäring på rikets säkerhet är ett gemensamt område för informationssäkerhetssamordnaren och säkerhetsskydds- och beredskapshandläggaren. Detta eftersom ett systematiskt informationssäkerhetsarbete är en förutsättning för det arbetet som görs inom säkerhetsskydd och beredskap då det är förebyggande. Övriga sekretessfrågor enligt OSL är ytterligare ett område där samarbete sker. Även incidenthantering av informationssäkerhetsincidenter och informationssäkerhetsskyddsincidenter samt allt som har med informationssäkerhet i övrigt att göra är av gemensamt intresse, t.ex. fysiskt skydd och frågor gällande medarbetare.

6.2 Motsättningar och svårigheter i samarbete

Inga motsättningar mellan rollerna. Det är däremot svårt för många medarbetare att förstå vilken roll de ska vända sig till i första hand. Det kan vi dock hantera eftersom vi är insatta i den andra rollens arbete.

6.3 Samarbete kring olika intressen

Vi samverkar genom att ta fram material gemensamt till informations- och utbildningsinsatser. Utbyte av kunskap och att ha en person med liknande kunskap, problem och förslag på lösningar underlättar arbetet. Vi arbetar bättre tillsammans än var för sig. Genom samarbetet underlättar vi för medarbetarna då det systematiska säkerhetsarbetet utvecklas med ytterligare funktioner så att det blir en process med flera inriktningar för verksamheten istället för många olika processer. Vi samarbetar i det dagliga arbetet och genom att ha stöd av den andra kompetensen under olika typer av möten där vi diskuterar hur information ska hanteras i olika verksamheter.

7. Verksamhetscontrollerns värld

Rollen som verksamhetscontroller innebär ett övergripande ansvar för att det finns en fungerande process för intern styrning och kontroll. Ledningens engagemang är avgörande för att arbetet och framtaget arbetssätt, processen ska fungera.

7.1 Gemensamma intressen

Gemensamma intressen mellan verksamhetscontroller och informationssäkerhetsansvariga är bl. a. att det ska finnas en fungerande riskhantering med en enhetlig struktur för riskarbetet, ett tydligt ägarskap till olika risker och uppföljning av beslutade riskåtgärder.

7.2 Motsättningar och svårigheter i samarbete

Sekretesshantering av frågor som berör säkerhetsåtgärder för att skydda information är naturligtvis nödvändig men det kan finnas motsättningar om organisationen uppfattar att information som klassats högt på konfidentialitet inte får delas med dem som behöver veta för att t.ex. ta fram tillräckligt bra beslutsunderlag så att ledningen kan fatta beslut på rätt grunder. Uppstår bristande transparens kan det t.ex. försvåra diskussioner om bl. a. prioritering av gemensamma resurser i ledning och styrning av verksamheten.

7.3 Samarbete mellan olika intressen

Eftersom riskhantering är en gemensam nämnare är erfarenhetsutbyte och goda exempel inom detta område framgångsfaktorer som kan bidra till att vardagen fungerar.

8. It-samordnarens värld

It-samordnaren arbetar med praktiska frågor som att ge stöd gällande it i den operativa verksamheten. Vanliga uppgifter är att exempelvis hantera it-utrustning och se till att rätt information finns på rätt plats. Det handlar även om strategiska frågor som avtal och hur riktlinjer påverkar arbetet samt utveckling av stöd gällande informationshantering till verksamheten. It-funktionen är kulturellt en servicefunktion som utför arbetsuppgifter inom ramen för fastställda ekonomiska förutsättningar. Som it-samordnare är det viktigt att informationsflödena och it-utrustningen fungerar som det är tänkt genom exempelvis behörighetsstyrning och liknande.

8.1 Gemensamma intressen

Det finns många gemensamma intressen, exempelvis måste de informationsflöden som hanteras i system vara godkända av informationssäkerhetsansvarig och säkerhetsorganisationen. Att arbeta tillsammans med andra roller inom informationssäkerhet är positivt. Flera av närliggande roller har stor erfarenhet t.ex. har dataskyddsombud också verksamhetskunskap och säkerhetschefen som kan alla organisationens arbetsprocesser. Det finns en närhet till goda förebilder och vi har goda relationer mellan oss.

8.2 Motsättningar och svårigheter i samarbete

Har inte några direkta motsättningar eftersom gruppen för informationssäkerhet har en samsyn kring hur information ska hanteras, däremot är det svårare när man vänder sig till verksamheten för att dom har synpunkter på hur lång tid vissa saker tar osv. Det finns olika intressen hos olika avdelningar. Dessa intressen behöver vi tillgodose. När verksamheten är under hög belastning kan det ibland vara svårt att få dom att förstå vikten av att ändå hantera information och utrustning säkert även om det tar mer tid. Det finns en dubbelhet hos organisationens olika avdelningar där många vill ha mer information samtidigt som de inte hinner ta emot eller är beredda att förändra sitt arbetssätt utifrån den information de får.

8.3 Samarbete kring olika intressen

Enheternas, it-samordnarens och informationssäkerhetssamordnarens, närhet till varandra underlättar dialog. Arbetsplatsen har ett förlåtande synsätt gällande att saker inte alltid blir bra och man tillåts att upptäcka och föreslå nya sätt att arbeta, uppnå säker informationshantering på. Genom att ha högt i tak kan man utveckla och förbättra efterhand. Det man trodde man skulle göra i början behöver inte bli slutprodukten utan nya sätt och saker undersöks. Vi samarbetar för att genomföra arbetet så att vi når gemensamt mål. Vi har en god förberedande dialog innan formella beslut fattas och nära till beslutsfattare. Vi kan ta stöd av varandra när något behöver utredas eller inför ett viktigt beslut.