Hendelsesrapportering i en organisasjon i norsk olje- og gassindustri

Ingar Smedstad

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2007

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Sammendrag

Denne studien omhandler hendelsesrapportering innen informasjonssikkerhet i en organisasjon innen olje- og gassindustrien i Norge. Studien er en kvalitativ intervjuundersøkelse. Hovedhensikten med studien er å belyse hvordan organisasjonen rapporterer i forhold til en nylig utviklet systemdynamisk modell for hendelsesrapportering. Resultatene indikerer at organisasjonen har et forbedringspotensial i forhold til enkelte områder i modellen. Disse områdene handler om kommunikasjon rundt hendelsesrapportering, spesielt tilbakemelding til de som rapporterer, informasjon om retningslinjer for rapportering samt kompetanseheving i forhold til å rapportere.

Abstract

This master thesis focuses on incident reporting for information security within an organisation in the Norwegian oil and gas industry. The study is based on qualitative interviews. The main purpose of this study is to discover how the organisation's incident reporting routines compares to a recently developed system dynamic model for incident reporting. The results indicate that the organisation has potential to do improvements regarding certain areas concerning communication about incident reporting. It also indicates that the organisation could profit from giving special attention to feedback toward reporting staff, information about guidelines within incident reporting in information security and also focus on educating the staff with regards to incident reporting.

Takk til

Takk til Jose Gonzalez for veiledning.

Takk til Finn Olav Sveen for veiledning.

Takk til informantene som brukte av sin arbeidstid og stilte opp til intervju.

Takk til familien og spesielt Linda for uvurderlig hjelp og støtte gjennom hele prosessen.

Og til Martin og Julie; nå er pappa endelig ferdig.

Ingar Smedstad

Innhold

Figurer

1 Innledning

1.1 Tema

Denne oppgaven omhandler hendelsesrapportering innen informasjonssikkerhet. Utgangspunktet er en systemdynamisk modell av Sveen, Rich og Jager [1]. Denne modellen blir brukt som et ideelt hendelsesrapporteringssystem i undersøkelsen. Det er laget noen hypoteser ut fra denne modellen, og disse har blitt undersøkt ved en bedrift innen norsk olje- og gassindustri som har innført hendelsesrapportering innen informasjonssikkerhet. Undersøkelsen er basert på kvalitative, strukturerte intervju med flere lag i organisasjonen. I tillegg har det blitt hentet støtte i litteratur.

1.2 Nøkkelord

Informasjonssikkerhet, hendelsesrapportering.

1.3 Bakgrunn

I industrien har man i mange år gått systematisk til verks for å samle informasjon om ulykker, og siden også nestenulykker og hendelser som kunne ført til ulykker. Den systematiske innsamlingen har åpnet for vitenskapelige undersøkelser og muligheten for grundig etterforskning for å avdekke årsaken til hendelsene/ulykkene, og har i siste instans gitt industrien og bedriftene muligheten til å innføre stadig bedre sikkerhetstiltak og -rutiner.

Flere forskere har tatt til orde for at det også innen informasjonssikkerhet bør kunne gå an å lage et slikt system. For bedrifter og organisasjoner som ønsker å sertifiseres etter ISO/IEC 17799 [2] standarden, heter det at formelle hendelsesrapporterings- og eskaleringsprosedyrer skal være på plass, og at alle ansatte og kontraktører skal være oppmerksomme på prosedyrene for å rapportere hendelser og også om sitt ansvar for å rapportere hendelser.

Spesielt i olje- og gassindustrien brukes det stadig mer fjernstyring ved hjelp av datanettverk i det som går under samlebegrepet Integrerte Operasjoner [3]. I tillegg til å medføre betydelig risiko i seg selv [4], kan dette fører til at informasjonssikkerhetshendelser i stadig økende grad også kan ha konsekvenser for helse, miljø og sikkerhet (HMS) [5]. Skillet mellom informasjonssikkerhet og HMS blir derfor stadig mindre tydelig.

Det er en del organisatoriske og personlige problemstillinger knyttet til hendelsesrapporteringssystemer både innen HMS og IS. Systemene er ofte plaget med underrapportering, selv i bedrifter som skryter av å ha en god sikkerhetskultur [6, 7, 8].

Sveen et al. [1] har laget en omfattende modell ved hjelp av systemdynamikk som skal hjelpe til med å identifisere de mange forskjellige fallgruvene et slikt system kan gå i, samt finne faktorer som kan føre til et bedre system for organisatorisk læring og utvikling. Denne modellen inngår også i Finn Olav Sveen sin doktorgrad.

1.4 Forskningsspørsmål

Denne oppgaven er en innledende undersøkelse og vil forsøke å belyse enkelte sider ved modellen til Sveen et al. Undersøkelsen er tenkt brukt som en del av datagrunnlaget i hans doktorarbeid. Hensikten med oppgaven er å bruke modellen normativt og sammenligne bedriftens rutiner for hendelsesrapportering innen informasjonssikkerhet med modellen. Det er utarbeidet en del hypoteser med utgangspunkt i modellen. Før hendelsesrapporteringssystemet har blitt undersøkt mot disse hypotesene, har det blitt sjekket om hypotesene har støtte i litteraturen.

Undersøkelsen vil kunne bidra med anbefalinger i forhold til organisasjonens hendelsesrapporteringssystem, og også bidra med kunnskap som kan være nyttig i videre utvikling av den systemdynamiske modellen. Forskningsspørsmålene blir da som presisert nedenfor:

1. Er det støtte i litteraturen for hypotesene utarbeidet med basis i modellen til Sveen et al.?
2. Hvordan forholder hendelsesrapportering innen en organisasjonen i oljesektoren i Norge seg i forhold til modellen?

2 Systemdynamikk

Modellen som er utgangspunkt for studien er systemdynamisk. Derfor vil jeg gi en kort redegjørelse for noen sentrale punkt rundt systemdynamikk. Selve modellen vil bli behandlet i et eget kapittel.

2.1 Hva er systemdynamikk?

Systemdynamikk er et sett med verktøy som muliggjør forståelse av strukturen og dynamikken i komplekse systemer [9]. Systemdynamikk er basert på teori om ikkelineær dynamikk og feedbackkontroll som kommer fra matematikk, fysikk og teknikk [10]. Fagfeltet har sin opprinnelse fra MIT i USA på 50-tallet, hvor Jay Forrester anses å være fagets grunnlegger.

En grunnleggende antagelse i systemdynamikk er at initialtilstanden og den kausale feedbackstrukturen i systemet bestemmer dets atferd over tid [10]. Når et system utvikler seg over tid, kan adferden til systemet endre den dominante strukturen. Systemdynamikk er slik sett en lovende tilnærming for å se på komplekse dynamiske problemer som akkumuleres over tid [11]. Systemdynamikk brukes ofte i utviklingen av formelle datamodeller og for simulering av tiltak og langsiktig utvikling i komplekse systemer. Systemdynamikk kan således oppfattes som et verktøy for læring og testing av strategier i en simulert verden.

Systemdynamikk som tilnærming er en filosofi og et verktøy for å modellere og analysere dynamiske systemer. Like viktig er det at tilnærmingen gir teknikker og verktøy for å undersøke nåværende beslutningstaking og å hjelpe beslutningstakere med å lære. Språket som anvendes er vanlig for alle typer systemer som medisin, økonomi og ledelse [12]. Når systemdynamiske verktøy blir anvendt på sosiale systemer med menneskelig beslutningstaking og -atferd, så inkorporerer systemdynamikk også teorier fra kognitiv- og sosialpsykologi, økonomi og andre samfunnsvitenskaper [10]. Systemdynamikk som tilnærming er derfor tverrfaglig.

Et viktig poeng med systemdynamikk er at modeller skal være lukkede systemer i motsetning til åpne systemer. Atferden til lukkede systemer avhenger av faktorer som er systeminterne. Dette er i klar kontrast til åpne systemer som er svært avhengig av verdiene til eksterne faktorer. For å kunne reprodusere nøkkelegenskapene til adferden i systemet som undersøkes, må forskeren være åpen for å se på problemet i videre perspektiv. Dette fører i retning av et mer helhetlig perspektiv i forhold til problemene og flytter fokus til problemenes grunnårsak [13].

Målet med systemdynamisk arbeid er i hovedsak prosessorientert, i motsetning til produktorientert (økonometri). Dette betyr at målet med modellering er å generere mer kunnskap.

2.2 Systemdynamisk metode

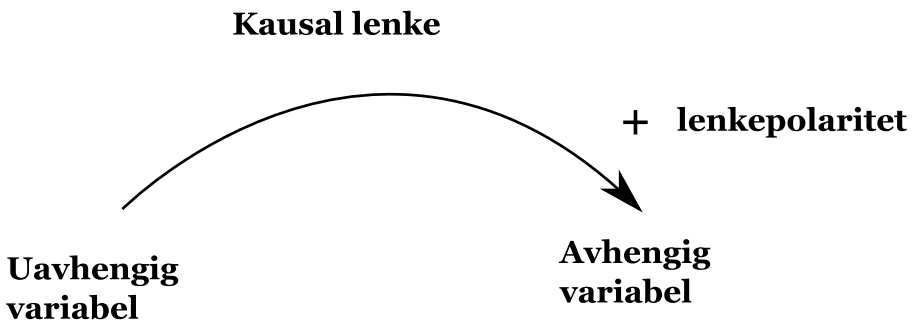
Systemdynamikk avhenger i stor grad av kvantitative data for å lage feedbackmodeller [14]. Flere anerkjenner likevel at innsamling og analyse av kvalitative data spiller

en sentral rolle i modelleringsprosessen [15, 16, 17, 18, 10, ref i [14]]. Samfunnsvitere har utviklet en serie forskningstilnærminger orientert mot innsamling og analyse av kvalitative data. Blant datainnsamlingsmetodene er intervju, fokusgrupper og deltagende observasjon. Dataanalyse kan skje som diskursanalyse, grounded theory-metodologi og etnografiske beslutningsmodeller [19, ref i [14]]. Disse framgangsmåtene ble utviklet både for å teste eksisterende teori og generere nye teorier. Luna-Reyes og Andersen [14] tror at en formell innlemming av disse samfunnsvitenskapelige metodene kan vise vei for systemdynamikere i modelleringsprosessen.

2.3 Kausale løkkediagram

Det er her nødvendig å redegjøre for ett av verktøyene som systemdynamikk bruker, kausale løkkediagrem, siden det er det som er brukt i modellen til Sveen et al.

