Opplæring, tilsyn, regelverk - gir det bedre informasjonssikkerhet?

Tom-Andre Skar

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

Abstract

This master's thesis report takes a closer look at what the effects of education, revision and laws have on information security. It's not always such means succeed giving better security. We take a closer look at the electric power business. And from our work we find if such means give the wanted effect and if maybe other in similar situations should do the same.

To find answers to this, we based our investigation on a questionnaire and some interviews. The questionnaire was conducted on some of the head of security in the electric power business in Norway. And in addition had been at one of the two educational courses NVE was in charge of in end 2006. A total of 40 respondents answered questions about their own age, experience, business, motivation.

This thesis has its contribution in giving new information on education, revision and laws and its effect on information security. At the same time, the situation in the electric power business will be reviled. It's important to have in mind that the electric power business is very important for the society to work.

On behalf of the study that has been carried out, it has been revealed that education, revision and laws does improve the security in general. In special, the security culture is improved with such measures and the revision is a good motivator. Laws should be easy to comprehend also if used.

Sammendrag

Denne masteroppgaven tar en nærmere titt på hvilke effekter opplæring, tilsyn og et regelverk har å si for informasjonssikkerheten. Det er ikke alltid slike tiltak lykkes og ved å benytte energibransjen forsøker vi å finne ulike faktorer som spiller inn. Vi finner da ut om slike tiltak gir bedre informasjonssikkerhet slik at også andre kan benytte seg av liknende tiltak.

For å kunne finne svar på dette har vi valgt å gjennomføre ulike undersøkelser i form av en spørreundersøkelse og noen intervju. Undersøkelsene ble gjennomført hos utvalgte IT-sikkerhetsleder i energibransjen i Norge som hadde gjennomført kurs i regi av NVE. Totalt ble 40 ulike besvarelser samlet inn. Her ble alder, erfaring, virksomhet, holdninger rundt emnene opplæring, tilsyn og regelverk kartlagt.

Rapportens bidrag er å gi nye erfaring rundt opplæring, tilsyn og regelverk som sikkerhetstiltak. Og for å se om sikkerheten bedres med bevisstgjøring. Rapporten vil samtidig avdekke situasjonen innenfor informasjonssikkerhet hos energibransjen som anses å være viktig for samfunnet.

På bakgrunn av gjennomført studie, kommer det frem at opplæring, tilsyn og regelverk gir bedre informasjonssikkerhet enn gjennomsnittet. Spesielt sikkerhetskulturen bedres med opplæring og tilsyn er en god motivasjonsfaktor for å arbeide med sikkerhet. Men det er viktig å ha klare og lett forståelige regler tilknyttet dette.

Forord

Takk til Carl Georg Abel og Arthur Gjengstø ved NVE som gjorde det mulig å gjennomføre en undersøkelse i energisektoren. Jeg vil også takke Tone Hoddø Bakås, min eksterne veileder og oppdragsgiver ved NorSIS som satt meg i kontakt med NVE.

En stor takk til alle virksomheter som bidro med data til oppgavens resultater i form av å delta i spørreundersøkelsen og i etterfølgende intervjuer. Uten deres bidrag hadde resultatene uteblitt. En takk også til doktorgradstudentene Janne Hagen og Eirik Albrechtsen for sammarbeidet med deler av undersøkelsene.

Til slutt vil jeg benytte anledningen til å takke min veileder, Frode Volden, som har vært en god støttespiller for meg i arbeidet med masteroppgaven. Han har vært tilgjengelig, vært til stor inspirasjon og hjelp i forbindelse med statistiske undersøkelser og bidratt med kritiske spørsmål og konstruktive kommentarer.

Tusen takk!

Tom-Andre Skar
Hamar, 30. juni 2007

Innhold

Abstract . . . . . **iii**
Sammendrag . . . . . **v**
Forord . . . . . **vii**
Innhold . . . . . **ix**
Figurer . . . . . **xi**
Tabeller . . . . . **xiii**
1 Innledning **1**
1.1 Tema 1
1.2 Problembeskrivelse 1
1.3 Motivering og gevinstpotensiale 1
1.4 Forskningsspørsmål 2
2 Sentrale begreper **3**
2.1 Informasjonssikkerhet 3
2.1.1 God sikkerhet 3
2.1.2 Risiko 4
2.2 Sikkerhetshendelser 4
2.3 Sikringstiltak 4
3 Tidligere arbeid **7**
3.1 Tidligere undersøkelser 7
3.1.1 Mørketallsundersøkelsen 8
3.1.2 BAS 3 8
3.2 Er opplæring veien å gå? 9
3.3 Opplæring i standarder 9
3.3.1 Feil fokus 10
3.4 Hvordan måle det umålbare? 10
3.5 Sikkerhetskultur 11
3.5.1 Holdninger 12
3.5.2 Motivasjon 12
4 Valg av metode **13**
4.1 Plan for forskningsarbeidet 13
4.2 Litteratur 14
4.3 Spørreundersøkelsen 14
4.3.1 Utvalget 15
4.3.2 Spørreskjemaet 15
4.3.3 Utsendelse 17
4.3.4 Gjennomgang og tolking av data 17
4.4 Oppfølgende intervjuer 17
4.5 Kvalitet 17
5 Datagrunnlag **19**
5.1 Besvarelse av spørreundersøkelsen 19

5.1.1 Kjønnsfordeling . . . 19
5.1.2 Alder . . . 19
5.1.3 Erfaring . . . 20
5.1.4 Antall ansatte . . . 20
5.1.5 Selskap . . . 20
5.1.6 Når de sist hadde opplæring . . . 20
5.1.7 Regi . . . 21
5.1.8 Funksjon i virksomheten . . . 21
6 Resultater og diskusjon . . . 23
6.1 Innleding . . . 23
6.2 Kurset . . . 23
6.3 Forbedring av informasjonssikkerheten . . . 26
6.4 Standarder, organisasjoner og fora . . . 28
6.5 Holdninger, atferd og motivasjon . . . 30
6.6 Virksomheten . . . 32
6.7 Effektivitet og risiko . . . 35
6.8 Sammenlignet med andre undersøkelser . . . 36
6.8.1 Mørketallsundersøkelsen . . . 36
6.8.2 I forhold til andre land . . . 37
6.8.3 I forhold til andre virksomheter . . . 38
7 Oppsummering og konklusjon . . . 39
7.1 Oppsummering . . . 39
7.2 Konklusjon . . . 40
8 Videre arbeid . . . 41
Bibliografi . . . 43
A Følgebrev . . . 47
B Vedlegg: Spørreskjema . . . 49
C Vedlegg: Intervjuguide . . . 57
D Vedlegg: Frekvensanalyser . . . 59

Figurer

1 Sikkerhetshendelser tilknyttet tilgjengelighet, konfidesialitet og integritet. [1] 4
2 3-lags sikkerhetskultur [2]. 11
3 Oversikt over prosessen 13
4 I hvilken grad ble målene dine for kurset oppfylt? 24
5 Har det blitt oppdaget flere sikkerhetshendelser som følge av kurset? . . . 26
6 Kjenner til en standard 29
7 Medlem av fora eller organisasjon 30
8 Holdninger og atferd 30
9 Motivasjon 31
10 Sikkerhetsnivået 32

Tabeller

1 Forståelsen etter kurset 24
2 Mer opplæring 25
3 Antall sikkerhetsoppgaver etter kurset 25
4 Kontroll og tilsyn 27
5 Bedre regelverk 27
6 Flere og bedre risikoanalyser 28

1 Innledning

1.1 Tema

Mange bransjer og enkeltbedrifter gjennomfører, på eget initiativ eller etter pålegg, opplæring og informasjon om informasjonssikkerhet. Mørketallsundersøkelsen [3] og andre undersøkelser indikerer at man ikke alltid lykkes med slike tiltak. Vi vil i denne oppgaven ta for oss faktorer som påvirker effektiviteten av slike tiltak. For å belyse dette vil vi ta for oss energibransjen, som er et godt eksempel på en bransje som bruker opplæring og pålegg i informasjonssikkerhet.

Nøkkelord: informasjonssikkerhet, opplæring, tilsyn, regelverk, energibransjen

1.2 Problembeskrivelse

Det finnes mange sårbare informasjonssystemer som et resultat av økende bruk av IT. I dag brukes IT-baserte systemer for flere typer arbeidsoppgaver, kontroll, overvåkning, styring osv. Fokus på informasjonssikkerhet er derfor viktig. De fleste virksomheter, offentlig og private, løser dette problemet ved å gjennomføre opplæring innen informasjonssikkerhet. Noen bransjer og virksomheter går så langt som å pålegge sine ansatte opplæring. Det kan være i form av lover og forskrifter eller ved et regelverk. Er dette en effektiv vei å gå?

NVE[1] fører tilsyn og holder kurs innenfor informasjonssikkerhet, bevisstgjøring av sikkerhetstiltak bør føre til holdningsendringer i energibransjen slik at tilfredsstillende sikkerhet blir opprettholdt. Som beskrevet i Beredskapsveiledningen § 6-1 [4] jf Bfk § 4-1 [5] (Beredskapsforskriften) skal det utnevnes en IT sikkerhetsleder, en mann. Muligheten for at disse virksomhetene ikke ser på seg selv som noe som kan brukes til kriminelt er til stedet. Fokuset er muligens rettet mot kun å levere for eksempel strøm.

Med undersøkelser av forhold knyttet til energibransjen vil denne oppgaven prøve å finne svar på om opplæring og informasjon er veien å gå.

1.3 Motivering og gevinstpotensiale

Informasjonssikkerhet kan ses på som en kostnadsfaktor, men det er nødvendig for å opprettholde konfidensialitet, integritet, tilgjengelighet. Forebygging vil i slike tilfeller være mye billigere enn hvis ulykken først skulle inntreffe.

Økonomisk innsparing og økt effektivitet er sentrale begreper for å beskrive dagens samfunnsutvikling innen bedrifter, virksomheter og organisasjoner, noe som ikke vil stoppe i framtiden [6]. Motivasjonen ligger i å få gjennomført en analyse for å se om sikkerheten bedres med bevisstgjøring i form av opplæring, regler og tilsyn.

Rapporten vil samtidig avdekke situasjonen innenfor informasjonssikkerhet hos energibransjen som anses å være viktig for samfunnet, det være seg befolkningen som unngår å sette liv og helse i fare, det kan være trafikk- og kloakksystemer som ikke fungerer uten strøm. Samtidlig vil man finne ut om informasjon i form av bevisstgjøring,

[1] Norges Vassdrag og Energidirektorat

opplæring og tilsyn vil forbedre informasjonssikkerheten. Vi kan da bruke disse resultatene for å trekke slutninger, ikke bare i energibransjen, men også i andre bransjer og enkeltbedrifter generelt.

1.4 Forskningsspørsmål

Under gjennomføring av prosjektet ønsker vi å finne svar på følgende spørsmål:

1. Opplæring, tilsyn, regelverk - gir det bedre informasjonssikkerhet?
2. Viser energibransjen en forbedring i forhold til resultatene i Mørketallsundersøkelsen[3] eller andre lignende undersøkelser?
   - Har de færre sikkerhetshendelser?
   - Er flere sikringstiltak gjennomført?
   - Har størrelsen på virksomheten noen innvirkning?
3. Bør sammenlignbare bransjer og enkeltbedrifter gjennomføre lignede tiltak?

2 Sentrale begreper

I denne oppgaven berører vi flere sentrale begreper, vi vil i dette kapitellet gå i gjennom betydningen vi legger i disse begrepene.

2.1 Informasjonssikkerhet

Vi benytter oss av en stor grad frihet fordi våre elektroniske tjenester er tilgjengelige hele tiden. Vi ønsker tilgang hele døgnet, hele året, men samtidig ønsker vi mest mulig sikkerhet for våre verdier.

Informasjonssikkerhet er knyttet til trygghet og kontroll over informasjon [7] og i de seinere år har informasjonssikkerhet fått en entydig definisjon; å sikre konfidensialitet, integritet og tilgjengelighet. Dette ser vi i litteraturen [8] og i standarder [9, 10, 11]. I tillegg til de tre nevnte er også autentisering ofte nevnt i sammenheng med disse.

Vi kan utdype dette yteligere ved å si at informasjonssikkerhet er tiltak for å ikke røpe informasjon for uvedkommende parter uten autorisasjon (konfidensialitet), at informasjon ikke uatorisert er skadet eller endret (integritet), og at vissheten om at kommunikasjon mellom to eller flere parter er mulig for å utføre ønskede oppgaver (tilgjengelighet).

Informasjonssikkerhet kan implementers på flere måter og kombinasjoner av disse.

- Metoder/tekniker: Kryptering, autentisering, signering, innbruddsdetektering, etc.
- Utstyr/programvare: Brannmur, viruskontroll, etc.
- Prosedyrer: Backup, sikkerhetsrevisjon, etc.
- Organisering/infrastruktur/kompetanse

Det stilles krav til informasjonssikkerheten i bedrifter, organisasjoner og nasjonalt. Nasjonalt legges det planer og strategier på et overordnet mål [12, 13], men også gjennom lover og forskrifter stilles det ofte krav til informasjonssikkerheten [13, 14, 15]. Som kjent fra kap. 1.2 har NVE utarbeidet egne lover og rettningslinjer som må følges for å opprettholde informasjonssikkerheten.

2.1.1 God sikkerhet

God informasjonssikkerhet kan vi forklare med følgende punkter:

- Beholder og opparbeider deg et godt rykte for å levere kvalitet (bygger tillit i markedet og offentligheten)
- Sikkerhetsbevisste brukere
- Hindrer hendelser med påfølgende inntektstap og kostnader
- Er i tråd med risikovurdering og tilhørende vedtatt akseptabelt risikonivå for virksomheten
- Kontroller og tilsyn vil ikke resultere i omfattende eller prinsipielle pålegg

For å tilfredstille disse punktene er det spesielt tre emner som må være på plass: Ledelse, holdninger og tekniske tiltak [16]. Under ledelse finner vi blandt annet risikostyring og regler.

Beviste medarbeidere og gode holdniger rundt temaer som personopplysninger, passordbruk, epost, utro tjenere, virus etc. bør også være på plass. Av tekniske tiltak har vi anti-virus, brannmur, oppdateringer, backup etc.

2.1.2 Risiko

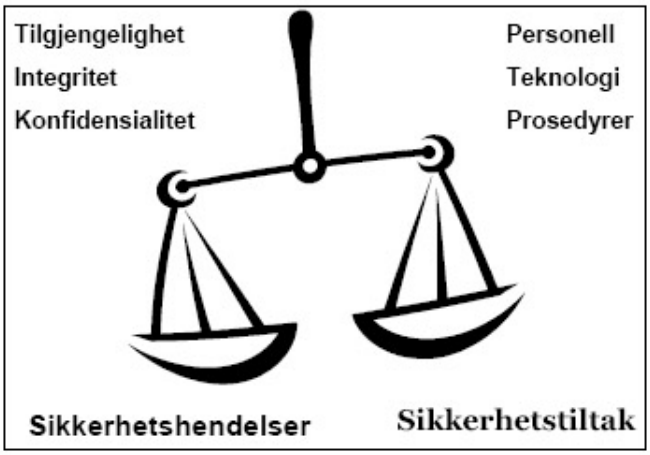
Risiko og sikkerhet henger sammen [17]. Jo høyere sikkerhet det er på f.eks. et system, jo mindre er risikoen for at noe galt skal skje med systemet. Og mottsatt, jo mindre sikkerhet det er, jo høyere risiko er det for at noe galt skal skje med systemet.

Unntaket fra "regelen" i dette tilfellet er at det ikke er sikkert det er noe interessant i systemet for uvedkommende og dermed hvis vi har lav sikkerhet vil dette gi oss en lav risiko.

Med risiko tenker vi på i all hovedsak trusler som kan resulterer i en sikkerhetshendelse. Hva er sannsynligheten for at en sikkerhetshendelse vil skje, og hva blir konsekvensene av at en sikkerhetshendelse inntreffer?

2.2 Sikkerhetshendelser

Sikkerhetshendelser er tilknyttet tilgjengelighet, konfidensialitet og integritet (Figur 1). Eller sagt på en annen måte, brudd på disse gjennom forskjellige hendelser som for eksempel mistet passord, tyveri av datautstyr, datainnbrudd, uautorisert sletting av data, missbruk av ressurser, phishing, virus og trojanere, for å nevne noen.



Figur 1: Sikkerhetshendelser tilknyttet tilgjengelighet, konfidesialitet og integritet. [1]

2.3 Sikringstiltak

Med sikringstiltak mener vi her hva som blir gjort eller har blitt gjort for å forebygge sikkerhetshendelser. Disse sikringstiltakene kan vi dele opp i tre hovedkategorier: Personell, teknologi og prosedyrer (Figur 1).

Når vi tenker på sikringstiltak knyttet til personell er vi innne på mye forebyggende tiltak som opplæring og holdningskapende arbeid hos medarbeidere og ledelse.

Teknologibiten består nok av flest mulige typer tiltak, vi kan nevne de viktigste som

brannmur, IDS[1], VPN[2], antivirus, spamfilter, autentiserings- og autorisasjonsmekanismer, PKI og elektroniske signaturer.

Når en sikkerhetshendelse skulle inntreffe er det viktig å ha de riktige prosedyrene på plass. Slik at man vet hva og hvordan man skal gripe ann situasjonen. Annerkjente standarder benyttes ofte som et utgangspunkt i arbeidet med å utarbeidet en policy.

