Myndigheten för samhällsskydd och beredskap

Att analysera värderingar bakom informations-säkerhet

FORSKNING

MSB:s kontaktpersoner:
Jan Byman, 010-240 43 76

Publikationsnummer MSB297

Förord

År 2008 påbörjade forskningsgruppen MELAB vid Örebro universitet ett forskningsprojekt kring mål- och värdekonflikter som existerar vid arbete med informationssäkerhet. Projektet har resulterat i en ökad kunskap om dessa typer av konflikter i organisationer. Att konflikterna existerar ses ofta som ett problem, men kan också ses som en utgångspunkt för verksamhetsutveckling. Det är givetvis problematiskt om anställda inte delar de mål- och värderingar som finns med informationssäkerhetsarbetet. Samtidigt är kunskapen om att konflikterna existerar och vilka de är en viktig utgångspunkt för ett förbättrat säkerhetsarbete – i form av ändrade regelverk och/eller att anställda förändrar sitt sätt att arbeta och resonera om informationssäkerhet.

För att genomföra analyser av vilka mål- och värdekonflikter som finns i informationssäkerhetsarbete krävs analysverktyg. Därför var ett viktigt resultat från forskningsprojektet en analysmetod, vilken presenteras i denna skrift. Under utvecklingsarbetet har metoden använts i ett flertal projekt för att analysera sociala aspekter av informationssäkerhet. Metoden har även utvärderats av ett antal nationella och internationella expertgrupper.

Forskningsprojektet har finansierat av Myndigheten för Samhällsskydd och Beredskap.

Örebro, september 2010

Fredrik Karlsson

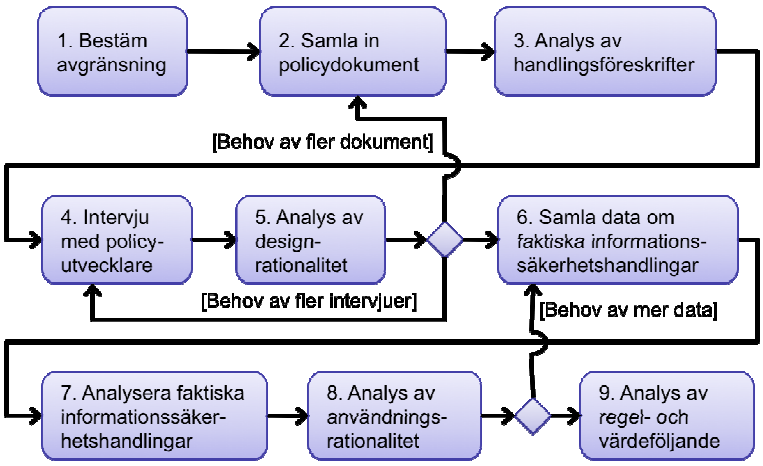
Projektledare

Innehållsförteckning

1. Introduktion

Att anställda inte följer den policy och de regler som finns för hantering av information och informationstillgångar är en utmaning för många organisationer. För att förbättra styrningen utvärderas ofta de anställdas handlingar i förhållande till föreskrifterna. En begränsning med många av metoderna som används för detta ändamål är att de fokuserar enbart på just handlingen i sig – inte de bakomliggande argumenten till varför en regel följs eller inte. Genom att gå bakom handlingarna och analysera hur mål och värderingar (rationaliteten) stämmer överens mellan det som föreskrivs och de mål och värderingar som de anställda har ges ökad kunskap om varför regler följs respektive inte följs. Denna kunskap kan sedan användas för att på ett bättre sätt rikta insatser i ledningsarbetet kring informationssäkerhet.

Här presenteras en metod bestående av nio arbetssteg för att analysera de olika rationaliteter som finns i en organisation och som påverkar informationssäkerhetsarbetet. Metodens övergripande struktur och arbetsstegens inbördes förhållande visas i Figur 1. Varje arbetssteg beskrivs med hjälp av ett kort exempel från en tänkt sjukhusmiljö.



Figur 1 Metodöversikt

2. Metoden i nio arbetssteg

2.1 Bestäm avgränsning

Syftet med detta arbetssteg är att bestämma avgränsningen för utvärderingsprojektet. Projektmedlemmarna bestämmer tillsammans med beställaren vilka aspekter av informationssäkerhet som skall vara i fokus. Det görs genom att:

a) definiera vad projektgruppen menar med informationssäkerhet,

b) bestämma den organisatoriska avgränsningen för analysen.