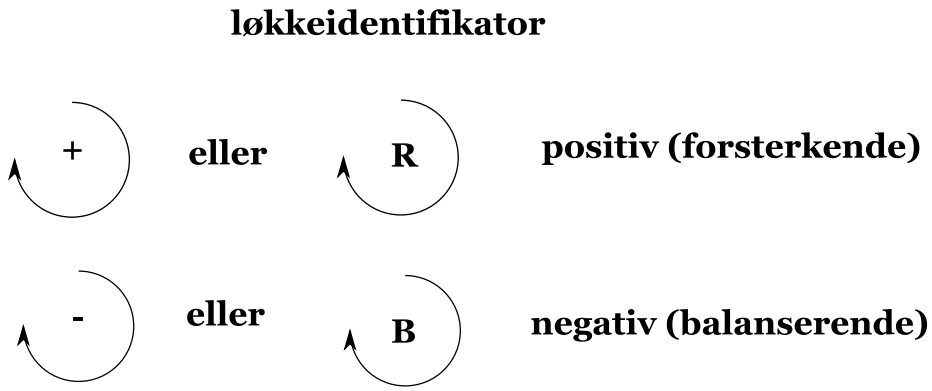
Feedback er kjernen i systemdynamikk. Et viktig verktøy for å presentere feedbackstrukturen i et system er kausale løkkediagram (heretter CLD (causal loop diagram)). Den konvensjonelle måten å lage slike diagrammer på er enkel, men bør følges nøye [10]. CLD består av variabler som er forbundet med piler, og disse angir den kausale påvirkningen mellom variablene (se figur 1).



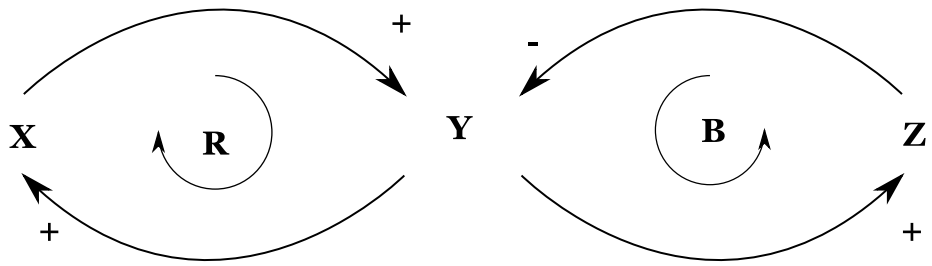
Figur 1: Kausal lenke

Polariteten viser hvordan den avhengige variabelen vil forandre seg når den uavhengige variabelen forandrer seg. Når lenker påvirker hverandre, dannes det løkker. Viktige løkker trekkes frem med løkkeidentifikatorer (se figur 2) som angir retningen på løkken og om løkken er forsterkende (positiv) eller balanserende (negativ).

Figur 3 viser et enkelt eksempel på et CLD. Når X vokser (minker) vil også Y vokse (minke) og motsatt. Dette danner en forsterkende løkke. En økning i Y vil gi en tilsvarende økning hos Z, mens når Z vokser, vil Y avta og vi får en balanserende løkke.



Figur 2: Løkkeidentifikator



Figur 3: Kausalt løkkediagram (CLD)

3 Hendelsesrapportering

3.1 Hendelser

NORSOK [20] definerer i sin standard for HMS følgende:

> **Hendelse** Et tilfelle eller kjede av tilfeller som har eller kunne ha forårsaket skade, sykdom og/eller skade (tap) på eiendom, miljø eller tredjepart.
>
> **Ulykke** Et tilfelle eller kjede av tilfeller som har forårsaket skade, sykdom og/eller skade (tap) på eiendom, miljø eller tredjepart.
>
> **Nestenulykke** Et tilfelle eller kjede av tilfeller som under litt andre omstendigheter kunne ha ført til uhell.

For informasjonssikkerhet kan vi bruke NorSIS [21] sin definisjon på hendelse:

> "Innen informasjonssikkerhet er en «hendelse» en situasjon som som gir, eller som har potensial til å gi, brudd på forventet nivå av konfidensialitet, integritet og/eller tilgjengelighet."

3.2 Hva er hendelsesrapportering?

Bruk av hendelsesrapporteringssystemer blir i økende grad brukt som en effektiv metode for å analysere hendelser. Målet med rapportering og analyse er å finne koblingen mellom hendelser for så å forebygge at de inntreffer igjen [22].

Mesteparten av forskning rundt hendelsesrapportering er gjort innen HMS. Teorien bak hendelsesrapportering bygger mye på observasjonen til Turner [23, ref i [24]] om at ulykker har en lang inkubasjonstid der faresignaler (eller hendelser) ikke oppdages, eller de ignoreres. Men organisasjoner som har et effektivt system for å lære av hendelser, kan reagere på disse hendelsene og forhindre ulykker i å inntreffe.

En grunnleggende antagelse er at ulykker kan forhindres ved systematisk erfaringstilbakemelding [25]. For at en bedrift skal kunne lære av disse tilbakemeldingene, må det være på plass et system som samler og håndterer dem. Et vellykket hendelsesrapporteringssystem krever en effektiv rapportering, formidling og læring av hendelser [26].

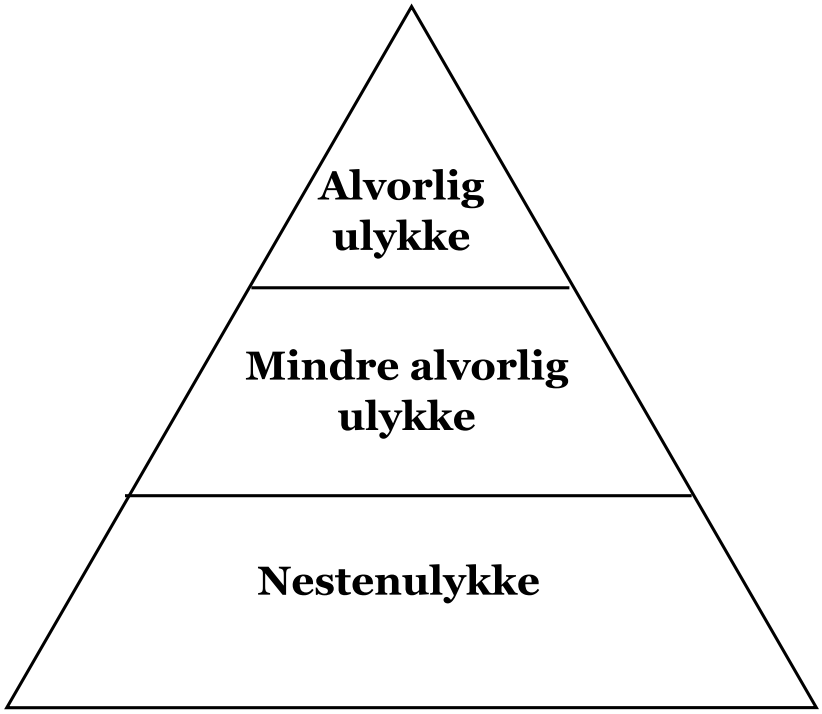
En annen grunnleggende antagelse for et rapporteringssystem er at hendelser og ulykker har samme kausale faktorer [25] (se figur 4), og at det er tilfeldigheter som gjør at en hendelse resulterer i en ulykke eller nestenulykke. Ideen om felles årsak ble først lagt frem av Heinrich i boken "Industrial Accident Prevention" i 1931 [27, ref. i [28]].

Jones, Kirchsteiger og Bjerke [29] argumenterer med at det å rapportere og undersøke nestenulykker er en viktig del av sikkerhetsarbeidet i industrien. De skriver:

> "It is good business practice in practically all industry sectors to collect information on incidents that have occurred and learn from them in order not to repeat mistakes."

De argumenterer med at dersom man antar at det forekommer nestenulykker regelmessig, så representerer det en stor mengde data som kan samles og læres av.

For å underbygge sin argumentasjon viser de blant annet til Norsk Hydro som på 1980-tallet begynte å fokusere på å rapportere nestenulykker offshore, og som erfarte en omvendt proporsjonalitet mellom antall rapporterte nestenulykker og ulykker.



Figur 4: Viktigheten av nestenulykker

De konkluderer med at å fokusere på å redusere nestenulykker vil senke antallet ulykker som skjer, og også at den inverse proporsjonaliteten mellom *rapporterte* nestenulykker og ulykker antyder at antall rapporter om nestenulykker er en numerisk indikator for sikkerhetsbevisstheten i industrien.

3.3 Mennesker og hendelsesrapportering

Et problem med hendelsesrapportering er at det veldig ofte er personer som er direkte berørt av hendelsene som har mulighet til å (og som bør) rapportere. Dette kan fort føre til en konflikt mellom personens plikt til å rapportere og personens ønske om å beskytte seg selv. Collins [8] undersøkte rapportering på oljeinstallasjoner i Nordsjøen. Han fant at prestasjonsmåling ofte fører til måling av ansatte, og at dette igjen har en negativ innvirkning på hendelsesrapportering, også i organisasjoner som mente de hadde en gjennomgående (all-pervasive) sikkerhetskultur. Selv om rapporteringsunnlatelse var en oppsigelsesgrunn, ville de ansatte ofte vegre seg for å rapportere eller dysse ned alvoret i rapportene de leverte.

Gonzales og Sawicka [30] ser på et enkelt fiktivt tilfelle, og bruker det som grunnlag for å lage en systemdynamisk modell som kan simulere de menneskelige faktorene ved informasjonssikkerhet, og som kan være med på å danne grunnlaget for mer robuste sikkerhetspolicyer.

Resultatene antyder at Kim, deres fiktive ansatte, er mest lydig overfor sikkerhetstiltak når hennes oppfattelse av risiko er høyest, og hennes følelse av risiko blir oppdatert av hendelser. Tilstedeværelse av hendelser øker hennes oppfattelse av risiko dramatisk, og motsatt; fravær av hendelser har en dempende effekt på hennes oppfattelse, og som en konsekvens, hennes lydighet.

3.4 Eksempler på hendelsesrapportering innen informasjonssikkerhet

National Institute of Standards and Technology (NIST) har laget en *Computer Security Incident Handling Guide* [31]. Den handler mye om *Computer Security Incident Response Team* (CSIRT), men har lite å si om den menneskelige delen av hendelsesrapportering. De nevner bare at hendelser også kan oppdages gjennom direkte rapport fra brukere.

Siponen [32] snakker om fem dimensjoner ved informasjonssikkerhet. Den ene dimensjonen er den organisatoriske dimensjonen, og han snakker da spesielt om forståelse og bevissthet om informasjonssikkerhet i organisasjonen.

Rollason-Reese [33] beskriver hvordan de har implementert en CSIRT i Eastern Connecticut State University for å håndtere hendelser. Disse hendelsene kan komme som følge av rapporter fra brukere, men det er er mer trolig at de kommer fra automatiske systemer som er laget for å detektere slike ting.

4 Modellen

Modellen (Se figur 5) består av et sett kausale løkker som beskriver hvordan hendelser rapporteres, evalueres og anvendes for en organisasjons læring. I modellen skilles det mellom "incident" (heretter kalt sikkerhetsbrudd) og "event" (heretter kalt hendelse). I litteraturen defineres disse begrepene ofte på ulike måter, men Sveen et al. [1] definerer en hendelse som en uforutsett situasjon eller nestenulykke, som håndteres med få eller ingen korttidskostnader. Hvis en hendelse ikke hanskes med og dempes, omdannes den til et sikkerhetsbrudd.