[1]Intrusion Detection System
[2]Virtual Private Network

3 Tidligere arbeid

3.1 Tidligere undersøkelser

Det er tidligere gjort utallige undersøkelser som sjekker informasjonssikkerhetsstatusen hos store og små bedrifter, både i utland og innland. Det er de små og mellomstore aktørene som kommet dårligst ut av undersøkelsene. Det er flere kommersielle selskap (IBM, Symantec, Microsoft) som har utført disse undersøkelsene [18, 19, 20]. De kan ha kommersielle interesser og dermed pyntet på statistikken, men de offentlig styrte og støttede undersøkelsene har fått de samme resultatene i [21, 22, 23]. Dette er undersøkelser blant annet gjennomført av CSI/FBI og DTI, henholdsvis USA og England. I undersøkelsem gjort av CSI/FBI [22] i 2006 ble 5000 spørreskjemaer besvart, 22 % var bedrifter eller organisasjoner med 1-99 ansatte. Dette resulterte i at 10 av 15 syntes ikke nok resurser ble investert i sikkerhetsopplæring. Sammenlignet med tidligere år, har det vært en økning i investeringene.

I undersøkelsen gjort av DTI [23] i 2006 intervjuet de 1000 bedrifter og organisasjoner. 1 av 6 spurte sier at de ikke har hatt noen form for opplæring i det hele tatt og at 62 % har hatt uønskede hendelser. Av de som hadde opplevd en større sikkerhetshendelse, svarte 25 % med at de gjennomførte ekstra opplæring etter hendelsen. Trenden sammenlignet med tidligere år viser at flere og flere gir sine nyannsatte opplæring og trening, men dette er for det meste de største organisasjonene som gjennomfører. Det er også en sammenheng med de som har en sikkerhetspolicy, det er disse som stort sett også gjennomfører trening. DTI anbefaler for øvrig at brukeropplæring blir gjennomført.

Tyskland gjennomfører også lignende undersøkelser. Disse undersøkelsene blir gjennomført av BSI[24] og sist var i 2005. Målet deres er å kunne garantere sikker bruk av informasjon og kommunikasjonsteknologier. Deres funn ang opplæring og trening sier at administrasjonsledelsen ikke er tilstrekkelig informert med tanke på sikkerhetsrelatert arbeid og at sikkerhetsrelatert trening ikke har skapt den ønskede effekten. Men sier vidre at dette mest trolig skyldes for lite midler til å opprettholde kontinuitet i opplæringsprosessen.

En undersøkelse gjort av Ernest & Young i 2005 [25] har vist oss hva som blir gjort og har blitt gjort innen informasjonssikkerhet for å tette igjen gapet til den økende risikoen inne IT. Dette var åttende året de gjennomførte en slik undersøkelse. Respondentene var ledere i globale virksomheter, statlige og ikke-statlige. Mer enn 1300 deltok fordelt på 55 land rundt om i verden. Som en del av undersøkelsen har de sett på hva som blir gjort av opplæring bevistgjøring av informasjonssikkerhet. Resultatene viser at det er ca halvparten som får opplæring i informasjonssikkerhet, vidre viser funnene at det er langt under halvparten som faktisk får opplæring i hva de skal gjør om en sikkerhetshendelse inntreffer. De foreslår at alle organisasjoner tar en titt på om deres ansatte har og blir opplært tilfredstillende.

Norge er ikke et unntak når det gjelder lignende undersøkelser, her gjennomføres det vi kaller Mørketallsundersøkelsen [3].

3.1.1 Mørketallsundersøkelsen

Mørketallsundersøkelsen 2006 [3] ble ferdigstilt mai 2006. Ved å sende ut et spørreskjema til et representativt utvalg av norske bedrifter, både offentlige og private. 749 svar ble mottatt av et representativt utvalg på 2000. Denne undersøkelsen kartla alt fra datainnbrudd, avhengighet, beskyttelsestiltak til organisatoriske tiltak. Spesielt er funnene om at bedrifter som anser seg selv for å være en del av en kritisk infrastruktur ikke hever seg vesentlig over andre når det gjelder sikringsnivå. Av undersøkelsen kommer det også imidlertidig fram at kun 40 % av bedriftene har gjennomført brukeropplæring av ansatte. Samtidig viser det seg at virksomhetene er godt rustet når det gjelder det tekninske aspektet. Av de som hadde uønskede hendelser hadde 95 % tekniske tiltak på plass. De organisatoriske tiltakene har heller ikke steget samtidig med trusseleksponeringen. Blant de store bedriftene med annsatte med over 200 har ca 90 % retningslinjer for sikker bruk, men bare hver fjerde blant de minste har det.

Man kan også lese videre i rapporten at så mange som 64 % ikke har hatt uønskede hendelser.

Undersøkelsen konkludere blandt annet med at bevistgjøring og holdninger har en vesentlig like stor rolle som tekninske sikringstiltak.

> "Informasjonssikring er ikke et produkt man kan kjøpe, men noe man må skape sammen i organisasjonen"

3.1.2 BAS 3

Siden 1991, da Energiloven [26] ble innført, har det vært en kommersialisering av kraftforsyningen med et stort fokus på økonomi. Det har siden 1991 blitt mer oppmerksomhet på sårbarheter i kraftforsyningen og som et resultat av dette ble det i mars 1999 startet et prosjekt, "Beskyttelse av samfunnet, del 3" (BAS3). Resultatene ble offentliggjort mai 2001. BAS prosjektene er en rekke av analyser som har i oppdrag å forbedre kunnskapen om samfunnets sårbarhet, del 3 er altså en analyse av sårbarhetsreduserende tiltak i kraftforsyningen. Aktørene bak BAS 3 har vært FFI[1], Justisdepartementet, Olje- og energidepartementet, DSB[2] og NVE.

Prosjektet har resultert i godt over 20 rapporter og i sluttrapporten, "En sårbar kraftforsyning - sluttrapport etter BAS 3" [6], blir det beskrevet flere viktige faktorer, anbefalinger, konsekvenser og tiltak. Det er et stort fokus på naturhendelser, krig og terror i form av fysiske hendelser som kan skje. Vi vil her oppsummere med tanke på IT-sikkerhet. Som følge av økende IT-avhengighet, knapphet på personell, effektivisering og internasjonalisering, vil informasjon sårbarheten øke i fremtiden. FFI anbefaler sikring av IT-systemer, satsing på personell og kompetanse og bedre gjenopprettings- og reparasjonsmuligheter. IT-sikkerhet kan ikke gjøres i skippertak, men må følges opp kontinuerlig, sies det i rapporten. Det er særlig drift-, styrings- og handelssystem som er utsatt for angrep utenfra pga IKT avhengigheten.

Det er grunn til å tro at forskriften om beredskap i kraftforsyningen [5], som ble vedtatt 16. desember 2002 av NVE, kom som en naturlig følge av funnene blant annet i BAS 3. Det er også utarbeidet en veiledning til beredskapsforskriften, kalt "Veiledning til forskrift om beredskap i kraftforsyningen" [4]. Dette er et omfattende regelverk, til sammen består disse dokumentene av flere hundre sider, noe som kan være vanskelig å følge til punkt og prikke, kanskje særlig for de små bedriftene.

[1] Forsvarets forskningsinstitutt
[2] Direktoratet for samfunnssikkerhet og beredskap

Liste over lover, forskrifter og veiledninger:

- Energiloven [26]
- Energilovforskriften [27]
- Forskrift om beredskap i kraftforsyningen [5]
- Veiledning til forskrift om beredskap i kraftforsyningen [4]

3.2 Er opplæring veien å gå?

Det ble nylig skapt litt blest om opplæring i informasjonssikkerhet fungerer som det skal. Det var svensken Stefan Gorling, en doktorgradstudent ved Royal Institute of Technology i Stockholm, som ved konferansen Virus Bulletin 11-13 oktober 2006 lanserte artikkelen "The myth of user education" [28]. I artikkelen diskuterer han flere spørsmål på en provoserende måte. Skal man anta at brukere er interessert i opplæring? Finnes det noe forskning som viser om det fungerer? Forandrer brukerens oppførsel seg til noe bedre etter opplæring? Er brukeropplæring rett vei å gå? Hans vinkling på dette er sett fra IT-avdelingens side, det er de som bør ha ansvaret og ikke brukeren. Brukeren skal ikke ta jobben fra IT-avdelingen sier han. Men skal brukeren involveres er det viktig å få de til å opptre som godt utdannede brukere. Han konkluderer videre med at det ikke bare er et spørsmål om kunnskap, men hvordan man får brukere til å bruke denne kunnskapen på en fornuftig måte og at det ikke alltid er avhengig av mengde. Videre sier han at brukeropplæring ikke alltid er løsningen til sikkerhetsspørsmål, men det kan ikke anses som et argument til å ikke gjøre det.

3.3 Opplæring i standarder

Mange organisasjoner følger annerkjente internasjonale standarder for informasjonssikkerhet. Disse brukes etter punkt og prikke eller som et utgangspunkt for hvordan organisasjonen skal implementere sikkerhetstiltak. De mest anerkjente standardene er ISO 17799 [9], ISF[3] [10], CobiT fra ISACA [11] og BSI[4] [29]. Disse har alle en seksjon der de omtaler bruk av opplæring, utdannelse og trening innen informasjonssikkerhet.

Standarden ISO 17799 [9] består av retningslinjer eller "Best practice" innen sikkerhetsadministrasjon og ledelse. Standarden gir konkrete anbefalinger for informasjonssikkerhetsarbeidet og i seksjon 6.2 står det skrevet om brukeropplæring og utdannelse. Der poengterer man at det skal foreligge opplæring slik at man reduserer potensielle sikkerhetsrisikoer. Opplæring innen følgende temaer er nevnt: krav til sikkerhet, juridiske ansvar, interne tiltak og opplæring i riktig bruk. Det er ikke poengtert i stor grad, men det er likevel med som en del av standarden.

Når det gjelder ISF [10] er det flere sider som forklarer hvordan og hvorfor der er viktig med opplæring og bevisstgjøring. De påpeker at det er viktig å trene og utdanne organisasjonen slik at de har kunnskap og evnen til å gjøre sikkerhetsarbeid. Alle skal forstå hva, hvorfor og hvordan. Standarden foreslår også noen konkrete måter å øke bevisstgjøringen og utdanningen som for eksempel å dele ut brosjyrer og henge opp plakater og at utdanningen er "computer-based". Her foreslåes det også å gjøre målinger av frekvensen innen sikkerhetshendelser som ett mål på hvordan det ligger ann i organisasjonen. På denne måten se om sikkerhetstreningen og bevisstgjøringen har lykkes.

[3] Information Security Forums Standard of Good Practice
[4] The IT Baseline Protection Manual

Rammeverket CobiT 4.0 [11] inneholder virksomhetsstyring og kontroll på IT-området, også denne er basert på "best practice". Rammeverket bruker i sin manual for standarden et kapittel på opplæring og trening. Her skrives det at arbeidsgiver skal gi sine ansatte den nødvendige treningen og sørge for å vedlikeholde kunnskapen gjennom kurs og lignende. Her foreslåes det også interne kontroller der de måler antall oppringinger til help-desken og antall prosent som er fornøyd med treningen. Det er en 3-stegs prosess som foreslåes; identifisere, trene og sjekke.

BSI[5] [29] har også utarbeidet en standard. Den er på hele 2377 sider og tar for seg det aller meste på et detaljert nivå. Her presiseres det at for at en god sikkerhet skal oppnås, må alle som er involvert være motiverte og deretter gjennomføre et treningsopplegg. Videre sies det at det er viktig å bevisstgjøre alle i organisasjonen med tanke på konfidensialitet, integritet og tilgjengelighet. Det beskrives nøye hva som opplæringen bør bestå av og hvordan den bør gjennomføres. Nevner temaer som virus, passordbruk, backup, persondata og soscial engineering. En merkbar andel av kunnskapen hver enkelt plukker opp på et kurs forsvinner fort sier de, kanskje så mye som 80 % av kunnskapen blir glemt i løpet av kort tid. De foreslår derfor regelmessig trening.

3.3.1 Feil fokus

Bruk av informasjonssikkerhetsstandarder er en av de mest brukte metodene for å opprettholde og nå god sikkerhet. Et av problemene ved å følge slike standarder slavisk er at de kan føre til feil fokus [30]. Siponen nevner i sin artikkel at det er viktig å fokusere mer på innholdet i prosessen i stedet for prosessen i seg selv. Vi kan lese i standardene at det er viktig å utføre risikoanalyse og gjennomføre et bevisthetsprogram, for eksempel. Men problemet ligger i at det ikke fokuseres mer på hvordan. Dette skaper problemer, standardene er mer opptatt av at aktivitetene eksisterer enn hvordan de blir utført, og at mange av aktivitetene og retningslinjene er abstrakte og vanskelige. Noe som gjør at det ønskelige resultatet med aktiviteten ikke blir nådd.

ISO 17799 [9] og ISF [10] blir spesielt nevnt av Siponen i [30].

3.4 Hvordan måle det umålbare?

God sikkerhet kan for mange tone seg som noe abstrakt. Hvordan skal man måle sikkerhet? Måler man da noe som er umålbart? [31] Kanskje er det slik at vi vet hva som er god sikkerhet når vi ser det? Det som gjør en metrikk god er i følge [32] dette: (1) At den måler det den skal, (2) kvantifiserbar, (3) måler nøyaktig og (4) at den kan valideres. I tilegg til disse fire kan man legge til billig å utføre, uavhengig resultater og skalerbar.

Det er opp gjennom årene kommet flere forslag til hvordan måle og tallfeste god sikkerhet. Man kan se på flere metrikker for å måle sikkerheten. Her er noen av dem: Risikoanalyse, IDS-basert, policy-basert, hendelsesbasert. Risikoanalyser tar hensyn til sansynelighet og skade. Det er en vanskelig metode å bruke, siden man her må ha forståelse for alle typer angrep og sansyneligheten for disse, samtidlig som man ser på konsekvenser av angrepene.

Ved bruk av en IDS-basert metrikk kan man for eksempel se nærmere på antall virus som er detektert hver dag eller man kan se nærmere på de som faktisk kommer seg gjennom og blir oppdaget på andre måter. Tilsvarende kan man jo også se nærmere på tall tilknyttet brannmuren. Er et system som oppdager flere innbrudd bedre enn et som

[5] The IT Baseline Protection Manual

ikke gjør det?

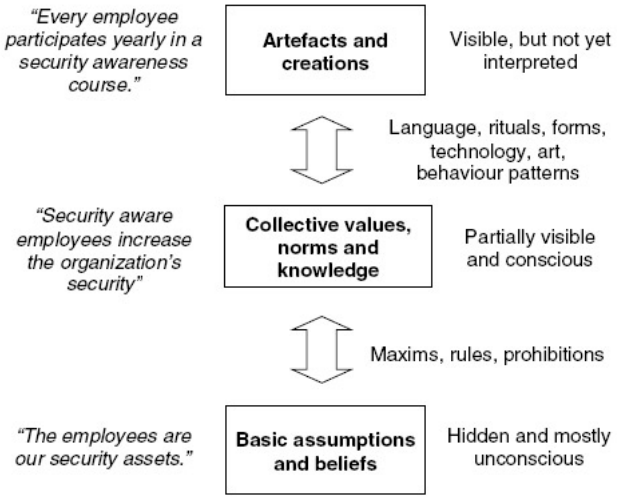
Når man bruker en policy-basert metrikk ser man for eksempel på tall som antall uatoriserte logginn forsøk, filer som er aksessert etc. Denne typen metrikk og IDS-basert, som nevt over, kan være metrikker som måler graden av brukertrening eller bevisthetsnivå og ikke systemets faktiske sikkerhet [32].

Hendelsesbaserte metrikker ser nærmere på angrepene som har lykkes. Frekvensen og hvilke skader som har skjedd. Dette er nok en metrikk som i større grad måler hvordan systemets sikkerhet faktisk er.

3.5 Sikkerhetskultur

I begrepet sikkerhetskultur inngår sentrale begreper som holdning og motivasjon [33]. Den enkelte virksomhet eller ansatt vil få store problemer ved å nå målene i sikkerhetsarbeidet hvis ikke de riktige holdningene og motivasjonene er til stede. Sagt på en annen måte vil ikke de ulike resursene som er satt inn for å beskytte informasjonen ha noen effekt dersom hver enkelt sammen ikke har god sikkerhtskultur.

Sikkerhetskultur hjelper til med å bygge nødvendig tillit mellom de forskjellig aktørene i virsomheten [2], og er et fenomen som kan vokse og forandre seg over tid. Det kan også til en vis grad formes av ledelsen. Sikkerhetskultur kan sies å være en del av organisasjonskulturen, som består av 3-lag (Figur 2).



Figur 2: 3-lags sikkerhetskultur [2].

Et tett samarbeid mellom NSM (Nasjonal Sikkerhetsmyndighet) og NTNU rundt emnet sikkerhetskultur har resultert i to rapporter [34, 35]. De foreløpige resultatene som fremkommer i disse rapportene tyder på at kulturelle forhold spiller inn. Små grupper som deltar aktivt virker mest effektivt på brukerene. Når det gjelder innstrukser ser det ut til at dette ikke har noe særlig virkning på brukerene. Å gjøre hver bruker oppmerksom på sikkerhetsansavaret ser ut til å ha en positiv effekt.