Exempel

Som utgångspunkt för att definiera informationssäkerhet kan oftast officiella dokument användas. Exempelvis kan ett sjukhus visionsdokument uttrycka följande: korrekt information till rätt personer, i rätt tid och vid rätt plats. Vid ett sjukhus hanteras många olika typer av information vilket gör det viktigt att avgränsa vilken typ av information och informationstillgångar som skall studeras. En studie kan exempelvis fokusera på patientinformation, dvs information som relaterar till en persons sociala, medicinska och övrigt personliga omständigheter. Slutligen bör en organisatorisk avgränsning göras. På ett sjukhus kan det exempelvis vara en klinik eller avdelning.

2.2 Samla in policydokument

Syftet med detta arbetssteg är att samla in bakgrundsmaterial kring hur informationssäkerhetshandlingar skall utföras. Dokument som faller inom projektavgränsningen samlas in. Dokumenten skall vara officiella dokument som används för att styra informationssäkerhetsarbetet, såsom policies, riktlinjer och handböcker.

Exempel

Officiella dokument samlas in kring aktuella föreskrifter. Vid ett sjukhus kan det röra sig om sjukhusets policy för informationssäkerhet, IT-strategin, IT-policy, riktlinjer från landstinget, och manualer för olika rutiner. De senare kan exempelvis vara lokala rutiner på kliniken.

2.3 Analys av handlingsföreskrifter

Syftet med detta arbetssteg är att skapa en lista över föreskrivna informationssäkerhetshandlingar baserat på insamlade policydokument. En föreskriven informationssäkerhetshandling är en regel kring vad som är tillåtet eller inte tillåtet att göra med information eller en informationstillgång. I detta arbete är det viktigt att ta hänsyn till att föreskrivna informations-säkerhetshandlingar kan vara beskrivna på olika nivå i olika policydokument. Det innebär att övergripande och detaljerade beskrivningar av samma typ av

handling grupperas tillsammans för att minska antalet handlingar som skall analyseras i projektet. Av samma anledning sorteras dubbletter bort.

Exempel

Här skapas en lista med föreskrivna handlingar. Exempel på sådana handlingar kan vara (Fö1) ”All viktig information om patienten måste omedelbart dokumenteras i journalen” och (Fö2) ”Patientinformation skall dokumenteras omedelbart efter mötet med patienten.”

2.4 Intervju med policyutvecklare

Syftet med detta arbetssteg är att skapa en djupare förståelse för policyarbetet i organisationen och argumenten bakom de regler som finns. Dessutom är intervjuerna en verifiering på att projektgruppen hittat de centrala informationssäkerhetsföreskrifterna. Intervjuerna skall fokusera på de mål som policyutvecklarna vill uppnå med reglerna och varför dessa mål anses viktiga – det senare visar på vilka värderingar som målen är förankrade i. Som utgångspunkt för intervjuerna används listan över föreskrivna informationssäkerhetshandlingar från arbetssteg 3. I själva intervjusituationen är det viktigt att tydliggöra syftet med intervjuerna och vad man menar med informationssäkerhet. Det skapar en avgränsning för intervjun. Efter det att ramarna för intervjun beskrivits påbörjas arbetet med att identifiera de mål och värderingar (designrationalitet) som policyutvecklarna vill uppnå med de föreskrivna informationssäkerhetshandlingarna. Varje informations-säkerhetshandling som listats i arbetssteg 3 ses som en policyformulering som valts framför en eller flera tänkbar policyformuleringar. Därför ställs frågor kring varför den föreskrivna informationssäkerhetshandlingen inkluderats i policydokumenten och vad som påverkat designen, såsom lagstiftning.

Exempel

Tänkbara funktioner att intervjua är roller som är involverade i utformningen av informationsrutiner såsom informationssäkerhetsansvarig, IT-chefen, och kvalitetsansvariga. Under intervjuerna kan hänvisningar göras till material som används som stöd för utvecklingsarbetet. I ett sjukhusexempel är tänkbara källor Patientdatalagen och ISO 27 000-standardserien. Dessa kan innehålla eller ha utgjort argument för hur de föreskrivna handlingarna Fö1 och Fö2 utformats. Exempelvis återfinns följande i Patientdatalagen ”en patientjournal ska föras för varje patient” och ”uppgifter som ska antecknas enligt 6-8 §§ ska föras in i journalen så snart som möjligt.” Intervjuerna kan också visa på vad policyskaparna velat uppnå såsom att ”information skall finnas där precis när du behöver den, när jag skall behandla patienten. Och inget skall vara undanhållet om jag har access.”