Sveen et al. forutsetter at hendelser og sikkerhetsbrudd reduseres i forhold til en erfaringskurve: med hver dobling av ordentlig undersøkte sikkerhetsbrudd reduseres forekomsten av hendelser og sikkerhetsbrudd med en viss prosent, noe som reflekterer gradvis læring via erfaring med hendelser og sikerhetsbrudd.

Modellen til Sveen et al. skiller mellom balanserende (negative) og forsterkende (positive) løkker. B i modellen står for balanserende (balancing), og det skilles mellom fire balanserende løkker:

B1: Læring av hendelser
B2: Læring av sikkerhetsbrudd
B3: Negative ettervirkninger som gjør at folk lar være å rapportere
B4: Overarbeidede etterforskere

R står for forsterkende (reinforcing) og det skilles mellom tre forsterkende løkker:

R1: Keeping the staff 'in the loop' "
R2: Bevissthet avler bevissthet
R3: Lotterier og små belønninger

Målet med et hendelsesrapporteringssystem er å dele informasjon om sikkerhetsbrudd for å unngå gjentagelse eller minimere skade. Når en hendelse eller et sikkerhetsbrudd inntreffer, vil vanligvis en operatør (for eksempel en sykepleier eller pilot) oppdage den og rapportere den. I et ideelt hendelseshåndteringsmiljø vil et undersøkende team overta på dette stadiet og prøve å finne systematiske årsaker til hendelsen. Når årsaken er funnet, kan sikkerhetstiltak settes i verk, personalet kan bli bevisst faren og problemet og dermed unngå fremtidige forekomster av samme sikkerhetsbrudd (B2) eller hvis det er en hendelse, unngå at den i fremtiden omdannes til et sikkerhetsbrudd (B1). I takt med at personalet blir mer bevisst på sikkerhet, blir de bedre til å finne potensielle hendelser og flere hendelser blir rapportert (R1).

I modellen er B1 og B2 balanserende feedbackløkker hvor et eksogent trykk vil bli balansert over tid. B1 og B2 beskriver hvordan en økning i raten av nye hendelser øker kunnskap som igjen øker bevisstheten og reduserer raten av hendelser i fremtiden.

R2 er en forsterkende feedbackløkke som beskriver hvordan en sterk sikkerhetskultur skaper press som videre styrker den.

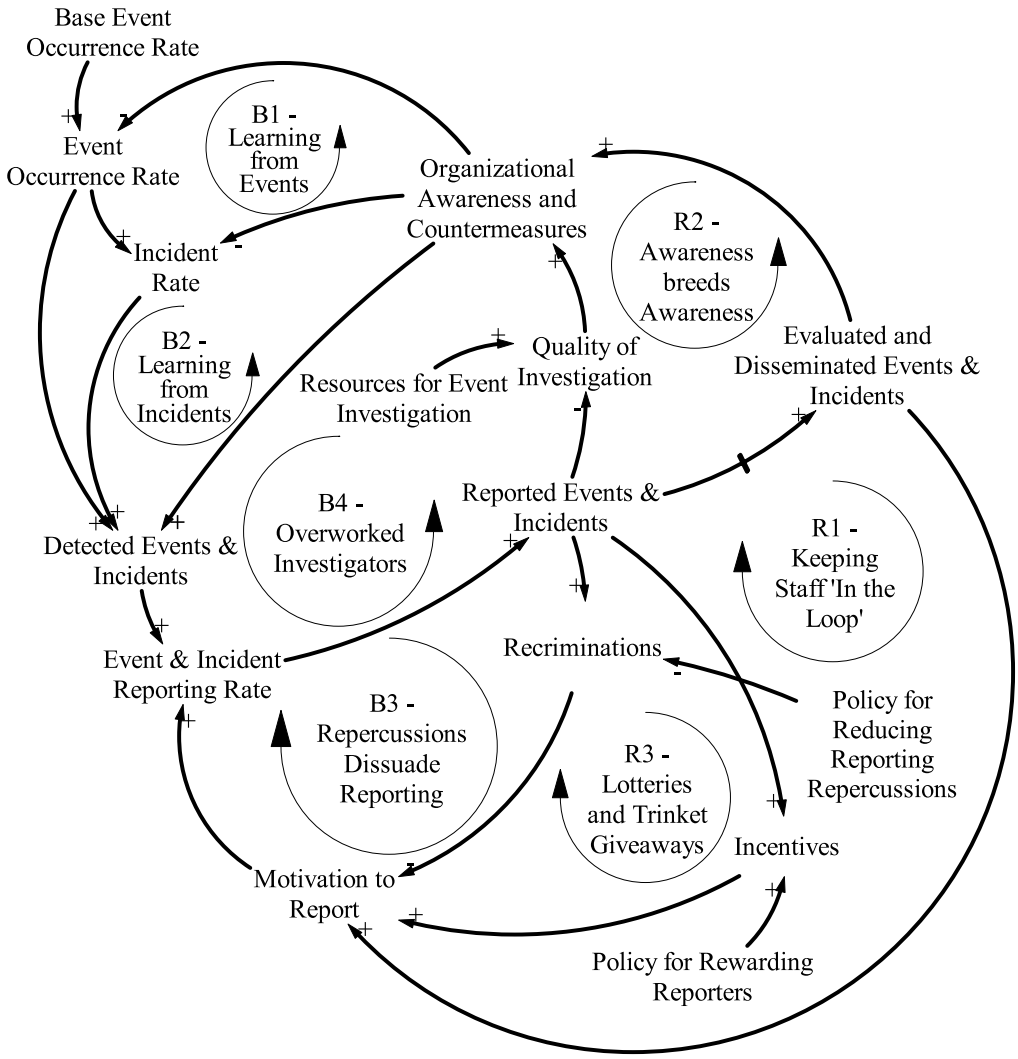
B3 og B4 er balanserende feedbackløkker som motvirker effekten av R2.

Dersom personell erfarer at rapportene deres blir tatt alvorlig og at deres deltagelse fører til sikkerhetsforbedringer, så øker motivasjonen deres (R1). Hvis rapporteringen derimot ikke fører til forbedringer, så vil ikke personalet fortsette å rapportere. Det er dette som kalles "keeping staff 'in the loop'".

Mange organisasjoner bruker insentiver for å øke rapporteringsraten (R3). En sterk, negativ motivasjonsfaktor for rapportering er forskjellige negative ettervirkninger som eksisterer i og mellom organisasjoner (B3). Det å få reprimande fra ledelsen, å bli sett på som illojal, å bli utsatt for mediafokusering, kanskje med påfølgende rettslige forfølgelse, er noen av faktorene som gjør at folk lar være å rapportere.

Den siste delen av modellen omhandler kvaliteten på undersøkelsene. Hvis kvaliteten er for lav, for eksempel hvis man ikke finner årsaken til hendelsen, vil organisasjonens bevissthet ikke øke, og sikkerhetstiltak vil ikke være effektive.

I modellen er kvaliteten på evalueringen forenklet til en funksjon av mengde tilgjengelige ressurser og arbeidsmengde. I realiteten vil en undersøkers øvingsnivå og erfaringsnivå også bidra. Alle hendelser og sikkerhetsbrudd har like stor alvorlighetsgrad i modellen, men i virkeligheten vil alvorlige hendelser mest sannsynlig motta tilleggsressurser under en undersøkelse.



Figur 5: IRS modellen

5 Hypotesene

Som nevnt innledningsvis er målet med denne oppgaven å anvende modellen normativt for å undersøke hvordan en bedrift i oljesektoren hendelsesrapporterer. For å få svar på dette forskningsspørsmålet, ble det utviklet en rekke hypoteser.

Denne oppgaven er en av tre masteroppgaver hvis resultater er tenkt å inngå i Sveens PhD-prosjekt. De to andre oppgavene ser på henholdsvis hendelsesrapportering i helsesektoren og i forsvaret. I prosessen med utvikling av hypotesene til undersøkelsen var det derfor viktig at de kunne undersøkes på alle tre bedriftene. Hypotesene ble derfor utviklet i samarbeid med Sveen og de andre studentene.

Vi tok utgangspunkt i modellen (figur 5) og dekomponerte denne til hypoteser. Til sammen kom vi frem til 32 hypoteser. Et intervju som dekker et slikt grunnlag ville ta flere timer å gjennomføre, og vi anså det som lite sannsynlig at vi ville finne informanter som var villig bruke så mye tid i en travel arbeidsdag. Vi lagde derfor våre prioriteringer av hypotesene. Disse ble så stilt opp mot hverandre og med et par rettelser og sammenslåinger av lignende hypoteser kom vi frem til følgende ti hypoteser:

1. Tilbakemelding til ansatte som rapporterer, er viktig for å motivere for rapportering i fremtiden. Dersom ansatte ikke ser at rapportering er nyttig og blir tatt seriøst, vil de slutte å rapportere.
2. Utydelige retningslinjer og andre former for usikkerhet angående rapportering av informasjonssikkerhetshendelser fører til suboptimal rapportering og dermed også til suboptimal læring. Hvis brukere for eksempel ikke vet hva de skal rapportere, hvem de skal rapportere til og hvordan de skal rapportere, vil ikke organisasjonen lære effektivt.
3. Kunnskap man har tilegnet seg gjennom undersøkelser av hendelser, gjør det mulig for organisasjonen å heve bevisstheten rundt informasjonssikkerhet og å sette i verk effektive tekniske og organisatoriske mottiltak for å redusere fremtidig sårbarhet. Dermed vil gjentagelser av tidligere hendelser kunne reduseres, angripere vil bli mindre motivert til å prøve å angripe og utilsiktede sikkerhetsfeiltrinn, som for eksempel glemte laptopper, vil antagelig bli mindre sannsynlig. Videre vil angrep og utilsiktede sikkerhetsbrudd kunne bli oppdaget og avverget før vesentlig skade oppstår. Med andre ord vil det være mindre fare for at hendelser skal eskalere til sikkerhetsbrudd.
4. Kunnskap fra hendelsesrapporter er avhengig av kvaliteten på etterforskningen. Dersom arbeidspresset er stort, vil kvaliteten på etterforskningen synke når etterforskerne må kutte noen svinger for å rekke alt. Etterforskere vil prioritere de viktigste rapportene dersom de ikke har nok ressurser, men selv om man prioriterer, vil likevel mindre viktige rapporter stjele tid og ha negativ innflytelse på den totale kvaliteten.
5. Rapporter kan medføre mottiltak som disiplinære sanksjoner, isolering fra medarbeidere og så videre.