For å kunne sjekke status for sikkerhetskulturen har NSM, NTNU og SINTEF utarbeidet et verktøy som måler de kulturelle sidene av sikkerhetsarbeidet, SjekkIT [36, 34]. Gjennom å bruke dette verktøyet kan den enkelte virksomhet komme med tiltaksplaner for eventuelle mangler i sikkerhetskulturen.

3.5.1 Holdninger

Hva er holdninger? Holdninger i følge Kaufmann & Kaufmann [37] er skjæringspunktet mellom individual- og sosialpsykologi. Vi vil i denne oppgaven se på emnet som en sosialpsykologisk prosess, hvor relasjonene mellom individer og sosiale objekter blir det sentrale. Når man ser nærmere på sosialpsykologien ligger holdningene nedfelt i vår personlighet og er derfor en viktig årsak til at vi utfører de handlingene vi gjør. Mennesket tilordner seg nye holdninger gjennom hele livet, ofte kan også holdniger endres gjennom tid og læring. De viktigste læremodellene er imitasjon, identifisering, internalisering og internering. Det blir videre nevt i [37] at vi kan dele holdninger inn i 3 komponenter.

Den kognintive komponenten er tankeinnholdet vårt, hva vi tror. For eksempel hvis ledelsen bestemmer seg for å holde et kurs for de ansatte. Da kan noen tenke: "Jeg trenger ikke opplæring". Den emosjonelle komponenten er hva vi føler om noe som skal til å skje. For eksempel at de ansatte ikke er fornøyd med tingenes tilstand og insinuerer at de ikke har gjort en god nok jobb. Siste komponenten er adferdskompnenten, hvordan vi er tilbøyelig til å handle. For eksempel hvis ledesen bestemmer seg for å gjennomføre dyre sikkerhetstiltak. Dette kan ikke de ansatte ha noe forståelse for er nødvendig, siden dette fører til mer jobb.

NSM legger særlig stor vekt på holdningene til ledere i [33], lederenes holdninger har stor innvirkning på kvaliteten til virksomhetens sikkerhetsarbeid. Det nevnes vidre at medarbeidernes holdninger ofte er en refleks av lederens holdning. Dette nevnes også i [37]. Ledere er rollemodeller og påvirker de ansattes holdninger og atferd.

Er det mulig å endre holdninger? I følge [37] er de holdninger vi har, i samsvar med våre behov. En holdingsendring skjer derfor når våre behov endres. Mange kan ha samme holdninger rundt et tema, men årsaken til dette kan være forskjellig gjennom forskjellige behov.

3.5.2 Motivasjon

Motivasjon består av mellomliggende variable som varierer med retning, styrke og mål. Kilder til motivasjon kan være biologiske faktorer, emosjonelle faktorer, kognitive faktorer og sosiale faktorer [38]. Man kan også si at motivasjon består av en kombinasjon av indre og ytre faktorer, henoldsvis mage- og hodevalg [39]. Motivasjon henger sammen med et ønske om å lykkes og redesel for å misslykkes og den er knyttet til selvbildet, en opplevelse av mestring og mening.

Erfaring fra Brønnøysundregistrenes opplæringsprogram i informasjonssikkerhet har blitt innhentet i form av en intervjuundersøkelse av brukere i bank og IT-bedrift, gjennomført av Albrechtsen og Melteig fra NTNU og Brønnøysundregistrene [40]. Her ble det funnet store gap mellom ord og handling. Det var få sikkerhetsbidrag pr bruker, men samtidig ga brukerene uttrykk for at de var motivert for å bidra i sikkerhetsarbeidet. Grunnen til at det er et gap mellom ord og handling kan tyde på problemer med motivasjonen.

Motivasjon kan føre til handling. *Motivus* - å sette i bevegelse [39].

4 Valg av metode

4.1 Plan for forskningsarbeidet

Gjennom arbeidet med oppgaven har det vært en plan for forskningsarbeidet, metoder for innsamling av data, statistisk analyse og vurdering av resultatene.

For a svare på oppgavens problemstillinger ble det valgt å inkludere både kvantitative og kvalitative elementer i det gjennomførte prosjektet. Informasjonen ble innhentet i form av:

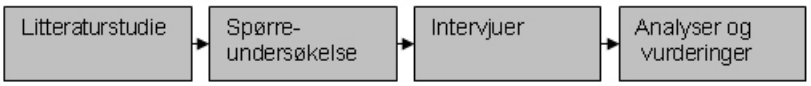
- Litteratur
- Spørreundersøkelse
- Intervju

Først og fremst foretok vi en spørreundersøkelse blant de som hadde gjennommført opplæring og i regi av NVE (kvantitativ). Statistiske data ga oss grunnlag til blant annet å sammenligne med Mørketallsundersøkelsen [3] samtidig som det ga oss informasjon om dagens situasjon. I tillegg har vi gjennomført intervjuer (kvalitativ) for å oppnå mer utfyllende og fullstendig informasjon. Det er ikke alltid man klarer å fange opp alle detaljer og hvorfor valg ble gjort ved en spørreundersøkelse. Intervjuene ga oss en supplerende effekt med viktig informasjon om tanker og valg som lå bak statistikken.

Vi valgte en forskningsmetode basert på hovedtilnærmingene i bøkene [41] og [42]. I tillegg til disse ble arbeidet som ble nedlagt i oppgavens forprosjekt [43] benyttet.

En kvantitativ tilnærming ga oss strukturert og systematisert kunnskap. Målinger og teori dannet grunnlaget for årsak og effekt tenking. Vi har gått i bredden og på den måten tok vi sikte på å formidle forklaringer. Dataene ble innhentet på forutbestemte instrumenter og formet om til målbare enheter som gjorde statistiske beregninger mulig.

Den kvalitative tilnærming ga oss meninger og opplevelser som ikke lot seg tallfeste eller måle. Kunnskapen vi fikk ble bygget primært på et konstruktivt og/eller deltakende perspektiv. Ved å gjøre en kvalitativ tilnærming fikk vi frem sammenheng og helhet. Vi oppnådde på denne måten å gå i dybden.



Figur 3: Oversikt over prosessen

Planen for forskningsarbeidet, og frem til rapportens skriftlige resultat kan beskrives med Figur 3. Der vi tar utgangspunkt i problemstillingen. På bakgrunn av problemstillingen er det derfor gjennomført en innsamling av data. Dette arbeidet var i form av litteratursstudie, spørreundersøkelse og intervjuer. Funnene i analyser og vurderinger av den statistiske delen sammen med intervjuene og litteraturen ga oss svar på forskningsspørsmålene og ny kunnskap i forhold til problemstillingen.

4.2 Litteratur

Det er viktig med en studie av relevant litteratur for blant annet å kunne kartlegge hva som er gjort tidligere og gjøre problemstillingen klarere for sin egen del. Og med en god litteraturstudie i ryggen, vil man kunne tilegne seg den kunnskapen som er viktig for å få gjennomført sin egen studie. Slik det er beskrevet i [41], kan man på en effektiv måte takle egne forskningsspørsmål ved å ha god kjennskap til det som er gjort tidligere.

Studie av relevant litteratur har hovedsaklig bestått at bøker, artikler, forelesningsnotater, publikasjoner og lignende, som har inneholdt fakta tilknyttet problemstillingen til denne oppgaven. Vi har blandt annet brukt:

- IEEE Xplore
- CiteSeer
- ISI - Web of science
- Springer Link
- Google
- Lovdata
- ACM
- Bibsys

Litteraturstudiet viser at det finnes mange ulike begreper knyttet til temaet. Også andre undersøkelser er gjort, og data fra disse er tilgjengelig til en hvis grad. Teorien har også dannet grunnlaget for spørreundersøkelsen.

4.3 Spørreundersøkelsen

Som nevnt tidligere i kapittelet ved den kvantitative tilnærmingen gjennom spørreundersøkelsen, kan dette gi oss et tverrsnitt på dagens situasjon. Resultatene fra spørreundersøkelsen og arbeidet med litteraturstudiet vil være den viktigste delen for å finne svar på forskningsspørsmålene i 1.4.

Det skulle vise seg at flere var interessert i å bruke kraftbransjen i en spørreundersøkelse. For å kunne finne svar på våre problemstillinger valgt vi å sammarbeide med Janne Hagen, doktorgradsstudent ved Høgskolen i Gjøvik og Eirik Albrechtsen, doktorgradsstudent ved NTNU. Deres oppgave var å se nærmere på organisatoriske informasjonssikkerhetstiltak i norske virksomheter. Med funnene vil de gi et bilde av bruken av organisatoriske sikkerhetstiltak og hvilke faktorer som bidrar til at sikkerhetstiltak oppnår effekt. Spørreundersøkelsen gikk ikke bare ut til kraftbransjen, men også til medlemmer i Kommunal Informasjonssikkerhet (KInS), IT-sikkerhetsForum (ISF), OLFs arbeidsgruppe for informasjonssikkerhet og utvalgte virksomheter i finanssektoren. Sammarbeidet kom som et ønske fra NVE hvor vi ble forespurt om å samarbeide ved innhenting av data. Vi innså at 2 undersøkelser kunne bli for mye, og at mest sansynelig bare en av oss fikk fornuftige deltakelse. Samtidig trodde vi at arbeidsmengden på denne måten ble mindre for respondentene. Spørreundersøkelsen ble avholdt i tidsrommet 26 februar til 12 mars, med utsendelse av purring 6 mars og 12 mars 2007.

Etter å ha sett nærmere på antall respondenter fra energibransjen ble det besluttet at vi skulle ta en ringerunde rundt til deltakerene av kursene og høre om de hadde anled-

ning til å delta i undersøkelsen. Vi hadde da plukket ut et mye mindre antall spørsmål, slik at tiden kom ned i 5-7 minutter, og kun vårt behov ble dekket. Ved å bruke telefonen fikk vi satt et litt mer personlig preg over undersøkelsen, samtidig som det virker mer forpliktende. Denne suplerende undersøkelse ble også holdt over internett, i tidsrommet 28 mars til 2 april.

4.3.1 Utvalget

Spørreundersøkelsens populasjon utgjør personer ansatt i energisektoren, næremere bestemt IT-sikkerhetsledere eller tilsvarende stillinger. Siden vi har sammarbeidet om undersøkelsen har også de som ikke har deltatt på kurs/opplæring av informasjonssikkerhet i regi av NVE vært med. Respondentene arbeider i virksomheter som i følge beredskapsforskriften [5] er pålagt stor fokus på informasjonssikkerhet med tanke på å sikre egne systemer og verdier, dette for å kunne sikre oppgaver når det gjelder drift og tjenester. Virksomhetene kan deles inn i to forskjellige deler, produksjon og nettselskap. Produksjonsvirksomhetene er ikke i så stor grad avhengig av IT som nettselskapene. Disse er avhengig av sikker bruk av IT med tanke på styringssystemer i driftsdelen. Det er store sprik i størrelsen på virksomhetene. De minste med bare et par ansatte til de virkelige store med flere hundre ansatte. Med størrelsen og type virksomhet vil nok kunnskapsnivået innen informasjonssikkerhet også variere.

NVE har i løpet av 2006 hatt 2 kurs over en dag fra 09.00-16.00, et kurs i mai og et i november. Til sammen var det et sted mellom 150 og 200 personer som deltok på kurset en av de to dagene i 2006. Det var også et fåtall som deltok begge dagene, grunnen for dette var at enkelte syntes informasjonsmengden var for stor til å få med seg alt på en dag. Man kan jo tenke seg at for enkelte er kurs en fridag eller en måte å komme seg bort fra hverdagen på. I all hovedsak besto deltakerne av ledere og IT-sikkerhetsledere. Det var ingen fra toppledelsen som deltok. Det ble ført en aktiv kampanje for kurset, men spesielt da mot de som ikke møtte opp første gangen kurset ble holdt. Det kan være av interesse å se om dette kan ha hatt noen innvirkning på resultatene, om en av gruppene skiller seg ut. Man kan jo tro det vil være forskjeller på blant annet holdningsmønsteret til de to gruppene.

Utvalget er ikke på noen måte tilfeldig eller representativt for norske bedrifter generelt, men representere en gruppe som i stor grad kan være til hjelp med å løse problemstillingene som berøres i denne oppgaven.

Det ble antatt at flere ikke ville delta av konfidensialitetshensyn og at andre ikke tok seg tid til aktiviteter som ikke vil være til nytte for seg selv eller virksomheten.

4.3.2 Spørreskjemaet

Spørsmålene er avgjørende for å få et godt resultat av spørreundersøkelsen. For at vi kunne ta et godt valg av spørsmål brukte vi litteraturstudie og oppgavens problemstillinger. Ved valg av uavhengige variable ble spørsmål knyttet til fakta om virksomhet og person. Noen av spørsmålene ble også valgt med omhu slik at en komparativ undersøkelse kunne gjennomføres. (Se vedlegg B)

Spørreundersøkelsen inneholdt spørsmål om:

- Kurs og opplæring
- Holdninger, atferd
- Hendelser

- Teknologier og beskyttelsestiltak
- Utkontraktering/outsourcing
- Virksomhet og person

Det ble lagt vekt på at undersøkelsen ikke skulle ta lang tid, men siden vi sammarbeidet med andre, måtte også deres behov dekkes. Resultatet ble et sted mellom 15 og 20 minutter, noe som bør være akseptabelt, men kan være for lang tid for de som arbeider under et stramt tidskjema.

I den suplerende undersøkelsen noen uker etter ble tidsaspektet vektlagt i håp om at flere skulle ta seg tid. Vi kom da ned i ca 5 minutter.

For at deltakerne skulle få informasjon om hva og hvorfor, ble det vedlagt et følgebrev med informasjon (vedlegg A). Her ble det også presisert at både person og virksomhet ble behandlet konfidensielt og alle svar ble anonymisert.

Til å gjennomføre spørreundersøkelsen ble et firma som NTNU har avtale med brukt, navnet er Active Dialogue [44]. De har også gått igjennom og kvalitetssikret undersøkelsen. De kjører surveys på web og leverer dataene i format til Excel eller SPSS.

Det ble først planlagt å bruke verktøyet QuestBack [45] til undersøkelsen, men siden vi samarbeidet ble dette brukt i den suplerende undersøkelsen og ved gjennomførelsen av pilot-undersøkelsen. Lisens ble skaffet gjennom NorSIS siden dette ikke er et gratis verktøy. QuestBack leverer tjenester relatert til spørreundersøkelser og er et webbasert verktøy for å lage spørreundersøkelser og lagrer data knyttet til undersøkelsene. I tillegg finnes det funksjoner for dataanalyse. QuestBack er en effektiv måte å innhente informasjon, samtidig som det er brukervennlig. Questback brukt til å gjennomføre en pilot.

Vi så på det som en mer effektiv måte å ta en webbasert spørreundersøkelse. Det vil være langt lettere for respondentene å krysse av skjemaer på web, enn om de skulle sittet med en papirutgave som i tillegg måtte returneres. Samtidig sparer også vi oss for arbeid knyttet til manuelt å taste inn resultatene. Respondentene er også tilstrekkelig kjent med epost og internett siden disse stort sett har en eller annen for tilknytning til IT i virksomheten.

Siden vi tar utgangspunkt i en epostliste er det naturlig og tro at det er riktig utvalg som svarer og ikke en hvilket som helst person i virksomheten.

Deltakerne svarte på de fleste spørsmålene ved å krysse av i bokser og svarene er forhåndsbestemt, noen av spørsmålene hadde også muligheten for at de kan utfylles med egne svar og kommentarer. På flere av spørsmålene spurte vi etter i hvilken grad de forskjellige deltakerne stod i forhold til temaene det spurtes om. Det var i disse tilfellene brukt en fempunktskala [46]. På disse spørsmålene var svaralternativet “Vet ikke” utelatt. Dette i håp om at deltakeren tenkte før han eller hun svarte og ikke valgt den letteste veien med et “Vet ikke” svar.

En pilotgruppe på 8 personer har vært med i arbeidet med å kvalitetssikre spørreundersøkelsen. To fra NVE, en fra NorSIS og de resterende fra informasjonssikkerhetsmiljøet på HiG. Resultatene ble nøye gjennomgått. Feil, mangler og missforståelser ble rettet opp. Det ble lagt stor vekt på spørsmålsstilling og betydning for å unngå missforståelser, samtidig gjøre det enklest mulig. Spørreundersøkelsen ble laget og gjennomført på norsk.

4.3.3 Utsendelse

Siden vi har benyttet oss av et eget firma i den første, hovedundersøkelsen, har de stått for invitasjon til spørreundersøkelsen. Dette skjedde pr epost. Konfidensialitet og personlig preg er opprettholdt ved at Active Dialogue sendte ut invitasjon til en og en, og ikke en til alle. Det samme ble gjort i Questback, der vi selv la inn liste som invitasjonen ble sendt til. Vi ser på dette som en effektiv måte å gjøre det på for respondenten. Vi forventet at respondentene var godt kjent med bruk av epost og internett og at dette sikrer oss større deltakelse enn ved en papirbasert utgave.

4.3.4 Gjennomgang og tolking av data

Resultatene av datainnsamlingen i undersøkelsen ga oss grunnlag til å foreta dataanalyse og tolking. Nye resultater gir ny kunnskap og en bedre forståelse rundt temaet. Med de nye resultatene i bakhodet kan vi da komme med forslag til forbedringer eller påpeke hva som har fungert godt.

Vi fikk en forholdsvis god nok svarprosent til å gjennomføre statistiske undersøkelser. De statistiske undersøkelsene ble gjennomført med SPSS [47, 48, 49]. Dette er er verktøy som er kraftigere og fungere bedre til vårt formål enn for eksempel Excel som innehar lignende funksjoner.