2.5 Analys av designrationalitet

Syftet med detta arbetssteg är att analysera vilken designrationalitet (mål och värderingar) som finns bakom de föreskrivna informations-säkerhetshandlingarna. Analysen görs genom ett så kallat WITI-test (Why-Is-This-Important) som består av två frågor. Först ställs följande fråga för varje listad handling: Varför är denna handling föreskriven i den här kontexten? Som

utgångspunkt för att besvara frågan används intervjusvaren och annat material som kommit fram under arbetsstegen 1 till 4, såsom informationssäkerhetsstandarder och lagstiftning. Om svaret beskriver ett verifierbart tillstånd inom ledningsarbetet med informationssäkerhet, så är det ett mål. De identifierade målen används sedan som utgångspunkt för nästa fråga: Varför är detta mål viktigt i denna kontext? Om svaret på frågan är ett ideal som delas av policyutvecklarna för att styra informationssäkerhetsarbetet, så är det en värdering.

Exempel

Här används listan med föreskrivna informationssäkerhetshandlingar, i vårt fall Fö1 och Fö2. En tänkbar analys skulle kunna se ut enligt följande. Om vi börjar med Fö1 ”All viktig information om patienten måste omedelbart dokumenteras i journalen” så finner vi i Patientdatalagen att journal måste föras om varje patient. Detta är ett tillstånd som måste uppnås och därmed ett mål, M1: Att föra patientjournal. Detta mål är i sin tur förankrat i två värden, (V1) fullständighet, dvs att det är viktigt att informationen är fullständig, och (V2) tillgänglighet, dvs att det är viktigt att informationen är tillgänglig för behöriga personer. Båda dessa värden kan spåras till Patientdatalagen och till ISO-27 000 standarden. Patientdatalagen innehåller ytterligare skyldigheter för sjukhuset, att de skall dokumentera ”2. väsentliga uppgifter om bakgrunden till vården, 3. uppgift om ställd diagnos och anledning till mera betydande åtgärder, 4. väsentliga uppgifter om vidtagna och planerade åtgärder.” Detta ger upphov till ett andra mål, M2, att det skall vara möjligt att följa patientens medicinska historia. Även detta mål skulle då vara förankrat i värdena V1 och V2 ovan.

Vår andra föreskrivna handling är Fö2 ”Patientinformation skall dokumenteras omedelbart efter mötet med patienten.” Den handlingen skall utföras för att möta målen M1 och M2, och är följaktligen förankrade i värdena V1 och V2.

2.6 Samla data om faktiska informationssäkerhetshandlingar

Syftet med detta arbetssteg är att samla in data kring hur informationssäkerhetsarbetet går till i organisationen. För att göra det delas arbetssteget i två moment som utförs i ett iterativt mönster: (a) intervjuer med policyanvändare, och (b) observation av policyanvändare. Under de första intervjuerna så ombeds policyanvändare att identifiera och beskriva centrala handlingar i sin arbetsvardag. Dessutom ombeds de beskriva vad de vill uppnå med dessa handlingar och varför de är viktiga för dem. De senare frågorna ställs för att fånga användningsrationaliteten (mål och värderingar) bakom handlingarna.

Intervjuerna följs sedan av observationer. Observationerna syftar till att verifiera om policyanvändarna utför handlingarna på det sätt som de har beskrivit dem. Vidare är det möjligt att via observationer hitta handlingar som utförs men som policyanvändarna inte beskrivit. Baserat på observationsresultaten kan det vara aktuellt med kompletterande intervjuer.

Detta beslut tas lämpligtvis efter nästföljande två arbetssteg där analys av det insamlade materialet görs. Om ytterligare intervjuer görs så fokuserar de primärt på rationaliteten bakom handlingar som inte beskrivits tidigare samt skillnader mellan hur man beskrivit sitt handlande och sitt faktiska handlande.

Exempel

Tänkbara roller att intervjua och observera vid ett sjukhus är läkare, sjuksköterskor, undersköterskor, och administrativa roller. Innan observationerna görs kan en lista över beskrivna handlingar skapas enligt steg 7. Det gör att man har ett observationsprotokoll att arbeta med. Men observationsprotokollet får inte bli så styrande att handlingar som inte beskrivits glöms bort.