6. Insentiver blir ineffektive dersom det eksisterer sterkt fordømmende holdninger overfor rapporterende. Dette vil for eksempel føre til en tilbøyelighet til å rapportere hendelser som ikke fordømmes, eller ikke rapportere i det hele tatt.
7. Informasjonssikkerhetshendelser og -brudd har liknende årsak.
8. Rapportering av nestenulykker er nyttig innen informasjonssikkerhet.
9. Toppledelsens støtte er avgjørende for at et rapporteringssystem for informasjonssikkerhetshendelser skal være vellykket.
10. Ansatte vil ikke overholde retningslinjene for rapportering hvis de ikke har tid eller kompetanse til å rapportere, eller hvis de ikke ser på rapportering som nyttig.

6 Metode

6.1 Valg av metode

Etter enighet rundt hypotesene var det viktig å velge en fremgangsmåte for undersøkelsen som gjorde det mulig å sammenligne resultatene fra de forskjellige bedriftene. Vi valgte å bruke kvalitative intervju som metode siden tilgang til skriftlig materiale er begrenset, og mye av kunnskapen vi var på jakt etter ikke finnes i skriftlig form.

For å gjøre det mulig å sammenligne data fra de tre organisasjonene falt valget på strukturert intervju. Modellen favner ganske vidt og omfatter mange lag i organisasjonen. Det ble bestemt at det skulle lages tre sett med spørsmål for henholdsvis ledere/prosesseiere, sikkerhetspersonell/policylagere og brukere. Alle tre studentene utviklet hver for seg spørsmål. Disse ble samlet, og sammen med Sveen ble det foretatt et utvalg av de beste alternativene til en felles intervjuguide. Denne guiden ble så kvalitetssjekket av Eliot Rich ved University at Albany.

I utgangspunktet ble vi enige om å teste intervjuprotokollen ved å intervjue hverandre, men tidsmessige og geografiske begrensninger gjorde at vi ikke hadde mulighet til å avholde pilotintervju. Vi lot derfor de første intervjuene være en retningslinje for kvalitet til intervjuguiden. Vi fikk noen tilbakemeldinger, og det ble ikke nødvendig å justere på mer enn ett spørsmål.

6.2 Valg av intervjukandidater

Når informantene skulle velges var det viktig at dette ble godkjent av ledelsen i selskapet, så prosessen startet der. Det ble tatt kontakt med sikkerhetsansvarlig ved bedriften og gitt informasjon om masteroppgavens formål og utfra dette bedt om samtykke til å rekruttere intervjupersoner. Dette ble møtt med positiv respons.

Ingen av informantene ble på forhånd spurt om de visste noe om hendelsesrapportering og det ble heller ikke gjort noe forsøk på å spore opp informanter som var mer informert enn andre.

Organisasjonen var på intervjutidspunktet inne i en omorganiseringsprosess og det var derfor ikke mulig å få tak i de ansvarlige sikkerhetspersonell som hadde med policyen å gjøre. Av den grunn dekker denne studien åtte av de ti felles formulerte hypotesene. De to andre vil likevel bli belyst i diskusjonsdelen, da med grunnlag i litteratur. Det ble til sammen utført seks intervju, tre fra ledere/prosesseiere og tre fra brukere.

6.3 Datainnsamling og transkripsjon

Før intervjuet ble gjennomført, fikk intervjupersonene en kort fremstilling av hensikten med undersøkelsen. Alle intervjuene er avtalt direkte med informantene selv. Det er ingen andre som sitter med en oversikt over hvem som har blitt intervjuet, noe som bidrar til anonymisering. I tillegg var det ett intervju som det av tekniske årsaker ikke ble gjort opptak av.

Alle intervjuene i denne oppgaven ble gjennomført muntlig, ansikt til ansikt og innspilt på bånd, etter muntlig samtykke fra informantene.

Intervjuene ble gjennomført høsten 2007. Alle intervjuene ble gjennomført på intervjuers kontor, og det var en og samme person som foretok samtlige intervjuer.

Alle intervjuene foregikk på norsk, og i etterkant ble de ordrett transkribert.

6.4 Analyse

Svarene fra informantene ble etter transkripsjon sortert etter spørsmål og lagt sammen i en tabell. Det ble deretter foretatt en meningsfortetting av svarene slik at det på hvert spørsmål var en samlet analyse av dem. Eventuelle uenigheter ble notert. Deretter ble spørsmålene gruppert og koblet sammen med de hypotesene spørsmålene omhandlet, og en endelig analyse foretatt.

6.5 Litteratur

Med unntak av noen få bøker er mesteparten av litteraturen hentet fra de elektroniske fulltekstdatabasene som har vært tilgjengelig via Høgskolen i Gjøvik. I de mest interessante kildene har referansene også blitt undersøkt for å finne litteratur som ikke har fremkommet ved egne søk. Søkeord som har vært brukt har hovedsakelig vært en kombinasjon av følgende:

- information security
- incident reporting
- near miss
- informasjonssikkerhet
- hendelsesrapportering
- hendelse
- nestenulykker

7 Funn

Organisasjonen har innført rapportering for informasjonssikkerhethendelser. Det var mulig å finne retningslinjene i dokumenthåndteringssystemet, men det var ikke noen åpenbar reklamering for den. I min studie har jeg i tillegg til disse retningslinjene brukt referater fra planleggingsmøter som gikk forut for innføring av systemet.

7.1 Beskrivelse av organisasjonens policy for hendelsesrapportering

Organisasjonen bruker allerede et hendelsesrapporteringssystem for å rapportere hendelser for HMS. Alle ansatte har tilgang til systemet, og det forventes at de registrerer hendelser som skjer i tillegg til potensielle farer de observerer. De skal nå også bruke dette systemet til å rapportere informasjonssikkerhetshendelser.

Datakvalitet

For å sikre kvaliteten på data om informasjonssikkerhet er det bestemt at det opprettes en spesiell rolle, hendelsesregistrator, med ansvar for å legge inn rapporter om informasjonssikkerhetshendelser.

Konfidensialitet

Detaljer rundt en del av disse informasjonssikkerhetshendelsene må klassifiseres som konfidensiell informasjon og skal ikke lagres i hendelsesrapporteringssystemet. Systemet vil håndtere lenker til detaljene, men informasjonen vil lagres i et dokumenthåndteringssystem som håndterer tilgangsadministrasjon. Bare spesielle roller vil få tilgang til informasjonen om disse sakene.

Informasjonskilder

Hovedkilden for hendelser er brukerne. De vil normalt kontakte brukerstøtte når de opplever problemer. Diverse team fra brukerstøtte og IT-avdelingen kan bli involvert i håndteringen av hendelser, og også IRT (Incident Response Team) dersom hendelsene er alvorlige.

IT-avdelingen og IRT vil rapportere hendelser til hendelsesregistrator.

Det er forventet at det vil være tilfeller der brukere informerer linjeledere eller andre i ledelsen. Disse må da rapportere til hendelsesregistrator om de finner det nødvendig.

Hva slags hendelser skal rapporteres?

Det vil til syvende og siste være opp til hendelsesregistrator hva slags hendelser som registreres. Sannsynlige tilfeller er:

- brudd på konfidensialitet
- alvorlige brudd på informasjonssikkerhetspolicy
- handlinger som tar sikte på å ødelegge informasjon eller forstyrre tjenester
- tyveri av data eller -utstyr

Generell utilgjengelighet av informasjonssystemer på grunn av tekniske problemer skal ikke rapporteres som en informasjonssikkerhetshendelse.

7.2 Intervjuene

Tilbakemelding til ansatte som rapporterer

Det er ingen av informantene som tror at det blir gitt personlig tilbakemelding etter at en rapport er levert, hverken underveis i prosessen eller når eventuell etterforskning er avsluttet. De som kjente til rapporteringssystemet fra HMS mente at informasjonen er tilgjengelig i systemet for de som er interesser i saken, men det må tydeligvis skje på eget initiativ.

> "Da ble det jo rapportert opp igjennom systemet og det var vel til slutt personal som tok seg av det, men vi fikk vel ikke så mye tilbakemelding egentlig."

Retningslinjer

Prosesseierne var mer informert om at det fantes retningslinjer for rapportering. Men når det gjaldt brukerne var situasjonen en annen. En av brukerne hadde blitt informert om slike retningslinjer ved ansettelse, mens de andre bare regnet med at det fantes noe slikt, uten at de visste hvordan de skulle finne frem til det.

Læring

Det var ingen av brukerne som kjente til detaljer om at sikkerhetspolicyen var blitt endret som følge av rapporterte hendelser, men prosesseierne ga uttrykk for at om en undersøkelse konkluderte med at det måtte innføres tiltak, så ble disse selvsagt fulgt opp.

> "Ja om policyen eller detaljer i løsningen, men ja det er jo en del av poenget. Hvis det oppdages uheldigheter så må en jo prøve å hindre at det skjer igjen ved å tette de hullene som . . . "

Disiplinære sanksjoner

Det var ingen som kjente til noen form for disiplinære reaksjoner mot de som rapporterte, hverken offisielle eller uoffisielle. De som hadde mest innsikt i rapporteringen i organisasjonen mente derimot at det var en en god rapporteringskultur i organisasjonen, med en lav terskel for å rapportere.

Insentiver

Det var en som mente at det var noe som het "Månedens sak" i rapporteringssystemet, men utover det var det ingen som kjente til noen form for insentiver for rapportering. På spørsmål om hva slags effekt de trodde insentiver ville ha, var det en generell oppfatning at det ikke var viktig.

Nestenulykker

Det var en klar mening at det var nyttig å rapportere nestenulykker.

Toppledelsens engasjement

Blant prosesseierne var det tydelige forskjeller i oppfatningene. Den informanten som mente at toppledelsen ikke var interessert, fulgte heller ikke opp rapporteringssystemet selv.

Brukerne hadde mer tiltro til toppledelsen. Selv om de ikke visste noe med sikkerhet, så var det en grunnleggende antakelse at ledelsen selvsagt måtte være interessert i dette. De understreket også sterkt hvor viktig det var at toppledelsen brydde seg.

> "Altså hvis ikke de hadde brydd seg så hadde vel ingen andre brydd seg heller..."

> "... det er jo alfa omega"

Ansattes tid og kompetanse

Bortsett fra en av informantene som var blitt gitt informasjon om rapporteringssystemet ved ansettelse, så var det ingen som kunne vise til noen form for grunnopplæring eller kompetanseheving rundt rapportering av informasjonssikkerhetshendelser. Det var også en klar oppfatning at det var rom for forbedringer i systemet, og at det sikkert var stort innslag av underrapportering. En av grunnene som ble oppgitt var at de er vant til at IT-systemer ikke virker, og dersom de skulle ha rapportert alt, ville det blitt for tidkrevende.

8 Diskusjon

I denne delen vil jeg diskutere funn ut fra hypotesene, jeg vil diskutere hva som kommer frem i annen forskning og diskutere organisasjonens rapporteringssystem sett i lys av hypotesene

Hypotese 1

> Tilbakemelding til ansatte som rapporterer er viktig for å motivere for rapportering i fremtiden. Dersom ansatte ikke ser at rapportering er nyttig og blir tatt seriøst, vil de slutte å rapportere i fremtiden.

Johnson [7] identifiserer noen påstander om fordeler ved et hendelsesrapporteringssystem. Blant annet:

> "Feedback keeps staff 'in the loop'."

Han har altså funnet at hendelsesrapportering oppmuntrer personalet til å bidra til en sikrere arbeidsplass. Han følger opp dette i sin bok [34] og vektlegger der at tillit mellom den som rapporterer og den som mottar rapporten er viktig for å øke motivasjonen for å rapportere. Videre hevder han at det er viktig at den som mottar rapporten melder tilbake til den eller de som rapporterte, at rapporten blir behandlet. I følge Johnson har det svenske luftfartsverket begynt med en elektronisk implementering som automatisk gir personalet tilbakemelding på hvordan rapporten håndteres i alle stadier av prosessen.

Van der Schaaf [35, side 88] finner i sin doktorgradsavhandling om rapportering av nestenulykker at noen av forutsetningene for å få et slikt system til å virke er:

- treningsprogram og støttefunksjoner utviklet i tett samarbeid med brukerne
- kontinuerlig tilbakemelding for å vise hvem som gjør hva med informasjonen og for å vise at det å rapportere hendelser er viktig

I intervjuene kom det fram at informantene ikke visste om det ble gitt tilbakemelding til rapporterende brukere. Både modellen til Sveen et al. og litteratur vektlegger tilbakemelding som en sentral del for å bevisstgjøre organisasjonen og brukerne om sikkerhetsarbeidet som gjøres, og er regnet som et viktig ledd i å bygge opp en sikkerhetskultur.

Hypotese 2

> Utydelige retningslinjer og andre former for usikkerhet angående rapportering av informasjonssikkerhetshendelser fører til suboptimal rapportering og dermed også til suboptimal læring. Hvis brukere for eksempel ikke vet hva de skal rapportere, hvem de skal rapportere til og hvordan de skal rapportere, vil ikke organisasjonen lære effektivt.

Vincent, Stanhope og Crowley-Murphy [6] har gjennomført en empirisk studie om årsaker til at uheldige hendelser ikke blir rapportert. I en tidligere studie av Stanhope, Crowley-Murphy, Vincent, O'Connor og Taylor-Adams [36] om hendelsesrapportering i forhold til uheldige hendelser ved fødeklinikker, fant de at personalet ved to utvalgte

fødeklinikker i London rapporterte mindre enn en fjerdedel av hendelsene til avdelingsledelsen. Forfatterne utviklet derfor et spørreskjema for å undersøke årsakene til at hendelsene ikke ble rapportert. Funnene deres viste blant annet at uklare retningslinjer var en av grunnene. De fleste blant personalet visste om hendelsesrapporteringssystemet ved avdelingen sin, men nesten 30% visste ikke hvordan de kunne finne en liste over rapporterte hendelser. Videre fant de stor variasjon i syn på nødvendigheten av å rapportere. Noen i personalet visste ikke i det hele tatt hva de skulle rapportere, andre tok selvstendige beslutninger og vurderte underveis om en hendelse var verdt å rapportere. De fleste (96%) mente de ville rapportert dersom mor døde ved fødsel, mens under halvparten (46%) ville rapportert uforventet tidlig fødsel. Forfatterne anbefaler blant annet klarere definisjoner av hendelser, enklere rapporteringsmetoder og feedback til personalet som rapporterer, slik at de forstår hensikten med et slikt system.

Johnson [34] mener at både metode og format i hendelsesrapporter må tilpasses informasjonsbehovet til mottakerne av rapporten. Hvis mottakerne har begrenset adgang til datamaskiner, så er det få fordeler ved å ha elektroniske presentasjonsteknikker. Og motsatt, hvis mottakerne stort sett arbeider på datamaskiner, så vil det være frustrerende å lete gjennom papirbunker med hendelsesrapporter.

Organisasjonen i min studie har retningslinjer for hva som skal rapporteres og hvordan. Informantene er derimot ikke informert, hverken om hvor disse retningslinjene befinner seg eller i noen særlig grad at de eksisterer. Flere undersøkelser støtter modellen til Sveen et al. på at for å få folk til å rapportere, så må de ha kunnskap om hvor, hvordan og til hvem dette skal gjøres. I et internt referat fra planlegging av rapporteringssystemet kommer det frem at bedriften er bekymret for at dersom de slipper "alle" til i rapporteringssystemet, så vil de drukne i saker. Det kan være derfor de er tilbakeholdende med å spre dette til alle.

Hypotese 3

> Kunnskap man har tilegnet seg gjennom undersøkelser av hendelser, gjør det mulig for organisasjonen å heve bevisstheten rundt informasjonssikkerhet og å sette i verk effektive tekniske og organisatoriske mottiltak for å redusere fremtidig sårbarhet. Dermed vil gjentagelser av tidligere hendelser kunne reduseres, angripere vil bli mindre motivert til å prøve å angripe og utilsiktede sikkerhetsfeiltrinn, som for eksempel glemte laptopper, vil antagelig bli mindre sannsynlig. Videre vil angrep og utilsiktede sikkerhetsbrudd kunne bli oppdaget og avverget før vesentlig skade oppstår. Med andre ord så vil det være mindre fare for at hendelser skal eskalere til sikkerhetsbrudd.

Nielsen, Carstensen og Rasmussen [37] undersøkte implementeringen av et hendelsesrapporteringssystem i to fabrikker i Danmark. Deres studie bygget på antagelsen om at en vellykket implementering av hendelsesrapporteringsskjema på en fabrikk skal kunne øke fabrikkens evne til å sette opp forebyggende tiltak. For et hendelsesmønster vil vise seg, og utfra dette kan fabrikken utvikle fokuserte forebyggingsstrategier. De fant at implementeringen av hendelsesrapporteringsskjema ble etterfulgt av fokuserte forebyggingstiltak basert på analyse av hendelsesmønstre. Dette ble så etterfulgt av en nedgang i hendelser. Nøkkelfaktoren til suksess slik forfatterne ser det, er forpliktelse hos ledelsen.

Informantene i min undersøkelse har registrert at det har foregått endringer i rutinene, men de kunne ikke si om dette er som direkte følge av rapporterte hendelser. Det er ikke noe i denne undersøkelsen som tyder på at det foregår en *organisasjonell* læring, noe Sveen et al. mener er et mål ved et hendelsesrapporteringssystem. Det er mulig å

stille spørsmål om hvorvidt organisasjonen ser på hendelsesrapportering som et verktøy for informasjonssikkerhetspersonell fremfor et verktøy som skal omfatte alle ledd i organisasjonen.

Hypotese 4

> Kunnskap fra hendelsesrapporter er avhengig av kvaliteten på etterforskningen. Dersom arbeidspresset er stort, vil kvaliteten på etterforskningen synke når etterforskerne må kutte noen svinger for å rekke alt. Etterforskere vil prioritere de viktigste rapportene dersom de ikke har nok ressurser, men selv om man prioriterer, vil likevel mindre viktige rapporter stjele tid og ha negativ innflytelse på den totale kvaliteten.

Gonzalez [38] understreker behovet for et informajonssikkerhetsrapporteringssystem. Han vektlegger behovet for en kvalitetsforbedringsprosess for å finne en riktig balanse mellom å reagere på hendelser og å lære fra hendelser.

Denne hypotesen fikk vi ikke dekket i intervjuet, men ut fra den policy som er laget om hendelsesrapportering, så kan det se ut til at organisasjonen er bekymret for at systemet skal bli overbelastet og derfor har innført et filter i form av dedikert personell som har som oppgave å filtrere bort saker som ikke trenger å undersøkes nærmere. Organisasjonen er prosessstyrt, og når en sak først er rapportert, så må prosessen gå sin gang. Dette kan være ressurskrevende selv om saken er triviell, og organisasjonen prøver derfor å løse dette problemet før det oppstår. De forsøker å gjøre prioriteringen *før* saken når rapporteringssystemet og hele etterforskningsprosessen settes i gang.

Det kan se ut til at organisasjonen i denne undersøkelsen deler modellens syn på at ressurser er avgjørende for god etterforskning og læring. Imidlertid kan det se ut til at de har valgt en mer "utradisjonell" måte å løse dette problemet på ved å begrense omfanget av rapporter fremfor å prioritere rapportene etter at de kommer inn i systemet.

Hypotese 5

> Rapporter kan medføre mottiltak som disiplinære sanksjoner, isolering fra medarbeidere og så videre.

Da Federal Railroad Administration i USA skulle lage en guide for hendelsesrapportering, kom det frem det at var tilfeller der ansatte ikke sa fra om ulykker eller mottok meldingspliktig behandling fra legen fordi de ønsket å unngå mulig trakassering fra ledelsen. Det var også tilfeller av straff forbundet med å rapportere slike hendelser [39, ref. i [7]].

Det er ingen ting hos mine informanter som tyder på at det finnes en straffende rapporteringskultur i organisasjonen.

Hypotese 6

> Insentiver blir ineffektive dersom det eksisterer sterkt fordømmende holdninger overfor rapporterende. Dette vil for eksempel føre til en tilbøyelighet til å rapportere hendelser som ikke fordømmes eller ikke rapportere i det hele tatt.

Dekker [40] argumenterer sterkt mot å ha menneskelig svikt som utgangspunkt i undersøkelse av ulykker. Han mener at det blir alt for lett å trekke den konklusjonen at menneskelig svikt er *årsaken* til ulykken og slå seg til ro med det. Dette fokuset vil ofte føre til en oppfatning av at systemet er sikkert, mens det er menneskene som er problemet. En vanlig måte å bekjempe menneskelig svikt på, er å straffe menneskene som begår alvorlige feil istedenfor å forsøke å finne ut hvorfor og hvordan de kunne gjøre disse feilene.

> "Fear as investment in safety? This is a bizarre notion. . . . the balance of scientific opinion is quite clear: fear doesn't work. In fact, it corrupts opportunities to learn."

Barach og Small [41] spør hvordan man skal kunne forandre en bebreidende motarbeidende kultur til en lærende kultur som øker sikkerheten. De mener det er nødvendig å introdusere normer som innprenter en lærende og ikkestraffende rapporteringskultur gjennom utdanning og kurs.

I følge utsagnene til mine informanter er det lite som tyder på at organisasjonen bruker insentiver som et aktivt redskap for å få folk til å rapportere. Tilsynelatende fravær av både fordømmende holdninger og bruk av insentiver gjør at det ikke er mulig å si noe om styrkeforholdet mellom disse to motstridene faktorene i organisasjonens hendelsesrapporteringssystem.

Hypotese 7

Informasjonssikkerhetshendelser og -brudd har liknende årsak.

I litteraturen rund hendelsesrapportering for HMS så er det en rådende oppfatning at det finnes en felles årsak mellom hendelser og ulykker, men jeg har ikke funnet noe forskning som viser at den samme antagelsen gjelder for informasjonssikkerhet. Det er mange som har begynt å kategorisere hendelser i informasjonssikkerhet, men det er ikke sikkert det er mulig å lage en komplett liste over ting som kan gå galt. Folk har prøvd på dette og i noen tilfeller laget lister som er meget omfattende. Det er åpenbart fare for at en slik liste ikke er endelig. Slike lister har derfor begrensede anvendelsesområder [42, ref. i [43]].

Ut fra organisasjonens policy for rapportering kan vi se at de har laget et forslag til hendelser de ser på som skal rapporteres. Modellen til Sveen et al. tar ikke stilling til hva slags hendelser som blir rapportert, men handler snarere om prosessen som settes i gang *etter* at en hendelse blir rapportert.

Hypotese 8

Rapportering av nestenulykker er nyttig innen informasjonssikkerhet.

I industrien er det mange studier som viser at det er nyttig å rapportere og undersøke nestenulykker. Jones et al. [29] gjorde en undersøkelse som begynte å fokusere på nestenulykker i Norsk Hydro på slutten av åttitallet. Når organisasjonen i en periode var mindre opptatt av nestenulykker, så steg antallet ulykker. Norsk Hydro fant ut at å fokusere på nestenulykker, fungerte som en vekker for folk. Det ble også observert at det var en omvendt proporsjonalitet mellom antall rapporterte nestenulykker og antall ulykker.

Informantene i min studie var av den oppfatning at det var nyttig å rapportere nestenulykker, men det må stilles spørsmål ved om dette utsagnet kommer som følge av deres erfaringer med hendelsesrapportering for HMS. For ut fra policy for rapportering kan det se ut som om organisasjonen først og fremst ønsker rapport om alvorlige hendelser.

Hypotese 9

Toppledelsens støtte er avgjørende for at et rapporteringssystem for informasjonssikkerhetshendelser skal være vellykket.

Nielsen et al. [37] fant i sin studie om implementering av hendelsesrapporteringssystem i to danske fabrikker at i den ene fabrikken var implementeringen vellykket og antall ulykker gikk merkbart ned. I den andre var det derimot ingen suksess, og Nielsen et al.

peker på toppledelsens manglende engasjement som hovedgrunn. Ledelsen var positive til ideen om å sette opp et rapporteringssystem, men fulgte ikke opp arbeidet i etterkant. Toppledelsens engasjement er ansett som å være en av de aller viktigste faktorene for alt arbeid med HMS [44, ref. in [37]].

Danielsson og Stubbs [45] har gjort en litteraturundersøkelse og også kommet frem til at den faktor som oftest blir trukket frem som skal ha størst innflytelse på utfallet til sikkerhetsarbeid, er aktiv deltakelse fra ledelsen. Derfor foreslår de at man bør utvikle en utdannelse for sikkerhet for bedrifter i likhet med MBA (Master of Business Administration).

Mine informanter gikk mer eller mindre ut fra at toppledelsen var engasjert i dette, og mente det var nødvendig for at systemet skulle fungere i det hele tatt. Det er derimot mulig at dette engasjementet ikke deles av alle ledd i linjeledelsen da det blant prosesseierne var varierende grad av kunnskap om rapporteringssystemet. I Sveen et al. sin modell er ikke toppledelsen direkte representert, men de oppfattes utvilsomt som en forutsetning. Ledelsen er indirekte involvert i modellen ved at det er de som er ansvarlig for policy og også for at det blir stilt ressurser til rådighet for undersøkelser. Videre har de muligheter til å påvirke ved å legge til rette for bruk av insentiver, og ved å bekjempe negative følger ved å rapportere hendelser.

Hypotese 10

> Ansatte vil ikke overholde retningslinjene for rapportering hvis de ikke har tid eller kompetanse til å rapportere eller om de ikke ser på rapportering som nyttig.

Sveen et al. [26] peker på en viktig forskjell i rapporteringssystemer i HMS og i informasjonssikkerhet. En HMS-hendelse kan åpenbart og veldig tydelig være en trussel mot egen helse, mens for informasjonssikkerhet så vil effekten av hendelser ofte ikke være mer enn et irritasjonsmoment eller rett og slett ikke ha noen effekt for brukerens umiddelbare arbeidssituasjon.

Gonzalez og Sawicka [30] finner i sin modell av en fiktiv ansatt, Kim, at hun er minst trolig til å følge policy om å rapportere når det ikke har skjedd hendelser. Hendelsene er med på å minne henne om at det kan skje noe galt, og at hendelsesrapporteringssystemet er der for å forhindre at noe alvorlig skjer.

I et omfattende litteratursøk identifiserte van der Schaaf og Kanse [46] fire kategorier for hvorfor individer ikke rapporterer hendelser:

- *redsel* for disiplinærtiltak eller medarbeideres reaksjoner
- *risikoaksept* (hendelser hører med til jobben; machokultur)
- *manglende nytteverdi* (oppfatning av at ledelsen ikke kommer til å bry seg og følgelig heller ikke gjøre noe med rapportene)
- *praktiske årsaker* (rapportering tar for lang tid eller er for vanskelig)

Vincent et al. [6] fant følgende i sin studie om årsaker til underrapportering av hendelser på fødeklinikker i London; Et betydelig antall av personalet formidlet at de ofte vurderte en hendelse som unødvendig å rapportere ut fra situasjonen som forelå. Dessuten formidlet flere at de ikke rapporterte fordi de rett og slett hadde det travelt og glemte det bort.

Ingen av mine informanter hadde fått noen form for kompetanseheving i forbindelse med rapporteringssystemet. Både modellen og funn fra litteratur indikerer at rapporterende personell må ha den nødvendige kunnskapen for å kunne rapportere. I tillegg kan det være nødvendig å legge til rette for at rapportering skal være så enkelt som mulig i en travel arbeidsdag. Modellen antyder at med økt kunnskap og gode tilbakemeldinger vil personell skjønne nytten av rapporteringssystemet og være mer tilbøyelig til å rapportere hendelser de opplever eller observerer.

8.1 Oppsummering

Mesteparten av litteraturen som støtter hypotesene er i all hovedsak hentet fra HMS. Jeg har ikke funnet mye relevant arbeid innen informasjonssikkerhet.

Det kan se ut som om organisasjonen har laget et hendelsesrapporteringssystem som på flere punkt avviker fra modellen til Sveen et al. Det kan være flere grunner til at organisasjonen har lagt seg på en slik linje. Det er for eksempel ikke sikkert at alle erfaringer med hendelsesrapportering for HMS er like overførbare til informasjonssikkerhet.

Toppledelsen er tilsynelatende interessert i arbeidet, men toppledelsen alene kan ikke drive prosjektet. Litteraturen viser at det er svært lite sannsynlig at et slikt prosjekt blir vellykket *uten* toppledelsens engasjement, men den er også klar på at slikt engasjement ikke er en garanti for suksess. Det kan se ut som at ikke alle lederne i linjen har samme oppfatning av prosjektets nytteverdi.

> "... vi har ikke så mye sensitiv informasjon i det vi holder på med. Det er vel ikke noen prioritert oppgave"

Det virker ikke som om den eksisterende rapporteringskulturen er plaget med negative reaksjoner fra ledelse eller medarbeidere. Men det er heller ingen tegn til at organisasjonen ser på insentiver som et nyttig virkemiddel for å få folk til å rapportere. Det ser ut til at de er mer interessert i at det bare skal være alvorlige saker som blir rapportert. Dette står i kontrast til de erfaringer man har fra HMS, der det har vist seg nyttig å få rapportert så mye som mulig.

Organisasjonen har tilsynelatende en velfungerende rapporteringskultur når det gjelder HMS, så utfordringen ligger i å få utvidet dette systemet på en naturlig måte til også å gjelde informasjonssikkerhet. Det er ikke mulig å si om rapporteringssystemet har ført til endrede rutiner, men det kan se ut til at de ikke utnytter systemet fullt ut med alle de effektene som blir beskrevet i litteraturen angående organisatorisk sikkerhetskultur. Det hjelper lite om IT-sjefen lærer litt om hva som er galt når dette ikke blir kommunisert tilbake til de ansatte på en forståelig måte.

Det kan virke som om informasjonen om dette systemet ikke har nådd ut til de ansatte. En av grunnen kan være at organisasjonen er bekymret for kapasiteten til etterforskerne og ikke interessert i at "alle og enhver" skal rapportere, men det kan også være at dette arbeidet er tidkrevende og at det fremdeles kan ta lang før det har nådd alle ledd i organisasjonen.

I mine intervju kom det frem at det ihvertfall blant disse informantene ikke var noen stor grad av kunnskap rundt organisasjonens rapporteringssystem. Selv om ansatte ikke i utgangspunktet hadde tilgang til selv å rapportere saker direkte i rapporteringssystemet så er det av betydning at de ansatte vet om at det finnes et system og hvor de skal rapportere hendelser de opplever eller observerer. Uten ansattes bevissthet og forståelse

av systemet vil det være nærliggende å tro at det er mye som ikke blir rapportert.

Manglende kunnskap om datamaskiner, nettverk og informasjonssikkerhet kan gjøre at det er vanskelig for ansatte som ikke jobber med problemstillingen til daglig å skille mellom hva som er hendelser som har innvirkning på informasjonssikkerheten og hva som er dagligdagse hendelser. Trusselbildet innen informasjonssikkerhet er et bevegelig mål som er i stadig forandring, og det er ikke noe man kan forvente at mennesker som ikke er spesialister på området skal kunne holde oversikt over.

Denne studien gir indikasjoner på at organisasjonen har et forbedringspotensial i forhold til kommunikasjon de som skal rapportere. Det er imidlertid mulig at undersøkelsen ikke har klart fange opp alle de sider ved hendelsesrapporteringssystemet som den har ønsket å finne. Det kan være begrensninger i begrepsbruken i intervjuspørsmålene. Spørsmålene ble utviklet på engelsk og kvalitetssjekket av en amerikansk professor før de ble oversatt til norsk, og det er spesielt ordene som har å gjøre med *hendelser* i forskjellig former som kan ha skapt problemer. Det finnes som nevnt ikke noen entydig taksonomi for *hendelser*, *ulykker* og *nestenulykker*. Det er mulig at det er en bedre forståelse for hva man legger i ordene på engelsk (incident, accident og event), men på norsk kan det fort oppstå vanskeligheter, og da særlig i forhold til informasjonssikkerhet.

Hvordan skal man definere *nestenulykke* innen informasjonssikkerhet? Er det en hendelse som kunne ha ført til et sikkerhetsbrudd eller er det et sikkerhetsbrudd som kunne ha ført til negative konsekvenser? Eller er det begge deler?

Det er trolig at en begrepsbruk som ligger for tett opptil det folk vanligvis oppfatter som noe som har med fysisk sikkerhet å gjøre, kan bli forvirrende når det spørres om informasjonssikkerhet. Det er ikke sikkert at informasjonen på forhånd har vært god nok på det området, og selv om informantene hadde blitt bedre informert, så er det ikke sikkert at dette ville fjernet problemet for de av informantene som har en lang tradisjon med hendelsesrapportering fra HMS.

9 Konklusjon og videre arbeid

9.1 Konklusjon om hendelsesrapportering i organisasjonen

Konklusjonen i denne studien er at det er mye litteratur som støtter opp under de hypotesene vi har utarbeidet. Mesteparten av denne litteraturen er imidlertid hentet fra HMS.

Videre kan vi konkludere med at dersom man skal ta utgangspunkt i modellen, så har organisasjonen et stykke igjen før de har innført et rapporteringssystem som fører til organisasjonell læring og økt kunnskapsnivå om informasjonssikkerhet og -hendelser. Det bør gjøres bedre kjent i organisasjonen, det bør gis opplæring i hva slags hendelser man ønsker at folk skal være oppmerksom på, og det bør arbeides systematisk med å holde rapporterende personell orientert om hva som skjer med hendelsene de rapporterer.

9.2 Videre forskning

Forskning på hendelsesrapportering innen informasjonssikkerhet er et forholdsvis nytt forskningsfelt. Ytterligere forskning på dette temaet kan bidra til økt kunnskap og ny læring for flere typer bedrifter og organisasjoner.

På sikt kunne det vært interessant å undersøke hvilke forskjeller det er mellom HMS og informasjonssikkerhet, slik at man bedre kan finne ut *hvilke* erfaringer man har gjort innen hendelsesrapportering i HMS som man kan ta med inn i arbeidet med hendelsesrapportering for informasjonssikkerhet.

Det synes også å være behov for videre forskning innen psykologi og sosiologi for å finne ut mer om hvilke menneskelige faktorer som er til hinder for rapportering og ikke minst hva slags tiltak som kan iverksettes for å bekjempe disse. Hendelsesrapportering er uten tvil et forskningsfelt som trenger forskning fra flere disipliner.

Videre kan det også være behov for å se nærmere på begrepsbruken; Hva er egentlig hendelser og nestenulykker i informasjonssikkerhet, og er dette begrep som gir noen mening?

Forhåpentligvis bidrar denne studien med funn som kan stimulere til ytterligere forskning på feltet.

Bibliografi

[1] Sveen, F. O., Rich, E., & Jager, M. forthcoming. Overcoming Organizational Challenges to Secure Knowledge Mangament. *Information Systems Frontiers*.

[2] ISO/IEC. 2005. *ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management*. International Organization for Standardisation.

[3] Oljeindustriens Landsforening. Integrerte operasjoner. http://www.olf.no/io/. (Besøkt januar 2008).

[4] Rich, E. & Gonzalez, J. J. 2006. Maintaining security and safety in high-threat E-operations transitions. In *HICSS*, 145. IEEE Computer Society.

[5] Radianti, J. & Gonzalez, J. J. 2007. Understanding Hidden Information Security Threats: The Vulnerability Black Market. In *HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, 156c, Washington, DC, USA. IEEE Computer Society.

[6] Vincent, C., Stanhope, N., & Crowley-Murphy, M. Febryary 1998. Reasons for Not Reporting Adverse Incidents. *Journal of Evaluation in Clinical Practice*, 5(1), 13–21.

[7] Johnson, C. W. 2002. Reasons for the Failure of Incident Reporting in the Healthcare and Rail Industries. In *Components of System Safety: Proceedings of the 10th Safety-Critical Systems Symposium*, Redmill, F. & Anderson, T., eds, 31–60, Berlin, Germany. Springer Verlag.

[8] Collinson, D. L. 1999. 'Surviving the Rigs': Safety and Surveillance on North Sea Oil installations. *Organization Studies*, 20(4), 579–600.

[9] Wikipedia. Systemdynamikk. http://no.wikipedia.org/wiki/Systemdynamikk. (Besøkt januar 2008).

[10] Sterman, J. D. 2000. *Business dynamics: systems thinking and modeling for a complex world*. Irwin/McGraw-Hill.

[11] Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. 2004. Limits to effectivness in computer security incident response teams. *23rd International Conference of the System Dynamics Society*.

[12] What is System Dynamics? http://www.ifi.uib.no/sd/sdinfo.html. (Besøkt januar 2008).

[13] Myrtveit, M. 2005. The World Model Controversy. In *Working papers in system dynamics 1/05*. The University og Bergen.

[14] Luna-Reyes, L. F. & Andersen, D. L. 2003. Collecting and analyzing qualitative data for system dynamics: methods and models. *System Dynamics Review*, 19, 271–296.

[15] Randers, J. 1980. Guidelines for Model Conceptualization. *Elements of the System Dynamics Method*, 117–139.

[16] Richardson, G. P. & Pugh, A. L. 1981. *Introduction to System Dynamics Modeling with DYNAMO*. MIT Press, Cambridge, MA, USA.

[17] Andersen, D., Roberts, N., Deal, R., Garet, M., & Shaffer, W. D. 1983. *Introduction to Computer Simulation: The System Dynamics Approach*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.

[18] Wolstenholme, E. F. 1990. *System enquiry: a system dynamics approach*. John Wiley & Sons, Inc., New York, NY, USA.

[19] Neuman, L. W. July 1999. *Social Research Methods: Qualitative and Quantitative Approaches*. Sage, Newbury Park.

[20] NORSOK. Helse, miljø og sikkerhet (hms) under bygging. Technical report, Norsk standard, 1996.

[21] NorSIS Senter for informasjonssikering. NorSIS - Sikkerhetspedia. http://www.norsis.no/leksikon/. (Besøkt januar 2008).

[22] Cassidy, D., Carthy, J., Drummond, A., Dunnion, J., & Sheppard, J. 2003. The use of data mining in the design and implementation of an incident report retrieval system. *Systems and Information Engineering Design Symposium, 2003 IEEE*, 13–18.

[23] Turner, B. 1978. *Man-Made Disasters*. Wykeham, London.

[24] Cooke, D. L. & Rohleder, T. R. 2006. Learning from incidents: from normal accidents to high reliability. *System Dynamics Review*, 22(3), 213–239.

[25] Kjellén, U. 2000. *Prevention of accidents through experience*. Taylor & Francis.

[26] Sveen, F. O., Sarriegi, J. M., Rich, E., & Gonzales, J. J. forthcoming. Toward Viable Information Security Reporting Systems. *Information Management and Computer Security*.

[27] Heinrich. 1931. *Industrial Accident Prevention*. McGraw-Hill, New York.

[28] Wright, L. & van der Schaaf, T. July 2004. Accident versus near miss causation: a critical review of the literature, an empirical test in the uk railway domain, and their implications for other sectors. *Journal of Hazardous Materials*, 111, 105–110.

[29] Jones, S., Kirchsteiger, C., & Bjerke, W. january 1999. The importance of near miss reporting to further improve safevty performance. *Journal of Loss Prevention in the Process Industries*, 12(1), 59–67.

[30] Gonzales, J. J. & Sawicka, A. 2002. A Framework for Human Factors in Information Security. *WSEAS International Conference on Information Security, Rio de Janeiro*.

[31] Grace, T., Kent, K., & Kim, B. Computer Security Incident Handling Guide. Special Publication SP 800-61, National Institute of Standards and Technology, January 2004.

[32] Siponen, M. 2001. Five Dimensions of Information Security Awareness. *SIGCAS Comput. Soc.*, 31(2), 24–29.

[33] Rollason-Reese, R. L. 2003. Incident handling: an orderly response to unexpected events. In *SIGUCCS '03: Proceedings of the 31st annual ACM SIGUCCS conference on User services*, 97–102, New York, NY, USA. ACM Press.

[34] Johnson, C. 2003. *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. University of Glasgow Press.

[35] van der Schaaf, T. W. *Near miss reporting in the chemical process industry*. PhD thesis, Technische Univ., Eindhoven (Netherlands)., 1992.

[36] Stanhope, N., Crowley-Murphy, M., Vincent, C., O'Connor, A. M., & E.Taylor-Adams, S. Febryary 1999. An evaluation of adverse incident reporting. *Journal of Evaluation in Clinical Practice*, 5(1), 5–12.

[37] Nielsen, K. J., Carstensen, O., & Rasmussen, K. 2006. The prevention of occupational injuries in two industrial plants using an incident reporting scheme. *J Safety Res*, 37(5), 479–486.

[38] Gonzalez, J. J. 2005. Towards a Cyber Security Reporting System – A Quality Improvement Process. *Computer Safety, Reliability, and Security*, 3688, 368 – 380.

[39] Federal Railroad Administration. 1997. *FRA Guide for Preparing Accident/incident Reports.* US Dept. of Transportation, Federal Railroad Administration, Office of Safety.

[40] Dekker, S. 2003. Punishing People or Learning from Failure? The choice is ours. *Unkown*.

[41] Barach, P. & Small, S. D. 2000. Reporting and preventing medical mishaps: lessons from non-medical near miss reporting systems. *British Medical Journal*, 320(7237), 759–763.

[42] Cohen, F. B. 1995. *Protection and security on the information superhighway*. John Wiley & Sons, Inc. New York, NY, USA.

[43] Howard, J. D. & Longstaff, T. A. 1999. A Common Language for Computer Security Incidents. *Sandia Report: SAND98-8667, Sandia National Laboratories*.

[44] Flin, R. 2003. Danger – men at work: Management influence on safety. *Human Factors and Ergonomics in Manufacturing*, 13(4), 261–268.

[45] Danielsson, M. & Stubbs, J. Desember 2000. Organisational accidents, safety programs and management participation. In *Proceedings of the 4th Asia Pacific Conference on Computer Human Interaction (APCHI 2000) and 6th S.E. Asian Ergonomics Society Conference (ASEAN Ergonomics 2000)*, In Lim, K., ed, 225–229. Elsevier.

[46] van der Schaaf, T. & Kanse, L. 2004. Biases in incident reporting databases: an empirical study in the chemical process industry. *Safety Science*, 42(1), 57–67.

A Alle hypotesene

1. Near-miss (event) reporting is useful within information security.
2. Feedback to reporting staff and other relevant staff is necessary to motivate for reporting in the future. If staff does not see that their reports are helpful and are taken seriously they will not report in the future.
3. Management may ensure a high quality of investigations through assigning sufficient resources.
4. Unclear guidelines and other insecurities regarding reporting of security events and incidents lead to sub-optimal reporting and thus sub-optimal learning. I.e. if users do not know what to report, whom to report it to and how to report it, the organization will not learn effectively.
5. A well working event / incident reporting system is a good basis for information security quality improvement.
6. Top management support is crucial for the success of an information security reporting system.
7. Events and incidents have similar causes.
8. Previous incidents and events and new incidents and events often have similar causes
9. Lessons learned from incident and event reports depend on the quality of investigation of reports.
10. Investigators prioritize the most important reports if resources are low.
11. Even if investigators prioritize reports, less important reports still steal time and negatively impacts overall quality.
12. If work pressure is high, quality of investigations goes down as investigators cut corners to reach over all the work.
13. Staff will not comply with a reporting policy if they do not have time and competence or see reporting as not useful.
14. Lessons learned from investigations of reports enable the organization to raise awareness about security and put in place technical and organizational countermeasures that are effective in reducing future vulnerability. I.e. repetition of previous incidents and events should be reduced.
15. Increased awareness and countermeasures reduces the organizations vulnerability towards incidents. I.e. attacks and unintended security breaches are detected and mitigated before they can cause substantial harm. In other words events do not escalate to attacks.

16. Increased awareness and countermeasures reduces the organizations vulnerability towards events. I.e. attackers will be deterred from attacking and unintended security lapses, e.g. misplaced laptops, will be less likely to occur.
17. Increased awareness, among staff and in the organization in general, enables the organizations and its staff to detect incidents and events that would otherwise have gone undetected.
18. Events and incidents that happen may be detected. More events and incidents leads to more events and incidents detected, given that previous incidents and events have similar causes to new incidents and events.
19. More detected incidents and events leads to more reported incidents and events, given that the motivation to report is constant.
20. Management may affect the reporting of incidents and events through a policy of incentives.
21. When more events happen more incidents will happen, given that events and incidents have the same causes.
22. The learning effect is greater if the root cause(s) of the event or incident is known.
23. More can be learned from high priority events and incidents than low priority events and incidents.
24. Lack of individual and organizational awareness of security problems lead to less awareness and cause a strengthening of misperceptions about security. Vice versa, awareness of security issues and their causes lead to less misperception about security.
25. Reports may be accompanied by incentives.
26. Incentives increase the motivation to report incidents and events.
27. Incentives are generally weaker than recriminations.
28. Incentives are rendered ineffective in the presence of strong recriminations. I.e. they may lead to a bias in reporting towards low-recrimination"incidents or towards no reporting at all.
29. Reports may be accompanied by recriminations such as disciplinary action, isolation by colleagues and so forth.
30. Management may contribute to creating a positive security culture through working towards reducing reporting recriminations.
31. The presence of recriminations may trigger a vicious circle. Strong recriminations lead to less motivation to report, which leads to less lessons learned, less awareness and less events and incidents detected, which in turn leads to less reports. Vice versa, encouragements to report from management, removal of recriminations, incentives conducive to reporting and sufficient investigative resources lead to a virtuous circle where more incidents are reported, leading to more lessons

learned, leading to more detected incidents which in turn leads to a higher fraction of reported incidents, yet more lessons learned etc.

32. Recriminations reduce the motivation to report incidents and events.

B Intervjuguide

B.1 Ledere og prosesseiere

1. Har din organisjasjon en policy for rapportering av informasjonssikkerhetsbrudd? Vennligst svar utfyllende.
   (a) Hvorfor har eller har dere ikke en slik policy?
2. Vennligst beskriv hvordan rapporter om informasjonssikkerhetshendelser blir samlet og håndtert.
   (a) Hvem gjennomfører etterforskningen / undersøkelsene? Finnes det et dedikert team?
3. Inkluderer policyen også informasjonssikkerhetshendelser og ikke bare brudd?
   (a) Tror du det er nyttig å rapportere informasjonssikkerhetshendelser?
4. Har det blitt laget retningslinjer / instruksjoner for å informere den enkelte bruker om rapporteringssystemet? Har brukerene fått noen form for trening eller kursing i hvordan de skal rapportere sikkerhetsbrudd og hvordan de kan gjenkjenne sikkerhetshendelser?
   (a) Hvorfor / hvorfor ikke?
5. Gjøres informasjon om sikkerhetsbrudd jevnlig tilgjengelig for brukere?
   (a) Hvorfor / hvorfor ikke?
6. Holdes rapporterende brukere informert om situasjonen og etterforskningen av sikkerhetsbruddet? Får de rapporterende brukerne informasjon når etterforskningen avsluttes?
   (a) Hvorfor / hvorfor ikke?
7. Er det noe oppfølging av innrapporterte hendelser, etter at saken ansees som løst?
   (a) Av hvem? Hvorfor?
8. Har informasjonssikkerheten blitt bedre etter innføringen av en formell prosess for rapportering av sikkerhetsbrudd?
   (a) Hvorfor / hvorfor ikke?
9. Har policy blitt endret som følge av rapporter om sikkerhetsbrudd?
   (a) Hvorfor / hvorfor ikke?
10. Vennligst beskriv rapporteringskulturen i din organisasjon. Hvorfor er kulturen slik den er?
11. Tradisjonelle rapporteringssystemer for sikkerhet på arbeidsplassen er ofte plaget med underraportering. Hvordan er situasjonen i din organisasjon for informasjonssikkerhet?
    (a) Hvorfor er situasjonen slik?

12. Inkluderer informasjonssikkerhetspolicyen noen form for disiplinærstraff?
    (a) Hvorfor har / har dere ikke disiplinærstraff som en del av policyen?
    (b) Hva tror du effekten av disiplinærstraff er?
    (c) Finnes det andre straffereaksjoner? (uformelle, skjulte, utfrysning osv, også de som ikke kommer fra ledere)
13. Inkluderer informasjonssikkerhetspolicyen insentiver for rapportering av sikkerhetsbrudd?
    (a) Hvorfor har / har dere ikke insentiver?
14. Følger du personlig opp rapporteringssystemet eller delegerer du det til en underordnet?
    (a) Hvorfor?
15. Følger dine overordnede opp rapporteringssystemet? Er de interessert i hva som foregår?

B.2 Sikkerhetspersonell

1. Har din organisjasjon en policy for rapportering av informasjonssikkerhetsbrudd? Vennligst svar utfyllende.
2. Vennligst beskriv hvordan rapporter om informasjonssikkerhetshendelser blir samlet og håndtert.
3. Inkluderer policyen også informasjonssikkerhetshendelser og ikke bare brudd?
   (a) Tror du det er nyttig å rapportere informasjonssikkerhetshendelser? Hvorfor?
   (b) Kan man lære fra sikkerhetshendelser for å forhindre sikkerhetsbrudd i fremtiden?
4. Har det blitt laget retningslinjer / instruksjoner for å informere den enkelte bruker om rapporteringssystemet?
   (a) Har brukerene fått noen form for trening eller kursing i hvordan de skal rapportere sikkerhetsbrudd og hvordan de kan gjenkjenne sikkerhetshendelser?
      i. Hvorfor / hvorfor ikke?
   (b) I hvilken grad?
5. Gjøres informasjon om sikkerhetsbrudd jevnlig tilgjengelig for brukere?
   (a) Hvorfor / hvorfor ikke?
6. Holdes rapporterende brukere informert om situasjonen og etterforskningen av sikkerhetsbruddet? Får de rapporterende brukerne informasjon når etterforskningen avsluttes?
   (a) Hvorfor / hvorfor ikke?
7. Hvordan er arbeidsbyrden til de som er ansvarlige for å etterforske sikkerhetsbrudd?
   (a) Hvem oppdager de fleste sikkerhetsbruddene og sikkerhetshendelsene? (automatisert deteksjon (brannmur, ids, osv) eller brukere?
   (b) Hvordan påvirker arbeidsbyrden kvaliteten på etterforskningen? Vennligst svar utfyllende.
8. Er det noe oppfølging av innrapporterte hendelser, etter at saken ansees som løst?
   (a) Av hvem? Hvorfor?
9. Har informasjonssikkerheten blitt bedre etter innføringen av en formell prosess for rapportering av sikkerhetsbrudd?
   (a) Hvorfor / hvorfor ikke?
10. Har policy blitt endret som følge av rapporter om sikkerhetsbrudd?
    (a) Hvorfor / hvorfor ikke?
11. Vennligst beskriv rapporteringskulturen i din organisasjon. Hvorfor er kulturen slik den er?
12. Tradisjonelle rapporteringssystemer for sikkerhet på arbeidsplassen er ofte plaget med underraportering. Hvordan er situasjonen i din organisasjon for informasjonssikkerhet?
    (a) Hvorfor er situasjonen slik?
13. Inkluderer informasjonssikkerhetspolicyen noen form for disiplinærstraff?

   (a) Hvorfor har / har dere ikke disiplinærstraff som en del av policyen?
   (b) Hva tror du effekten av disiplinærstraff er?
   (c) Finnes det andre straffereaksjoner? (uformelle, skjulte, utfrysning osv, også de som ikke kommer fra ledere)

14. Inkluderer informasjonssikkerhetspolicyen insentiver for rapportering av sikkerhetsbrudd?
   (a) Hvorfor har / har dere ikke insentiver?

15. Er toppledelsen aktivt interessert i rapporteringssystemet?
   (a) Hva er konsekvensen av toppledelsens innstilling og hvor viktig tror du dette er?

B.3 Brukere

1. Har din organisjasjon en policy for rapportering av informasjonssikkerhetsbrudd?
   (a) Hvordan ble du gjort oppmerksom på denne policyen? (kursing, skrevne matrialer, ved ansettelse, etc)
2. Har du blitt gitt retningslinjer for å informere deg om sikkerhetsrapporteringssystemet og rapporteringsprosessen?
   (a) I hvilken grad?
3. Blir informasjon om sikkerhetshendelser som har skjedd i organisasjonen gjort tilgjengelig for deg?
   (a) På hvilken måte?
4. Vennligst beskriv et sikkerhetsbrudd som du eller en kollega rapporterte. Hvordan ble rapporten fulgt opp? Hva slags tilbakemeldinger fikk du etter at du rapporterte?
5. Har informasjonssikkerheten blitt bedre etter innføringen av en formell prosess for rapportering av sikkerhetsbrudd?
   (a) Hvorfor / hvorfor ikke?
6. Vet du om policy har blitt endret som følge av rapporter om sikkerhetsbrudd?
   (a) Hvorfor / hvorfor ikke?
7. Vennligst beskriv rapporteringskulturen i din organisasjon. Hvorfor er kulturen slik den er?
8. Har du eller en av dine kollegaer blitt utsatt for disiplinærstraff etter at du eller en av dine kollegaer rapporterte et sikkerhetsbrudd?
   (a) Hva tror du effekten av disiplinærstraff er?
   (b) Hvor ofte blir disiplinærstrff benyttet?
   (c) Finnes det andre straffereaksjoner? (uformelle, skjulte, utfrysning osv, også de som ikke kommer fra ledere)
9. Finnes det insentiver for rapportering av sikkerhetshendelser?
   (a) Hva tror du effekten av insentiver for rapportering av sikkerhetshendelser er?
   (b) Hvor ofte blir insentiver benyttet?
10. Omfavner toppledelsen rapportering av sikkerhetsbrudd?
    (a) Hvorfor tror du det?
11. Hva er konsekvensene av toppledelsens innstiling og hvor viktig tror du dette er?
12. Følger dine overordnede opp rapporteringssystemet? Er de interessert i hva som foregår?