I analysen har vi benyttet oss av følgende undersøkelser:

- Frekvensanalyser - beskriver hvordan observasjoner fordeler seg basert på en variabel
- Variansanalyser(ANOVA) - sammenligner flere grupper for å avdekke variasjon innen og mellom gruppene
- "Independent samples T-test" - sammenligner gjennomsnittsverdien i to grupper av tilfeller
- Krysstabeller(Kji-kvadrat) - ser på hvordan observasjoner fordeler seg på to eller flere variabler

Signifikansnivået(p-verdi) ble satt til en verdi på 0,05. Hvis noe annet ble valgt er dette oppgitt i forbindelse med resultatene.

4.4 Oppfølgende intervjuer

I tillegg til spørreundersøkelsen, ble det gjennomført en intervjurunde, kvalitativ data. Dette ble gjort for å gå mer i dybden og få frem flere detaljer rundt problemstillingene. Det var resultatene fra spørreundersøkelsen som dannet grunnlaget for intervjurunden. Respondentene fikk der mulighet til å melde seg frivillig på en oppfølgingssamtale, enten ved epost eller telefonnummer, der de godtok å bli oppringt på et senere tidspunkt. Intervjuene ble satt til å ha en maksimaltid på ca 15 minutter. Men det kunne være vanskelig å følge klokka på et intervju siden flere spørsmål dukket opp som følge av et svar og derfor ble også intervjuene anderledes fra person til person.

4.5 Kvalitet

I alle typer forskning vil det være relevant å sjekke om resultatet man får er av god kvalitet. Dette påpekes også litteraturen [41, 42]. Videre blir elementer som ligger under god kvalitet diskutert. Reliabelt, validitet og egen rolle i forskningen. Med reliabilitet menes det her om resultatet er pålitelig. Det er selvsagt viktig å kunne stole på resultatene

som blir generert i forskningen. Med validitet menes det her om resultatet er gyldig, at resultatet er sant og at det måler det som skal måles.

En mulig svakhet ved alle spørreundersøkelser er om de korrekte spørsmålene er stilt og at tilsvarende svaralternativer er riktige. Det er ønskelig å gi et så riktig bilde som mulig ved hjelp av undersøkelsen. Med på å gjøre dette mulig har vi da brukt pilotgruppen aktivt, samtidig som veileder også har bidratt sterkt med sine synspunkter. Til sammen har dette vært med på å kvalitetssikre undersøkelsen. Intervjuene vil også kunne hjelpe til med å avdekke feil eller mangler ved spørreundersøkelsen.

Ved å bruke følgebrevet til å opplyse om at dette var en frivillig spørreundersøkelse og at alle svarene ville bli behandlet konfidensielt og anonymisert, håper vi at dette har sørget for at så mange som mulig svarte ærlig og ikke ut i fra hva de tror de skulle ha svart, siden en slik undersøkelse på mange måter kan sees på som en egenevaluering. Gjennom lovverket stilles det store krav til integritet og konfidensialitet. Det er dermed grunn til å tro at mange av respondentene har erfaring fra å utveksle informasjon knyttet til informasjonssikkerhet.

Når det er sagt, antar vi at det ovenfornevnte har gitt resultater fra spørreundersøkelsen som er tilstrekkelig pålitelige.

En annen vesentlig del av å oppnå god kvalitet på resultatene, er at riktig målgruppe nås. Vi mener at ved å holde denne undersøkelsen hos virksomheter i energibransjen som har gjennomført opplæring vil nettopp treffe den riktige målgruppen, vi vil kunne innhente informasjon fra flere aspekter rundt temaet.

Ved å kombinere de kvantitative og kvalitative dataene kan man sjekke gyldigheten i resultatene. Intervjuene i etterkant viste nettopp dette. Det var samsvar med spørreundersøkelsen. Dette styrker resultatene som ble gjort i spørreundersøkelsen.

En svakhet ved slik forskning gjennom undersøkelser er faren for at resultatene blir for subjektive [42], en for stor del av personlige meninger og vurderinger blir brukt. Vi håper å ha unngått dette ved å ha en god dialog med veileder samtidig som andre uavhengige ressurspersoner har bidratt med kvalitetssikring.

5 Datagrunnlag

En spørreundersøkelse ble gjennomført hos IT-sikkerhetsledere og andre i lignende stillinger i energibransjen over hele landet. Siden det ble sammarbeidet om undersøkelsen ble også undersøkelsen sendt ut til noen av de som ikke hadde deltatt på NVE sine kursdager i slutten 2006. Spørmålene fra undersøkelsen er med på kartlegge respondentenes kunnskapsnivå, tanker og meninger rundt temaet opplæring, holdninger og tilsyn av informasjonsikkerhet, og presenteres i det følgende.

I dette kapitlet vil vi presentere datagrunnlaget fra undersøkelsen. Diskusjoner og drøftinger av resultater, konklusjoner og videre arbeid kommer i kapitelene 6, 7 og 8. I vedlegg D finnes frekvenstabeller fra spørreundersøkelsen.

5.1 Besvarelse av spørreundersøkelsen

Til sammen ble 118 invitasjoner sendt ut til virksomhetene i energibransjen, den total responsen ble på 40 stykker. Dette ga en svarrate på 33 prosent, noe som var litt under det vi hadde håpet på, men nok til at vi kunne utføre analyser.

Vi hadde mulighet til å sammenligne med det samlede totalresultatet fra hvert spørsmål, men da kun på organisatoriske spørsmålene, siden spørsmålene tilknyttet opplæring kun ble tilgjengelig for energibransjen. I tilegg til de 100 fra energibransjen ble undersøkelsen sendet ut til 256 andre virksomheter i andre bransjer. Se vedlegg B for spørsmålene.

Den lave svarprosent skyldtes i stor grad at energibransjens invitasjoner ble glemt den først uken, etter en glipp fra Active Dialogue. Dette er selvsagt noe som ikke skulle skje, men som var utenfor våre hender. Vi prøvde å bøte på dette med å forlenge fristen med noen dager, samt ett par ekstra purringer med anmodning fra NVE om at deltakelsen hadde stor betydning for oppgavens utfall. Noen flere besvarelser ble innhentet på denne måten, men ikke nok. Som nevnt tidligere ble det da foretatt en ringerunde, dette virket effektivt og resultatet ble ca 80 % flere respondenter. Det er grunn til å tro at lav svarprosent i den første undersøkelsen skyldes at det tok såvidt lang tid å besvare den.

I tilegg er det vært å nevne at ikke alle svarte på alle spørsmålene.

5.1.1 Kjønnsfordeling

- 33 av respondentene var menn (82,5 %)
- 6 av respondentene var kvinner (15,0 %)

Vi fikk et godt flertall med menn, et ønsket resultat kunne vært mer eller mindre lik kjønnsfordeling, men dette er nok ikke så galt i forhold til kjønnsfordelingen hos sikkerhetslederne. Med et større antall kvinner kunne vi med bedre sikkerhet avdekke eventuelle forskjeller i hvordan kvinner og menn svarte på undersøkelsen. Men kjønnsforskjeller var ikke hovedfokus i denne undersøkelsen.

5.1.2 Alder

- 1 av respondentene var i aldersgruppen 18-29 (2,5 %)

- 9 av respondentene var i aldersgruppen 30-39 (22,5 %)
- 16 av respondentene var i aldersgruppen 40-49 (40,0 %)
- 12 av respondentene var i aldersgruppen 50-59 (30,0 %)

Vi har i undersøkelsen en forholdsvis jevn fordeling i 3 av aldersgruppene. Dette muliggjør undersøkelser basert på om alder har hatt noen innvirkning i besvarelsen fra respondentene.

5.1.3 Erfaring

- 3 av respondentene har 0-1 år erfaring fra informasjonssikkerhetsarbeid (7,5 %)
- 12 av respondentene har 1-5 års erfaring fra informasjonssikkerhetsarbeid (30,0 %)
- 14 av respondentene har 6-10 års erfaring fra informasjonssikkerhetsarbeid (35,0 %)
- 8 av respondentene har 11-25 års erfaring fra informasjonssikkerhetsarbeid (20,0 %)
- 2 av respondentene har over 25 års erfaring fra informasjonssikkerhetsarbeid (5,0 %)

Hvor lang erfaring de enkelte har fra arbeid med informasjonssikkerhet totalt for både den virksomheten de jobber i nå, og for tidligerere, kan være en variabel som kan være utslagsgivende i forhold til hvordan respondenten besvarer spørreskjemaet. Noe det også er tatt høyde for ved å kartlegge denne variabelen i spørreundersøkelsen.

5.1.4 Antall ansatte

- 7 av respondentene jobber i en virksomhet med 1-24 ansatte (17,5 %)
- 24 av respondentene jobber i en virksomhet med 25-199 ansatte (60,0 %)
- 4 av respondentene jobber i en virksomhet med 200-499 ansatte (10,0 %)
- 5 av respondentene jobber i en virksomhet med 500 eller flere ansatte (12,5 %)

Vi har valgt å ta med størrelsen på virksomheten slik at vi kan sjekke om dette spiller inn som en mulig faktor på resultatene. Størrelse på virksomheten kommer frem av Mørketallsundersøkelsen [3] og andre lignende undersøkelser at dette er en avgjørende faktor.

5.1.5 Selskap

- 13 av respondentene jobber med produksjon (32,5 %)
- 22 av respondentene jobber i et nettselskap (55,0 %)
- 3 av respondentene jobber i en virksomhet som består av begge deler (7,5 %)

Bakgrunnen for at vi ønsket å ta med spørsmålet om de kom fra nettselskap eller produksjon, var for å avdekke om det faktisk er forskjeller blandt de to. Siden nettselskap i utgangspunktet er mer avhengig av IT enn hva produksjonsselskapene er.

5.1.6 Når de sist hadde opplæring

- 14 av respondentene hadde sist opplæring 0-6 mnd siden (35,0 %)

- 14 av respondentene hadde sist opplæring 6-12 mnd siden (35,0 %)
- 1 av respondentene hadde sist opplæring mer enn 12 mnd siden (2,5 %)

Får å kunne avdekke om respondentene deltok i det første eller andre kurset (mai eller november 2006) delte vi opp i hendholsvis 0-6 mnd siden og 6-12 mnd siden. Dette ble gjort for å finne eventuelle forskjeller blandt de to gruppene. Her var vi heldig med fordelingen og fikk et likt antall respondenter.

5.1.7 Regi

- 39 av respondentene tok sist et kurs i regi av NVE (97,5 %)
- 1 av respondentene tok sist et kurs i regi av andre enn NVE (2,5 %)

Grunnen til at en ikke deltok på kurset i regi av NVE kan være at de ikke hadde fått med seg hvem som var arrangør eller mest sansynlig har den personen deltatt på et nytt kurs som omhandlet informasjonssikkerhet etter kursene i regi av NVE.

5.1.8 Funksjon i virksomheten

- 1 av respondentene er daglig leder i virksomheten (2,5 %)
- 22 av respondentene er IT-ansvarlig i virksomheten (55,0 %)
- 1 av respondentene er økonomiansvarlig i virksomheten (2,5 %)
- 5 av respondentene er sikkerhetsansvarlig i virksomheten (12,5 %)
- 11 av respondentene har en annen funksjon i virksomheten (27,5 %)

Det kan tenkes at respondentenes funksjon i virksomheten kan kan ha en sammenheng med resultatene, derfor ble dette tatt med i spørreundersøklesen.

Når det gjelder stillingene til de 11 som svarte “Annet” på funksjon i virksomheten består disse stillingene av: Avdelingsleder, driftsingeniør, HMS, IKT sikkerhetsansvarlig, IT-konsulent, konsulent, 2 stk nettsjef, overingeniør, senior IT konsulent og teknisk sjef.

6 Resultater og diskusjon

6.1 Innleding

Resultatene fra spørreundersøkelsen er behandlet statistisk med det i tankene å besvare forskningsspørsmålene:

1. Opplæring, tilsyn, regelverk - gir det bedre informasjonssikkerhet?
2. Viser energibransjen en forbedring i forhold til resultatene i Mørketallsundersøkelsen[3] eller andre lignende undersøkelser?
   - Har de færre sikkerhetshendelser?
   - Er flere sikringstiltak gjennomført?
   - Er sikkerheten bedre hos de store virksomhetene i forhold til de små?
3. Bør sammenlignbare bransjer og enkeltbedrifter gjennomføre lignede tiltak?

Resultatene fra spørreundersøkelsen gir oss nye erfaringer om tiltak tilknyttet opplæring og tilsyn innen informasjonssikkerhet. Dette anses som nyttig informasjon for å kunne si noe om effektiviteten av slike tiltak. Virksomheter i energibransjen har hatt et stort fokus på informasjonssikkerhet de siste årene og derfor kan de hjelpe til med å belyse tiltakene. Med bakgrunn i dette kan vi også komme med forslag til lignende eller andre tiltak for andre bransjer og virksomheter.

For å kunne besvare spørsmålene nevnt ovenfor var det nødvendig å se nærmere på ulike faktorer som kan spille inn, så vel som faktorer som spiller en stor rolle. Svaret ligger i en kombinasjon av forskjellige variable som vil bli nærmere diskutert videre i kapittelet.

6.2 Kurset

For å kunne finne ut litt om motivet bak kurset respondentene hadde deltatt på, ba vi de om å svare på hvorfor de deltok på kurset.

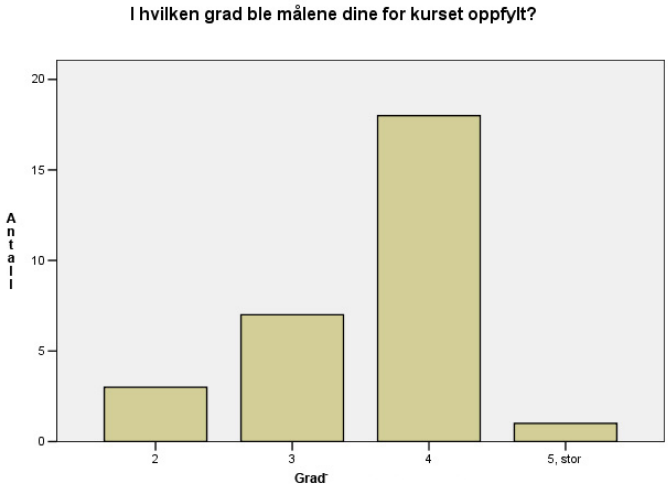
Hvorfor meldte du deg på kurset?

- 15 av respondentene sa de ble pålagt av arbeidsgiver (37,5 %)
- 20 av respondentene sa at de ser nytten i å tilegne seg ny kunnskap (50,0 %)
- 10 av respondentene sa at det var for å dekke et behov for nye impulser (25,0 %)
- 1 av respondentene sa det var for å få nye utfordringer (2,5 %)
- 11 av respondentene sa at de har en interesse for temaet (27,5 %)
- 1 av respondentene sa noe annet (2,5 %)

Svarene fra respondentene fordelte seg på en noe uventet måte. Det ble sagt fra NVE sin side at det var ingen av deltakerene som på noen måte hadde blitt pålagt å delta på

kurset. Men det hadde blitt ført en aktiv kampanje mot potensielle deltakere om å delta. Vi kan da se av resultatene at denne kampanjen av nesten 40 % av respondentene ble sett på som et pålegg fra arbeidsgiver. Dette er et høyt tall og mye av motivasjonen og ønske om å lære noe nytt kan bli borte. Vi så nærmere på hva de samme respondentene hadde svart ellers på svaralternativene, og det vi da kunne se var at 5 av de 15 hadde kun svart "pålagt", mens de resterende 10 hadde i tillegg krysset av en av de andre svaralternativnene som "ser nytten i å tilegne meg ny kunnskap".

Respondentene ble også bedt om å gradere sine mål for kurset samt å gradere ulike spørsmål i tilknytning til hvordan arbeidet og forståelsen med informasjonssikkerhet hadde blitt etter kurset. Svarene ble delt inn i fem mulige graderinger, der 1 var liten forståelse og deretter stigende opp til 5, stor. Vi ser av Figur 4 at 19 av de 29 responden-



Figur 4: I hvilken grad ble målene dine for kurset oppfylt?

tene som svarte (11 valgte av en grunn ikke å svare) på dette spørsmålet sier at deres mål ble i nokså stor grad oppfylt. Dette tyder på at de som kom for å tilegne seg ny kunnskap eller dekke et annet behov fikk innfridd dette, mer eller mindre grad.

På spørsmålet der de ble bedt om å gradere om forståelsen har blitt bedre etter kurset ser vi av Tabell 1 at vi kan dele inn i to grupper, der ca halvparten ikke fikk noe særlig mer ut av det, mens den andre halvparten syntes dette var bra for forståelsen av informasjonssikkerhet. Det vi også kan legge merke til er at det er tilsvarende inndeling på spørsmålet om de syntes det var nødvendig med mer opplæring.

Vil du si at forståelsen for informasjonssikkerhet er bedret etter kurset?

Grad	Antall	Prosent
1	0	0
2	5	17,2
3	9	31,0
4	14	48,3
5	1	3,4

Tabell 1: Forståelsen etter kurset

Synes du det er nødvendig med mer opplæring?

Grad	Antall	Prosent
1	0	0
2	2	6,9
3	10	34,5
4	14	48,3
5	3	10,3

Tabell 2: Mer opplæring

For å se nærmere på denne sammenhengen benyttet vi oss av krysstabell (kji-kvadrat). Her skulle det vise seg at det var en viss positiv sammenheng, men ikke signifikant nok med en $p > 0,05$. Dette kan likevel tolkes som en indikasjon på at forståelsen ikke ble bedret etter kurset samtidig som de syntes at de heller ikke trengte noe mer opplæring. Og det samme motsatt, de som økte forståelsen for informasjonssikkerhet ville ha mer opplæring.

For å kikke nærmere på denne sammenhengen foretok vi en rekoding av dataene der vi delte inn i 2 grupper i stedet for graderingen 1 til 5. Gruppene ble da delt på "midten", mindre og lik 3 og større enn 3. Det vi da fant var en signifikant sammenheng.

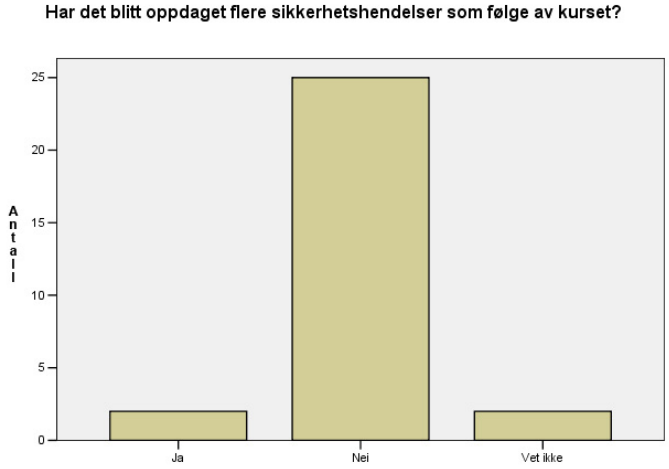
Et slikt resultat hadde vi ikke direkte ventet, men en mulig årsak til funnet kan værer at når man først har skjønt hva problemet er så ser man også lettere hvor stort problemet er og hvor stort området informasjonssikkerhet er. Altså kan vi si at de med størst bevisthetsnivå rundt sikkerhet ser behovet mest.

Har du kommet i gang med flere sikkerhetsoppgaver etter kurset?

Grad	Antall	Prosent
1	0	0
2	8	20,0
3	5	12,5
4	15	37,5
5	1	2,5

Tabell 3: Antall sikkerhetsoppgaver etter kurset

Som de foregående spørsmålene var det også 11 personer her som ikke hadde avgitt svar, men som vi ser av Figur 5 var det et stort overtall av respondenter som ikke hadde oppdaget flere sikkerhetshendelser (25 av 29). Vi håpet å kunne se at man vil kunne oppdage flere hendelser som følge av kurs og opplæring når kunnskapsmengden øker rundt emnet, slik at vi på den måten kan se om opplæringen har hatt ønsket effekt. Det kan se ut til at dette ikke er et godt mål, vi ser at de enkelte har kommet igang med flere sikkerhetsoppgaver etter kurset (se Tabell 3. Det kan tyde på at disse oppgavene som er igangsatt ikke har ført til en økning, men heller det mottsatte. De har resultert i at flere usynelige hendelser har blitt stoppet. Vi kan jo også tro at de enda ikke har kommet opp på et kunnskapsnivå der de er i stand til å se de nye hendelsene, eller sagt på en annen måte, at de har igangsatt tiltak som brannmur og antivirus der de nødvendigvis ikke er klar over hvilke hendelser som er stoppet.



Figur 5: Har det blitt oppdaget flere sikkerhetshendelser som følge av kurset?

6.3 Forbedring av informasjonssikkerheten

- Kurs og opplæring
- Hyppigere kontroller og tilsyn
- Tydeligere og bedre regelverk
- Bedre programvare og utstyr
- Flere og bedre risiko anlyser

Dette var alle ulike sikkerhetstiltak respondentene selv skulle gradere viktigheten med i arbeidet med informasjonssikkerheten gjennom spørsmålet:

> Hvilke sikkerhetstiltak og i hvor stor grad føler du at det er viktig å jobbe med disse temaene for å forbedre informasjonssikkerhet?

Mer kurs og opplæring ble ikke overraskende noe av det samme med spørsmålet i forbindelse med kurset, der vi lurte på om de trengte mer opplæring (se tabell 2). Mer eller mindre likt, altså de synes at opplæring og kurs er en viktig del av arbeidet med sikkerheten. Dette kom også frem under intervjuene, der de alle var enige i at opplæring var en nødvendighet og de forsto at det kunne føre til større bevisthet.

I energibransjen blir det utført tilsyn i forbindelse med en kontroll av sikkerheten i de forskjellige virksomhetene. Det kan for noen muligens være til bryderi, men samtidig et godt hjelpemiddel til å sette en finger på de ulike problemene man eventuelt finner ved tilsyn. Av tabell 4 ser vi at et ønske om hyppigere kontroller og tilsyn er et faktum. Tar vi med oss de som kun befinner seg over midten er dette ca 43 % av respondentene. Det kan tyde på at for noen er tilsyn og kontroller en fin motivasjonsfaktor til å jobbe med informasjonssikkerhet og at noen kanskje trenger en "'storebror" som følger med for å yte. Om ikke tilsyn så kan enkelte kontroller muligens være et godt hjelpemiddel for å heve standarden i organisasjoner eller virksomheter. Kanskje ikke som et enkelttiltak, men sammen med andre tiltak som opplæring osv. Som det ble sagt under et av inter-

vjuene er det lettere og sløve seg igjennom en opplæringstime, men under tilsyn går ikke dette. Siden de da er et fåtall som sitter rundt et bord. Dette blir mer interaktivt for alle parter.

Grad	Antall	Prosent
1	1	2,7
2	9	24,3
3	11	29,7
4	11	29,7
5	5	13,5

Tabell 4: Kontroll og tilsyn

Energibransjen skal leve etter et stort antall lover, forskrifter og veiledninger. Det kan sikkert for mange av de små fortone seg som veldig voldsomt å sette seg inn i. Dette kan jo forsåvidt også gjelde de større virksomheten. Vi fant ut at å jobbe med et tydligere og bedre regelverk kan være med på å øke forståelsen og dermed forbedre informasjonssikkerheten. Vi kan lese av tabell 5 at det er ca 60 % som ønsker mer enn middels et tydligere og bedre regelverk. Under prosjektet har vi hatt kontakt med NorSiS [50], og under ett av disse møtene kom det også frem at de skulle jobbe med å forbedre, gjøre forskriftene og veiledningene fra NVE bedre. Med bedre menes det at de skulle gå igjenom og omskrive slik at de enkelte brukerene vil kjapt og enkelt kunne sette seg inn i regelverket.

For at et regelverk skal fungere opptimalt er det klart at dette må være tydelig, og ved eventuelt bruk i andre virksomheter og oranisasjoner er dette et kriterie som bør oppfylles. Noe av problemet kan ligge i juristers manglende forståelse for informasjonssikkerhet ved arbeidet med regelverket.

Grad	Antall	Prosent
1	1	2,7
2	3	8,1
3	11	29,7
4	15	40,5
5	7	18,9

Tabell 5: Bedre regelverk

Risikoanalyser er et godt hjelpemiddel til å innse problemområder for senere kunne gjøre noe med disse. Har man en forståelse for risikoen man står ovenfor i de forskjellige systemene og lignende har man kommet et godt stykke på veien for eventuelt å gjøre noe med disse. Risiko og sikkerhet henger som kjent sammen [17] og det er viktig å tenke konskvenser for hva som kan skje. Med et gjennomsnitt på 3,68 og en median på 4 skulle dette tilsi at det er et flertall som bikker mot flere og bedre risikoanalyser av respondentene (Tabell 6).

Grad	Antall	Prosent
1	0	0
2	2	5,4
3	14	37,8
4	15	40,5

5	6	16,2

Tabell 6: Flere og bedre risikoanalyser

Som en av mange forutsetninger for å kunne ha en tilfredstillinede sikkerhet, må vi ha noe programvare og utstyr. Vi vet ikke hvor gammelt eller nytt utstyret og programvaren er i energibransjen, men det er helt tydlig at det er et ønske om fornying for å kunne forbedre informasjonssikkerhet. Ca 60 % er over middels og med den oppfatning at nyere programvare og utstyr vil forbedre informasjonssikkerheten. Men selv om noen bruker eldre utstyr er det også viktig å oppdatere sine versjoner. Nytt er ikke nødvendigvis bra nok for å gjøre forbedringer.

6.4 Standarder, organisasjoner og fora

Det er ofte at organisasjoner og virksomheter etc. bruker annerkjente standarder som utgangspunkt eller følger disse slavisk i en utarbeidelse av sikkerhetspolicy. Det var derfor av interesse å undersøke om energibransjen kjente til noen av informasjonssikkerhetsstandardene som finnes. Vi spurte derfor følgende spørsmål:

> Kjenner du til noen av disse standardene innen informasjonssikkerhet?

- ISO 17799/BS 7799 eller en nasjonal variant
- Information Security Forum (ISF) Standard of Good Practice
- CobiT fra ISACA
- The IT baseline Protection Manual (BSI)
- Ingen

Som vi kan se av Figur 6 sa 15 respondenter (37,5 %) at de ikke hadde noe kjennskap til noen av de nevnte standardene. Når det gjelder fordelingen av de resterende svarende, viser det seg at ISO 17799 er den standarden som de fleste kjenner til. 15 respondenter (37,5 %) kjente til standarden. Hakk i hel kom ISF sin Standard of Good Practice med 11 respondenter (27,5 %). CobiT fra ISACA kjente 5 respondenter til og The IT baseline Protection Manual (BSI) kjente kun en respondent til.

Det er et forholdsvis høyt antall som ikke kjente til noen av standarderene. Vi hadde trodd at et større antall som har stillinger innen informasjonssikkerhet hadde større kjennskap til standarder. Bruk av standarder er også en av de mest brukte metodene for å opprettholde og nå god sikkerhet. Men på en annen side må man være forsiktig med hvordan man bruker disse standardene. ISO 17799 [9] og Standard of Good Practice for Information Security [10] blir spesielt nevnt av Siponen i hans artikkel [30]. Det er også disse to som bemerker seg i undersøkelsen vår som de mest kjente. Samtidig som man benytter seg av standarder må man ikke bli for opphengt i følge disse slavisk, da dette kan føre til at man muligens kan se seg blind. Man har innført en standard og føler seg dermed trygg på sikkerheten, men det er selve innholdet i prosessen man må fokusere på, ikke prosessen.

Hvis man er medlem i et fora eller en organisasjon som arbeider med informasjonssikkerhet er det naturlig å tro at man er interessert i temaet og man vil få oppdateringer, tips/triks og hjelp i arbeidet med sikkerhet, man tar lærdom av andre. Det var derfor naturlig for oss å undersøke om respondenten eller bedriften var med i et slikt fora eller organisjasjon.

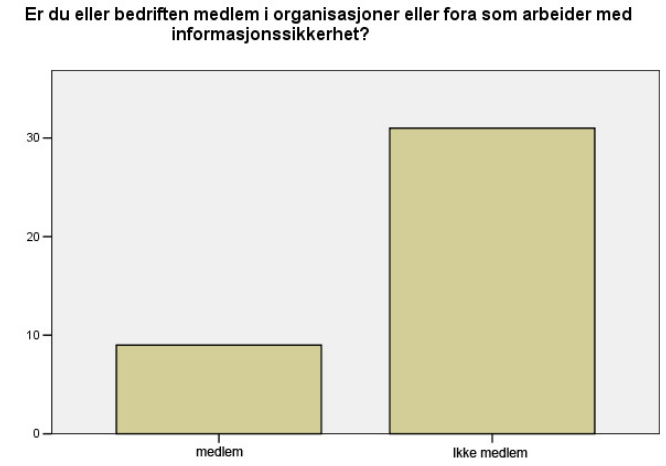
Figur 6: Kjenner til en standard

Er du eller bedriften medlem i organisasjoner eller fora som arbeider med informasjonssikkerhet?

- Ikke medlem
- ISF
- KInS
- NSR
- ISACA
- Bluelight
- PKI-forum

Vi kan se av Figur 7 at så mange som 31 respondenter (77,5 %) svarte av verken de eller bedriften er medlem i en organisasjon eller fora (true). Dette høye resultatet kan ha en sammenheng med funnet av at så mange ikke har kjennskap til standarder innen informasjonssikkerhet. Av de som hadde et medlemsskap var disse jevnt fordelt på ISF og ISACA.

Vi har foretatt en kji-kvadratstest der vi fant en signifikant sammenheng mellom de som ikke er medlem i noe fora eller lignende og de som ikke har kjennskap til noen standrad. Resultatet ble en p-verdi = 0,008. Kausaliteten mellom disse to verdiene kan det være vanskelig å si om, har ingen kjennskap til standarder fordi de ikke er medlem i et fora eller lignende eller er det andre mulige årsaker som ligger bak? Mest sansynlig kan vi tenke oss at det er en mulig tredjevariabel som ligger bak, som for eksempel bevisthetsnivået. Er respondentene beviste på sikkerhet er de også medlem av fora samtidig som de har kjennskap til standarder, der ikke nødvendigvis medlemskapet i forumet er direkte årsak til kunnskapen rundt standarder, men for noen kan nok dette stemme.

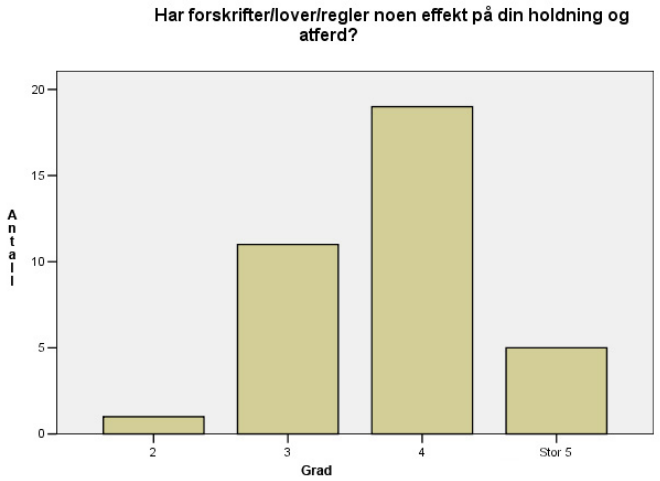


Figur 7: Medlem av fora eller organisasjon

6.5 Holdninger, atferd og motivasjon

Energibransjen er en bransje som er kritisk for samfunnet vårt. Vi er alle avhenging av produksjons- og nettselskapene for produksjon og distrubiering av elektrisitet rundt om i landet vårt. Det er nok derfor NVE har innført lover, regler og forskrifter for bransjen. I denne oppgaven ser vi som sagt nærmere på informasjonssikkerheten, og derfor har vi tatt med spørsmål som har kikket nærmere på de enkelte respondentenes holdninger, motiavsjon og atferd i forbindelse med dette.

Har forskrifter/lover/regler noen effekt på din holdning og atferd?



Figur 8: Holdninger og atferd

Av de totalt 36 som svarte på dette spørsmålet (Figur 8) svarte en tredel, hvis vi slår sammen til to grupper, at det til en viss grad hadde noe innvirkning på deres holdning

og adferd. De resterende to tredelene svarte at store deler av deres holdninger og adferd blir påvirket av lover og regler. Det er tydelig at lover og regler mer eller mindre har en innvirkning på respondentene og at deres adferd endres etter dette. Vi vil anta at dette har en positiv effekt, og at ikke adferden og holdningene endres til noe negativt, men har en positiv effekt slik at lovene og reglene følges.

Er du motivert til å bidra med sikkerhetsarbeid?

Figur 9: Motivasjon

Hadde lover og regler hatt en negativ effekt på respondenten ville vi nok ha sett dette på motivasjonen til å bidra med i sikkerhetsarbeidet. Som vi ser av Figur 9 ser dette ut til å stemme. Graderingen går fra 1 til 5, der fem som sagt er størst. Kun 3 stykker havner midt på treet og sier dermed at de er noe motivert. Men det hyggelige er at de resterende 33 av respondentene på dette spørsmålet sier at deres motivasjon er stor til delvis stor. Det er tydelig at selv om lover og regler har en effekt på holdningene og adferden, ser det ut til at det ikke har noe å si for motivasjonen til å arbeide med sikkerhet. Det ser ikke ut til at det er noe store gap mellom ord og handling, siden vi så at arbeidet med nye sikkerhetstiltak står i samsvar med motivasjonen.

Har ledelsen/sjefen påvirket dine holdninger til sikkerheten?

Ledere og ledelse kan ha stor innvirkning på holdningene til sikkerhetsarbeidet, vi valgte derfor å undersøke om dette også var tilfelle i energibransjen. Som det ble nevnt av NSM [33] og i [37] at ledere rollemodeller og påvirker derfor de ansatte. I vårt tilfelle er det mer eller mindre 50/50 som sier de har blitt påvirket i liten og stor grad. 44 % av respondenete velger å tro at de har blitt påvirket noe (3), mens det da er jevnt fordelt over og under av de resterende respondentene. Henholdsvis 26 og 30 %. Det er her tydelig at det NSM med fler sier, er riktig. De ansattes holdninger blir påvirket av ledere og ledelse. Når vi ba respondentene ta stilling til følgende påstand: “Toppledelsen ved virksomheten er engasjert i informasjonssikkerhet” fikk vi til svar at 38 % av respondenete

var uenige i dette, mens 36 % stilte seg i kategorien både og. Det kan jo her tenkes at hvis ledelsen var mer engasjert ville dette smitte over på de ansatte.

Vi antok at det kunne være en sammenheng mellom de respondentene som sa de hadde blitt pålagt opplæring også i større grad ble påvirket av leder eller ledelse med tanke på holdninger til sikkerhet. Vi rekodet svarene på spørsmålet om hvorfor de meldte seg på kurset til en tvang-indeks der de enten hadde blitt pålagt eller ikke. Ved hjelp av en T-test på disse variablene ble det fastslått at det ikke var en signifikant sammenheng. Og det var da ikke grunnlag for å konkludere med at det er noen forskjell på de som følte seg pålagt og ikke.

Med samme tvangs-indeks foretok vi også analyser for å sjekke om faktoren "pålagt" hadde noe si på forståelse og motivasjonen. Det var her naturlig å tro at kanskje særlig motivasjonen ikke var på topp etter å ha blitt pålagt å lære. Det viste seg at vi ikke kunne finne en signifikant sammenheng. En veldig liten forskjell, men i retning vår antagelse.

6.6 Virksomheten

For å kunne si noe om hvordan opplæringen, regelverket og tilsyn har virket inn på energibransjen tok vi med noen spørsmål som omhandlet virksomhet. Vi kartla organisatoriske tiltak og hendelser de siste 3 årene. Av organisatoriske tiltak har vi sett nærmere på IT-driften, opplæring og holdningsskapende aktiviteter, rapportering og analyser. Vi ville også at hver enkelt respondent skulle vurdere sikkerhetsnivået i virksomheten. Energibransjen bør ligge over gjennomsnittet på sikkerhetsnivået. Grunnen til dette er at en slik samfunnskritisk bransje bør ha noe bedre sikkerhet enn gjennomsnittet. Også sett i forhold til regelverket som skal følges.

Hvordan vil du vurdere sikkerhetsnivået i virksomheten?

Figur 10: Sikkerhetsnivået

Nesten 50 % sier at de vurderer sikkerhetsnivået som gjennomsnittelig. Overraskende nok fordeler de resterende seg til 40 % og 10 % på henholdsvis noe bedre og mye bedre. At det er så mange som halvparten som rangerer seg som bedre enn gjennomsnittet synes

vi er en positiv overraskelse. Vi hadde trodd at flere ville rangere seg som gjennomsnittet. Men her kan det være en sammenheng med type virksomhet de enkelte kommer fra. Som sagt er et nettselskap mer avhengig av IT enn produksjonsselskapene og dermed kan det hende de har ulike syn. Nettselskapene tror bedre om seg selv enn produksjonselskapene til en viss grad. Det var en liten forskjell vi fant når vi tok en T-test på de to, men ikke signifikant.

I tillegg til at de skulle rangere virksomhetens sikkerhetsnivå serverte vi også påstanden om at sikkerhetssystemet ved virksomheten oppfyller de myndighetskrav det er krav om. 14 av respondentene var enige og 15 var uenig, mens de resterende befant seg i både og kategorien. Det er noe bekymringsfult at så mange sier de ikke oppfyller kravene som er stilt til virksomheten. Kjenner de ikke til hva som forventes av dem i regelverket, er det for omfattende? Tidligere så vi at de ønsket et tydligere regelverk, dette kan være noe av årsaken, de er ikke sikre på om de har fullført alt av sikringsoppgaver som kreves. Andre mulige sammenhenger og faktor som spiller inn blir diskutert videre i oppgaven.

Hvordan er IT-driften organisert i virksomheten?

Når det gjelder organiseringen av IT-driften i virksomhetene skulle det vise seg at mange bruker en kombinasjon av outsourcing og som en del av egen virksomhet med egne ansatte. Kun et fåtall hadde satt helt og fult bort IT-driften, 3 virksomheter for å være eksakt. 19 av virksomhetene hadde driften selv og 17 benyttet seg av kombinasjonen. Ved videre undersøkelse viste det seg at mange av produksjonsselskapende velger å holde IT-driften i egen virksomhet i forhold til nettselskapene som velger å outsource deler eller alt, dette skyldes nok i hovedsak at de ikke er så avhengig eller ikke har et så avansert IT-system som nettselskapene. Som mer eller mindre forventet fant vi en signifikant forskjell på IT-driften i de to, produksjon og nett. $p = 0.043$. Nettselsakapene outsourcer mer enn produksjon.

Gis ansatte opplæring i sikker bruk av IT?
Er det gjennomført holdningsskapende aktiviteter?

På spørsmålene som omhandlet opplærings- og holdningsskapende aktiviteter ble det avdekket et ikke helt overraskende resultat, men vi hadde håpet et mindre antall. Vi var klar over at mange ikke tilbyr sine annsatte opplæring, men vi hadde håpet på en større prosentandel enn 52,5 % som ga sine annsatte opplæring. Nesten det samme resultatet gjaldt også holdningsskapende aktiviteter, 45 % hadde gjennomført dette. Siden disse resultatene var såpass like var det nærliggende å tro at det kunne være en sammenheng mellom disse variablene. Vi undersøkte krysstabellen med en kji-kvadrat-test mellom de to spørsmålene. Det vi da fant var en $p = 0{,}270$. Med andre ord ikke en tilfredsstillende signifikant sammenheng, men samtidig verdt å nevne at det er en viss sammenheng mellom de to.

For å følge opp spørsmålene fikk vi respondentene til å velge ulike typer opplæring og holdningsskapende aktivitet som har blitt gjort. Av opplæring som har blitt gjort har det stort sett vært introduksjonskurs/informasjon for nyansatte (ikke interaktivt) og noe oppfølgingskurs av faste ansatte. Av holdningsskapende aktiviteter har det vært størst tyngde på utsendelse av e-post og oppslag på intranett. Tett bak der igjen finner vi store og små fellesmøter/avdelingsmøter. Samtidig har det også vært skjermsparere og informasjon til lederer som blir anmodet om å ta med seg denne informasjonen videre inni organisasjonen.

Dobbelt så mange av de som gjennomfører opplæring rangerer seg som bedre enn gjennomsnittet. Men ser vi på de som ikke har opplæring, er det kun 6 som rangerer seg noe bedre. Som nevnt tidligere hadde vi også en kategori "mye bedre", der var det ingen som befant seg av de som ikke gjennomførte opplæring sammenlignet med 5 respondenter for de som gjennomførte. Vi foretok en t-test som resulterte i $p < 0{,}05$. Vi kunne da se at det er en signifikant forskjell på hvordan respondentene graderer sikkerhetsnivået i virksomheten med opplæring som en avhengig faktor om de graderer seg som gjennomsnittet eller bedre.

Vi kunne ikke se en lik sammenheng når det gjaldt holdningsskapende arbeid. Der var resultatene nokså likt fordelt på svaralternativene.

Rapporterer ansatte om uønskede avvik, forhold eller hendelser?

Ca 92 % svarer at de ansatte helt eller delvis rapporterer om avvik, forhold eller hendelser. Dette er høyt antall, noe som tyder på at bevistheten rundt viktigheten av å rapportere er tilstede. Dette er en viktig faktor i arbeidet med informasjonssikkerhet, det er tydlig at de ansatte muligens ser at rapportering er nødvending for å ta hånd om hendelser som skjer og hindre disse i å gjenta seg. På den måten skape en sikrere virksomhet.

Hvorfor utføres det risikoanalyser?

Det ligger som sagt forskjellige grunner til hvorfor vi bør gjøre risikoanalyser, vi har med dette spørsmålet prøvd å finne svar på hvorfor energibransjen gjør slike analyser, for sin egen del eller andres?

Når 65 % av respondentene svarer de gjør dette for å tilfredstille myndighetenes krav, kan vi lure på om de gjør dette bare fordi de må og ikke fordi de bør. 5 av respondentene som hadde valgt "å tilfredstille myndighetenes krav" hadde kun valgt dette, altså 19 %. De resterende hadde i tilegg sagt at risikoanalyser utføres for:

- Endringer i teknisk system (27,5 %)
- Endringer i organisasjon (15 %)
- Endringer i omgivelser (7,5 %)
- Sertifisering (10 %)
- Utløses av hendelser (22 %)
- En del av det planlagte løpende sikkerhetsarbeidet (32,5 %)

Det er tydlig at det ikke bare er for å tilfredstille myndighetene, men også til en viss grad for sin egen del.

Hvilke av følgende sikkerhetshendelser har virksomheten opplevd de siste 3 årene?

Her var vi avhengig av at respondentene svarte ærlig og stolte på at alle svar var anonyme og ble behandlet konfidesielt. Det kan nok være et ømt tema for mange sikkerhetsansvarlige å dele slik informasjon. Det kan tenkes at de ikke har oversikt over dette, men samtidig svarte de at de ansatte i virksomheten var flinke til å rapportere.

Den store "vinneren" av sikkerhetshendelsene ble menneskelige feilhandlinger med 47,5 %. De resterende pallplasseringene tok tyveri av IT-utstyr og missbruk av IT-ressurser

med henholdsvis 17,5 % og 15,0 %. Kun et fåtall av respondentene hadde opplevd datatyveri, målrettede aksjoner som har til hensikt å redusere tilgjengeligheten (DoS-angrep)og trusler om å angripe IT-systemer.

Ikke overraskende er det menneskelige feilhandlinger som topper listen. Vi gjør alle feil en gang i blandt, men det er muligheter for å gjøre noe med dette gjennom opplæring og holdningsskapende arbeid. Det falt oss derfor naturlig å sjekke om det var en sammenheng mellom de som hadde opplæring e holdningsskapende arbeid. Det var et flertall som ikke hadde opplæring som hadde hatt menneskelige feilhandlinger, men ingen signifikans forskjell. Det var likt fordelt mellom de som hadde noen form for holdningsskapende aktiviteter, altså ingen sammenheng.

For å komme litt dypere inn i problemet ble de her presentert påstanden "Ansatte er et større problem for sikkerheten enn de er ressurser til sikkerhetsarbeidet". Nær halvparten stilte seg uenige til denne påstanden, hvilket er et respektabelt antall siden mange også havnet i kategorien både og. Det var forøvrig ingen sammenheng mellom de virksomhetne som hadde opplæring for sine ansatte og de som så på ansatte som et sikkerhetsproblem.

6.7 Effektivitet og risiko

Fra to av spørsmålene lagde vi to forskjellige sammenlagt poengsummer. Den ene summen gikk på effektivitet av forskjellige tiltak og den andre summen var et resultat av hva slags risiko respondentene oppfattet virksomheten stod ovenfor, på mange måter en "paranoid"-sum. Vi fant ingen korrelasjon mellom gjennomsnittet på de to.

Effektivitetssummen adderte de forskjellige alternativene, ingen, liten, noe, god, til svært god effekt. Hver av disse fikk rangering fra 1 til 5, der 1 er ingen effekt osv. Tilsammen ga dette en maksimal poengsum på 50 poeng. Alternativene tilgjengelig var disse:

- Gjennomføring av risikoanalyser
- Opplæring av ansatte
- Holdningsskapende aktiviteter
- Aktivt involvere ansatte i sikkerhetsarbeidet
- Tilsyn fra offentlige myndigheter
- Ledelsens engasjement
- Redundans i kritiske systemer
- Innbruddsdetekteringssystem (IDS)
- Anti-virus programvare
- Brannmur for nettet

Det var særlige effekten av anti-virus og brannmur som tydlig har bemerket seg som to gode sikkerhetstiltak i energibransjen, de skilte seg spesielt ut med kun gode og svært gode effekter som svar. Eller så vi at ledelsens engansjemnet også ble sett på som et tiltak med god effekt, og kanskje derfor vi ser et ønske om mer engasjement fra ledelsen. Det var i det heletatt en gjennomsnittelig godtroende gruppe respondenter, gjennomsnittet

ble på 40 poeng.

På samme måte som med effektiviteten, ble det gjort det samme med "paranoid"-summen. La sammen rangeringene fra 1 til 5. Totalsummen ble på dette 75 poeng. Alternativene tilgjengelig var disse:

- Virusinfeksjoner
- IT-relaterte menneskelige feilhandlinger
- Datainnbrudd
- Spam-post
- Bruk av virksomhetens IT-utstyr og programvare til ulovlige formål
- Tap av taushetsbelagt informasjon
- Utro tjenere
- Sikkerhetshull i programvare
- Tyveri av IT-utstyr
- Uforsiktig bruk av internett
- Misbruk av taushetsbelagt informasjon
- Slurv av ansatte, eks. forlate PCen ulåst
- Bruk av virksomhetens IT-utstyr og programvare til private formål
- Uforsiktig bruk av e-post
- Ansatte som blir lurt av fremmede, f.eks oppgi passord over telefon

De største risikoene som respondentene i energibransjen synes var størst ble IT-relaterte feilhandlinger, tap av taushetsbelagt informasjon, missbruk av taushetsbelagt informasjon og slurv av ansatte. Som funnene om at det forekom mye menneskelige feilhandliler i bransjen, ser vi også her at de også er sett på som den største risikoen.

Produksjonselskapene fant vi var litt mer paranoid enn nettselskapene men ikke noen signifikant forskjell, grunnen til dette kan henge sammen med outscourcing der nettselskapene føler seg trygg på de som har ansvaret, men dette er ikke noe vi med sikkerhet kan si.

Vi kunne ved å kikke nærmere på gjennomsnittene på de to variablene se at gjennomsnittet på effektene ga 40 poeng av 50 mulig. Dette viser at respondentene har stor tro på tiltakene. Dette kan muligens settes i sammenheng med hvorfor de ikke er fult så paranoide. Der var gjennomsnittet 45 poeng av 75 mulige.

6.8 Sammenlignet med andre undersøkelser

6.8.1 Mørketallsundersøkelsen

Antall fra energisektoren med?

Sammenligner vi hendelsene i Mørketallsundersøkelsen kan vi se at det er en noe lavere prosentvis andel av tyveri av IT-utstyr. Dette var en hendelsestype som scoret høyt i Mørketallsundersøkelsen. Det kan her tyde på at sikringsnivået er noe høyere i energi-

bransjen. Men vi kan heller ikke utelukke at bærbart utstyr ikke fult er så populært, og dermed ikke lett å bli offer for tyveri. Også Misbruk av IT ressurser scoret høyt hos begge parter, men vi har ikke noe grunnlag for å si om dette er noe vesentlige forskjell i fra energisektoren. Menneskelige feilhandlinger er hos begge et stort problem.

Av tekniske beskyttelsestiltak i Mørketallsundersøkelsen kom det frem at det er en økning i bruk av slike tiltak. Spesielt bruken av brannmur, anti-virus og spam-filter er utbredt. Dette kan vi se igjen i troen på slike tiltak i energibransjen. Det er naturlig å tro at bruken av disse tiltakene kan settes i sammenheng med hva de enkelte tror har størst effekt som sikringstiltak. Dette ser vi igjen i vår undersøkelse der alle respondentene mener at brannmur og anti-virus gir en god til svært god effekt som sikringsmekanismer. Noe overraskende er det en skepsis til effekten av innbruddsdetekteringssystem (IDS), hvor nesten 40 % av respondentene mener dette gir en liten til ingen effekt. Av virksomhetene i Mørketallsundersøkelsen var det et stort flertall av de virkelig store virksomhetene med over 200 ansatte som brukte IDS og det var en klar sammenheng med størrelse. I vårt tilfelle er ikke dette riktig, det er en nokså jevn fordeling på størrelsen sammenlignet med hva de synes om effektiviteten av IDS.

Lite duplisering av kritiske komponenter som kan være en grei og god løsning for å forsikre mot avbrudd. Der scorer energisektoren bra, de er også pålagt av lov å ha redundans i kritiske systemer. Dette ser vi også på spørsmålet om hva slags effekt dette gir, alle utenom 2 respondenter mener dette er god til svært god effekt.

Ser vi nærmere på organisatoriske tiltak ser vi at risikoanalyser blir gjennomført av 83 % respondentene i Mørketallsundersøkelsen, dette er et tilfredstillinde høyt antall, vi kan anta at de ser viktigheten i analysene. I vår undersøkelse blir det bekreftet, at inntrykket av effektiviteten er høy.

40 % av virksomhetene i Mørketallsundersøkelsen gjennomfører opplæring av ansatte. Dette er en noe mindre andel sammenliknet med energisektoren der halvparten gjennomfører opplæring.

64 % har ikke hatt uønskede hendelser, 30 % vet ikke antallet. Bevisstheten hos de ansatte i energisektoren kan antas å være noe større, der rapporterer ca 90 % av de ansatte om uønskede hendelser, forhold eller avvik.

6.8.2 I forhold til andre land

Sammenligner vi med undersøkelsene gjort i kapitell 3.1 finner vi noen punkter som er til det bedre og andre som ikke fult er så bra. Undersøkelsen gjort av CSI/FBI[22] viste at det var de små virksomhetene som var dårligst nåår det gjaldt oppløringstilltak. Vi kunne ikke finne en slik sammenheng i vår undersøkelse.

DTI[23] på sin side kunne avsløre at i England fikk 5 av 6 opplæring, her ser vi at energisektoren igjen er under snittet på opplæringsbiten. For en fjerdedel av respondentene ble det også gjennomført ekstra opplæring etter at en hendelse var oppdaget.

BSI[24] avdekket i Tyskland at det blir brukt for lite midler på informasjonssikkerhet for å kunne opprettholde en kontinuitet. Ved påstanden om at virksomheten bruker mer ressurser på tekniske informasjonssikkerhetstiltak enn organisatoriske tiltak ble svarene tilnærmet normaltfordelt. Tidligere i dette kappitellet har vi sett att det finnes et ønske om mer tekniske forbedringer som bedre programvare og utstyr. Vi kan se en viss sammenheng med at det er et ønske og/eller behov for mer midler til forbedringer.

6.8.3 I forhold til andre virksomheter

Vi sammarbeidet med to doktorgradsstudenter på deler av spørreundersøkelsen. De så nærmere på organisatoriske tiltak og derfor er det kun det vi har sammenligne med. Vi har kun hatt tilgang på frekvenstabbelene. Totalt sett er det 64 % av virksomhetene i undersøkelsen som gjennomfører opplæring, dette er et antall som ligger noe overraskende høyere enn energibransjen. Hovedmengden er enige om at opplæring og holdningskapende arbeid gir en god effekt. Det samme gjaldt forøvrig om effekten av tilsyn, der i overkant av 70% syntes dette ga eller vil gi en god eller bedre effekt på informasjonssikkerheten.

Det var kun et fåtall som var sikre på om de ansatte rapporterte om hendelser i sin virksomhet. Her er energibransjen flinkere. energibransjens ansatte er flinke til å rapportere der de ser eller oppdager hendelser, avvik eller lignede. Noe vi skulle tro er et viktig verktøy for å kunne oppdage feil og mangler for så å gjøre utbedringer der det trengs.

32 % har ingen hendelser. Dette er riktig nok hendelser som ikke er oppdaget, men vi synes dette er høyt antall virksomheter som ikke har registert noen hendelser. 3 variabler som spiller inn på resultatet kan være uvisshet om hva en hendelse er og dermed ikke vet at de har hatt en hendelse, eller at de ikke har tatt i bruk hjelpemidler som oppdager disse hendelsene. Der er energibransjen god, i den grad det er bra å ha sikkerhetshendelser, men det som er bra er at disse blir registert og tatt hånd om. Som i energibransjen er det også ellers i de forskjellige virksomhetene menneskelige feilhandlinger som forekommer flest ganger når det gjelder sikkerhetshendelser, der svarer over halvparten at de har vært berørt av menneskelige feilhandlinger.

7 Oppsummering og konklusjon

Oppgavens intensjon er å se nærmere på om vi kan se en forbedring i informasjonssikkerheten ved hjelp av lover, regler, tilsyn og opplæring. Rapporten beskriver litteratur fra tidligere arbeidere innen forskning og fra bøker.

Oppgaven har gjennom spørreundersøkelsen skaffet resultater som sier noe om effekten av lover, regler, tilsyn og opplæring gjennom 40 respondenter fra virksomheter i energibransjen som kan anses som et representativt utvalg for å se nærmere på problemområdene. Rapporten beskriver virksomhetene og respondentene som deltok i spørreundersøkelsen og analyserer spørreundersøkelsens data. Vi har da kunnet bruke disse resultatene til å trekke slutninger, ikke bare nødvendigvis trenger å gjelde bare i energibransjen, men også i andre bransjer og enkeltbedrifter generelt.

For å komplettere data fra spørreundersøkelsene ble det også gjennomført intervjuer for å utdype dataene. Til en hvis grad ga intervjuene et dypere innblikk og tilleggsinformasjon til resultatene fra spørreundersøkelsen.

Spørreundersøkelsen ga grunnlag for å drøfte statistiske data og intervjuene komplimenterte noe utover dette. Forskningsspørsmålene kunne dermed besvares.

7.1 Oppsummering

> Opplæring, tilsyn, regelverk - gir det bedre informasjonssikkerhet?

Det er klart at opplæring er en nødvendighet for å tilegne seg ny kunnskap og følge med i utviklingen av informasjonssikkerhet. Ny kunnskap kan gjøre noe med innsikten i problemer vedrørende sikkerhet. Hvis man kan se hvor stort området informasjonssikkerhet er, og bli bevisste på dette ser man også behov for utbedringer for sin egen del og for virksomheten bedre. Vi har sett at det er en signifikant forskjell på virksomhetene som har opplæring for sine ansatte og de som ikke har dette, opplæring gir bedre informasjonssikkerhet.

Mye av svaret som gir bedre sikkerhet ligger i en god sikkerhetskultur og gjennom arbeidet med opplæring og kurs, for på den måten å synliggjøre problemområdet har energibransjen skapt gode holdninger og økt motivasjonen for å arbeide aktivt med informasjonssikkerhet. Det er enkelt for “alle” å innføre tekniske sikkerhetstiltak, men når det gjelder sikkerhetskultur er dette noe som må skapes gjennom bevisstgjøring hos de enkelte.

Tilsyn har en positiv effekt på informasjonssikkerheten i den grad at virksomhetene får påpekt feil og mangler, slik at disse kan utbedres. Dette skaper en slags “storebror”-effekt og kan for noen være nødvendig for at arbeide skal bli gjort tilfredsstillende og som en god motivator. I tillegg kan også tilsyn få en kontinuitets effekt på arbeidet. Det må hele tiden jobbes aktivt for å holde sikkerheten på et akseptert nivå. I tilknytning til tilsyn er det også et regelverk. Det er viktig at dette er lett forståelig, skal det gi ønsket effekt. Vi så at mange av respondentene ikke oppfylte alle krav i regelverket.

> Viser energibransjen en forbedring i forhold til resultatene i Mørketallsundersøkelsen[3] eller andre lignende undersøkelser?

- Har de færre sikkerhetshendelser?
- Er flere sikringstiltak gjennomført?
- Er sikkerheten bedre hos de store virksomhetene i forhold til de små?

Energibransjen viser både en forbedring og forverring i forhold til Mørketallsundersøkelsen [3] og andre undersøkelser. Resultatene tyder på at energibransjen har satt i gang bedre sikringstiltak når det gjelder å få ned tyveriraten blant virksomhetene. Videre fant vi større bevissthet rundt hendelser og rapportering av disse, med stort sett de samme sikringstiltakene. Motivasjonen for å arbeide med sikkerhet er god, ingen klare tegn som sier at den ikke er det. Størrelsen på virksomhetene hadde her ingen innvirkning på resultatene som mange av de andre, men her kan dette skyldes et litt for lite antall respondenter til å kunne se noen klare skiller.

> Bør sammenlignbare bransjer og enkeltbedrifter gjennomføre lignede tiltak?

Dette er helt klart et tiltak som enkelte organisasjoner og bransjer kan ha nytte av å innføre, men de må kikke nærmere på bruk av ressurser tilknyttet tilsyn før dette innføres og veie dette opp mot effektene. Dette vil nok best skape en effekt hos større bransjer og organisasjoner enn enkeltbedrifter.

7.2 Konklusjon

På bakgrunn av gjennomført studie kommer det frem at opplæring, tilsyn og regelverk gir bedre informasjonssikkerhet. Mange bransjer og bedrifter har tekniske tiltak på plass, men det er et behov for noe mer, for eksempel brukeropplæring og bevissthet innen temaet informasjonssikkerhet. Energibransjen viser at ved hjelp av opplæring vil bevisstheten øke og sikkerhetskulturen bedres i form av bedre holdninger og økt motivasjon.

Og med tilsyn og et godt regelverk vil dette skape kontinuitet og en vil for mange være en god motivator.

8 Videre arbeid

Denne oppgaven har tatt en nærmere kikk på hvilke effekter opplæring, tilsyn og et regelverk har å si for informasjonssikkerheten. Dette har vært en ambisiøs oppgave og nærmere undersøkelser vil det alltid være behov for. Vi har forsøkt og nå en gruppe som er representativ for vårt problem. Det kan allikevel være at andre lignende bransjer eller bedrifter vil skape andre resultater eller bekrefte funnene gjort i denne oppgaven.

Det kan være interessant å se nærmere på effektene av de nye veiledningene når de er på plass og i tilegg se nærmere på effektene av tiltakene som enkeltstående mekanismer.

Man bør også være klar over at det kanskje også eksisterer bedre metoder for datainnsamling, enn det datagrunnlaget en spørreundersøkelse gir. Vi fikk i vår undersøkelse et forholdsvis lite antall respondenter og derfor gjøre en mer omfattende undersøkelse som er mer detaljspesifikk kan være en mulig videre vei å gå.

Bibliografi

[1] Bakås, T. H. God praksis for måling av informasjonssikkerhetsnivå. Master's thesis, Gjøvik University College, 2005.

[2] *Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture*, 14th International Workshop on Database and Expert Systems Aplications (DEXA03). IEEE, 2003.

[3] Datakrimutvalget i Næringslivets sikkerhetsråd (NSR). 2006. Mørketallsundersøkelsen 2006.

[4] Norges vassdrags- og energidirektorat. 2004. Veiledning til forskrift om beredskap i kraftforsyningen.

[5] Olje- og energidepartementet. 2002. Beredskapsforskrift for kraftforsyningen.

[6] Forsvarets forskninginstitutt ved Fridheim Håvard, Hagen Janne, Henriksen Stein. 2001. Beskyttelse av samfunnet, del 3 (bas3).

[7] Jansen, A. 2004. Informasjonssikkerhet for alle - hvordan er det mulig? Foredrag på AFINs jubileumskonferanse 7.september.

[8] Sjølstad, T., Melgård, B., Høie, T. A., & Gulbrandsen, R. 2002. Håndbok i datasikkerhet.

[9] ISO. *NS-ISO/IEC 17799 Norsk standard*, 2001.

[10] Information Security Forum. *The Standard of Good Practice*, 2005.

[11] ISACA. *CobiT 4.0 - Control Objectives for Information and related Technology*, 2005.

[12] Statens-offentliga-utredningar. 2004. Informationssakerhet i sverige och internatonellt. Stockholm.

[13] Regjeringen. 2003. Nærings og handelsedepartementet/ forsvarsdepartementet/ justis og politidepartementet. *E-norge - Nasjonal strategi for informasjonssikkerhet*. Oslo.

[14] Justisdepartementet. 2000. Personopplysningsloven.

[15] Forsvarsdepartementet. 1998. Sikkerhetsloven.

[16] NorSIS. Veiledninger. http://www.norsis.no/veiledninger.

[17] Høgskolen i Gjøvik - imt1041. 2006. Hva er informasjonssikkerhet? http://www.hig.no/imt/index.php?id=687.

[18] IBM. 2005. Ibm survey shows security and regulatory compliance an increasing issue for small- and medium-sized businesses. http://www-935.ibm.com/services/us/index.wss/summary/imc/a1023291?cntxt=a1000405.

[19] Symantec. 2004. Symantec survey reveals 63 percent of new zealand small businesses have been impacted by a malicious attack. http://www.symantec.com/region/au_nz/press/2004/nz_040415.html.

[20] All covered Inc. 2006. Network security survey of small businesses. http://www.allcovered.com/pdf/AllCovered-Security-Survey.pdf.

[21] Security Solutions & Services by Jim Slaby. 2005. Efficiently securing your business through it security outsourcing: A call to action for smbs. http://admin.digitalriver.com/v2.0-img/operations/nai/media/yankeegrp_SMB-call-to-action.pdf.

[22] Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. 2006. Csi/fbi - computer crime and security survey.

[23] Pricewaterhouse Coopers og DTI. 2006. Information security breaches survey 2006.

[24] Federal Office for Information Security (BSI). 2005. The it-security situation in germany 2005.

[25] Ernst & Young. 2005. Global information security survey 2005 - reporting on the widening gap.

[26] Olje- og energidepartementet. 1990. Energiloven.

[27] Olje- og energidepartementet. 1990. Energilovforskriften.

[28] Gorling, S. 2006. The myth of user education. Virus bulletin conference october 2006.

[29] BSI. *The IT Baseline Protection Manual*, 2004.

[30] Siponen, M. 2006. Information security standards - focus on the existence of process not its content. In *Communications of the ACM*. ACM Press.

[31] McHugh, J. 2006. Quality of protection: measuring the unmeasurable? In *QoP '06: Proceedings of the 2nd ACM workshop on Quality of protection*. ACM Press.

[32] Saydjari, O. S. 2006. Is risk a good security metric? In *QoP '06: Proceedings of the 2nd ACM workshop on Quality of protection*. ACM Press.

[33] sikkerhetsmyndighet, N. 2006. Nsms risikovurdering 2006.

[34] Nordby, Y. & Hansen, C. W. 2005. Informasjonssikkerhet - atferd holdninger og kultur. ROSS (NTNU) - NSM.

[35] Kufås & Mølmann. 2003. Informasjonssikkerhet og innsiderproblematikk. ROSS (NTNU) - NSM.

[36] Sjekkit. http://www.sintef.no/content/page1____6776.aspx.

[37] Kaufmann, G. & Kaufmann, A. 1998. *Psykologi i organisasjon og ledelse 2.utg.* Fagbokforlaget.

[38] Stormark, K. M. Motivasjon og emosjon. Forelesing UiO - PS101 Psyk. grunnfag.

[39] Andersen, L. K. 2006. Motivasjon og læring hos voksne. Start-konferanse - Basiskompetanse i arbeidslivet.

[40] Albrechtsen, E. & olav Melteig. 2006. Om mus og menn. Brønnøysundregistrene og NTNU.

[41] Leedy, P. D. & Ormrod, J. E. 2005. *Practical research - Planning and design, 8th edition*. Pearson Education International.

[42] Booth, W. C., Colomb, G. G., & Williams, J. M. 2003. *The craft of research 2nd ed.* University of Chicago Press.

[43] Skar, T.-A. 2006. opplæring av informasjonssikkerhet - virker det? Forprosjektrapport.

[44] Active dialogue. http://www.active-dialogue.com/.

[45] Questback as. http://www.questback.no/.

[46] Haraldsen, G. 1999. *Spørreskjemametodikk: etter kokebokmetoden*. Ad Notam Gyldendal.

[47] Spss. http://www.spss.com/no/.

[48] George, D. & Mallery, P. 2006. *SPSS for Windows step by step: a simple guide and reference 6th ed.* Allyn and Bacon.

[49] Cristophersen, K.-A. 2006. *Databehandling og statistisk analyse med SPSS*. Unipub.

[50] Norsis - norsk senter for informasjonssikkerhet. http://www.norsis.no.

A Følgebrev

Denne spørreundersøkelsen er laget av Tom-Andre Skar. Jeg holder fortiden på med masteroppgave i informasjonssikkerhet ved Høgskolen i Gjøvik der jeg ser nærmere på opplæringstiltak, tilsyn og regelverk.

Kvaliteten på min masteroppgave er i stor grad avhenging av at du besvarer denne spørreundersøkelsen. Jeg vil derfor sette pris på om du kunne avse noen minutter til å besvare undersøkelsen.

Spørsmålene besvares ved å merke av i bokser.

Alle svar på spørreundersøkelsen vil bli behandlet konfidensielt og anonymisert. Dette gjelder både person og selskap.

På forhånd takk for at du deltar i spørreundersøkelsen.

Med vennlig hilsen
Tom-Andre Skar

B Vedlegg: Spørreskjema

Vedlagt ligger spørsmålene som ble stilt gjennom Questback. Dette er de spørsmålene som var aktuelle for vår oppgave. (Spørsmålene som doktorgradstudentene stilte er utelatt her.)

Har du hatt noen form for opplæring/kurs?

☐ Ja ☐ Nei

I hvilken regi ble opplæringen/kurset holdt?

☐ NVE ☐ Annet

Når hadde du sist opplæring/kurs innen temaet informasjonssikkerhet?

☐ 0-6mnd ☐ 6-12mnd ☐ mer enn 12mnd

Det kan være lett å glemme, når synes du en oppfriskning bør skje?

☐ 0-6mnd ☐ 6-12mnd ☐ mer enn 12mnd

Kjønn:

☐Kvinne ☐Mann

Alder:

18-29 ☐
30-39 ☐
40-49 ☐
50-59 ☐

Hvor mange ansatte er det i virksomheten?

1-24 ☐
25-199 ☐
200-499 ☐
500 eller flere ☐

Hva er din funksjon i virksomheten? [KUN ETT SVAR]

Daglig leder ☐
IT-ansvarlig ☐
Økonomiansvarlig ☐
Sikkerhetsansvarlig ☐
Annet, spesifiser:_____ ☐

Innenfor hvilken type virksomhet arbeider du?

☐ Produksjon ☐ Nettselskap

Hvor lang erfaring har du med informasjonssikkerhetsarbeid i virksomheter (totalt for både den virksomhet du jobber i nå og tidligere virksomheter)?

☐ 0-1år
☐ 1-5 år
☐ 6-10 år
☐ 11-25 år
☐ Over 25 år

Hvorfor meldte du deg på kurset? [FLERE SVAR MULIG]

☐ Pålagt av arbeidsgiver
☐ Ser nytten i å tilegne meg ny kunnskap
☐ For å dekke et behov for nye impulser
☐ For å få nye utfordringer
☐ Har en interesse for temaet
☐ Vet ikke
☐ Annet, spesifiser:_____

Har det blitt oppdaget flere sikkerhetshendelser som følge av kurset?

☐ Ja ☐ Nei ☐ Vet ikke

I hvilken grad vil du si at…

	1 Liten	**2**	**3**	**4**	**5 Stor**
Kurset oppfylte dine mål?	☐	☐	☐	☐	☐
Forståelsen for informasjonssikkerhet er bedret etter kurset?	☐	☐	☐	☐	☐
Det er nødvendig med mer kurs?	☐	☐	☐	☐	☐
Du har kommet i gang med flere sikkerhetsoppgaver?	☐	☐	☐	☐	☐
Det har blitt større bevissthet om sikkerhetshendelser etter kurset?	☐	☐	☐	☐	☐

I hvilken grad vil du si at…

	1 Liten	**2**	**3**	**4**	**5 Stor**
Forskrifter/lover/regler har noen effekt på din holdning og atferd?	☐	☐	☐	☐	☐
Du er motivert til å bidra med sikkerhetsarbeid?	☐	☐	☐	☐	☐
Ledelsen/sjefen har påvirket dine holdninger til informasjonssikkerheten?	☐	☐	☐	☐	☐

I hvor stor grad føler du det er viktig å jobbe med disse temaene for å forbedre informasjonssikkerheten?

	1 Liten	**2**	**3**	**4**	**5 Stor**
Mer kurs og opplæring	☐	☐	☐	☐	☐
Hyppigere kontroller og tilsyn	☐	☐	☐	☐	☐
Tydeligere og bedre regelverk	☐	☐	☐	☐	☐
Flere og bedre risikoanalyser	☐	☐	☐	☐	☐
Bedre programvare og utstyr	☐	☐	☐	☐	☐

Kjenner du til noen av disse standardene innen informasjonssikkerhet? [FLERE SVAR MULIG]

☐ ISO 17799/BS 7799 eller en nasjonal variant
☐ Information Security Forum (ISF) Standard of Good Practice
☐ Standard of Good Practice
☐ CobiT fra ISACA
☐ The IT baseline Protection Manual (BSI)
☐ Ingen

Er du eller bedriften medlem i organisasjoner eller fora som arbeider med informasjonssikkerhet? [FLERE SVAR MULIG]

Ikke medlem	☐
ISF	☐
KInS	☐
NSR	☐
ISACA	☐
Bluelight	☐
PKI-forum	☐
Andre, spesifiser_____	☐

Hvordan er IT-driften organisert i virksomheten?

☐ Som en del av egen virksomhet med egne ansatte
☐ I andres regi ("outsourcing")
☐ En kombinasjon
☐ Vet ikke

Hvordan vil du vurdere sikkerhetsnivået i virksomheten?

☐ Som gjennomsnittet
☐ Noe bedre
☐ Mye bedre

Gis ansatte opplæring i sikker bruk av IT?

☐ Ja
☐ Nei
☐ Vet ikke

Hvilken type opplæring gis? [FLERE SVAR MULIG]

Interaktiv opplæring av nyansatte	☐
Introduksjonskurs/informasjon for nyansatte (ikke interaktivt)	☐
Oppfølgingskurs til fast ansatte (ikke interaktivt)	☐
Interaktiv opplæring av fast ansatte	☐
Konkurranser, spill	☐
Praktiske øvelser	☐
Annet, spesifiser_____	☐

Er det gjennomført holdningskapende aktiviteter

☐ Ja
☐ Nei
☐ Vet ikke

Hvilke typer holdningsskapende aktiviteter er gjennomført?

Utsendelse av e-post	☐
Plakater i fellesområder	☐
Oppslag på intranett	☐
Formell informasjon på avdelingsmøter	☐
Store fellesmøter	☐

Utdeling av gaver (f.eks. penner, musematter)	☐
Små informasjonsmøter med aktiv deltakelse av ansatte	☐
Brosjyrer, nyhetsbrev o.l.	☐
Informasjon til ledere som de blir anmodet om å ta med videre inn i organisasjonen	☐
Klistremerker	☐
Konkurranser, spill	☐
Personlig tilstedeværelse av sikkerhetsansvarlig, f.eks. ved uformelle samtaler	☐
Skjermsparer	☐
Annet, spesifiser_____	☐

Rapporterer ansatte om uønskede avvik, forhold eller hendelser?
☐ Ja
☐ Ja, delvis
☐ Nei

Hvorfor utføres det risikoanalyser? Flere svar mulig
☐Tilfredsstille myndighetskrav1
☐Endringer i teknisk system2
☐Endringer i organisasjon3
☐Endringer i omgivelser4
☐Sertifisering5
☐Utløses av hendelser6
☐En del av det planlagte løpende sikkerhetsarbeidet7
☐Annet, spesifiser_____

På hvilken måte involveres brukere? FLERE SVAR MULIG
☐Deltakelse i risikoanalyser
☐Utvikling av det dokumenterte sikkerhetssystemet
☐Aktiv deltakelse i opplærings- og informasjonsmøter
☐Innspill i design, utvikling og/eller implementering av tekniske sikkerhetssystemer
☐Brukerpanel
☐Annet, spesifiser_____

Hvilke av følgende sikkerhetshendelser har virksomheten opplevd *de siste 3 årene*?

Datainnbrudd	☐
Datatyveri	☐
Uautorisert endring/sletting av data	☐
Misbruk av IT-ressurser	☐
Spredning av ulovlig/opphavsrettslig beskyttet materiale	☐
Målrettede aksjoner som har til hensikt å redusere tilgjengeligheten	☐

Trusler om å angripe IT-systemer	☐
Tyveri av IT-utstyr	☐
Menneskelige feilhandlinger	☐

Hvor enig eller uenig er du i disse påstandene?

	Svært enig	**Enig**	**Både og**	**Uenig**	**Svært uenig**
Toppledelsen ved virksomheten er engasjerte i informasjonssikkerhet	☐	☐	☐	☐	☐
Jeg opplever at HMS-arbeid har høyere prioritet i organisasjonen enn informasjonssikkerhet	☐	☐	☐	☐	☐
Informasjonssikkerhet er et frekvent tema på ledermøter	☐	☐	☐	☐	☐
Ansatte er et større problem for sikkerheten enn de er ressurser til sikkerhetsarbeidet	☐	☐	☐	☐	☐
Sikkerhetssystemet ved virksomheten oppfyller de myndighetskrav det er krav om	☐	☐	☐	☐	☐
I vår virksomhet brukes mer ressurser på tekniske informasjonssikkerhetstiltak enn organisatoriske tiltak	☐	☐	☐	☐	☐

Vurder effektiviteten av disse informasjonssikkerhetstiltakene og -aktivitetene.

	Ingen effekt	**Liten effekt**	**Noe effekt**	**God effekt**	**Svært god effekt**
Gjennomføring av risikoanalyser	☐	☐	☐	☐	☐
Opplæring av ansatte	☐	☐	☐	☐	☐
Holdningsskapende aktiviteter	☐	☐	☐	☐	☐
Aktivt involvere ansatte i sikkerhetsarbeid	☐	☐	☐	☐	☐
Tilsyn fra offentlige myndigheter	☐	☐	☐	☐	☐
Ledelsens engasjement	☐	☐	☐	☐	☐
Redundans i kritiske systemer	☐	☐	☐	☐	☐
Innbruddsdetekteringssystem (IDS)	☐	☐	☐	☐	☐
Anti-virus programvare	☐	☐	☐	☐	☐
Brannmur for nettet	☐	☐	☐	☐	☐

Hvilken risiko føler du disse hendelsene representerer for en virksomhets daglige funksjon?

	Ingen risiko	**Liten risiko**	**Middels risiko**	**Høy risiko**	**Svært høy risiko**
Virusinfeksjoner	☐	☐	☐	☐	☐
IT-relaterte menneskelige feilhandlinger	☐	☐	☐	☐	☐
Datainnbrudd	☐	☐	☐	☐	☐
Spam-post	☐	☐	☐	☐	☐
Bruk av virksomhetens IT-utstyr og programvare til ulovlige formål	☐	☐	☐	☐	☐
Tap av taushetsbelagt	☐	☐	☐	☐	☐

informasjon					
Utro tjenere	☐	☐	☐	☐	☐
Sikkerhetshull i programvare	☐	☐	☐	☐	☐
Tyveri av IT-utstyr	☐	☐	☐	☐	☐
Uforsiktig bruk av internett	☐	☐	☐	☐	☐
Misbruk av taushetsbelagt informasjon	☐	☐	☐	☐	☐
Slurv av ansatte, eks. forlate PCen ulåst	☐	☐	☐	☐	☐
Bruk av virksomhetens IT-utstyr og programvare til private formål	☐	☐	☐	☐	☐
Uforsiktig bruk av e-post	☐	☐	☐	☐	☐
Ansatte som blir lurt av fremmede, f.eks oppgi passord over telefon	☐	☐	☐	☐	☐

C Vedlegg: Intervjuguide

Du deltok i en spørreundersøkelse tidligere i år. I den forbindelse ønsker jeg å stille noen spørsmål i tilknytning til spørsmålene på undersøkelsen. Jeg holder for tiden på med en masteroppgave ved Høgskolen i Gjøvik der jeg ser på opplæringstiltak, tilsyn og regelverk.

Har du tid og anledning til noen ekstra spørsmål, knyttet til samme tema. Det vil ta ca 15 minutter. Hva du svarte på spørreundersøkelsen er ikke avgjørende. Er det muligheter for at dine anonymiserte utsagn eventuelt kan benyttes i min oppgave?

1. Hva slags tanker gjør du deg rundt følgende tema: Opplæring, tilsyn, regelverk?
2. Hva slags nytte verdi ser du i disse?
3. Finnes det noe bedre?

Det ble her snakket løst rundt temaene slik at også andre spørsmål dukket opp for å få klarhet i spørsmål og svar.

D Vedlegg: Frekvensanalyser

I dataanalysen utført med spss ble blant annet en frekvensanalyse utført. De neste sidene inneholder et utdrag av denne.

Når hadde du sist opplæring/kurs innen informasjonssikkerhet?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-6mnd	14	35,0	48,3	48,3
	6-12mnd	14	35,0	48,3	96,6
	mer enn 12mnd siden	1	2,5	3,4	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

Hvorfor meldte du deg på kurset?: Pålagt av arbeidsgiver

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	false	25	62,5	62,5	62,5
	true	15	37,5	37,5	100,0
	Total	40	100,0	100,0	

I hvilken regi ble opplæringen/kurset holdt?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	NVE	28	70,0	96,6	96,6
	Annet	1	2,5	3,4	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

I hvilken grad ble målene dine for kurset oppfylt?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	3	7,5	10,3	10,3
	3	7	17,5	24,1	34,5
	4	18	45,0	62,1	96,6
	5, stor	1	2,5	3,4	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

I hvilken grad…: Vil du si at forståelsen for informasjonssikkerhet er bedret etter kurset?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	5	12,5	17,2	17,2
	3	9	22,5	31,0	48,3
	4	14	35,0	48,3	96,6
	Stor 5	1	2,5	3,4	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

I hvilken grad…: Synes du det er nødvendig med mer opplæring?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	5,0	6,9	6,9
	3	10	25,0	34,5	41,4
	4	14	35,0	48,3	89,7
	Stor 5	3	7,5	10,3	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

I hvilken grad…: Har du kommet i gang med flere sikkerhetsoppgaver etter kurset?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	8	20,0	27,6	27,6
	3	5	12,5	17,2	44,8
	4	15	37,5	51,7	96,6
	Stor 5	1	2,5	3,4	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

Har det blitt oppdaget flere sikkerhetshendelser som følge av kurset?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja	2	5,0	6,9	6,9
	Nei	25	62,5	86,2	93,1
	Vet ikke	2	5,0	6,9	100,0
	Total	29	72,5	100,0	
Missing	System	11	27,5		
Total		40	100,0		

Hvilke sikkerhe: Mer kurs og opplæring

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Liten 1	1	2,5	2,7	2,7
	2	1	2,5	2,7	5,4
	3	14	35,0	37,8	43,2
	4	12	30,0	32,4	75,7
	Stor 5	9	22,5	24,3	100,0
	Total	37	92,5	100,0	
Missing	System	3	7,5		
Total		40	100,0		

Hvilke sikkerhe: Hyppigere kontroller og tilsyn

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Liten 1	1	2,5	2,7	2,7
	2	9	22,5	24,3	27,0
	3	11	27,5	29,7	56,8
	4	11	27,5	29,7	86,5
	Stor 5	5	12,5	13,5	100,0
	Total	37	92,5	100,0	
Missing	System	3	7,5		
Total		40	100,0		

Hvilke sikkerhe: Tydligere og bedre regelverk

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Liten 1	1	2,5	2,7	2,7
	2	3	7,5	8,1	10,8
	3	11	27,5	29,7	40,5
	4	15	37,5	40,5	81,1
	Stor 5	7	17,5	18,9	100,0
	Total	37	92,5	100,0	
Missing	System	3	7,5		
Total		40	100,0		

Hvilke sikkerhe: Bedre programvare og utstyr

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Liten 1	1	2,5	2,7	2,7
	2	6	15,0	16,2	18,9
	3	8	20,0	21,6	40,5
	4	18	45,0	48,6	89,2
	Stor 5	4	10,0	10,8	100,0
	Total	37	92,5	100,0	
Missing	System	3	7,5		
Total		40	100,0		

Hvilke sikkerhe: Flere og bedre risikoanalyser

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	5,0	5,4	5,4
	3	14	35,0	37,8	43,2
	4	15	37,5	40,5	83,8
	Stor 5	6	15,0	16,2	100,0
	Total	37	92,5	100,0	
Missing	System	3	7,5		
Total		40	100,0		

I hvor stor gra: Har forskrifter/lover/regler noen effekt på din holdning og atferd?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	1	2,5	2,8	2,8
	3	11	27,5	30,6	33,3
	4	19	47,5	52,8	86,1
	Stor 5	5	12,5	13,9	100,0
	Total	36	90,0	100,0	
Missing	System	4	10,0		
Total		40	100,0		

I hvor stor gra: Er du motivert til å bidra med sikkerhetsarbeid?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	3	7,5	8,3	8,3
	4	21	52,5	58,3	66,7
	Stor 5	12	30,0	33,3	100,0
	Total	36	90,0	100,0	
Missing	System	4	10,0		
Total		40	100,0		

I hvor stor gra: Har ledelsen/sjefen påvirket dine holdninger til sikkerheten?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Liten 1	5	12,5	13,9	13,9
	2	4	10,0	11,1	25,0
	3	16	40,0	44,4	69,4
	4	10	25,0	27,8	97,2
	Stor 5	1	2,5	2,8	100,0
	Total	36	90,0	100,0	
Missing	System	4	10,0		
Total		40	100,0		

Kjenner du til noen av disse standardene innen informasjonssikkerhet?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	false	25	62,5	62,5	62,5
	true	15	37,5	37,5	100,0
	Total	40	100,0	100,0	

Er du eller bedriften medlem i organisasjoner eller fora som arbeider med informasjonssikkerhet?: Ikke medlem

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	false	9	22,5	22,5	22,5
	true	31	77,5	77,5	100,0
	Total	40	100,0	100,0	

Hvordan vil du vurdere sikkerhetsnivået i virksomheten?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Som gjennomsnittet	18	45,0	46,2	46,2
	Noe bedre	16	40,0	41,0	87,2
	Mye bedre	5	12,5	12,8	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Hvordan er IT-driften organisert i virksomheten?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Som en del av egen virksomhet med egne ansatte	19	47,5	48,7	48,7
	I andres regi (`outsourcing`)	3	7,5	7,7	56,4
	En kombinasjon	17	42,5	43,6	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Gis ansatte opplæring i sikker bruk av IT?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja	21	52,5	53,8	53,8
	Nei	16	40,0	41,0	94,9
	Vet ikke	2	5,0	5,1	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Er det gjennomført holdningskapende aktiviteter?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja	18	45,0	46,2	46,2
	Nei	19	47,5	48,7	94,9
	Vet ikke	2	5,0	5,1	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Rapporterer ansatte om uønskede avvik, forhold eller hendelser?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ja	15	37,5	38,5	38,5
	Ja, delvis	21	52,5	53,8	92,3
	Nei	3	7,5	7,7	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Hva er din funksjon i virksomheten?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Daglig leder	1	2,5	2,5	2,5
	IT-ansvarlig	22	55,0	55,0	57,5
	Økonomiansvarlig	1	2,5	2,5	60,0
	Sikkerhetsansvarlig	5	12,5	12,5	72,5
	Annet:	11	27,5	27,5	100,0
	Total	40	100,0	100,0	

Hvor lang erfaring har du med informasjonssikkerhetsarbeid i virksomheter (totalt for både den virksomhet du jobber i nå og tidligere virksomheter)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-1år	3	7,5	7,7	7,7
	1-5 år	12	30,0	30,8	38,5
	6-10 år	14	35,0	35,9	74,4
	11-25 år	8	20,0	20,5	94,9
	Over 25 år	2	5,0	5,1	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Kjønn?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Mann	33	82,5	84,6	84,6
	Kvinne	6	15,0	15,4	100,0
	Total	39	97,5	100,0	
Missing	System	1	2,5		
Total		40	100,0		

Alder?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-29	1	2,5	2,6	2,6
	30-39	9	22,5	23,7	26,3
	40-49	16	40,0	42,1	68,4
	50-59	12	30,0	31,6	100,0
	Total	38	95,0	100,0	
Missing	System	2	5,0		
Total		40	100,0		

Selskap

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Produksjon	13	32,5	34,2	34,2
	Nettselskap	22	55,0	57,9	92,1
	Begge	3	7,5	7,9	100,0
	Total	38	95,0	100,0	
Missing	System	2	5,0		
Total		40	100,0		

Hvor mange ansatte er det i din virksomhet?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-24	7	17,5	17,5	17,5
	25-199	24	60,0	60,0	77,5
	200-499	4	10,0	10,0	87,5
	500 eller flere	5	12,5	12,5	100,0
	Total	40	100,0	100,0	