2.7 Analysera faktiska informations-säkerhetshandlingar

Syftet med detta arbetssteg är att skapa en lista över faktiska informationssäkerhetshandlingar. En faktisk informationssäkerhetshandling är en handling där policyanvändaren hanterar information/informations-tillgångar i sitt dagliga arbete. Precis som med föreskrivna handlingar kan de faktiska handlingarna beskrivas på olika nivå. Därför grupperas abstrakta och detaljerade beskrivningar av en handling tillsammans för att minska antalet handlingar att analysera. Likaså sorteras dubbletter bort.

Exempel

Här skapas en lista med faktiska handlingar. Exempel på sådana handlingar kan vara (Fa1) ”Om informationen inte leder till någonting, några åtgärder, eller att det inte finns någon som är i behov av den så tycker jag man kan vänta med att dokumentera. För att dokumentera i journalen ger extra arbete för sekreterarna” och (Fa2) ”Man är försiktig med vad man skriver i journalen. Man kanske inte vill bryta ett förtroende med patienten genom att skriva något känslig för du vet att andra kan läsa det. Därför skriver du ”familjeproblem” istället för det exakta problemet.”

2.8 Analys av användningsrationalitet

Syftet med detta arbetssteg är analysera vilken användningsrationalitet (mål och värderingar) som finns bakom de faktiska informations-säkerhetshandlingarna. Som utgångspunkt används listan med faktiska informationssäkerhetshandlingar och intervju- och observationsutskrifterna. Analysen är snarlik det WITI-test som användes på föreskrivna informationssäkerhetshandlingar. Först ställs följande fråga för att identifiera mål bakom handlandet: Varför utförs handlingen i den här kontexten? Om svaret beskriver ett verifierbart tillstånd i policyanvändarens arbete, så är det ett mål. Efter att ett mål identifieras ställs nästa fråga: Varför är detta mål viktigt i denna kontext? Om svaret på frågan är ett ideal som hålls av policyanvändaren så är det en värdering.

Om det inte är möjligt att identifiera mål och värderingar för en handling så krävs antagligen kompletterande intervjuer. Det kan dessutom vara värt att

kontrollera om samtliga beskrivna handlingar har blivit observerade. Om så inte är fallet så kan även kompletterande observationer behövas.

Exempel

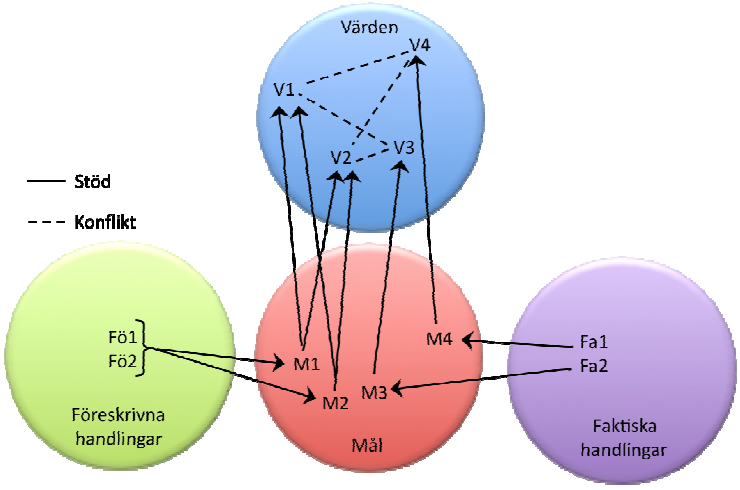
I föregående arbetssteg identifierades två faktiska handlingar, Fa1 och Fa2. Fa1 visar en läkare som väntar med att dokumentera patientinformation, om han eller hon inte anser att informationen behövs omgående i den kommande vården. Rationaliteten grundar sig i målet att vara effektiv (M4). Det är i sin tur baserat på en värdering om att det är viktigt att vara effektiv (V4). En liknande handling görs i Fa2, där en annan medarbetare ibland utelämnar känslig patientinformation i journalen. Här kan exempelvis de tidigare intervjuerna ha avslöjat att medarbetaren är rädd om patientens privatliv (M5). Bakom detta mål finns ett integritetsvärde (V5), att det är viktigt att garantera patientens integritet.

2.9 Analys av regel- och värdeföljande

Syftet med det sista arbetssteget är att analysera argumenten bakom regelföljande och regelbrott. Den horisontella dimensionen i Tabell 1 klassificerar regelföljande sett till handlingen i sig, där handlingen antingen är korrekt utförd eller inte. Den vertikala dimensionen fokuserar på om rationaliteten bakom policyanvändarens handling och om den stämmer överens med rationaliteten bakom den föreskrivna handlingen. De två dimensionerna skapar fyra kategorier av regelföljande/regelbrott. I det övre vänstra hörnet finns överrensstämmelse både på handlings- och rationalitetsdimensionen. Den faktiska handlingen utförs korrekt och policyanvändaren delar värderingarna bakom policyn. Detta är den ideala situationen. I det övre högra hörnet delar policyanvändaren värderingarna bakom policyn, men utför handlingen felaktigt. Användaren är inte medveten om felet eller klarar inte av att utföra handlingen korrekt. I den tredje kategorin, det nedre vänstra hörnet utförs handlingen som den skall, men användaren delar inte värderingarna som finns bakom föreskriften. Således finns det en risk för framtida regelbrott. Den fjärde kategorin, i det nedre högra hörnet av tabellen har brott identifierats både på handlings- och rationalitetsdimensionen. I den här kategorin hittas medvetna regelbrott.

		Handlingsdimension	
		Regelföljande	**Regelbrott**
Rationalitetsdimension	**Värdeföljande**	(I) Rationalitetsöverens-stämmelse och hand-lingen utförs korrekt.	(II) Rationalitets-överensstämmelse men handlingen utförs inte korrekt.
	Värdebrott	(III) Rationaliteterna stämmer inte men handlingen utförs korrekt.	(IV) Rationaliteterna stämmer inte och handlingen utförs inte korrekt.

Tabell 1 Klassificering av regelföljande och regelbrott



Föreskrivna handlingar:
Fö1: All viktig information om patienten måste omedelbart dokumenteras i journalen.
Fö2: Patientinformation skall dokumenteras omedelbart efter mötet med patienten.

Faktiska handlingar:
Fa1: Om informationen inte leder till någonting, några åtgärder, eller att det inte finns någon som är i behov av den så tycker jag man kan vänta med att dokumentera. För dokumentera i journalen ger extra arbete för sekreterarna.
Fa2: Man är försiktig med vad man skriver i journalen. De kanske inte vill bryta ett förtroende med patienten genom att skriva något känslig för du vet att andra kan läsa det Därför skriver du "familjeproblem" istället för det exakta problemet.

Mål:
M1: Att föra patientjournal.
M2: Att det skall vara möjligt att följa patientens medicinska historia.
M3: Att vara effektiv.
M4: Att värna om patientens integritet.

Värden:
V1: Det är viktigt att informationen är fullständig.
V2: Det är viktigt att informationen är tillgänglig för behöriga personer.
V3: Det är viktigt att vara effektiv.
V4: Det är viktigt att garantera patientens integritet.

Figur 2 Rationalitetskonflikter i exemplifierade säkerhetshandlingar

Exempel

I det avslutande arbetssteget ställs de föreskrivna handlingarna och dess rationalitet mot de faktiska handlingarna som identifieras, och den rationalitet de är baserade på. Här är det möjligt att identifiera en konflikt på handlingsnivå mellan Fö2 och Fa1 där patientinformation inte dokumenteras direkt. När fokus läggs på rationaliteten bakom dessa handlingar visas det att Fö2 är förankrad i fullständighetsvärden (V1, V3) samt ett tillgänglighetsvärde (V2). Men handlingen Fa1 är grundat på ett effektivitetsvärde (V4). Det innebär att sjukhuspersonalen prioriterar effektivitet före fullständighet och tillgänglighet. Det finns även en konflikt mellan det andra handlingsparet Fö1 och Fa2. Även bakom denna konflikt finns skillnader i rationalitet. Den föreskrivna handlingen är grundad i ett fullständighetsvärde (V1) och ett tillgänglighetsvärde (V2). Dessa värden står i konflikt med integritetsvärdet (V5) som styr den medicinska personalens handlande (Fa2). Således hamnar båda dessa konflikter i kategori IV i Tabell 1: Rationaliteterna stämmer inte och handlingen utförs inte korrekt.

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB297