God praksis for måling av informasjonssikkerhetsnivå

Tone Hoddø Bakås

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Institutt for informatikk og medieteknikk
Høgskolen i Gjøvik, 2005

Masterprogrammet i informasjonssikkerhet
har blitt kjørt i samarbeid med
Kungliga Tekniska högskolan (KTH),
Stockholm, Sverige

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

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

Sammendrag

Rapporten søker å avdekke parametere som påvirker hva som er god praksis for måling av informasjonssikkerhetsnivå i virksomheter, som antas «å være ledende» innen informasjonssikkerhet. For å finne ut hvordan virksomheter i dag måler informasjonssikkerhet må det undersøkes hva som utføres i praksis i næringslivet. En spørreundersøkelse er gjennomført og supplert med enkelte intervjuer av sikkerhetsledere. Besvarelsene er fra 49 europeiske virksomheter, hvor IT antas å utgjøre en vesentlig del av, eller er tett integrert i forretningsprosessene. 23 av virksomhetene er fra Norge, 17 er fra andre nordiske land og 9 fra andre land i Europa. Disse representerer store virksomheter i nordisk sammenheng, med egne ansatte innen informasjonssikkerhet og med medlemskap i sikkerhetsorganisasjoner. Den gjennomførte studien i rapporten knyttes også til relevant litteratur og forskning innen temaene informasjonssikkerhet, samt måling generelt og av informasjonssikkerhet.

Et av rapportens bidrag er en beskrivelse av hva som kjennetegner virksomheter som måler informasjonssikkerhet. I alt 67 % av virksomhetene i spørreundersøkelsen måler eget nivå for informasjonssikkerhet. Statistiske analyser viser at finansielle og tjenesteytende bransjer måler informasjonssikkerhet mer enn andre bransjer. Virksomheter som har utkontraktert hele eller deler av sine IT funksjoner er også mer opptatt av å måle informasjonssikkerhetsnivå. Det samme er virksomheter som har ansatt egen sikkerhetsleder eller har flere enn fem ansatte i sentral sikkerhetsenhet. I tillegg ser det ut til at måling generelt, og spesielt bruk av balansert målstyring, inspirerer til måling av informasjonssikkerhetsnivå.

Rapporten gir også en oversikt over hvilke metoder som benyttes i praksis for måling av informasjonssikkerhetsnivå. Mange virksomheter fra spørreundersøkelsen benytter flere metoder, og 85 % benytter kvantitative målemetoder. Egenutviklede metoder benyttes av mange, og medlemmer av Information Security Forum benytter i stor grad metoder herfra. De som måler gjør det mot hele virksomheten og mot IT-avdelingen.

Virksomhetene vurderer at de viktigste formålene for måling er å kommunisere status til ledelsen, samt å vise til samsvar med standarder for informasjonssikkerhet. De som ikke måler begrunner dette med at ledelsen ikke etterspør det. Hele 67 % av virksomhetene som måler rapporterer status til toppledelsen. De viktigste vurderte effektene av måling, anses å være økt involvering av ledelsen og bedrede holdninger til informasjonssikkerhet. Bedre beskyttelse av informasjonen blir rangert sist som en effekt av måling. Måling av informasjonssikkerhet anses ut fra dette primært å være et ledelsesverktøy og bare sekundært gi økt informasjonssikkerhet.

Rapporten bidrar til slutt med å skissere et forslag til en prosess for måling av informasjonssikkerhet. Den er laget ut fra tilgjengelig relatert arbeid, resultater fra spørreundersøkelsen og intervjuene, samt egne erfaringer. Prosessen er ment å bidra i utviklingen av «god praksis» for måling av informasjonssikkerhetsnivå.

Abstract

This report seeks to disclose what is considered to be good practice, in measuring information security levels, within organizations which deem “to be in the lead” in information security. To find out how organizations measure their information security a research of what is actually practiced in business today is necessary. A survey is carried out over 49 European organizations, where IT is considered to play an important role, or is closely integrated in the business. The survey is supplemented with a few interviews of security managers. 23 of the organizations are from Norway, 17 from other Nordic countries and 9 are from other countries in Europe. These represent large organizations from a Nordic view. They have their own security staff and are members in security organizations. The careful study in the report is also tied to relevant literature and research within the subject of information security, measurements in general and for information security.

One of the reports contributions is to describe what characterizes organizations that measure information security. In all 67% of the companies in the survey measure their own level of information security. Statistical analysis shows that financial and service related branches more often measures information security than others. Organizations that have outsourced all, or part of, their IT functions do measure information security more often. And organizations that have security manager or have more than five employees in central security positions, measure security more often than others. In addition it appears that measurement in general and especially the use of balanced scorecard is an inspiration to the measuring of information security levels.

The report also gives a general view over which methods are used in practice for the measuring of information security levels. Many organizations from the survey use several methods and 85% use quantitative measurement methods. Self made methods are used by many and members of the Information Security Forum make use of methods from this organization. Organizations that measure information security intends to measure the whole company and the IT department.
The organizations consider that the most important purpose for measuring is to communicate status to management, and show compliance to information security standards. Those that do not measure excuse it by replying that management has not requested it. A total of 67% of organizations that measure, report the status to top-management. The most important considered effect of the measuring seems to be increased involvement by managers and improved attitudes to information security. Better protection of information comes last on the list as an effect of measuring. The measuring of information security appears to show that it is, primarily, a management tool and only subsequently accounts for an improvement of the information security.
Summarizing available research, results from this survey and interviews together with own experience the report concludes by outlining a proposal for the measurement of information security. The process is meant as a contribution to the development of “good practice” measuring information security level.

Forord

Denne masteroppgaven vil fullføre min mastergrad innen informasjonssikkerhet ved Høgskolen i Gjøvik. Mastergraden er gjennomført på deltid fra høsten 2002 til våren 2005, og masteroppgaven er utført i perioden 3.01 - 30.06.2005. På samme tid har jeg arbeidet som seniorrådgiver i informasjonssikkerhet hos sentralbankssjefens stab i Norges Bank.

Jeg har arbeidet med informasjonsteknologi i 20 år. De første årene med systemutvikling og prosjektledelse, og de siste seks årene spesifikt innen informasjonssikkerhet.

Måling av informasjonssikkerhet og utfordringen med å sette nivå for informasjonssikkerhet og måle i forhold til dette, er et tema jeg selv har erfaring fra og har sett utfordringer med. I tillegg har undervisning i faget «Security Metrics» ved Høgskolen i Gjøvik økt min nysgjerrighet for å se nærmere på teorier og praktiske bruk av måling av informasjonssikkerhetsnivå. Arbeidet med denne oppgaven har gitt meg ny informasjon om teorier for måling, og ikke minst ny kunnskap om hva «de beste i markedet» gjør. I tilegg har den gitt meg mulighet til å bringe ny kunnskap til området videre gjennom resultater fra en spørreundersøkelse og utvikling av en prosess for måling av informasjonssikkerhet.

Masteroppgaven finnes også i engelsk utgave. I tillegg er det utarbeidet et utkast til «paper» basert på oppgaven, se vedlegg E.

Takk til

Min veileder Frode Volden ved Høgskolen i Gjøvik har bidratt med uvurderlig støtte gjennom hele arbeidet med oppgaven. Han har vært tilgjengelig, vært til stor inspirasjon og hjelp i forbindelse med statistiske undersøkelser og bidratt med kritiske spørsmål og konstruktive kommentarer.

Takk til min arbeidsgiver, Norges Bank, som har støttet meg gjennom tre år med studier.

Takk til Jan-Erik og Tore for godt samarbeid og god støtte gjennom hele masterstudiet.

Takk til Jan-Olof Andersson, Sveriges Riksbank og Rune Ask som har bidratt med konstruktive og gode kommentarer, samt til Information Security Forum, for innledende diskusjoner og vurderinger av tema.

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.

Den største takken går likevel til min mann Halvar, som også nå har tatt sin del av driften av familien. Mine døtre Nina og Sigrid har også vist stor tålmodighet med mitt skolearbeid, men ser nok fram til at mamma ikke lenger har lekser. Takk til dere for støtte og tålmodighet.

Tusen takk!

Lillehammer, 25.6.2005

Tone Hoddø Bakås

Innholdsfortegnelse

Figurer

Tabeller

1 Innledning

1.1 Tema

Denne rapporten søker å beskrive god praksis for måling av informasjonssikkerhetsnivå i virksomheter. Gjennom å samle inn data fra virksomheter har vi funnet hva som kjennetegner virksomheter som måler informasjonssikkerhet, hvilke metoder de benytter og hvorfor de måler.

1.2 Nøkkelord

Sikkerhetsmetrikker, Informasjonssikkerhetsstatus, Måling av informasjonssikkerhet, benchmarking.

1.3 Keywords

Security Metrics, Information Security Status, Security Measurement, Benchmarking.

1.4 Problemstilling

Mange virksomheter har forretningskritiske IT-systemer med tilhørende informasjon og infrastruktur. Lover, forskrifter og standarder setter krav til informasjonssikkerhet, men det finnes ikke en «god skikk og bruk» for måling av informasjonssikkerhet. Å velge riktig sikkerhetsnivå med tilhørende riktige sikkerhetstiltak er ikke alltid gitt. Å etablere praktiske metoder for planlegging av etterlevelse av kravene, samt å kommunisere eget sikkerhetsnivå kan derfor være en utfordring.

Forskning og teorier beskriver behovet for, nytten av og metoder for måling av informasjonssikkerhetsnivå. Empiriske undersøkelser knyttet til måling av informasjonssikkerhetsnivå eksisterer imidlertid i mindre grad. Det er derfor uklart i hvilken grad måling av informasjonssikkerhet skjer i praksis. Dersom måling skjer i næringslivet, er det uklart hvilke metoder som eventuelt benyttes og hvorfor virksomheter måler eget nivå for informasjonssikkerhet.

For å finne ut hvordan virksomheter i dag måler informasjonssikkerhet må man undersøke hva som faktisk skjer i næringslivet i praksis. Undersøkelser må skje hos virksomheter som kan anses å være blant de beste i markedet på måling av informasjonssikkerhet. Disse virksomhetenes erfaringer vil sammen med relevant forskning bidra til utvikling av «god praksis» for måling av informasjonssikkerhetsnivå.

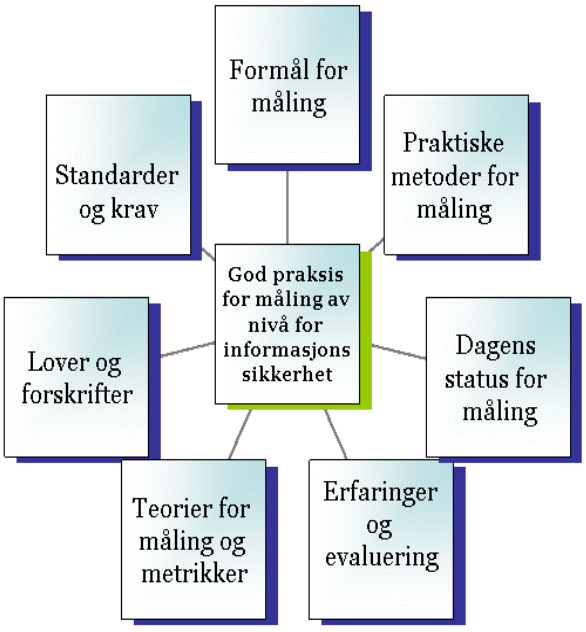
1.5 Motivasjon og begrunnelse

Rapporten vil ut fra datainnsamlinger i næringslivet analysere hva som kjennetegner virksomheter som måler eget informasjonssikkerhetsnivå. Undersøkelsene vil også omfatte hvilke metoder som benyttes i praksis og hva som anses å være formålet med og effektene av målingene. Resultatene kan avklare om det finnes en praktisk og omforent

metodikk rundt måling av informasjonssikkerhet. God praksis på området og innsikt i hva anerkjente virksomheter gjør kan inspirere andre virksomheter.
Rapporten vil bidra med å avdekke faktorer som anses å være og å påvirke god praksis for måling av informasjonssikkerhetsnivå. «God praksis» benyttes i mange fagområder, og med «god praksis» forstås i det følgende[1]:

> «Good practice is learning from other organizations that have developed successful projects or approaches to problems».

Figur 1 skisserer en forenklet modell for oppbygging av god praksis for måling av informasjonssikkerhet. Forskning innen informasjonssikkerhet beskriver teorier for måling av informasjonssikkerhet. Lover, forskrifter, internasjonale og lokale standarder setter krav til informasjonssikkerhet. Virksomhetens leder er ansvarlig for å sikre tilfredsstillelse av lover, forskrifter og sikkerhetsstandarder. Mange virksomheter har stort fokus på sikkerhet og har et ideal om å etterleve fastsatte sikkerhetskrav. Å kunne måle på en ensartet måte i hvilken grad virksomheten har tilfredsstillende sikkerhet kan da være et viktig styringsinstrument. Næringslivet har enkelte praktiske metoder for måling i dag. Det finnes litteratur og forskning til disse temaene. Det er imidlertid ikke gitt at teoriene sammenfaller med hva som anses som god praksis i det virkelige liv. Andre deler av modellen i Figur 1 er ikke dokumentert i dagens litteratur. Dette gjelder hva som kjennetegner virksomheter som måler, hva de selv mener er formålet med å måle, hva som måles og hvilke metoder som benyttes. Dette er ny kunnskap som denne rapporten vil søke å avdekke.



Figur 1 God praksis for måling av informasjonssikkerhetsnivå

Datainnsamling og vurderinger fra sikkerhetsledere i meget store virksomheter samt egne erfaringer fra mange år i arbeidslivet med IT og informasjonssikkerhet danner grunnlaget for arbeidet. Mål er en tilstand vi søker å nå, og måling gir anledning til å bedømme fremgang [2].

Styringssystemer med metoder og verktøy for planlegging, kontroll [3] og rapportering av nøkkeltall til ledelsen kan være viktig for mange. En situasjonsmåling for informasjonssikkerhet kan gi bedre oversikt og innsikt i egen status sett i forhold til de krav som stilles til informasjonssikkerhet. Måling kan kommunisere grader av tilfredsstillelse av sikkerhetskrav, men kan også gi andre effekter for virksomheten.

Forskning om måling av informasjonssikkerhet beskriver viktigheten av å måle. Frost [4] beskriver at innen sikkerhet bør en basere seg på å være på linje med beste praksis, og beskriver en prosess for å måle i et ledelsesperspektiv. NIST [5] mener måling av informasjonssikkerhet drives ut fra lovmessige, finansielle og organisatoriske årsaker. Wang [6] begrunner måling ut fra nødvendigheten av en bedre forståelse og ledelse av informasjonssikkerhet, og mener at muligheten til å sammenligne er verdifull. Mens Payne [7] sier at sikkerhetsledere vil bli holdt ansvarlige for å bevise at sikkerhetstiltakene er effektive, og at nøkkelen til dette er sikkerhetsmetrikker.

1.6 Forskningsspørsmål og hypoteser

Basert på det foregående vil rapportens forskningsspørsmål beskrives på to nivåer.

1. Hva kjennetegner virksomheter som måler informasjonssikkerhet?
2. Hva er god praksis for måling av informasjonssikkerhetsnivå?

Forskningsspørsmål 2 kan igjen deles i følgende spørsmål:

- Hvilke metoder benytter virksomheter i dag for å måle informasjonssikkerhet?
- Hva anser virksomheter å være formålet med å måle informasjonssikkerhet?
- Hvilke effekter mener virksomheter det gir å måle informasjonssikkerhet?

Litteratur og teorier stiller i noe grad krav og spesifikasjoner til metrikker for informasjonssikkerhet, men gir få svar på hvordan måling av informasjonssikkerhet skjer i praksis. Næringslivet har fokus på inntjening, effektivitet og praktiske løsninger. Det kan derfor være et annet syn på måling av informasjonssikkerhet i det praktiske liv enn i teoriene. Måling av informasjonssikkerhet synes også å være et komplekst fagområde. Det antas derfor at praktisk måling av informasjonssikkerhet gjennomføres blant et fåtall virksomheter, selv blant virksomheter som er opptatt av informasjonssikkerhet. Blant disse antas det å være virksomheter fra finanssektoren, virksomheter som er aktive i sikkerhetsorganisasjoner og de som utkontrakterer sine IT-funksjoner som måler mer enn andre.

På forhånd er det knyttet stor usikkerhet til hvilke metoder som eventuelt benyttes for å styre informasjonssikkerhet i virksomheter slik at det støtter opp om virksomhetens måloppnåelse. Teorier fokuserer på at måling av informasjonssikkerhet skal være

kvantitativ [5,7]. Forventningen er at praktiske løsninger, i den grad de finnes, i større grad vil være basert på kvalitative eller blandede metoder. Det antas også at det finnes samarbeidsprosjekter knyttet til metoder og verktøy i for eksempel ulike bransjer eller sikkerhetsorganisasjoner som virksomheter benytter. En annen hypotese er at måling av informasjonssikkerhet er et instrument for de sikkerhetsansvarlige.

Det antas at det er viktig for virksomheter å kunne vise til samsvar med lover og forskrifter samt å kunne informere interessenter om status på eget informasjonssikkerhetsnivå. Frost [4] beskriver at ved å fokusere på gitte mål og stille ledere til ansvar for å nå målene antas det forbedringer på målefaktorene. Det antas derfor at måling av informasjonssikkerhet kan ha positiv effekt på virksomhetens sikkerhet.

2 Relatert arbeid

Forskning og teorier definerer og begrunner måling av informasjonssikkerhet, og i det følgende redegjøres det for noe relatert arbeid knyttet til måling av informasjonssikkerhet.

2.1 Informasjonssikkerhet

Informasjonssikkerhet har etter hvert fått en anerkjent og noenlunde entydig definisjon; å sikre konfidensialitet, integritet og tilgjengelighet slik vi ser det i litteraturen [8] og i standarder [9-11]. På nasjonalt plan legges strategier, formål og overordnede mål for informasjonssikkerhet [12,13].

Juridiske aspekter med lover og forskrifter [13-16] setter i noen grad krav til informasjonssikkerhet, også i form av krav til oppfølging og dokumentasjon til at reglene blir fulgt. IT sikkerhetsforum i Norge har dokumentert lover og regler som har krav til informasjonssikkerhet i Norge [16]. Informasjonsteknologi opererer i stor grad på tvers av landegrensene. Ut fra dette er det et stadig tettere internasjonalt og spesielt europeisk samarbeid knyttet til lovgivingen, særlig innenfor behandling av personopplysninger [17,18], men også innen området «cybercrime» [17,18]. Strenge krav er også satt til virksomheter som er registrert på amerikansk børs, Sarbanes-Oxley [19].

Virksomheter har ofte en egen sikkerhetspolicy som setter krav til hvilke sikkerhetstiltak virksomheten skal implementere. Anerkjente internasjonale standarder for informasjonssikkerhet benyttes gjerne som et utgangspunkt, som f eks ISO/IEC 17799 [9], Information Security Forums Standard of Good Practice [20] og CobiT fra ISACA [11].

Aktuell litteratur gir en god oversikt over hva informasjonssikkerhet er, og tilhørende rammeverk. Dette legges til grunn som en av rammebetingelsene for måling av informasjonssikkerhet.

2.2 Teorier for måling av informasjonssikkerhet

En viktig basis for å avdekke dagens praksis for måling av informasjonssikkerhet er relevante teorier og forskning knyttet til temaet. Det finnes få bøker på området, og en gjennomgang av artikler og rapporter tyder på at fagfeltet er relativt nytt.

Etter en studie av relevant litteratur og forskning knyttet til måling av informasjonssikkerhet kan en sitte med inntrykk av at

- Ulike begreper benyttes for å omtale måling av informasjonssikkerhet. Eksempelvis metrikker[5], sertifisering[9], benchmarking[21], status [22].
- Litteraturen fokuserer på definisjoner, egenskaper og prosesser [4-7,23]
- Fagfeltet er nytt og umodent i forhold til f eks software metrikker [24]

- Det fokuseres på kvantitative målinger [5,7,25]

Dette underbygges av teorier og forskning beskrevet i det følgende.

2.2.1 Definisjoner

Teoriene for måling av informasjonssikkerhet har et til dels tvetydig begrepsapparat. Begreper som for eksempel metrikker, sertifisering, benchmarking, sjekklister, status, kvalitet, indikatorer og målstyring benyttes. Med måling (measuring) forstås [26]:

> «Dimensions, quantity, or capacity as ascertained by comparison with a standard.
> A reference standard or sample used for the quantitative comparison of properties.
> A unit specified by a scale or by variable conditions.
> A system of measurement, such as the metric system. »

Metrikker er hentet fra det latinske «metricus», som er relatert til «measurement» og blir definert som en standard for måling [26]. Payne [7] mener det er vesentlig å skille mellom målinger og metrikker, mens NIST [5] benytter måling og metrikker om hverandre, og beskriver metrikker som:

> «Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. IT security metrics must be based on IT security performance goals and objectives. »

Måling er opptatt av kvantitative forhold, og kan være i form av omfang som tid, lengde, frekvenser, antall eller andre og mer abstrakte indikatorer. Innen informasjonssikkerhet finnes det imidlertid få naturlige kvantitative forhold.

Måling kan skje på strategisk, taktisk og operativt nivå. Virksomheter bør da ha et bevisst forhold til om alle nivåer av virksomheten skal måles og eventuelt hvilke som skal prioriteres. Ulike formål og begrunnelser for å måle informasjonssikkerhet krever gjerne måling på ulike nivåer og med ulike metoder. En arbeidsgruppe gjennom ACSA[1] med 34 erfarne deltakere på området og med utgangspunkt i 30 innleverte «paper» [27] karakteriserte en metrikk med produktet av hva du trenger å måle, formål med måling og til hvem du måler for. De definerte en informasjonssikkerhetsmetrikk som:

> «An information security metric is a value, selected from a partially ordered set by some assessment process that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence. »

Geisler [23] definerer en metrikk som et system av måling som inkluderer elementet som måles, enheten det måles i, og verdi på enheten. Metrikker kan være i form av ett

[1] Applied Computer Security Associates

enkelt mål, en indeks, et forholdstall eller et integrert måltall som kombinerer flere metrikker.

2.2.2 Egenskaper og prosesser ved måling

Payne [7] fokuserer på egenskaper ved gode metrikker, og skisserer et program for sikkerhetsmetrikker for å forbedre den overordnede sikkerheten, og derigjennom bidra til at å utvikle organisasjonen som en helhet. Payne mener gode metrikker skal være «SMART», dvs. Spesifikke, målbare, akseptable, repeterbare og tidsuavhengige, noe som også støttes av Lowans [24]. Ladegård [28] stiller noen av de samme krav ved generelle mål, men mener i tillegg at mål må fokusere bare på det vi selv kan endre, samt være kompatibel med belønninger.

Geisler [23] mener at måleinstrumenter kan karakteriseres med ulike attributter ut fra hvor gode de er, og beskriver trinn i konstruksjon av metrikker. Dette er å avgjøre hva vi ønsker å måle, formål med måling, tilgjenglige målinger, samt at gyldighet og pålitelighet må vurderes. Kunder og interessenter vil bidra til å påvirke valg av metrikker med egne kriterier for evaluering. Det vil derfor være ulike årsaker til hva de enkelte velger å evaluere. På samme måte beskriver Ladegård [28] en mer generell prosess for målsetting. Hun legger bl.a. vekt på å involvere ulike parter og hvilke aspekter som er relevant, samt ser på årsakssammenhenger.

Solms ser på måling av informasjonssikkerhet som en av mange dimensjoner [29]; strategisk, organisatorisk, policy, beste praksis, etisk, juridisk osv. og likestiller disse med den tekniske dimensjon, som ofte får mye fokus.

Wang og Wulf fremhever viktigheten av en klar definisjon av hva som skal måles [6]. Kunnskap om hva som skal måles og valg av sikkerhetsindikatorer er starten på en måleprosess. Deretter må en avdekke hvordan måling skal skje. Målinger må ofte tolkes og de kan sammenlignes med tidligere målinger for å avdekke endringer.

Frost beskriver bruk og definisjon av metrikker på et sikkerhetsledelsesnivå [4]. Han mener sikkerhetsmetrikker, rammeverk og modeller for sikkerhetsmåling er i en tidlig fase av utviklingen og det er ikke etablert «best practice» for området. Utvalget av sikkerhetsmetrikker må holdes på et minimum, og samtidig under kontinuerlig evaluering. Frost beskriver eksterne og interne metrikker. Han definerer en metode, hvor første trinn er å finne hovedemner som man ønsker å undersøke. For hvert hovedemne defineres kritiske suksessfaktorer med tilhørende ytelsesindikatorer. Metrikkene kan sammenlignes med indikatorer i balansert målstyring [30].

Benchmarking er en på forhånd definert posisjon, brukt som en referanse å måle opp mot. Andersen og Pettersen beskriver benchmarking som en metodikk for forbedring, gjennom å sammenlikne med virksomheter, anerkjent som best på et område [21]. Sammenlikning er knyttet til prosesser, det skjer på en strukturert måte og har fokus på læring. Sammenlikningen kan skje internt, mot konkurrenter, med funksjoner eller generisk. Praktiske metoder for benchmarking av informasjonssikkerhet finnes [22,31,32].

SANS Institute beskriver sikkerhetsmetrikker for nettverk [24] og sammenligner disse med software metrikker, som er et mer modent fagfelt. Metrikker er den eneste måten å måle nettverkets kvalitet og sikkerhet på, for å kunne rapportere status til ledelsen. Viktige attributter ved og mål for metrikker beskrives. Vanlige fallgruver fra måling av programvareutvikling er oppsummert for å unngå at sikkerhetsmetrikker gjør tilsvarende. SANS mener metrikkprogrammer er verdt innsatsen og investeringene, ut fra tapene som kan oppstå uten måling.

Wood og Bouchard mener at et mål på sikkerhetsnivå er å vurdere ressursinnsatsen en angriper må benytte for å forberede og gjennomføre et angrep [33]. Tid og kostnader fienden må benytte bestemmer robusthet og sikkerhetsnivå. En nasjonal trusselvurdering av Kredittilsynet i Norge kan tyde på at svært mange sikkerhetshendelser er knyttet til svikt i interne rutiner [34], noe som ikke måles i tester knyttet til fiendtlig aktivitet.

Motstandere av måling finnes også. McHugh hevder at det vitenskapelige grunnlaget ved å bruke kvantitative verdier for å klassifisere informasjonssikkerhet mangler [35]. Det kan ikke bevises at kvantitative måltall dokumenterer sikkerhetstilstand. Programvare er umoden og mennesker er kompliserte, og det er derfor vanskelig å fastslå måleenheter. McCallam [36] mener at numeriske mål ikke kan benyttes da informasjonssikkerhet er en integrert del av prosess, teknologi og menneskelige faktorer.

2.2.3 Metoder og verktøy

International Organization for Standardization (ISO) [37] har så langt ingen spesifikke standarder for måling av informasjonssikkerhet eller sikkerhetsmetrikker. I samtale med norsk representant i ISO bekreftes det at det arbeides med metrikker og målinger av «Information security management».

National Institute of Standards and Technology (NIST) har utarbeidet retningslinjer for å bistå ledelsen i å beslutte hvor sikkerhetstiltak skal iverksettes ved bruk av sikkerhetsmetrikker og kvantifiserbar informasjon [5]. Et modenhetsprogram for å bestemme typer av metrikker, ulike målemetoder, mal for og forslag til metrikker er utviklet. De beskriver at metrikker er verktøy som samler inn, analyserer og rapporterer relevante ytelsesdata med formål å overvåke status på ulike aktiviteter.

KITH[2] har omsatt sikkerhetsmetrikker fra NIST [5] til praktisk bruk gjennom indikatorer for informasjonssikkerhet [32] for helsevesenet i Norge. Dette for å kommunisere status til ledelse og myndigheter, følge utviklingen på sikkerhetsområdet og iverksette nødvendige tiltak innen helseforetak. Formålet er å bedre informasjonssikkerheten ved å synliggjøre tilstand, sette det på dagsorden, å gi tilbakemeldinger og å kunne sammenligne ulike helseforetak.

[2] Kompetansesenter for informasjonsteknologi for helse og velferd

Bakås, Hagen og Orderløkken [38] har benyttet retningslinjene fra NIST for å utvikle sikkerhetsmetrikker for utkontraktering av driftstjenester. Metrikkene er inkludert i avtale mellom kunde til og leverandør av utkontrakteringstjenester. Deisz, Ingebrigtsen og Nilsen [39] evaluerer gjennom et praktisk case hvordan en kan måle informasjonssikkerhet i et utkontraktert miljø. Metrikkene benyttes i en virksomhet i Norge og har utviklet seg over flere år. De presenteres i regneark, basert på ulike egenvurderingsmetoder og består av mange ulike målinger.

ISF har forslag til metrikker [40] i et foreløpig regneark [25] med et utvalg på mer enn 700 metrikker basert på andre metoder og verktøy fra ISF. ISF beskriver også betenkninger som bør vurderes knyttet til måling av sikkerhet. De nevner at det kan være svært ressurskrevende, inkludere mye manuelt arbeid, samt at verdi og nøyaktighet til metrikkene kan variere. Det bør derfor vurderes om nytten ved måling er større enn kostnaden.

Med utgangspunkt i trusselbeskrivelse av «cybercrime» mot den finansielle sektor og egne krav for e-securtity for å få sikkerhet i dybden har World Bank [31] utarbeidet en sjekkliste. Sjekklisten er laget med tanke på å gi sikkerhetsledere, IT-ledere, systemadministratorer og andre ledere en måte å måle og verifisere sikkerhetsnivå i egen organisasjon. Målet er å redusere konsekvensene av økonomiske tap ved «cybercrime». Metoden er bygd opp med prosesser som kan overvåkes, og det er et mål å lage en benchmark for å måle nødvendig nivå for «e-security».

Prosjektet «Security Reporting» [41] ønsker å undersøke hvordan sikkerhetsindikatorer til ledelsen kan bidra til å redusere sårbarheter i kritisk infrastruktur. BAS5-prosjektet[3] «Critical Information Infrastructure Protection», startet i april 2004 og gjennomføres gjennom bl.a. Forsvarets Forskningsinstitutt [42]. Prosjektet vil anbefale tiltak for å redusere sårbarheter, basert på en rangering ut fra kostnadseffektivitet og ulike andre metoder.

Nygård [43] beskriver mulige sikkerhetsmetrikker for driftskontrollsystem. Fokus settes på risikostyring for å avdekke hvilke utfordringer man står overfor. Risikostyring skal bidra til at ledelsen kan styre og avgjøre tiltak for å håndtere trusler mot informasjonssikkerhet, og for å gjennomføre sikringstiltak for å beskytte mot disse truslene [9]. Utarbeidelse av konkrete sikkerhetsmål og akseptkriterier for risiko skal gi føringer.

2.3 Metoder fra sikkerhetsorganisasjoner og næringslivet

Dokumentasjon og analyser basert på metoder som finnes i næringslivet kan gi verdifull informasjon om hva som er gjennomførbart og virkningsfullt. Et utvalg av disse er i det følgende beskrevet.

Uavhengige gjennomganger og sikkerhetsrevisjoner [27] er anerkjente og praktiske metoder. Det er usikkert i hvilken grad resultatene er gode metrikker, da de ikke alltid

[3] Beskyttelse av samfunnet

er komplette og ikke lett å gjenta. Uavhengige gjennomganger kan i noen grad sammenlignes med teorier knyttet til Adversary Work Factor [33].

Risikoanalyser som f eks NS 5814 [44] vurderer trusler og sårbarheter, som kan baseres på detaljert modellering, tallfesting av ulike verdier, kvantitative analyser og kost/nytte vurdering av sikkerhetstiltak opp mot akseptabel risiko. Risikoanalyser rapporteres ofte til ledelsen. Broder mener risikoanalyser ved å kvantifisere muligheter og kostnader er et fordelaktig ledelsesverktøy [45].

Mange virksomheter bruker ISO/IEC 17799 [9] som sin standard for informasjonssikkerhet, og enkelte velger å sertifisere seg mot BS 7799, del 2. Stamland [46] beskriver i «Is BS7799 worth the effort» at virksomheter som er sertifisert etter BS 7799-2 har en høyere grad av modenhet enn virksomheter som benytter metoden på en mer uformell måte. Virksomheter som bruker standarden uformelt har høyere grad av modenhet enn virksomheter som ikke har implementert et «Information Security Management System». Hans konklusjon er at sertifisering i henhold til BS 7799 er verdt innsatsen.

ISF har etablert standarden «Standard of Good Practice» (SoGP) [20] med tilhørende elektronisk egenevalueringsskjema og benchmarkingsverktøy Status Survey [22]. Undersøkelsen har spørsmål hentet fra SoGP og ISO/IEC 17799 [9]. Sammenligning mellom virksomheter og utregning av benchmarkverdier skjer hvert annet år [47]. En forenklet versjon av Status Survey, Healthcheck, er under utvikling. ISF har også metoder for å håndtere risikoanalyser, med Fundamental Information Risk Management (FIRM) [48], SARA [49] og SPRINT [50]. Metodene fra ISF er kun for medlemmene, mens standarden er fritt tilgjengelig.

SBA Check, som står for «SårBarhetsAnalys» [51] er en sjekklistebasert programvare, med formål å støtte evaluering av informasjonssikkerhet i virksomheter. SBA Check leveres med ulike sett med sjekklister, bla for ISO/IEC 17799 [9] og svenske krav i lov om personopplysninger [52]. Målet er gjennom en nåsituasjonsanalyse å legge planer for forbedringer og nye informasjonssikkerhetstiltak. Programvaren genererer automatiske rapporter til ulike interessenter. Programmet ble utgitt første gang i 1994. Björk [53] beskriver erfaringer og metodiske bruk av verktøyet, gjennom et kurs og bruk av en pilotgruppe.

COBIT [11] er en akseptert internasjonal standard for IT sikkerhet fra revisjonsorganisasjonen ISACA[4], og gir et rammeverk for ledelse, brukere, revisjon og sikkerhetspersonell. COBIT gir ledelsen mulighet til å måle IT gjennom verktøy for å måle de 34 IT-prosessene i COBIT. Verktøyene inneholder en liste over målbare elementer, kritiske suksessfaktorer for hver IT-prosess og en modenhetsmodell som kan bidra i benchmarking og i å beslutte forbedringer.

[4] Information Systems Audit and Control Association

2.4 Generelle målemetoder

Etzioni [2] beskriver funksjoner for å male og sette mål for virksomheter. Et mål gir en orientering ved å beskrive en fremtidig tilstand og gir anledning til å bedømme fremgang i forhold til dyktighet og effektivitet. Slike fremtidige tilstander har en betydelig sosiologisk kraft som påvirker handlinger og reaksjoner. Effektiviteten til en organisasjon blir bestemt av i hvilken utstrekning den virkeliggjør sine mål. Lawler m fl [54] beskriver måleteknikker og prosesser som er nødvendig for å kunne forbedre organisasjoner. Til grunn for måling er det viktig med innsamling av gyldige data om dagens status, effektivitet og påvirkning.

ITIL (IT Infrastructure Library) [55] er en akseptert internasjonal standard for IT drift. ITIL har også en egen sikkerhetsmodul, samt akkrediterte opplæringsorganisasjoner av verktøy for implementering og vurdering. ITIL både støtter og er støttet av BS15000, IT Service Management Standard [56]. Det er også etablert et verktøy for egenvurdering, som kan benyttes for å måle eget nivå i forhold til standarden.

Ledelsen i virksomheter følger gjerne opp mange typer nøkkelinformasjon for IT gjennom f eks tjenesteleveranseavtaler eksternt og internt, i form av Service Level Agreements «SLA» [57]. Tjenesteleveranseavtaler bygger gjerne på krav fra ITIL, informasjonssikkerhetsstandarder samt andre krav virksomheten har til f eks kvalitet, systemutvikling, funksjonalitet, prosjektledelse osv. Avtaler som ikke overholdes er kostbare, og kan være motivasjon for å i større grad benytte kvantitative verdier for å måle informasjonssikkerhet.

Balansert målstyring (BMS) eller balanced scorecard, benyttes i styring mot forutbestemte mål [3,28,30,58]. BMS fokuserer på at ønsket situasjon skal bestemme virksomhetens fremtidige utvikling og resultere i strategier i form av visjoner, ambisjoner og ressurser og et sett av formål, mål og essensielle planer for å nå disse målene. Styringsinformasjon om virksomheten skal holde kursen mot målene. Styringsparametere eller Key Performance Indicators (KPI) er ikke alltid kvantitative, og skal primært dekke områdene økonomi, brukere og interessenter, interne prosesser og rutiner samt læring og fornyelse. BMS fokuserer på iverksettelse, løpende styring av strategiene og søker å etablere den lærende organisasjonen, som kontinuerlig forbedrer sin evne til å skape sin egen fremtid.

Helse, miljø og sikkerhet (HMS) og internkontroll [59] av dette er en annen side av sikkerhetsbegrepet og kan tenkes å være relatert til måling av informasjonssikkerhet. Sikkerhet omfatter her safety-delen. HMS er et ufravikelig krav, også fordi HMS gjerne påvirker andre forhold på arbeidsplassen. Myndighetene stiller krav til internkontroll for systematisk, veldokumentert og målbevisst arbeid med HMS, samt til overholdelse av norske lover og forskrifter. Linjeleders ansvar poengteres og vurdering av resultater kreves og må følges opp.

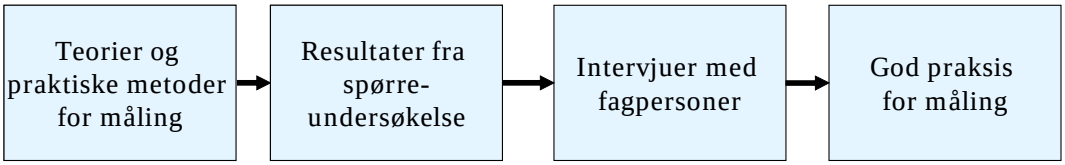
3 Metodevalg

3.1 Forskningsstrategi

Rapportens metodikk inkluderer forskningsstrategi, metode for innsamling av informasjon, statistisk analyse og vurderinger. Valg av forskningsdesign [60-63] er basert på planlegging av arbeidet utført denne oppgaves forprosjekt [64].

Det ble valgt en blandet metode med sekvensiell prosedyre i forskningen [60] for å få best mulig datagrunnlag for analyse av resultater. En spørreundersøkelse blant større europeiske virksomheter er den viktigste datakilden. I tillegg er det valgt en mindre formalisert datainnsamling, i form av intervjuer av enkelte frivillige sikkerhetsledere og rådgivere fra spørreundersøkelsen. Data fra intervjuene er ment å supplere resultatene fra spørreundersøkelsen.

Prosessen frem til rapportens skriftlige resultat er beskrevet i Figur 2.



Figur 2 Prosessen

3.2 Litteratur

En viktig metodisk tilnærming til forskningstemaet er vurdering av relevant litteratur. Bibliotekenes kataloger og anerkjente databaser, som ISI Web of Science, Academic Search Premier, CiteSeer og Springer Link er benyttet. I tillegg er ulike søkemotorer på Internett og rapporter fra flere sikkerhetsorganisasjoner benyttet.

Litteraturstudiet viser at det finnes mange teorier knyttet til måling av informasjonssikkerhet, samt noen praktiske metoder for å måle sikkerhet. Empiriske data finnes i mindre grad. Måling av informasjonssikkerhet er et umodent praktisk fagfelt, som også beskrives med mange ulike begreper. Teoriene har dannet utgangspunkt for spørreundersøkelsen.

3.3 Spørreundersøkelsen

Spørreundersøkelsen er sammen med relevant litteratur den viktigste delen av datainnsamlingen. Systematisk og strukturert datainnsamling med kvantitative metoder muliggjør sammenligninger og statistiske beregninger, som kan gi et tverrsnitt av dagens situasjon blant virksomheter med fokus på informasjonssikkerhet. Resultater fra spørreundersøkelsen skal gi svar på hypoteser og forskningsspørsmål, og bidra til god praksis for måling av nivå for informasjonssikkerhet.

3.3.1 Utvalget

Spørreundersøkelsens populasjon utgjør virksomheter hvor informasjons- og kommunikasjonsteknologi antas å utgjøre en vesentlig del av, eller er tett integrert i forretningen. Virksomhetene er ment å være et utvalg av virksomheter som kan anses å være blant de beste på markedet innen informasjonssikkerhet, og ikke ment å være representative på generelt grunnlag. I all hovedsak er virksomhetene i nordiske sammenheng ansett å være meget store. I følge Statistisk sentralbyrå [65] er store virksomheter i Norge over 100 ansatte, og utgjør 0,6 % av totalt antall bedrifter. Denne spørreundersøkelsen har kun en besvarelse med færre enn 100 ansatte. Utvalget er ikke tilfeldig, men stratifisert og trukket i en form for makelighetsutvalg [63], noe som kan være en svakhet. Det er imidlertid tilfeldig i den grad at det er virksomheter fra ulike bransjer og fra ulike land. Virksomhetene antas å ha stort fokus på informasjonssikkerhet med tanke på å sikre informasjon og systemer, egne og andres verdier, å kunne utføre oppgaver og tjenester, samt sikre sitt renommé i markedet.

På samme måte som internasjonale standarder for informasjonssikkerhet [9,10] i stor grad er utviklet gjennom studier av praktiske sikkerhetsmetoder, forventes det at disse virksomhetene vil være ledende i utvikling og bruk av måling av informasjonssikkerhet. Meget store virksomheter antas også å i større grad ha ansatt egne sikkerhetsledere, med ansvar for og ressurser til å være pådrivere for sikkerhetsarbeidet på bred basis i virksomheten. Mange i utvalget er medlemmer i Information Security Forum (ISF). ISF er en «non-profit» interesseorganisasjon, som leverer praktiske veiledninger og løsninger for informasjonssikkerhet. Pr 1.6.2005 består organisasjonen av 267 bedrifter verden over, inkludert 50 % av «Fortune 100»-bedrifter. Dette antas å være en av styrkene til ISF. Det forventes at virksomheter som er aktive i ISF har høy fokus på informasjonssikkerhet. Disse vil trolig også være blant de ledende innen måling av informasjonssikkerhet.

Det er søkt å nå de virkelige store virksomhetene i Norden. Disse vil dekke en meget liten andel av virksomhetene, men intensjonen er å nå de som er ledende i utviklingen innen informasjonssikkerhet. Informasjon om masteroppgaven ble tidlig lagt ut på ISFs hjemmeside. Enkelte virksomheter i Europa er nådd gjennom denne hjemmesiden.

Sikkerhetsledere, eller andre med tilsvarende stillinger, er aktuelle respondenter. Det ble også antatt at flere ikke ville oppgi informasjon av konfidensialitetshensyn, mens andre ikke tar seg tid til aktiviteter som ikke direkte gagner eget arbeid. Utvalget er hentet fra eget faglige nettverk, noe som påvirker representativiteten, men som anses å ha sine fordeler.

3.3.2 Spørreskjemaet

Spørsmålene i spørreskjemaet avgjør hvilke resultater som kan hentes ut. Til grunn for spørsmålsvalgene lå litteraturstudier og aktuelle hypoteser. Spørsmål knyttet til faktainformasjon om virksomheten ble valgt med tanke på uavhengige variable til statistiske undersøkelser. Spørsmålene ble prioritert og foredlet ut fra målet om at spørreundersøkelsen skulle kunne besvares i løpet av 15 minutter. En kan tenke seg svært mange spørsmål for å avdekke fullt og helt hva som er god praksis for måling av

informasjonssikkerhet. Det er imidlertid valgt å ha få spørsmål, noe som hemmer å få svar på mange spørsmål knyttet til hvordan og hva virksomheter måler knyttet til informasjonssikkerhet, men kan ha som styrke at flere svarer på spørreundersøkelsen. Spørreskjemaet inneholder spørsmål om:

1. Standard for informasjonssikkerhet
2. Måling av informasjonssikkerhet
3. Holdninger og vurderinger til måling av informasjonssikkerhet
4. Fakta om virksomheten

Et informasjonsbrev ble integrert i spørreskjemaet for å gjøre det enkelt for mottaker. Det ble lagt vekt på å forsikre respondenten om konfidensiell behandling og at alle data og resultater ville bli anonymisert. Første avsnitt i informasjonsbrevet ble vektlagt betydelig for å pirre mottakers nysgjerrighet. I tillegg ble første spørsmål i spørreundersøkelsen utformet enkelt for å motivere til å gjennomføre spørreundersøkelsen.

De fleste spørsmål har forhåndsbestemte svaralternativer, med mulighet for å komplettere med egne svar og kommentarer. Med formål om å oppnå et riktigere bilde av virkeligheten og forhindre feil svar ble svaralternativet «vet ikke» inkludert. Flere av spørsmålene har bipolære skalaer med både positive og negative svar i forhold til et gitt midtpunkt. For disse ble det valgt en fem punkts skala [63], i tillegg til «vet ikke»-alternativet.

Spørreskjemaet, som ble laget både på norsk (se vedlegg A) og engelsk (se vedlegg B), ble kvalitetssikret på innhold, form og språk av en pilotgruppe på seks personer. To av personene i pilotgruppen er engelske, og profesjonelle innen informasjonssikkerhet. Fire i pilotgruppen arbeider med sikkerhet på heltid, og de resterende to har det som deltidsarbeide. Innhold og betydning av ord ble gjennomgått nøye med tanke på å unngå misforståelse.

3.3.3 Utsendelse

Det ble lagt vekt på å få til en personlig, men effektiv utsendelse av spørreskjemaet. Spørreskjemaet ble utsendt med e-post, noe som anses som effektivt for respondenten. Dette er respondenter som i stor grad er vant til å kommunisere elektronisk, og bruk av e-post er forventet å gi større deltakelse enn papirbasert utsendelse. For å sikre konfidensialitet og få en mer personlig utsendelse ble det valgt å sende til en og en respondent. Litteratur om spørreundersøkelser anbefaler å sende ut et forvarsel ved postale spørreundersøkelser [63]. Dette ble ikke gjort, da mange mottar svært mye e-post. Å sende flere e-post om samme tema antas derfor å kunne irritere mer enn gagne saken.

3.3.4 Tolking av data og statistiske undersøkelser

Resultater av datafangsten ga muligheter til å se på mulige sammenhenger mellom variablene i datainnsamlingen. Dataanalyse og tolkning av resultatene er prosessen som bidrar til å få ny og fornuftig kunnskap og forståelse ut av innsamlet data. Analytiske

spørsmål, nedskriving av notater og fortolkning av resultatene var viktige steg i prosessen.
Noen få spørsmål ble ikke gitt faste svaralternativer i spørreundersøkelsen, men ble kodet eller gruppert i etterkant. Dette gjaldt antall ansatte i virksomheten, antall ansatte med ansvar for informasjonssikkerhet og stillingsbetegnelse for respondenten.

God svarprosent fra spørreundersøkelsen ga mulighet for statistiske undersøkelser [66] av dataene. Til dette ble verktøyet SPSS [67,68] benyttet. Frekvensanalyser, Pearsons kjikvadrattest, «independent sample» T-test og variansanalyser ble benyttet. I tillegg ble faktoranalyser brukt for med tanke på å finne sammenhenger mellom variable som beskriver respondentens holdninger og vurderinger til måling av informasjonssikkerhet. For alle statistiske beregninger ble et signifikansnivå (p-verdi) på 0,05 valgt som tilfredsstillende. Meget signifikant benyttes hvor resultatet ga et signifikansnivå på mindre enn 0,01.

3.4 Oppfølgende intervjuer

I tillegg til spørreundersøkelsen, ble det foretatt en kvalitativ datainnsamling i form av intervjuer for å utdype og komplettere data fra spørreundersøkelsen. Om lag 20 % av de som måler informasjonssikkerhet er intervjuet. De fleste av intervjuene er tatt over telefon. Resultater fra spørreundersøkelsen har dannet grunnlaget for intervjuguiden [63]. På grunn av oppgavens utforskende art vil enkelte spørsmål kunne oppstå underveis, og kan være ulike fra intervju til intervju. Personer som hadde deltatt i spørreundersøkelsen og akseptert å delta i oppfølgende samtaler, ble intervjuet. Intervjuene varte maksimalt tjue minutter slik avtalen på forhånd var. Intervjuguide er i vedlegg C.

3.5 Kvalitet

Litteratur knyttet til forskningsdesign og metode beskriver viktigheten av god kvalitet ved forskningen [60,61]. I det følgende er elementer knyttet til pålitelighet, gyldighet og egen forskerrolle diskutert.

En generell svakhet ved spørreundersøkelser er faren for at spørsmålene og svaralternativene ikke er de riktige eller ikke relevante, og at dette ikke oppdages. Det er viktig at resultatet av spørreundersøkelsen gir et så korrekt bilde som mulig. Pilotgruppe og bruk av veiledere bidro med kvalitetssikring av spørreskjemaet. Intervjuer i etterkant vil også kunne avdekke mangler ved spørreundersøkelsen, samt supplere eventuelle mangler. Statistiske undersøkelser vil også i noen grad hindre at sporadiske feil slår ut. Spørreskjemaet er laget slik at det er mulig å reprodusere resultatene. Det antas derfor at data fra spørreundersøkelsen i stor grad er gyldige.

En spørreundersøkelse er en egenevaluering hvor respondenten i noen grad kan ønske å skjønnmale situasjonen. Det er lagt vekt på å forsikre deltakerne om konfidensiell behandling og anonymisering av data og resultater, slik at det ikke skal ligge til grunn motiver for å svare uærlig. Respondentene sto også fritt til å besvare spørreundersøkelsen og delta i intervjuene. Kun et fåtall oppga at de ikke ønsket å

besvare. Respondentene har relativt høye stillinger med krav til høy integritet, og i mange tilfeller stilles det også krav til vandelsattester eller sikkerhetsklarering for å kunne inneha stillingen. De er godt kjent med terminologi og fagfeltet og er kvalifiserte til å besvare spørsmålene.

Mange av respondentene arbeider i det daglige alene på fagfeltet i virksomheten. For å få faglige diskusjonspartnere har de derfor erfaring med å utveksle informasjon knyttet til informasjonssikkerhet i lukkede fora, hvor krav til konfidensialitet er høye. Utveksling av informasjon skjer også ofte med formål om å bidra til å heve nivået på informasjonssikkerhet. Av den grunn mener vi det i hovedsak er grunn til å tro at besvarelsene er gjort etter beste evne og på en ærlig måte. Det er dermed grunn til å anta tilfredsstillende pålitelige resultater fra spørreundersøkelsen og intervjuene.

Kvalitative data i form av intervjuer har mest fokus på det spesielle ved den enkelte. Gyldighetsaspektet ved de kvalitative data er dermed ikke så relevant å bestemme. En kombinasjon av kvantitative og kvalitative metoder vil bidra til å påvise gyldigheten til dataene. Intervjuene i etterkant viste samsvar med dataene i spørreundersøkelsen, noe som også styrker tilliten til oppgavens resultater.

Subjektive meninger kan også prege arbeidet [60]. Det kan være problematisk å avdekke hva eller hvor stor del av resultatet som er personlige vurderinger. Med andre ord om resultatene ville blitt annerledes om andre hadde gjennomført dataanalysen. Vurderingene er imidlertid diskutert med veileder og flere uavhengige ressurspersoner for å hindre dette.

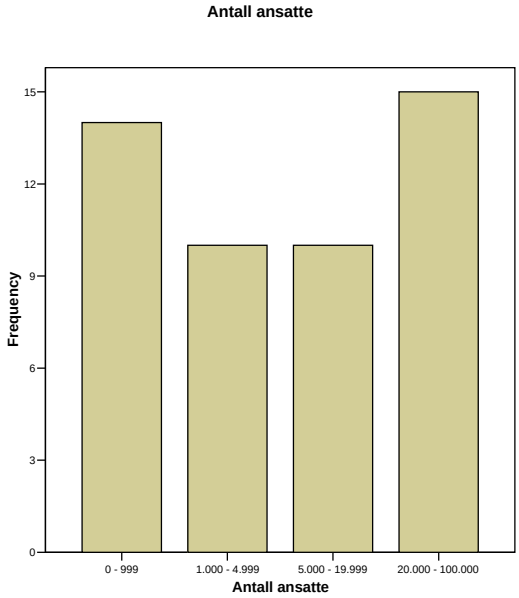
4 Datagrunnlag

Teoriene og metodene fra kapittel 2 har sine styrker og svakheter, men i hovedsak er det bruken og erfaringer som avgjør kvaliteten, slik ordtaket «The proof of the pudding is in the eating» beskriver det. Det er også praktiske erfaringer som bestemmer «god praksis» for måling av informasjonssikkerhet. En spørreundersøkelse med 49 besvarelser fra ulike virksomheter er behandlet. Enkelte spørsmål fra spørreundersøkelsen er med på å karakterisere virksomhetene, og presenteres i det følgende. Drøftinger, konklusjoner og ny kunnskap på området av resultatene er omtalt i kapitlene 5 og 6. Øvrige frekvensanalyser for alle variable fra spørreundersøkelsens resultater finnes som vedlegg D.

4.1 Besvarelse av spørreundersøkelsen

Spørreskjemaet ble sendt til 78 virksomheter som tilfredsstilte kravene nevnt i kapittel 3.3.1. 54 virksomheter ga tilbakemelding, noe som er en meget tilfredsstillende svarprosenten på 69. Fem av disse virksomhetene ville ikke eller kunne ikke svare på spørreskjemaet. Til sammen 49 spørreskjema er derfor behandlet, i praksis en svarprosent på 63. Antall ansatte i virksomhetene er fra 50 til 100.000.

Figur 3 viser fordelingen på antall ansatt fordelt på gruppene 0-999, 1.000 – 4.999, 5.000 – 19.999 og mer enn 20.000 ansatte for virksomhetene. X-aksen viser de fire gruppene for ansatte, mens y-aksen viser antall virksomheter. Som figuren viser er det en forholdsvis jevn fordeling mellom disse gruppene. Gjennomsnittlig antall ansatte for virksomheter som besvarte undersøkelsen er 16.250. 15 besvarelser var fra virksomheter med flere enn 20.000 ansatte.



Figur 3 Spredning av antall ansatte

Noen virksomheter bidrar til å dra opp det aritmetiske gjennomsnittet. Et riktigere mål på gjennomsnitt her er derfor median, som er den midterste verdien i et sortert datasett. Median for antall ansatte er 6.000.
Mange virksomheter utkontrakterer hele eller deler av sine IT funksjoner. Av de 48 virksomheter som har oppgitt informasjon om dette, er det 14 (30 %) som ikke utkontrakterer, 29 (60 %) som delvis utkontrakterer og 5 virksomheter (10 %) som utkontrakterer alle sine IT funksjoner.
Virksomheter fra ti ulike land deltok i spørreundersøkelsen. Noen land har bare en eller to besvarelser og er samlet i kategorien «andre europeiske». En oversikt over hvilke land virksomhetene som deltok i spørreundersøkelsen kommer fra er vist i tabell 1. Det er en overvekt av norske virksomheter med 47 % av det totale antallet. Til statistisk behandling er det også gjort en gruppering av virksomhetene i gruppene Norge, Norden (utenom Norge) og EU-land gjort.

Tabell 1 Geografisk fordeling

Land	Antall
Norge	23
Sverige	6
Danmark	5
Finland	5
Storbritannia	4
Andre europeiske	6

Det ble lagt vekt på å få svar fra ulike bransjer til spørreundersøkelsen. SSB [65] benytter atten ulike næringsinndelinger, mens spørreskjemaet ga mulighet til å velge blant tolv ulike alternativer. For å få tilstrekkelig antall virksomheter til statistiske analyser, samt å sikre konfidensialitet, ble en rekoding til fem ulike bransjemessige grupperinger foretatt. Pga kontaktflaten og utvalgskriteriene er det forholdsvis mange sentralbanker med i undersøkelsen, og det er derfor valgt å kategorisere disse i en egen gruppe.

Tabell 2 Bransjemessig fordeling

Bransjer	Antall
Bank, finans, forsikring	9
Sentralbanker	8
Produksjon, industri	12
Offentlig sektor	7
Tjenesteyting og varer	13

Respondentene som besvarte spørreundersøkelsen kunne i hovedsak kategoriseres etter tre funksjoner eller stillinger. 25 av de som besvarte hadde stilling eller tittel sikkerhetsleder (52 %) eller lignende. 6 av spørreskjemaene kom fra personer som var leder av annen enhet (12,5 %), og da gjerne IT-avdeling. De siste 17 respondentene

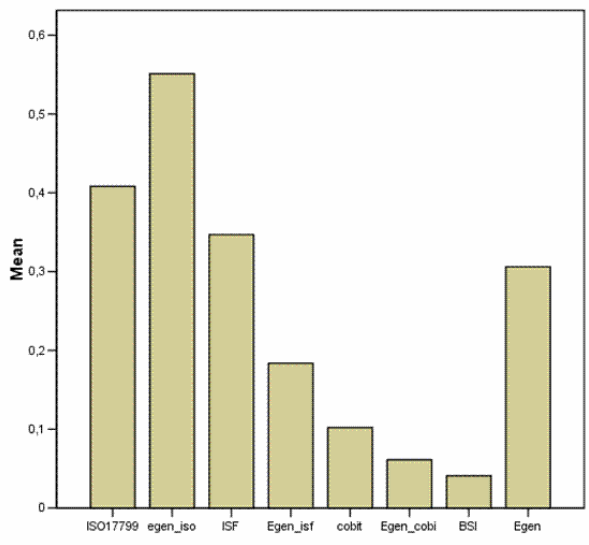
hadde rådgiver eller konsulentstillinger (35,5 %) innen sikkerhet. Gruppene er i resten av oppgaven betegnet som sikkerhetsleder, annen leder og rådgiver.

30 av de 49 virksomhetene (61 %) som deltok i spørreundersøkelsen er medlemmer av sikkerhetsorganisasjonen Information Security Forum (ISF). Motivasjon for medlemskap i ISF er for enkelte virksomheter muligheten til benchmarking, mens mange også er medlem for å få resultater av de mange prosjektene ISF årlig gjennomfører.

4.2 Informasjonssikkerhetsstandard

ISO/IEC 17799 [9] begynner nå å bli en anerkjent standard for informasjonssikkerhet. Likevel benytter bare 41 % av virksomhetene i denne spørreundersøkelsen ISO-standarden for informasjonssikkerhet. Meget få benytter bare denne som sin standard. Dette kan skyldes at endringshyppigheten i ISO-regimet er på om lag fem år, noe som kan synes langsomt på et området hvor trusselbilde og teknologi er i stadig endring. Flest virksomheter benytter egne standarder ut fra en eller flere av følgende internasjonale standarder: ISO/IEC 17799, ISFs Standard of Good Practice, COBIT fra ISACA og The IT baseline Protection Manual (BSI). X-aksen i Figur 4 viser hvilke standarder som benyttes. Betegnelsen «Egen_» referer seg til bruk av egen standard basert på den angitte anerkjente standarden. Y-aksen viser den gjennomsnittlig prosentandelen sikkerhetsstandarder som benyttes av virksomhetene. Mange virksomheter bruker flere standarder, noe figur 4 indikerer ved at summen av andelene overstiger 1 flere ganger.

Det kan også være andre årsaker til at mange velger egne standarder, f eks ønske om egne spesialtilpassede løsninger for både informasjonssikkerhetsstandard og måling. Figur 4 viser fordelingen av informasjonssikkerhetsstandarder som benyttes. Sorteringen er i henhold til svarene i spørreskjemaet og er: ISO/IEC 17799, Egen standard basert på ISO/IEC 17799, ISFs standard, Egen standard basert på ISFs standard, COBIT, Egen standard basert på COBIT, BSI og bare egen standard.



Figur 4 Informasjonssikkerhetsstandarder som brukes

4.3 Måling av informasjonssikkerhet

Måling av informasjonssikkerhet synes å være et umodent teoretisert fagfelt og det antas derfor at måling skjer i mindre grad i det praktiske liv. En hypotese var at et mindretall, dvs. mindre enn 50 % av virksomheter med fokus på informasjonssikkerhet, måler informasjonssikkerhet. Et av de viktigste spørsmålene i spørreundersøkelsen er:

«Er det satt mål for eller måler virksomheten informasjonssikkerhet?».

67 % av virksomhetene i spørreundersøkelsen svarte positivt på dette spørsmålet. Spørsmålet er noe åpent i formuleringen, slik at det er vanskelig å ut fra dette si noe om kvaliteten og omfang av målingen. Det viser imidlertid at virksomhetene i denne spørreundersøkelsen er opptatt av måling av informasjonssikkerhet. Hypotesen om at et fåtall virksomheter, selv blant de med fokus på informasjonssikkerhet, gjennomfører måling av informasjonssikkerhet kan dermed avkreftes.

5 Diskusjon av resultater

5.1 Innledning

Resultatene fra spørreundersøkelsen er behandlet statistisk med tanke på å finne svar på oppgavens forskningsspørsmål, som er:

1. Hva kjennetegner virksomheter som måler informasjonssikkerhet?
2. Hva er god praksis for måling av informasjonssikkerhetsnivå?

Forskningsspørsmål 2 kan igjen deles i følgende spørsmål:

- Hvilke metoder benytter virksomheter i dag for å måle informasjonssikkerhet?
- Hva anser virksomheter å være formålet med å måle informasjonssikkerhet?
- Hvilke effekter mener virksomheter det gir å måle informasjonssikkerhet?

Resultater fra den utsendte spørreundersøkelsen gir nye erfaringer om hvordan og hvorfor virksomheter måler nivå for informasjonssikkerhet. Dette anses som nyttig kunnskap for å kunne etablere god praksis på området. Virksomhetene fra spørreundersøkelsen antas å være blant de «beste i markedet» innen informasjonssikkerhet og vil være trendsettende for andre virksomheter.

5.2 Kjennetegn på virksomheter som måler informasjonssikkerhet

Hypotesene og antagelsene i forkant av spørreundersøkelsen var at praktisk måling av etterlevelse av sikkerhetskrav i mindre grad blir gjennomført, selv blant virksomheter som anses å være blant de beste i markedet. Det ble likevel forventet at dersom måling av informasjonssikkerhet skjer, er det hos de virkelig store virksomhetene, innen den finansielle sektor og hos virksomheter som er aktive i sikkerhetsorganisasjoner. I denne undersøkelsen måler to tredeler (67 %) av virksomhetene informasjonssikkerhet, noe som må sies å være et stort fokus på måling av informasjonssikkerhet. Resultater fra spørreundersøkelsen viser at virksomheter som måler informasjonssikkerhet i større grad enn andre:

- Har utkontraktert deler av sin IT funksjon
- Tilhører finansiell eller tjenesteytende sektor
- Har ansatt sikkerhetsleder
- Har fem eller flere ansatte i sentral sikkerhetsfunksjon
- Er generelt mer opptatt av måling, og spesielt bruk av balansert målstyring

I det følgende er resultatene fra spørreundersøkelsen knyttet til hvilke virksomheter som måler informasjonssikkerhet diskutert.

5.2.1 Virksomhetens størrelse

Antagelsen på forhånd var at størrelsen påvirker om måling av informasjonssikkerhet skjer. Det antas at jo større virksomheten er jo mer opptatt er den av måling. Gjennomsnittlig antall ansatte for virksomheter som ikke måler er 13.200, mens det for virksomheter som måler er 17.700 ansatte. Statistiske sammenligninger mellom måling av informasjonssikkerhet og størrelse på virksomhetene viser ingen sammenheng. Virksomhetene i spørreundersøkelsen er alle relativt store i nordisk sammenheng, og resultatene viser at størrelsen ikke påvirker om virksomheter måler informasjonssikkerhet. Spørreundersøkelsen inkluderte mange virksomheter med ansatte under 1.000, men resultatet kunne blitt annerledes om flere virksomheter med færre enn f eks 100 ansatte var med. Da utvalget består av så mange store virksomheter hindrer det selvsagt at en kan trekke generelle slutninger for alle virksomheter.

5.2.2 Medlemskap i ISF

Hypotesen var at virksomheter som investerer i medlemskap i ISF måler i større grad enn andre. I 2003 deltok i overkant av 30 % av medlemmene i ISFs Status Survey [47], som er en benchmarking knyttet til ISFs standard for informasjonssikkerhet.

Resultatene fra spørreundersøkelsen viser at:

- 73 % av virksomhetene som er medlem av ISF måler (andelen av ISF)
- 58 % av virksomhetene som ikke er medlem i ISF måler

Virksomheter med medlemskap i ISF virker i denne spørreundersøkelsen å være noe mer opptatt av måling enn andre virksomheter, men også mange som ikke er medlem av ISF måler. Resultatet kan ikke tillegges betydelig vekt, da kjikvadrattest ikke er tilfredsstillende signifikant.

5.2.3 Virksomhetens geografiske tilhørighet

Alle virksomheter som deltok i spørreundersøkelsen er europeiske, og det ble antatt at det ikke var vesentlig forskjell mellom de ulike landene knyttet til om måling skjer eller ikke. Dersom virksomhetene grupperes etter Norge, Norden og EU-land viser resultatene fra spørreundersøkelsen at norske virksomheter måler i 65 % av tilfellene, Nordiske virksomheter måler i 82 % av tilfellene og EU-land måler i 44 % av tilfellene. Resultatet fra kjikvadrattest er imidlertid ikke tilfredsstillende signifikant ($p = 0,14$), og slutninger om sammenheng mellom virksomhetenes geografiske tilhørighet og om de måler informasjonssikkerhet kan ikke trekkes.

5.2.4 Bransjetilknytning

Det ble på forhånd antatt at virksomheter fra bank- og finanssektoren i større grad måler enn virksomheter fra andre sektorer. Gjennomsnittlig måler 67 % av alle virksomhetene. Resultatene fra spørreundersøkelsen viser sammenheng med tilfredsstillende signifikans ($p < 0,05$) ved bruk av kjikvadrattest med variablene måling og bransje. Tabell 3 viser at finanssektoren og den tjenesteytende sektor måler betydelig mer enn gjennomsnittet. Bank og finans sektoren har i mange år benyttet ISF

Status Survey mest, samt vært ledende i forhold til benchmark resultater. I 2000 var 62,6 % av deltakerne i Status Survey fra bank, finans og forsikring [69]. I 2003 var andelen endret til 37 % [47] og den totale deltakelsen økte samtidig med 40 %. Benchmark resultatet ble også redusert, og en av teoriene at den prosentvise deltakelse fra finanssektoren ble redusert.

Tjenesteytende og varesektoren ligger like bak finanssektoren i forhold til hvor mye de måler (85 %). Offentlige virksomheter måler betydelig mindre enn andre sektorer. Trekkes offentlig sektor ut fra resultatene, er det til sammen 73,8 % av virksomheter i spørreundersøkelsen som måler informasjonssikkerhet. En forholdsvis høy andel virksomheter er sentralbanker, som kan kategoriseres inn under offentlig sektor eller i sektor sammen med bank, finans og forsikring, men er valgt å kategorisere som en egen sektor i denne spørreundersøkelsen. Målemessig ligger de også mellom finansinstitusjoner og offentlige sektor. Produksjon og industri ligger på gjennomsnittet (67 %).

Tabell 3 Måling fordelt på ulike bransjer

Bransje	Antall totalt	Antall som måler	Andel som måler
Bank, finans, forsikring	9	8	89 %
Tjenesteytelse og vare	13	11	85 %
Produksjon, industri	12	8	67 %
Sentralbanker	8	4	50 %
Offentlig sektor	7	2	29 %

5.2.5 Utkontraktering

En hypotese er at virksomheter som utkontrakterer har et generelt økt fokus på avtaler og rapportering i forhold til måltall, noe som antas å påvirke viljen til å måle informasjonssikkerhet positivt. Resultater fra spørreundersøkelsen viser også at virksomheter som utkontrakterer sine IT-funksjoner måler mer enn de som ikke gjør det. Statistisk analyse med kjikvadrat viser et tilfredsstillende signifikant ($p < 0,05$) resultat på at 77 % av de som delvis utkontrakterer måler, i motsetning til at bare 43 % av de som ikke utkontrakterer måler informasjonssikkerhet.

Ved utkontraktering er det gjerne mer fokus på skriftlige avtaler i form av Service Level Agreements (SLA). Totalt 10 virksomheter bruker SLA som målemetode. Alle disse har utkontraktert hele eller deler av sin IT-funksjon. En utvikling til at SLA-ene vil inneholde sikkerhetsmetrikker som inneholder alle egenskaper ved informasjonssikkerhet antas å skje [38]. Deisz, Ingebrigstsen og Nilsen [39] beskriver positive erfaringer med å gjøre dette. De beskriver imidlertid at dette er en prosess det tar lang tid å utvikle.

Utkontraktering er også i en viss grad bransjerelatert. Resultatene i Tabell 4 viser hvilke virksomheter som velger utkontraktering, samt i hvilken grad de måler henholdsvis

totalt og dersom de utkontrakterer. Det vises for øvrig til kapittel 5.2.4 som beskriver forskjellene mellom de ulike bransjene.

Ved å filtrere bort virksomheter som ikke utkontrakterer sine IT-funksjoner pr bransje blir andelen som måler annerledes. Innen finanssektoren har alle som deltar i spørreundersøkelsen utkontraktert hele eller deler av sin IT funksjon. I offentlig sektor er det kun to av syv virksomheter som utkontrakterer sine IT-funksjoner, og kun en av disse måler. Datagrunnlaget er noe lite til kunne vurdere resultatet, og gir derfor ingen signifikante funn.

Tabell 4 Måling inndelt etter bransje og andel som utkontrakterer

Bransje	Antall	Antall som utkontrakterer	Andel som måler	Andel som måler og utkontrakterer
Bank, finans, forsikring	9	9	(8 av 9) 89 %	(8 av 9) 89 %
Sentralbanker	8	3	(4 av 8) 50 %	(3 av 5) 60 %
Produksjon, industri	12	8	(8 av 12) 67 %	(5 av 8) 63 %
Offentlig sektor	7	2	(2 av 7) 29 %	(1 av 2) 50 %
Tjenesteytelse og vare	13	10	(11 av 13) 85 %	(9 av 10) 90 %

5.2.6 Sikkerhetsorganisasjon

Det ble antatt at respondentens stilling/ tittel ikke vil ha betydning for grad av måling av informasjonssikkerhet. Litt over halvparten av de som besvarte spørreskjemaet er sikkerhetsledere, og litt under halvparten (48 %) er leder av annen enhet eller rådgivere innen informasjonssikkerhet. Svarene fra spørreundersøkelsen viser at 80 % av virksomhetene, hvor sikkerhetsleder besvarte, måler informasjonssikkerhet. Mens bare 52 % av besvarelsene fra andre ledere eller rådgivere måler informasjonssikkerhet. Statistisk analyse med kjikvadrat viser at resultatet er tilfredsstillende signifikant ($p < 0,05$). Måling av informasjonssikkerhet er et ledelsesverktøy og innsalg til ledelsen er dermed essensielt. Spørreundersøkelsen viser at virksomheter med sikkerhetsleder har bedre forutsetninger for måle informasjonssikkerhet. ISF beskriver også [47]:

> «Management commitment, security awareness and security classification remain key factors in the 2003 Survey at enterprise level. This indicates that a strong 'driving force' is essential for information security to be effective. »

Antall virksomheter med personale knyttet mot informasjonssikkerhet har økt betraktelig de siste årene, noe som f eks økningen i medlemslisten i organisasjonen IT sikkerhetsforum [70] i Norge viser. Måling krever planlegging, tilrettelegging og gjennomføring og er ressurskrevende, og det ble på forhånd antatt at jo flere ressurser virksomheter bruker på konsernovergripende sikkerhetsfunksjoner, jo større er mulighetene for at informasjonssikkerhet måles. Spørreundersøkelsen viser at virksomheter med fem eller færre ansatte i sentral sikkerhetsfunksjon måler i noe mindre grad (58 %) enn virksomheter med flere enn fem ansatte i sentrale

sikkerhetsfunksjoner (87 %). Kjikvadrat viser at dette resultatet er tilfredsstillende signifikant ($p < 0,05$).

5.2.7 Sikkerhetsstandard

Det var antatt at det er sammenhenger mellom måling og hvilken standard for sikkerhet som benyttes. Statistisk analyse med kjikvadrat viser imidlertid ikke sammenheng mellom om virksomheter måler og hvilken sikkerhetsstandard som benyttes.

Det er heller ingen sammenheng mellom hvilket nivå i organisasjonen sikkerhetsstandarden er godkjent på (styrenivå, administrerende direktør eller sikkerhetssjef) og om virksomheten måler informasjonssikkerhet.

5.2.8 Måling av andre faktorer

En hypotese er at virksomheter som har stort fokus på å måle ulike nøkkeltall, også oftere måler informasjonssikkerhet. Resultatene fra spørreundersøkelsen viser at virksomheter som er mer opptatt av måling på en generell basis også er mer opptatt av å måle informasjonssikkerhet. En t-test viser dette med i nærheten av tilfredsstillende signifikans ($p = 0,06$).

Tabell 5 presenterer resultater fra spørreundersøkelsen som viser i hvilken grad virksomhetene gjennomsnittlig måler andre faktorer enn informasjonssikkerhet. Angitt poengskala er fra 1 til 5, hvor 1 er i liten grad og 5 i stor grad. Tabell 5 viser gjennomsnittlig poengsum for henholdsvis de som måler (JA) og de som ikke måler informasjonssikkerhet (NEI), og er sortert i forhold til hva de som måler informasjonssikkerhet, måler mest av. Økonomi får f eks en gjennomsnittlig poengsum på 4,94 for de som måler informasjonssikkerhet. Noe som forteller at nesten alle har svart fem på dette spørsmålet.

Tabell 5 Måling av andre faktorer

(Tallene viser gjennomsnittlig verdi på skala fra 1 til 5, hvor 5 er i stor grad)

I min virksomhet blir følgende andre måltall rapportert til ledelsen:	Måling av informasjonssikkerhet	
	JA	NEI
Økonomi; budsjett, regnskap og lignende	4,94	4,88
Helse, miljø og sikkerhet/ safety (HMS)	4,32	4,25
Kundetilfredshet	4,27	3,60
Salgstall	4,17	3,25
Produksjonstall	4,14	3,75
Balansert målstyring (BMS)	3,92	2,80
Samfunnsrelasjoner	3,16	2,60
Likestilling (kjønn, rase, handikap osv.)	3,15	2,64

Noen få av målefaktorene i denne spørreundersøkelsen skiller seg ut ved å bli målt noe mer enn andre hos virksomheter som måler informasjonssikkerhet. Dette gjelder spesielt balansert målstyring (BMS) hvor t-test viser en tilfredsstillende signifikant sammenheng ($p < 0,05$). En sikkerhetsrådgiver uttaler:

> «Måling av IT-sikkerhet er tett integrert med BMS, og er pakket inn i kvalitetsbegrepet. Målingen ble egentlig initiert av BMS. Økonomi var hovedfokus i starten, men ble på forrige rapportering til ledelsen rapportert som siste parameter».

Det er for øvrig ingen sammenheng med om BMS benyttes og variable som land, ISF medlemskap og utkontraktering. Imidlertid er det en viss sammenheng mellom hvilke bransjer som benytter BMS og hvilke som måler informasjonssikkerhet.

Tabell 6 viser at de to bransjene som benytter BMS i størst grad, også er de som i største grad måler informasjonssikkerhet. Det er også en viss sammenheng med at de to bransjene som i minst grad benytter BMS er de som i minst grad måler informasjonssikkerhet.

Tabell 6 Måling av informasjonssikkerhet pr bransje og bruk av BMS

(Tallene viser gjennomsnittlig verdi på skala fra 1 til 5, hvor 5 er i stor grad)

Bransje	Grad av BMS	Andel som måler informasjonssikkerhet
Tjenesteytelse og vare	4,00	85 %
Bank, finans, forsikring	3,78	89 %
Produksjon, industri	3,60	67 %
Offentlig sektor	3,00	29 %
Sentralbanker	2,57	50 %

Helse, miljø og sikkerhet (HMS) har tradisjoner for å måle og å følge opp, og det stilles krav [55]. For informasjonssikkerhet burde det vært mye å lære av dette miljøet. Det er imidlertid ingen signifikante sammenheng mellom måling av informasjonssikkerhet og måling av HMS, selv om HMS kommer høyt opp i forhold til faktorer som måles.

5.3 Metoder for måling av informasjonssikkerhet

Resultatene fra spørreundersøkelsen, som viser hvilke metoder virksomhetene benytter for å måle informasjonssikkerhet, er diskutert i dette kapitlet og kan oppsummeres med:

- God praksis er bruk av både kvalitative og kvantitative metoder.
- Flere metoder brukes gjerne for å måle informasjonssikkerhet.
- Egenutviklede metoder brukes av mange, f eks regnearkbaserte presentasjonsmåter. Revisjoner og uavhengige gjennomganger gir grunnlag for målingene.
- Mange ISF medlemmer benytter ISFs Status Survey.
- Måling søker å dekke hele virksomheten og IT-avdelingen.
- Kommersielle og standardisert verktøy, som er åpne i markedet, brukes i liten grad. Det synes å ta lang tid å etablere anerkjent metodikk for måling av informasjonssikkerhet.

5.3.1 Kvantitativ eller kvalitativ måling

Forventningen er at praktiske løsninger, i den grad de finnes, i stor grad vil være basert på kvalitative eller blandede metoder. Tabell 7 viser at over halvparten av virksomhetene i spørreundersøkelsen som måler informasjonssikkerhet, benytter seg av både kvantitative og kvalitative målemetoder. Kun 15 % bruker bare kvalitative målinger med skriftlige fremstillinger.

Tabell 7 Kvantitative eller kvalitative målinger

Er målene/ metrikkene …	
1. Kvantitative	26 %
2. Kvalitativ	15 %
3. Blandet (Noe kvantitativt og noe kvalitativt)	59 %

Ut fra dette kan en si at så mange som 85 % i noen grad benytter kvantitative målinger, til tross for at alle aspekter innen informasjonssikkerhet ikke så lett direkte kan kvantifiseres. Virksomhetene understøtter med andre ord i stor grad teoriene om bruk av kvantitative målinger [5,7].

ISF har flere metoder med kvantitativ representasjon som kan benyttes til måling av informasjonssikkerhet. Medlemmer av ISF er også overrepresentert av de som benytter kvantitative metoder, noe som kan tyde på at medlemskap i ISF inspirerer til bruk av kvantitative metoder. Kun 1 av 22 (5 %) av medlemmene i ISF benytter bare kvalitative metoder. For respondenter som ikke er medlem av ISF benytter 4 av 12 (33 %) bare kvalitative metoder. Spørreundersøkelsen viser med tilfredsstillende signifikans ($p <$

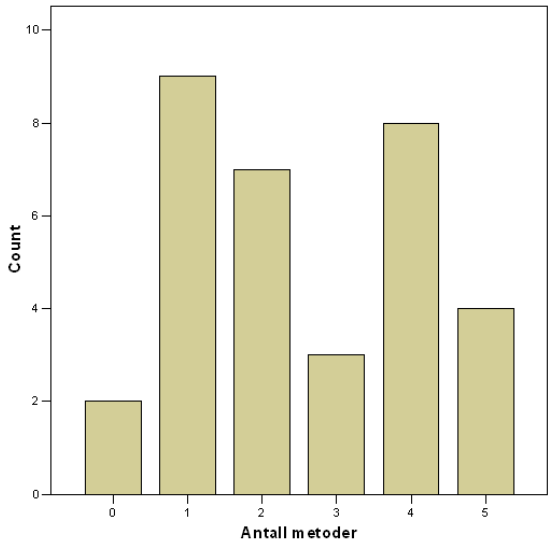
0,05) at respondenter som ikke er medlem av ISF, i større grad benytter bare kvalitative metoder.

Informasjonssikkerhet er både et teknisk og et administrativt fagområde, som ikke er lett tilgjengelig for andre enn profesjonelle innen fagfeltet. Det kan av den grunn være en fordel å forenkle status ved å kvantifisere og i tillegg supplere med mer deskriptiv og forklarende rapportering av status, dvs. en blandet metode. God praksis synes å være bruk av både kvalitative og kvantitative metoder.

5.3.2 Metoder som benyttes

Det ble på forhånd antatt at det finnes samarbeidsprosjekter i f eks ulike bransjer eller sikkerhetsorganisasjoner for måling av informasjonssikkerhet, som virksomheter i dag benytter. Resultater fra spørreundersøkelsen viser at gjennomsnittlig verdi for antall metoder er 2,5.

Figur 5 viser at flest virksomheter benytter bare en metode, men mange benytter også opptil fem metoder. Bruk av mange metoder kan skyldes at det ikke finnes standardiserte metoder eller god skikk og bruk i markedet. Virksomheter som ikke utkontrakterer benytter flere metoder, gjennomsnittlig 3,3 mot de som utkontrakterer med 2,3 metoder.



Figur 5 Antall metoder brukt til måling

Det er en forskjell her, men stor variasjonen gir ikke signifikant resultat ved statistisk analyse med t-test. Der hvor respondenten er sikkerhetsleder rapporteres det om bruk av gjennomsnittlig 2,7 metoder i forhold til 2,1 fra andre respondenter.
ISF medlemmer benytter noe færre metoder enn de som ikke er ISF medlemmer med gjennomsnittlig 2,9 mot 2,4 for ISF medlemmene. Kjikvadrat viser ingen signifikante resultater da spredningen er stor.

Tabell 8 viser også lite bruk av bransjevise anerkjente metoder, mens egenutviklede metoder, måling av sikkerhetshendelser og uavhengige gjennomganger kommer høyt. Blant ISF medlemmene benyttes ISFs Status Survey hyppig.

Undersøkelsen omfatter mange virksomheter med medlemskap i ISF og 74 % benytter metoder og verktøy fra ISF til måling av sin informasjonssikkerhetsstatus. ISF Status Survey [22] er det mest benyttede verktøyet, som tabell 8 viser. Denne metoden er også en benchmarking, noe som muliggjør sammenligning med andre. I 2003 benyttet ca 40 % av alle medlemmene i ISF Status Survey og trenden er at en økende andel av medlemmene benytter verktøyet. I denne spørreundersøkelsen er prosentandelen på 58.

Tabell 8 Metoder for måling av informasjonssikkerhet

Hvilke metoder brukes for å måle status for informasjonssikkerhet?	
ISF Information Security Status Survey	55,9 %
Uavhengig gjennomganger/ ekstern revisjon med angitte indikatorer	38,2 %
Egen utviklet metode/ indikatorer	41,2 %
Måling av sikkerhetshendelser og brudd	38,2 %
Tjenesteleverandøravtaler (SLA) med måltall/ metrikker	29,4 %
Egenevaluering med forhåndsbestemte indikatorer	23,5 %
Andre målemetoder fra ISF	16,0 %
Sertifisering i henhold til BS 7799	11,8 %
COBIT fra ISACA	8,8 %
Anerkjente indikatorer/ metoder innen industrisektoren	5,9 %
SBA Check	2,9 %

Spørreundersøkelsen hadde et begrenset utvalg virksomheter. SBA Check er et verktøy for måling av informasjonssikkerhet som har solgt over 600 lisenser i Sverige, jfr telefonsamtale med Dataföreningen i Sverige pr 2.5.2005. De fleste fornyer også sine lisenser, noe som gir grunn til å tro at det brukes i stor grad. Både store og små virksomheter i Sverige bruker verktøyet. Oppgavens spørreundersøkelse viser imidlertid at bare en av respondentene benytter SBA Check. Årsaken til dette kan skyldes et skjevt utvalg fra Sverige, hvor alle er ISF-medlemmer og dermed har tilgang til et konkurrerende verktøy.

Mange har utviklet egne metoder, og med til dels individuelle måleinstrumenter antas det varierende grad av kvalitet på målingene. Spørreundersøkelsen var begrenset og det er derfor ikke mulig å vurdere kvalitet på metoder og verktøy i noen grad her. Dette er noe det bør arbeides videre med. Resultatene tyder på at det finnes få industristandarder knyttet til måling av informasjonssikkerhet. Godt over halvparten synes det er vanskelig å måle informasjonssikkerhet, men det er imidlertid bare et fåtall som mener at informasjonssikkerhet ikke kan måles, som tabell 11 viser.

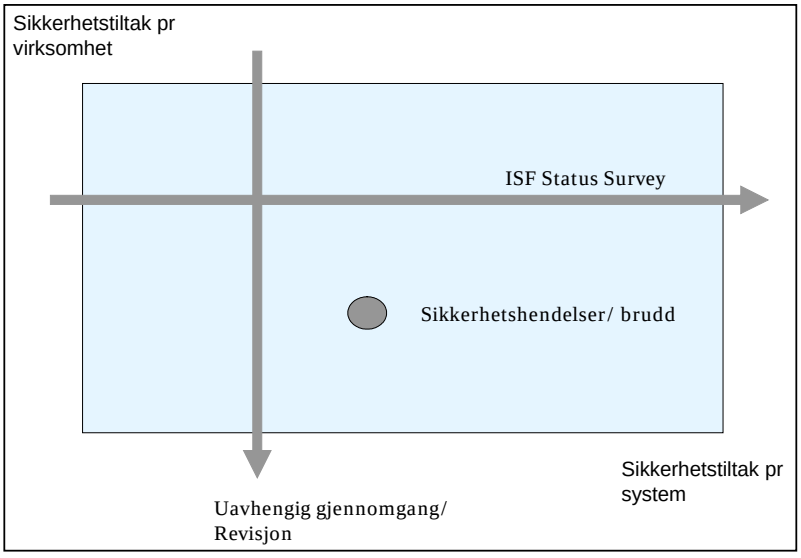
En sikkerhetsrådgiver uttaler:

> «Å måle er fryktelig vanskelig. Det ser vi spesielt når sjefen ønsker en status. Å finne en kontrollmåte som måler kvaliteten er ikke lett.»

Det finnes noen få kommersielle og standardiserte metoder og verktøy på det åpne markedet. Disse benyttes i liten grad av virksomhetene i dette utvalget. Enkle verktøy i form av f eks regneark vil trolig inspirere til måling, øke kvaliteten og forenkle kommunikasjon av informasjonssikkerhet. Dette kan synes å være trenden langt fram i tid. Spørreundersøkelsens mest brukte verktøy er fra ISF, og krever medlemskap i organisasjonen.

5.3.3 Hvor skjer måling?

Informasjonssikkerhet kan måles på mange måter. Virksomheter kan måle bredt for ett system, eller smalt og teknologisk for flere systemer, og det kan måles på enkeltpunkter. Figur 6 forsøker å illustrere med noen eksempler noen få målinger, hvor noe er måling i bredden, ved f eks bruk av ISF Survey. Andre målinger skjer mer i dybden og på et smalere felt, som sikkerhetsrevisjoner. Måling av sikkerhetshendelser og brudd er illustrert som et punkt. Dette er forhold som det ikke er spurt om i særlig grad i spørreundersøkelsen, slik at oppgaven ikke har resultater å vise til i forhold til hvor måling skjer. Svarene på andre spørsmål tyder imidlertid på at måling skjer i IT-avdelingen og på bred basis i virksomheten. Det antas derfor at det meste av målingene er på bred og overordnet basis i virksomheten.



Figur 6 Modell for hvor måling kan skje

Spørreundersøkelsens resultater viser at av de 33 virksomhetene som måler, skjer dette mot flere deler av virksomheten. Tabell 9 viser at om lag halvparten av virksomhetene i spørreundersøkelsen har fokus på en generell måling som skal dekke hele virksomheten, og ikke detaljer i forretningsområdene, samt måling av IT-avdelingens

informasjonssikkerhet. Færre virksomheter har fokus på måling av informasjonssikkerhet i forretningsprosessene og de ulike virksomhetsområdene. Kun 27 % setter fokus på måling av leverandører og bare 3 % måler alle forretningsprosesser. Til ledelsen er det naturlig å rapportere på et overordnet nivå, for å få et totalt og overordnet bilde av virksomhetens informasjonssikkerhetsstatus. Resultatene fra spørreundersøkelsen indikerer ut fra dette at måling av informasjonssikkerhet er et ledelsesverktøy.

Tabell 9 Hvilke deler av virksomheten blir målt

I hvilken del av virksomheten er måling av informasjonssikkerhet iverksatt?	
1. I hele virksomheten	52 %
3. I IT avdelingen	45 %
7. I kritisk infrastruktur	36 %
2. I enkelte forretningsområder/ avdelinger	30 %
4. Mot leverandører	27 %
5. I kritiske forretningsprosesser	21 %
6. I alle forretningsprosesser	3 %

5.4 Formål og effekter ved måling

Resultatene fra spørreundersøkelsen knyttet til formål og effekter ved måling er i det følgende beskrevet og diskutert.

- Måling av informasjonssikkerhet vurderes som et ledelsesverktøy. Dette understøttes av:
  - De som ikke måler informasjonssikkerhet begrunner det med at ledelsen ikke etterspør det.
  - Mål for informasjonssikkerhet blir rapportert til ledelsen.
  - Fokus for måling er på overordnet nivå i virksomheten og ikke detaljer i forretningsområdene.
- Måling av informasjonssikkerhet benyttes i stor grad til oppfølging av utkontrakterte IT-tjenester.
- De viktigste vurderte effektene av å måle er å øke ledernes oppmerksomhet mot og bedre holdninger til informasjonssikkerhet.

5.4.1 Formål med måling

Tabell 10 viser hva virksomhetene fra spørreundersøkelsen vurderer å være de viktigste formålene med å måle informasjonssikkerhet. Både de som måler og de som ikke måler er bedt om å besvare spørsmålet. Vurderingen er gjort på en skala fra 1 til 5, og tabellen viser gjennomsnittlig poengsum for henholdsvis de som måler (JA) og de som ikke måler informasjonssikkerhet (NEI). Resultatene fra spørreundersøkelsen viser at formålet med å gjennomføre måling i all hovedsak er rettet mot å informere ledelse om

status på informasjonssikkerhet (gjennomsnittlig poeng på 4,56) samt å vise til samsvar med informasjonssikkerhetsstandarder (gjennomsnittlig poeng på 4,32). Dette anses viktig for alle, men for de som måler informasjonssikkerhet er det ansett som betydelig viktigere. T-test viser at denne sammenhengen er meget signifikant ($p < 0,01$).

Resultatene fra spørreundersøkelsen viser at måling av informasjonssikkerhet oppfattes å være et ledelsesverktøy. Det viktige er å informere ledelsen om status, slik det gjøres på andre områder i virksomheten. Dette bekreftes i stor grad med at de som ikke måler, som tabell 11 viser, begrunner det med at ledelsen ikke etterspør måling av informasjonssikkerhet. Det ble på forhånd antatt at det å kunne bekrefte overfor myndigheter at lover og forskrifter overholdes var et viktig argument for måling, men det ble likevel rangert nest sist.

Tabell 10 Formål med måling

(Tallene viser gjennomsnittlig verdi på skala fra 1 til 5, hvor 5 er i stor grad)

Formålet med å måle informasjonssikkerhet er...	Måling av informasjons sikkerhet	
	JA	NEI
Å kommunisere informasjonssikkerhet status til ledelsen	4,56	4,00
Å vise til samsvar med informasjonssikkerhetsstandard	4,32	3,50
Grunnlag for beslutninger/ ledelses støttesystem	4,13	3,67
Å informere interessenter om informasjonssikkerhetsstatus	3,88	3,63
Å vise til samsvar med lover og forskrifter	3,66	3,57
Støtte til beregning av innsparing av investering (ROI)	2,94	2,80

Kun en tredel av virksomhetene i spørreundersøkelsen måler ikke informasjonssikkerhet. På en skala fra en til fem ble respondentene bedt om å angi hvorfor de ikke måler informasjonssikkerhet, og tabellen viser gjennomsnittlig poengsum ut fra denne skalaen. Tabell 11 viser at den desidert viktigste årsak til at informasjonssikkerhet ikke blir målt er at ledelsen ikke etterspør det. Dette henger også sammen med hva som oppfattes som det viktigste formålet med å måle; rapportering av status til ledelsen. Det er kun et fåtall som mener at informasjonssikkerhet ikke kan måles, selv om påstanden om at måling er vanskelig, blir gradert forholdmessig høyt.

Tabell 11 Årsak til at virksomheter ikke måler

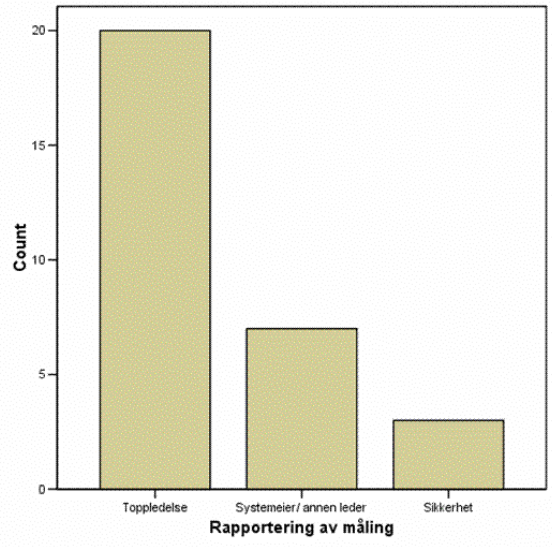
(Tallene viser gjennomsnittlig verdi på skala fra 1 til 5, hvor 5 er i stor grad)

Årsaker til at virksomheter ikke måler informasjonssikkerhet	Gjennomsnitt verdi
Ledelsen spør ikke etter mål for informasjonssikkerhet	3,62
Måling av informasjonssikkerhet er vanskelig	3,36
Det er ingen metoder eller verktøy for å måle	2,79
Det er ikke diskutert	2,54
Virksomheten måler generelt sett ikke	2,38
Informasjonssikkerhet kan ikke måles	2,14

5.4.2 Rapportering av måling

Resultatene fra spørreundersøkelsen viser at formålet med å måle informasjonssikkerhet er i stor grad å kommunisere dette til ledelse. Dette bekreftes også av figur 7, som viser hvilket rapporteringsnivå som benyttes. Frekvensanalyser viser at 67 % av virksomhetene rapporterer status til administrerende direktør eller styre i virksomheten. 23 % rapporterer til systemeier og forretningsområde og for bare 10 % av virksomhetene stopper rapporteringen hos sikkerhetsleder. Rapporteringsnivå endrer seg ikke om virksomheten er medlem av ISF, om den utkontrakterer eller om det er sikkerhetsleder som har besvart undersøkelsen.

Et styringssystem for en virksomhet består gjerne av metoder og verktøy for planlegging og kontroll [3]. Rapportering til ledelse kan i noen grad bestemmes av fagmiljøet, her sikkerhetsledelsen, men kan også i noen grad motiveres av modenhet og utvikling i virksomhetens øvrige metoder for styring og rapportering. Ledelsen selv vil også bidra til å bestemme hvilke tema som skal løftes opp til ledergruppe eller styre. Måling av informasjonssikkerhet kan ut fra å være et ledelsesverktøy være en av styringsparametrene i en virksomhets styringssystem. Utfordringen er dermed å få ledelsen til å etterspørre måling av informasjonssikkerhet. Dette krever sikkerhetsleder eller tilsvarende stillingskategori med mulighet til å møte, skape dialog og å influere ledelsen.



Figur 7 Rapporteringsnivå for målene

Resultatene viser også at flere virksomheter måler der hvor sikkerhetsleder har besvart spørreundersøkelsen, ref. kapittel 5.2.6 side 26. Det ser dermed ut til å være enklere for en sikkerhetsleder å selge inn måling av informasjonssikkerhet til ledelsen enn for andre i dette utvalget.

Spørreundersøkelsens resultater viser også at måling av informasjonssikkerhet benyttes til oppfølging av utkontrakterte IT-funksjoner. Dette er gjerne store økonomiske kontrakter, som kan inneholde beregning av bøter i forhold til ikke oppnådde mål, og er viktig for ledelsen å følge opp [39].

5.4.3 Vurderte effekter ved måling

Folk blir gjerne flinke på det de blir målt på [2,4], noe som er både en fordel og en risiko knyttet til måling av informasjonssikkerhet. Parametere som måles vil få fokus og forbedres, mens de som ikke måles kan bli ignorert. Ved å fokusere på gitte mål og stille ledere til ansvar for å nå målene antas det at det skjer forbedringer på disse faktorene. Ledere og medarbeidere ønsker å fremstå som flinke overfor sine ledere og omgivelsene [41]. Dette poengteres også av Wold [71] som mener at virksomheter som utfører «måling, rapportering og oppfølging» enten på virksomhetsnivå eller av sikkerhetspolicyen oppnår bedre resultater på «effekt». Resultatene i denne oppgaven indikerer også at overvåkning og måling av det aktuelle miljøet fører til høyere nivå med hensyn på fokus og kontroll. En hypotese er at målingen i seg selv har positiv effekt på sikkerheten.

Svarene fra oppgavens spørreundersøkelse er respondentens oppfattelse og vurderinger av hvilke effekter måling av informasjonssikkerhet har og må vurderes i denne kontekst. Vurderingen er gjort på en skala fra 1 til 5, og tabellen viser gjennomsnittlig poengsum for de som henholdsvis måler (JA) og de som ikke måler informasjonssikkerhet (NEI). Tabell 12 viser resultatene fra spørreundersøkelsen som bekrefter at respondentene

vurderer måling til å være et ledelsesverktøy og et viktig verktøy for bevisstgjøring av informasjonssikkerhet. Å få oppmerksomhet på informasjonssikkerhet er ikke lett, og en sikkerhetsansatt sier:

«Jeg kan vel ikke ønske meg hendelser, men...».

Rapportering av måling kan være et bedre alternativ. Å lettere lede og styre informasjonssikkerheten er også høyt vurdert av de som måler informasjonssikkerhet.

Tabell 12 Effekter av måling

(Tallene viser gjennomsnittlig verdi på skala fra 1 til 5, hvor 5 er i stor grad)

Vurderte effekter ved måling av informasjonssikkerhet	Måling av informasjonssikkerhet	
	JA	NEI
Økt involvering av ledelsen i informasjonssikkerhetssaker	4,25	3,94
Bedre holdninger til informasjonssikkerhet	4,19	3,93
Det er lettere å lede og styre informasjonssikkerheten	4,16	3,47
Mer oppmerksomhet på informasjonssikkerhet	4,06	3,75
Det er lettere å prioritere mellom sikkerhetstiltak	3,91	4,00
Det er lettere å budsjettere informasjonssikkerhet	3,56	3,67
Informasjonen blir bedre beskyttet	3,47	3,07

Måling og fokus på et område gir ofte en endring, da mennesker ønsker å nå mål som settes og vil ha fokus på de faktorer som følges opp og måles. Det er interessant å se at det er enighet om at måling ikke primært gir økt beskyttelse av informasjonen. Dette antas å ha en sekundær effekt, ved økt ledelsesinvolvering og bedrede holdninger. Disse svarene bekrefter mange av de andre vurderingene.

5.4.4 Faktoranalyse

Statistiske analyser i form av faktoranalyse [72] forsterker beskrivelsen av at måling av informasjonssikkerhet anses å være et ledelsesverktøy. Faktoranalysen er gjennomført med variable hvor respondentene har gitt sine vurderinger til følgende spørsmål:

- Måling av informasjonssikkerhet kan ha tilleggseffekter som:
- Formålet for å måle informasjonssikkerhet er:
- I min virksomhet blir følgende andre måltall rapportert til ledelsen:

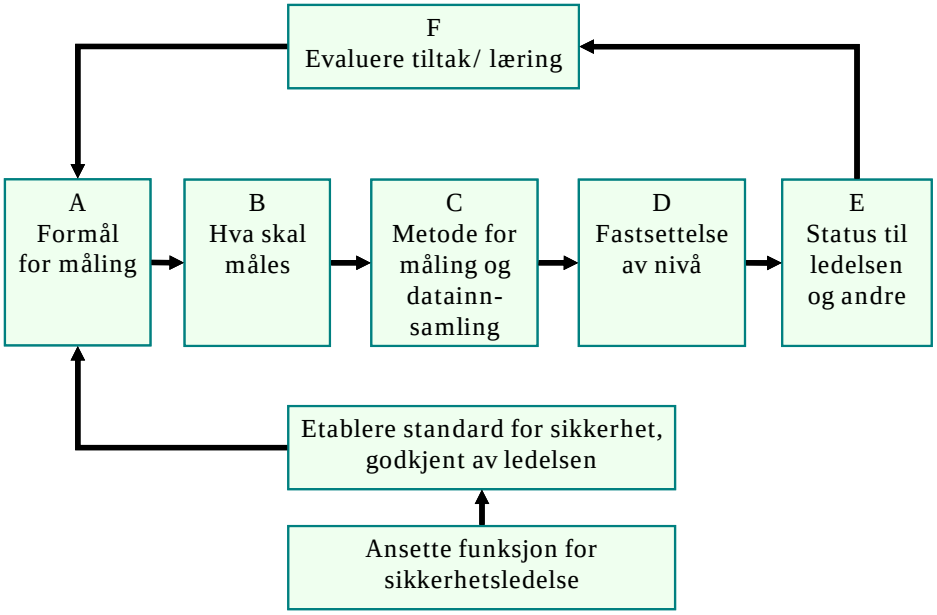
Analysene ble gjennomført kun for virksomheter som måler informasjonssikkerhet. Faktoranalysen viser at tre komponenter til sammen forklarer 47 % av variansen, hvorav komponent 1 forklarer hele 24 %. Innholdet i første komponent er alle variable knyttet til ledelse og bekrefter resultatet om at måling er ledelsesinstrumenter. En regresjonsanalyse viser at komponent 1 også har tilfredsstillende signifikant sammenheng med om virksomhetene måler informasjonssikkerhet.

Komponent 1 består av: Måling gir økt involvering fra ledelsen og mer oppmerksomhet på informasjonssikkerhet. Formålet med å måle er å kommunisere til ledelsen, og de viktigste andre måltall som benyttes av virksomhetene er salg og produksjon.

Komponent 2 har flere variable som understøtter resultatene knyttet til at måling av andre faktorer i virksomheten er viktig for de som måler informasjonssikkerhet. Komponent 2 har negativ samvariasjon med at måling av informasjonssikkerhet er et ledelsesinstrument. Regresjonsanalyse av Komponent 2 viser en tilfredsstillende signifikant ($p < 0,05$) sammenheng med medlemskap i ISF. I tillegg er det et signifikansnivå som nærmer seg tilfredsstillende for sammenhengen mellom Komponent 2 og utkontraktering ($p=0,06$).
De viktigste variablene i komponent 2 er av måling av andre parametere som kundetilfredshet, salg og produksjon.

6 Forslag til prosess for måling av informasjonssikkerhetsnivå

Et forslag til prosess for måling av informasjonssikkerhet er utviklet. Dette er gjort ut fra relatert forskning, teorier og praktiske metoder knyttet til måling av informasjonssikkerhet fra kapittel 2. I tillegg er erfaringer fra oppgavens spørreundersøkelse, intervjuer fra enkelte sikkerhetsansatte og egne erfaringer benyttet. Prosessen er trinnvis og er tenkt gjennomført fra trinn A til F som Figur 8 viser. Prosessen er ikke ment å være en detaljert kokebok, som gir løsninger på alle momenter knyttet til måling av informasjonssikkerhet. Den er ment å gi et grovt rammeverk for å kunne starte en prosess for måling av informasjonssikkerhet i virksomheter. Prosessen kan også knyttes mot risikovurdering i virksomheten [43].



Figur 8 Prosess for måling av informasjonssikkerhetsnivå

ISF kunne etter både Status Survey i 2000 og i 2003 konkludere med [47]

> «When it comes to improving security management enterprise-wide, the main message is that there are no quick wins, no silver bullet. »

Selv om det ikke er en bestemt faktor som er avgjørende for å forbedre en virksomhets informasjonssikkerhet, vil ledelsens oppmerksomhet kunne være en viktig faktor. Resultater fra spørreundersøkelsen konkluderer med at måling er et ledelsesverktøy, som skaffer fokus på informasjonssikkerhet hos ledelsen. Det beskrives at det er et stort

behov for kunnskap om informasjonssikkerhet til ledelsen i organisasjoner [73]. For å nå fram til ledelsen er det nødvendig å kommunisere på riktig måte. Måling av status og avsjekking av nivå blir en konkret kommunikasjonsform, som kan minne om statusavlevering på andre områder, som salg, produksjon og likestillingstall. Gjennom å få ledelsens oppmerksomhet vil en få økt fokus på informasjonssikkerhet, også hos andre ledere. Periodisk oppfølging kan gi ringvirkninger i virksomheten, og en får til slutt oppmerksomhet på alle de daglige rutinene som til sammen gir god informasjonssikkerhet. Som Etzioni [2] beskriver kan måling påvirke handlinger og reaksjoner.

6.1 Grunnmuren

or å lykkes med å måle informasjonssikkerhetsnivå viser kapittel 5.2.6 at det er viktig å ha en funksjon som sikkerhetsleder. En sikkerhetsleder kan være organisert under ulike funksjoner i virksomheten. Statistisk analyse med kjikvadrattest av resultater fra spørreundersøkelsen viser med tilfredsstillende signifikans at de fleste rapporterer til IT-avdeling og til administrerende direktør og styre. Det er også signifikante funn at måling oftere skjer hos virksomheter med flere enn fem ansatte i sentral sikkerhetsfunksjon. Sikkerhetsledere fra intervjuene understreker viktigheten av å ha en sterk pådriver og nevner bla følgende kritiske suksessfaktorer for å få til måling:

> «Først og fremst å nå ut i organisasjonen! Her har vi en sikkerhetskoordinator ute i hver enhet. Deretter at vi snakker samme språk, som gjør det mulig å gjøre faget kjent. Sikkerhet er en naturlig ting i hverdagen.»

> «Det er å rekke ut til linjen, og få den enkelte linjeansvarlige til å ta ansvar.»

En sikkerhetsstandard er neste trinn for å etablere en solid grunnmur. Det er etablert flere standarder i markedet, som ISO/IEC 17799 [9], CobiT [11] og Standard of Good Practice [10]. Likevel viser kapittel 5.2.7 at de fleste benytter egenutviklede sikkerhetsstandarder, oftest basert på anerkjente standarder i markedet. Måling av informasjonssikkerhet kan skje mot hele eller deler av sikkerhetsstandarden.
Beslutning om ansettelse av sikkerhetsleder og godkjenning av sikkerhetsstandard bør forankres hos virksomhetens ledelse.

6.2 Formål for måling (A)

Virksomheten bør diskutere og beskrive formålet med å iverksette en prosess for måling av informasjonssikkerhet [7] [32]. Formålet vil til en stor grad avgjøre om resten av organisasjonen ser nytten av å måle og vil delta i prosessen. Ved å integrere informasjonssikkerhet til virksomhetens øvrige organisasjon vil flere lettere kunne se formålet og være villige til å bidra og lære av prosessen. Et anerkjent ledelsesprinsipp er også [7]:

> «An activity cannot be managed if it cannot be measured».

To sikkerhetsansatte uttaler følgende som kritisk faktor for måling:

> «Kompetanse i måling og organisasjonsutvikling – i god kombinasjon!»

> «En må gi resultater som forretningssiden skjønner, gi resultater som kan påvirke sikkerheten og gjøre det enkelt å sette inn tiltak.»

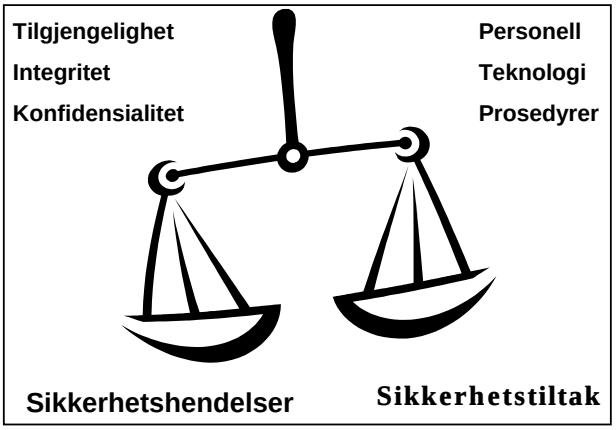
Flere formål kan gjerne brukes og anbefales av Etzioni [2], da det pleier å være mer effektivt enn bare ett. Dette vil tilfredsstille flere og gir plass for tilpasninger. Eksempel på formål kan være å kunne kommunisere eget sikkerhetsnivå til ledelsen, å kunne vise samsvar med standarder, lover og forskrifter eller å kunne avdekke behov for sikkerhetstiltak.

6.3 Hva skal måles (B)

Informasjonssikkerhet består av mange dimensjoner, og det må vurderes hvilke aspekter av informasjonssikkerhet som skal inkluderes i målingene. En sikkerhetssjef i en norsk virksomhet benytter et gammelt ordtak for å beskrive et komplekst valg ved måling av informasjonssikkerhet:

> «You measure what you treasure, and you treasure what you measure».

Du måler med andre ord det som verdsettes, og verdsetter det som måles. Ved valg av feil eller for mange parametere, kan de videre beslutningene bygges på feil grunnlag. Viktige parametere som burde hatt fokus blir kanskje uteglemt. Dette, og det Etzioni kaller overmåling [2] er en fare med å sette måling av informasjonssikkerhet i fokus. Dersom en imidlertid måler de riktige parametrene, vil dette medføre at virksomheten blir opptatt at de riktige tiltakene. Det er derfor viktig å ha definerte formål for måling, slik at virksomheten er bevisst hva den skal måle mot.
Målingene kan etablere en balanse mellom sikkerhetshendelser og sikkerhetstiltak. Figur 9 illustrerer at sikkerhetshendelser knyttet til tilgjengelighet, konfidensialitet og integritet kan måles samtidig som sikkerhetstiltak knyttet til personell, teknologi og prosedyrer måles. Resultater fra spørreundersøkelsen viser at det er viktig å få et helhetsbilde for hele virksomheten. Det anbefales å starte med et minimum antall metrikker [4] for deretter å etter hvert utvikle det i et modenhetsprogram [5] for å kunne håndtere og følge opp metrikkene [39]. Måling kan knyttes opp mot egen sikkerhetsstandard.



Figur 9 Både sikkerhetshendelser og sikkerhetstiltak

Flere dimensjoner bør måles [29], og en bør ikke utelukkende ha fokus på det tekniske. Erfaringer underveis vil bidra til at ledelse, kunder og interessenter påvirker valg av metrikker [23].
Som flere sier om prosessen:

«Det er en tredelt prosess» og
«Vi har flere prosesser...».

Resultater fra spørreundersøkelsen viser at avtaler med leverandører bør inkludere måling av informasjonssikkerhet. Resultatene viser også at virksomheter som har utkontraktert har større behov for å måle informasjonssikkerhet.

Mange fra spørreundersøkelsen måler også informasjonssikkerhet for egen IT-avdeling. Ved en eventuell senere utkontraktering vil interne prosesser for måling av informasjonssikkerhet kunne videreutvikles til å følge opp informasjonssikkerhet ved en eventuell utkontraktering. Ved utkontraktering kan også metrikkene benyttes for å beregne økonomiske straffereaksjoner for leverandøren [39].

6.4 Metode og verktøy for måling (C)

Teoriene setter strenge krav til metrikkene og fokuserer på kvantifiserbar informasjon [5,7,24]. Spørreundersøkelsens resultater viser at de fleste virksomheter har både kvantitative verdier og kvalitative beskrivelser av informasjonssikkerhetsstatus. Resultater fra spørreundersøkelsen viser at mange virksomheter benytter flere metoder for å måle informasjonssikkerhetsnivå, og at måling gjerne er tilpasset den enkelte virksomhet. Sikkerhetsorganisasjoner tilbyr egne medlemmer flere målemetoder, og spørreundersøkelsen viser at medlemmer av ISF benytter disse, også for benchmarking [21] [22] av informasjonssikkerhetsstatus. For øvrig benytter mange egenutviklede metoder. Deisz, Ingebrigtsen og Nilsen [39] beskriver bruk av flere ulike målinger satt sammen i egne utviklede regneark.

En større europeisk virksomhet forteller om månedlige og halvårlige rapporter, basert på NISTs retningslinjer [5]. Virksomheten har lagt vekt på en enkel presentasjonsmåte med bruk av regneark. Farger og layout er med på å forenkle og gjøre dette til et effektivt

ledelsesverktøy, som forretningsområdene må bidra med data til. Andre omsetter også NIST sine sikkerhetsmetrikker til praktisk bruk [32,38].

SBA Check [51] har en etablert metode med sjekklister for benchmarking av informasjonssikkerhetsnivå. Verktøyet er pr mai 2005 kjøpt av over 600 virksomheter. De fleste fornyer årlig sine lisenser og benytter derfor trolig verktøyet.

Risikoanalyser [44] [45] er et tankesett som ledere også er kjent med fra risikovurderinger på den forretningsmessige siden. Uavhengige gjennomganger og sikkerhetsrevisjoner, som f eks penetrasjonstest [27], er metoder spørreundersøkelsen viser blir benyttet. En sikkerhetsekspert fra en større norsk virksomhet uttaler at

> «Måling må forankres i det operasjonelle og driften. Det er letteste å hente data fra driftsmiljøet ».

Datainnsamlingen vil i mange tilfeller være arbeidskrevende, og målinger må ofte tolkes [6]. Målingene bør også kunne sammenlignes med andre eller egne tidligere målinger for å avdekke endringer. En utfordring er å få driftsmiljøer og systemeiere til å levere data til målingene. En sikkerhetsrådgiver uttaler:

> «Initially we did struggle to get them in a timely manner, but as we have moved forward the varying business units have refined their processes and now most units deliver the information on time. There are still some areas of the business that cannot answer all questions but again as time moves on these are becoming fewer»

En ISO standard for måling av informasjonssikkerhet er under utarbeidelse. Det er flere synspunkter knyttet til standard for måling av informasjonssikkerhet blant de som ble intervjuet:

> «Når du sier ISO, blir folk skrekkslagen! Det oppfattes som tungt og rigid.»

> «Jeg får problemer med alle disse standardene! Vi har prøvd mange av ISF-metodene, men standarder må knas uansett.»

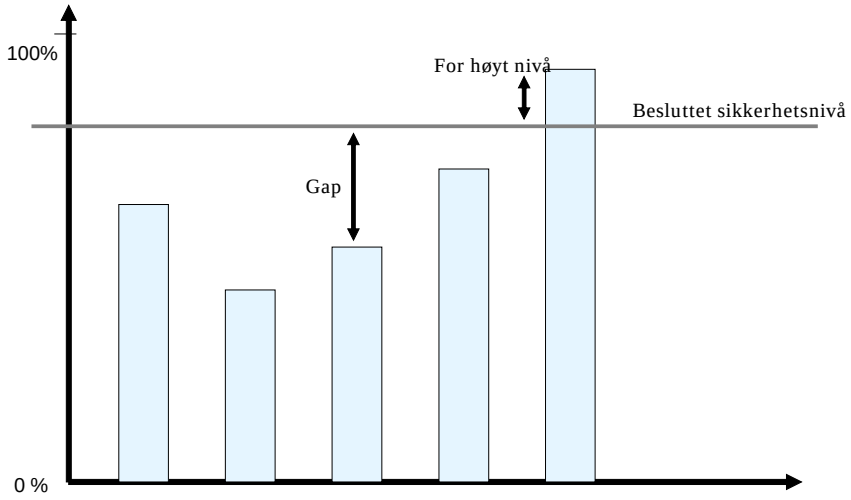
> «Sikkerhet er vanskelig å måle, så derfor - JA!»

> «Det ville ha hjulpet stort. »

6.5 Fastsettelse av nivå (D)

Å fastsette riktig nivå er en vanskelig beslutning. Et eksempel er skissert i Figur 10 og viser et besluttet nivå for informasjonssikkerhet i form av den vannrette linjen. Sikkerhetstiltak for ulike ressurser er skissert som søyler med ulike sikkerhetsnivå. I dette eksemplet er det besluttede sikkerhetsnivået satt likt for alle ressurser (systemer,

infrastruktur og informasjon). En kan imidlertid tenke seg grupperinger av ressurser ut fra kritikalitet med ulike sikkerhetsnivåer.
Nivået vil tilsvare akseptnivået i en risikovurdering [44] [45], og bør fastsettes av den instansen hvor resultater av målingen skal rapporteres. Et sikkerhetsnivå beskriver virksomhetens ambisjon for det som skal måles.



Figur 10 Nivå for informasjonssikkerhet

I denne spørreundersøkelse rapporterer to tredeler av virksomhetene status til administrerende direktør eller styret i virksomheter, og disse må derfor fastsette nivå på informasjonssikkerhet. En sikkerhetsleder sier:

> «Virksomhetens ledergruppe har årlig «ledelsens gjennomgang» hvor truslene, sikkerhetsstatus og i hvilken grad sikkerhetstiltakene anses som tilstrekkelige gjennomgås.»

Sikkerhetsnivået må besluttes ut fra diskusjoner om ressursenes kritikalitet og aktuelt trusselbilde, men kan vanskelig settes til «100 % sikkerhet». Trusselbilde er i stadig endring, og tiltakene henger gjerne etter i forhold til å sikre mot nye trusler. Ressurser som ligger under besluttet sikkerhetsnivå må innføre tiltak slik at det nås. Ressurser som ligger over besluttet sikkerhetsnivå bør vurdere kostnadene ved etablerte sikkerhetstiltak. Mål for informasjonssikkerhet kan vurderes i forhold til innsats på sikkerhetstiltak og i forhold til sikkerhetshendelser, slik Figur 9 viser. Oversikt over sikkerhetshendelser (incidents) kan fortelle om besluttet sikkerhetsnivå er riktig. Likevel kan det være at ressurser som har riktig sikkerhetsnivå opplever sikkerhetshendelser, men det kan likevel være viktig å holde på sikkerhetsnivåene [4]. Ved å beslutte sikkerhetsnivå og måle de ulike ressursenes sikkerhetsstatus opp mot dette, kan investeringer i sikkerhetstiltak enklere rettferdiggjøres.

En sikkerhetsrådgiver i en større virksomhet mener at absolutte nivåer kan være vanskelig å sette. Da er det bedre å beskrive nivået ut fra egen forandring i forhold til endringer i omgivelsene. Endring av trusselbilde vil f eks føre til endring av eget nivå. Andre uttaler:

«Det er ikke satt nivå. Folk sliter med det og er redde for å forplikte seg».

Benchmarking gir mulighet til å fastsette nivå ut fra endringer hos flere virksomheter. Resultater fra spørreundersøkelsen viser at mange av ISF-medlemmene benytter seg av Status Survey, som gir mulighet til å sammenlikne seg mot andre. En sikkerhetsdirektør i en virksomhet som benytter ISFs Status Survey uttaler at virksomheten har satt tre ulike nivåer ved måling.

> «Meget kritisk infrastruktur og systemer skal ligge på benchmarknivå til enhver tid, kritiske skal være på minst 25 % av benchmark, mens øvrige systemer og infrastruktur skal minst være på gjennomsnittet. »

6.6 Rapportering av status til ledelsen (E)

Spørreundersøkelsen viser at det viktigste formålet for måling av informasjonssikkerhet er å rapportere status til ledelsen, og de fleste rapporterer til toppledelsen. Rapportering bør beskrive virksomhetens fremtidige utvikling gjennom å se på forholdet mellom nåsituasjon og ønsket situasjon [30,58]. En sikkerhetsrådgiver sier:

> «Styret er begeistret for BMS. Vi bruker farger og piler for å vise status og trender. På den måten får en enkelt og greit oversikt over status med å kaste et blikk på rapportene. Det synliggjør avvik overfor styret og det fungerer bra.»

Ved utkontraktering vil leveransene og eventuelle sanksjoner ofte være av betydelig økonomisk størrelse. Ledelsen bør få presentert de økonomiske konsekvenser, samt hvilke faktiske trusler dette medfører for virksomheter.

6.7 Evaluere tiltak og læring (F)

Oppfølging og læring underveis er viktig i tankegangen knyttet til benchmarking [21] og balansert målstyring [30]. Samme tankegang bør benyttes for informasjonssikkerhet, for å kontinuerlig forbedre egen evne til å påvirke egen fremtid. Å sette mål har en sosiologisk kraft som påvirker handlinger og reaksjoner[2]. Veien kan i noen grad også være målet. To sikkerhetsrådgivere uttaler:

> «Prosessen for måling er et langt løp og vi er ikke i mål ennå. Vi er i en modningsprosess.»

> «Initially there was a large amount of resistance, with little or no understanding of what the benefits would be. But I think now the value of the figures is being seen and they also provide a focus for business units to improve. »

Dette forteller viktigheten av at innføring av informasjonssikkerhetsmåling må modnes, og måling må ses på som en prosess hvor egne erfaringer må danne grunnlag for forbedringer.

Ut fra målingene og statusrapportering, vil svake og sterke sider ved informasjonssikkerheten avdekke seg. Det er viktig å benytte denne informasjonen til å utarbeide planer for å evaluere nye eller endrede sikkerhetstiltak knyttet til systemer, infrastruktur, informasjon eller generelt i virksomheten, f eks i form av bevisstgjøringstiltak. Ved skriftlig statusrapportering vil det være naturlig med en skriftlig oppfølging av innføring og endringer av sikkerhetstiltak.

7 Oppsummering og konklusjon

Oppgavens intensjon er å bidra i arbeidet med å etablere god praksis for måling av informasjonssikkerhetsnivå. Rapporten beskriver litteratur fra forskningsarbeider og bøker, men også fra sikkerhetsorganisasjoner og praktiske måter å måle informasjonssikkerhet på fra næringslivet.

Oppgaven har gjennom en spørreundersøkelse skaffet erfaringer om måling av informasjonssikkerhet fra 49 virksomheter, som i hovedsak er meget store i nordisk sammenheng. Virksomhetene er i hovedsak nordiske, men enkelte er også fra andre land i Europa. Rapporten beskriver virksomhetene som deltok i spørreundersøkelsen og analyserer spørreundersøkelsens data. Resultatene ga svar på i hvilken grad virksomheter som anses som trendsettende innen informasjonssikkerhet måler informasjonssikkerhetsnivå og med hvilke metoder det skjer. Resultater fra spørreundersøkelsen bidro også til å få virksomhetenes vurderinger av hvilke effekter og formål det anses at måling av informasjonssikkerhetsnivå har.

For å utdype og komplettere data fra spørreundersøkelsen ble det i tillegg gjennomført oppfølgende intervjuer. Intervjuene bekreftet i noen grad resultater fra spørreundersøkelsen, og ga en dypere innsikt i prosesser og utfordringer i virksomhetene. Spørreundersøkelsen ga grunnlag for å drøfte statistiske data og intervjuene ga et innsyn ut over dette. Ut fra dette kunne oppgavens forskningsspørsmål besvares.

7.1 Hva kjennetegner virksomheter som måler informasjonssikkerhet?

Resultater fra spørreundersøkelsen viser at måling skjer hos 67 % av de som deltok. Måling av informasjonssikkerhet synes dermed å være viktig i utvalget av virksomheter som deltok i spørreundersøkelsen. Sammenfattet kan en si at virksomheter som måler informasjonssikkerhetsnivå:

- I større grad har utkontraktert deler av sine IT funksjoner
- I hovedsak tilhører finansiell eller tjenesteytende sektor
- Har fem eller flere ansatte i sentral sikkerhetsfunksjon
- Har ansatt sikkerhetsleder
- Er generelt mer opptatt av måling av andre faktorer, og er mer opptatt av å bruke balansert målstyring

Imidlertid bekreftet ikke resultater fra spørreundersøkelsen at medlemmer av ISF måler betydelig mer enn andre. Det er ikke avgjørende hvilket land virksomheten kommer fra og hvilken sikkerhetsstandard som benyttes.

7.2 God praksis for måling av informasjonssikkerhetsnivå

33 av virksomhetene som deltok i spørreundersøkelsen måler eget nivå for informasjonssikkerhet. Resultater fra spørreundersøkelsen avdekker øvrige forskningsspørsmål. I det følgende har alle resultater tilfredsstillende signifikans.

7.2.1 Hva anses å være formålet med å måle informasjonssikkerhet?

Resultater fra spørreundersøkelsen og intervjuer viser at de viktigste formålene med å måle er å kommunisere status på informasjonssikkerhet til ledelsen, å vise til samsvar med informasjonssikkerhet standard samt å gi ledelsen grunnlag for beslutninger. De som ikke måler begrunner dette i hovedsak med at ledelsen ikke etterspør måling av informasjonssikkerhet. Ut fra dette kan en konkludere med at måling av informasjonssikkerhet benyttes som et ledelsesverktøy i virksomhetene.

7.2.2 Hvilke metoder benyttes i dag for å måle informasjonssikkerhet?

Spørreundersøkelsens resultater viser at så mange som 85 % av virksomhetene bruker kvantitative metoder i sine målinger. Godt over halvparten kombinerer kvantitative og kvalitative målinger. Medlemmer av ISF benytter i større grad kvantitative metoder, og benytter også i stor grad metoden Status Survey fra ISF. Mange virksomheter benytter flere metoder for måling, noe som bygger opp om at det synes å være få bransjevise anerkjente metoder. Utover ISFs metoder er det bruk av uavhengige gjennomganger/ revisjoner, egenutviklede metoder og måling av sikkerhetshendelser som er mest vanlig. Måling av informasjonssikkerhet skjer i all hovedsak på bred basis i virksomheten samt i IT-avdelingen, noe som tyder på at måling er et ledelsesinstrument. Dette bekreftes av at hele 67 % rapporterer status på informasjonssikkerhet til styre eller administrerende direktør.

7.2.3 Hvilke effekter antas det at måling av informasjonssikkerhet gir?

En hypotese er at måling i seg selv har positiv effekt på sikkerheten. Resultater fra spørreundersøkelsen viser at svært mange vurderer at måling gir positive effekter i form av økt involvering av ledelsen i informasjonssikkerhetssaker, bedrede holdninger og gjør det lettere å lede og styre informasjonssikkerheten. Faktoranalyse viser at det finnes to komponenter som til sammen forklarer nærmere halvparten av variansen. Komponent 1 viser signifikant sammenheng med om virksomheter måler informasjonssikkerhet, og inneholder i hovedsak variable knyttet til ledelse.

7.3 Forslag til prosess for måling av informasjonssikkerhet

Internasjonale standarder for informasjonssikkerhet, som ISO/IEC 17799 og «Standard of Good Practice», er utarbeidet gjennom å samle erfaringer fra det praktiske liv på hvilke sikkerhetstiltak som er effektive. På samme måte ønsker denne rapporten å presentere et forslag til en prosess som kan bidra til å utvikle «god praksis» for måling av informasjonssikkerhet. En trinnvis prosess og viktige momenter for å etablere god praksis for måling av informasjonssikkerhetsnivå i en virksomhet er beskrevet. Prosessen er utviklet ut fra erfaringer fra spørreundersøkelsen og intervjuer, teorier om egenskaper og metoder for måling, praktiske metoder som finnes i næringslivet, samt egne erfaringer. Prosessen er ment å dekke viktige utviklingstrinn i en løpende prosess for å bidra til å styre informasjonssikkerhet i virksomheter. Dette med tanke på at arbeidet med informasjonssikkerhet skal støtte opp om virksomhetens måloppnåelse.

8 Videre arbeid

Denne rapporten bidrar i arbeidet med å etablere god praksis for måling av informasjonssikkerhetsnivå. Etablering av en god praksis er imidlertid et meget ressurs- og tidkrevende arbeid som krever praktisk erfaring og læring. Det vil derfor alltid være et generelt behov for å evaluere bruk av måling i virksomheter og forskning på området for å videreutvikle god praksis for måling av informasjonssikkerhetsnivå.

Denne oppgavens spørreundersøkelse har et ganske enkelt og lite omfattende spørreskjema. Interessant videre arbeid er å kunne avdekke flere detaljer om hvordan måling av informasjonssikkerhet skjer i virksomheter i dag. Dette kan kanskje gjøres ved bruk av en mer omfattende spørreundersøkelse, men det kan også være at andre metoder for datainnsamling gir et bedre datagrunnlag.
Det er også interessant å skaffe informasjon om andre typer virksomheter. Dette kan være virksomheter i andre verdensdeler eller mindre virksomheter i Norge og Norden.

En mer spesifikk videreføring av arbeidet er å teste i hvilken grad metodene for måling av informasjonssikkerhet faktisk verifisere kvaliteten på en virksomhets informasjonssikkerhet. Dette er et tema denne rapporten ikke har berørt, men som er interessant for å kunne bidra til å vurdere hvilke typer metoder som gir pålitelige resultater. Spørreundersøkelsen gir ikke svar på i hvilken grad målingene skjer med strukturerte metoder, da det ble lagt vekt på å ha et kortfattet spørreskjema. En grundig undersøkelse av metodikk og struktur knyttet til kvalitet på målingene vil måtte gå detaljert til verks og være svært arbeidskrevende, og kan ikke omfattes av denne oppgaven.

Denne rapporten har samlet inn resultater på hva virksomheter anser å være effekter av å måle. Det er imidlertid ikke gitt at de antatte effektene er de samme som de reelle effektene. Å undersøke hva de faktiske effektene ved måling anses heller ikke å kunne gjennomføres med dette prosjektets ressurser.

Enkelte elementer i modellen i Figur 1 på side 2 eksisterer ennå ikke, som f eks detaljert erfaring fra måling og metodebruk for måling av informasjonssikkerhet. Dette er informasjon som kan bygge videre på kunnskap denne oppgaven gir og kan være neste trinn for å videreutvikle god skikk og bruk for måling av informasjonssikkerhet.

9 Referanser

[1] Ministry-of-the-Environment, *Definition of good practice*, www.mos.gov.pl/mos/publikac/Raporty_opracowania/manual/glosry_1.html Visited 23.05.2005

[2] Etzioni A. 1964. *Modern Organizations*. New York/Oslo: Tanum - Norli,

[3] Lindøe P. 1988. *Målstyring - en flerfaglig tilnærming*. Stavanger: Rogalandsforkning, pp. 10.

[4] Frost B. 2000. Measuring Performance - *Using new metrics to deploy strategy and improve performance*.

[5] Swanson M, Bartol, Nadya, Sabato, John, Hash, Graffo, Laurie.2003; *Security Metrics Guide for Information Technology Systems*. NIST publication 800-55 (USA: US Department of Commerce).

[6] Wang C.1997; *A framework for security measurement*. (NISSC).

[7] Payne SC.2001; A Guide to Security Metrics. SANS Security Essentials GSEC Practical Assignment.

[8] Daler T, Gulbrandsen, Roar, Høie, Tore Audun, Melgård, Birger, Sjølstad, Torbjørn. 2002. *Håndbok i datasikkerhet*. Oslo: Tapir akademisk forlag,

[9] ISO. 2001. ISO Standard ISO/IEC 17799: *Code of practice for information security management*.

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

[11] ISACA, CobiT - *Control Objectives for Information and related Technology*, CobiT, www.isaca.org, Visited 30.03.2005

[12] Statens-offentliga-utredningar. 2004. *Informationssakerhet i Sverige och internatonellt*. Stockholm,

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

[14] Justisdepartementet, *Personopplysningsloven*, http://www.lovdata.no/all/nl-20000414-031.html, Visited 02.04.2005

[15] Forsvarsdepartementet, *Sikkerhetsloven*, http://www.lovdata.no/all/nl-19980320-010.html, Visited 02.04.2005

[16] IT-Sikkerhetsforum. 2004. Veiledning: *Lover og regler med betydning for informasjonssikkerhet* (Begrenset tilgang til medlemmer av norsk ISF).

[17] EU, *Data protection legislative documents*, http://europa.eu.int/comm/internal_market/privacy/law_en.htm, Visited 2.04.2005

[18] EU, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, http://europa.eu.int/comm/justice_home/fsj/crime/cybercrime/fsj_crime_cybercrime_en.htm, Visited 02.04.2005

[19] SEC U, *Sarbanes-Oxley Act of 2002*, www.sec.gov/divisions/corpfin/faqs/soxact2002.htm, Visited 30.03.2005

[20] ISF. 2003. *The Forums Standard of Good Practice*. Information Security Forum.

[21] Andersen B, Pettersen, Per-Gaute. 1995. *Benchmarking*. Otta: Tano AS,

[22] Information Security Forum I. 2005. *Information Security Status Survey 2005*: Running the Survey. London: ISF.

[23] Geisler E. 2000. *The metrics of science and technology*. Westport: Quorum books,

[24] Lowans PW.2002; *Implementing a Network Security Metrics Program*. (SANS Institute):11.
[25] Information Security Forum I. 2005. *Security Metrics Preliminary List*. London: ISF.
[26] Dictionary, *Dictionary online*, www.dictionary.com, Visited 30.302005
[27] ACSA. 2001. *Information System Security Attribute Quantification or Ordering*. In: Associates ACS, editor. Workshop on Information Security System Scoring and Ranking. Williamsburg, Virginia: ACSA and MITRE, pp. 70.
[28] Ladegård G. 1993. *Kriterier for effektiv målstyring*. Bergen: Norges Handelsshøgskole, pp. 19.
[29] Solms BV.2001; *Information Security - A multidimensional Discipline*. Computers Security:504-8.
[30] Hoff KG, Holving, Per Aksel. 2001. *Balansert målstyring*, Balanced Scorecard på norsk. Oslo: Universitetsforlaget,
[31] World Bank Integrator Unit and TRE Security Team Collaboration TWB. 2004. *Technology Risk Checklist* 7.3. The World Bank, pp. 31.
[32] KITH. 2004. *Indikatorer for informasjonssikkerhet*.
[33] Wood BJ, Bouchard, Julie F. *Red Team Work Factor as a Security Measurement*. (Cyber Defence Research Centre).
[34] Kredittilsynet. 2004. *Årlig nasjonal risikoanalyse*.
[35] McHugh J.2001; *Quantitative Measures of Assurance*: Prophecy, Process, or Pipedream? CERT/CC (Software Engineering Institute, Carnegie Mellon University).
[36] McCallam D. *The Case Against Numerical Measures for Information Assurance*. (Logicon Northrop Grumman Company).
[37] ISO, *International Organization for Standardization*, http://www.iso.org/iso/en/ISOOnline.frontpage, Visited 27.05.2005
[38] Bakås-Hagen-Orderløkken. 2003. *Sikkerhetsmetrikker for outsourcing av driftstjenester*. Gjøvik: Gjøvik University College, pp. 35.
[39] Deisz-Ingebrigstsen-Nilsen. 2004. *An evaluation of a practical case of measuring security in an outsourced environment*. Gjøvik: Gjøvik University College, pp. 27.
[40] Information Security Forum I. 2005. *Security Metrics*. London: ISF.
[41] Snekkenes E.2004; *Security Reporting*. (Søknadsnummer ES98333).
[42] Hagen J.2004; BAS5 - *Critical Information Infrastructure Protection*. (Forsvarets Forskningsinstitutt).
[43] Nygård A-R. 2004. *Risikostyrt informasjonssikkerhet i driftskontrollsystem*. IT. Gjøvik: Høgskolen i Gjøvik.
[44] standardiseringsforbund N. 1991. *Norsk Standard: Risikoanalyse NS 5814*.
[45] Broder JF. 2000. *Risk Analysis and the security survey*: Elsevier Science,
[46] Stamland F-A. 2004. *Is BS7799 worth the effort?* Gjøvik: Høgskolen i Gjøvik, pp. 80.
[47] Information Security Forum I. 2004. *Information Security Status Survey 2003*: Consolidated Results - Improving Security Management (enterprise-wide) Presentation. London: ISF.
[48] Information Security Forum I. 2000. *FIRM: Implementation Guide*. London.
[49] Information Security Forum I. 1993. *SARA: Simple to Apply Rsik Analysis for Information Systems*. London.
[50] Information Security Forum I. 1997. *SPRINT: Directory of Controls*. London.
[51] Dataföreningen. 1999. *SBA Check*. Stockholm: Dataföreningen.
[52] Regeringskanseliets_rättsdatabaser, *Personuppgiftslag*, http://62.95.69.15/cgi-bin/thw?%24%7BHTML%7D=sfst_lst&%24%7BOOHTML%7D=sfst_dok&%24

%7BSNHTML%7D=sfst_err&%24%7BBASE%7D=SFST&%24%7BTRIPSHOW%7D=format%3DTHW&BET=1998%3A204%24, Visited 20.05.2005
[53] Björk F. 2001. *Security Scandinavian Style*. Royal Institute of Technology. Stockholm: Stockholm University, pp. 120.
[54] Lawler EE, Nadler, David A, Cammann, Cortlandt. 1980. *Organizational Assessment*. Michigan: Wiley-Interscinece Publications,
[55] OGC OoGC-, *ITIL*, http://www.ogc.gov.uk/index.asp?id=2261, Visited 02.05.2005
[56] BSI, BS15000 *IT Service Management Standard*, http://www.bs15000.org.uk/, Visited 06.05.2005
[57] Holt J. 2004. *Getting the Right Service Level Agreement*. Computing Magazine.
[58] Wincentsen T, *Strategiimplementering ved hjelp av balansert målstyring*, http://www.umb.no/sevu/fap/foredrag/trond_wincentsen.pdf, Visited 17.03.2005
[59] Klepper J. 1992. *Internkontrollhåndboken*. Fredrikstad,
[60] Creswell JW. 2003. Research Design: *Qualitative, quantitative, and mixed method approaches*: SAGE Publications,
[61] Booth WC, Colomb, Greogory G, Williams, Joseph M. 2003. *The craft of research*. Chicago: The University of Chicago Press.,
[62] Holme IM, Solvang, Bernt Krohn. 2004. *Metodevalg og metodebruk*. Otta: Tano Aschehoug,
[63] Haraldsen G. 1999. *Spørreskjemametodikk etter kokebokmetoden*. Oslo: ad Notam Gyldendal AS,
[64] Bakås TH. 2004. *Forprosjektrapport for «god praksis for måling av informasjonssikkerhet»*. Gjøvik: Gjøvik University College, pp. 24.
[65] SSB, *Bedrifter etter ansattgrupper og næring pr 1. januar 2005*, http://www.ssb.no/emner/10/01/bedrifter/tab-2005-01-28-01.html, Visited 1.03.2005
[66] Løvås G. 1998. *Statistikk - for universiteter og høgskoler*. Harstad: Universitetsforlaget,
[67] McGraw-Hill. 2005. *SPSS Student*.
[68] Pallant J. 2005. *SPSS Survival Manua*l. Berkshire: Open University Press,
[69] Information Security Forum I. 2001. *Information Security Status Survey 2000*: Initial Overview of Key Statistics. London: ISF.
[70] IT-Sikkerhetsforum, *Medlemssider*, www.isf.no, Visited 11.05.2005
[71] Wold G. 2004. *Key factors in making Information Security Policies effective*. Gjøvik: Gjøvik University College, pp. 89.
[72] George A Marcoulides RHH. 1998. *Modern Methods for Business Reasearch*. Manao: Lawrence Erlbaum Associates,
[73] Krisberedskapsmyndigheten. 2005. *Samhällets informationssäkerhe*t. Stockholm, pp. 26.

Vedlegg A – Norsk spørreskjema

Lillehammer, 27.1.2005

MÅLING AV INFORMASJONSSIKKERHET
SPØRRESKJEMA

Det finnes mange teorier knyttet til måling av informasjonssikkerhet eller sikkerhetsmetrikker, men ingen standardiserte metoder. Noen virksomheter har også funnet sine praktiske metoder å måle status på informasjonssikkerhet på. Denne spørreundersøkelsen vil bidra til å etablere «god skikk og bruk» for måling av informasjonssikkerhet i virksomheter.

Denne spørreundersøkelsen er sent til deg fra Tone Hoddø Bakås. Jeg er seniorrådgiver i informasjonssikkerhet i Norges Bank, sentralbanken i Norge. I tillegg studerer jeg til master i informasjonssikkerhet. Studiet er et samarbeid mellom Høgskolen i Gjøvik og KTH i Stockholm. Tema for min masteroppgave er «GOD SKIKK OG BRUK FOR MÅLING AV STATUS FOR INFORMASJONSSIKKERHET». Kvaliteten på masteroppgaven vil avhenge av at du besvarer denne spørreundersøkelsen. Jeg setter derfor pris på om du kan avse 15 minutter til å fylle ut spørreskjemaet på de neste sidene. Det er like viktig at du fyller ut spørreskjemaet selv om din virksomhet ikke måler informasjonssikkerhet.

Dine svar vil bli analysert for å:

- Få en forståelse for hvordan virksomheter måler informasjonssikkerhetsstatus
- Indikere hvorfor måling utføres og effektene ved å måle informasjonssikkerhet
- Gi et bidrag for å etablere «god skikk og bruk» for måling av informasjonssikkerhet

De fleste spørsmålene besvares med å krysse av i bokser til høyre i spørreskjemaet. Jeg setter pris på om du legger inn tilleggskommentarer og utfyllende svar.

Alle svar vil bli behandlet konfidensielt og i oppgaven vil alle data bli anonymisert.

Vennligst returner spørreskjemaet før torsdag 10. februar 2005. ved:

- E-post til Tone.bakaas@norges-bank.no eller
- Post til Norges Bank, Tone Bakås,
  Stortorget 1, 2609 Lillehammer, NORWAY

På forhånd tusen takk for at du deltar i spørreundersøkelsen.

Med vennlig hilsen
Tone Hoddø Bakås

1 INFORMASJONSSIKKERHETS KRAV

For hvert spørsmål, vennligst kryss av relevante boks(er).

1.1 Hvilken standard for informasjonssikkerhet bruker din virksomhet?	
1. ISO 17799/ BS 7799 eller nasjonal variant	
2. Egen standard basert på ISO 17799	
3. Information Security Forums (ISF) Standard of Good Practice	
4. Egen standard basert på Standard of Good Practice	
5. COBIT fra ISACA	
6. Egen standard basert på COBIT	
7. The IT baseline Protection Manual (BSI)	
7. Egen standard	
8. Annet (vennligst spesifiser):	

1.2 Hvem har godkjent din virksomhets standard for informasjonssikkerhet?	
1. Styre/ Styrenivå	
2. Administrerende direktør	
3. Sikkerhetsleder/ Person med ansvar for informasjonssikkerhet	
4. Ingen/ ikke godkjent	
5. Annet (vennligst spesifiser):	

2 MÅLING AV INFORMASJONSSIKKERHETSSTATUS

Måling, metrikker, måltall, mål, eller indikatorer for informasjonssikkerhet er verktøy eller metoder for å gi relevant informasjon for informasjonssikkerhetsstatus og mulighet til sammenligning. Det kan også benyttes for å styre innsatsen knyttet til informasjonssikkerhet i virksomheten.

For hvert spørsmål, vennligst kryss av relevante boks(er).

2.1 Er det satt mål for eller måler virksomheten informasjonssikkerhet?	JA	NEI

SVARER DU NEI, VENNLIGST GÅ TIL SPØRSMÅL 3.1

2.2 I hvilken del av virksomheten er måling av informasjonssikkerhet iverksatt?	
1. I hele virksomheten	
2. I enkelte forretningsområder/ avdelinger	
3. I IT avdelingen	
4. Mot leverandører	
5. I kritiske forretningsprosesser	
6. I alle forretningsprosesser	
7. I kritisk infrastruktur	
8. Annet (vennligst spesifiser):	

2.3 Hvem har godkjent virksomhetens mål for informasjonssikkerhet?	
1. Styre/ Styrenivå	
2. Administrerende direktør	
3. Sikkerhetsleder/ Ansvarlig for informasjonssikkerhet	
4. Ingen/ ikke godkjent	
5. Annet (vennligst spesifiser):	

2.4 Hvem blir mål for og måling av informasjonssikkerhet rapportert til?	
1. Styre/ Styrenivå	
2. Administrerende direktør	
3. Sikkerhetsleder/ Ansvarlig for informasjonssikkerhet	
4. Systemeiere	
5. Leder for forretningsområde eller lignende	
6. Ingen	
7. Annet (vennligst spesifiser):	

2.5 Hvilke metoder brukes for å måle status for informasjonssikkerhet?	
1. Anerkjente indikatorer/ metoder innen indistrisektoren	
2. Tjenesteleverandøravtaler (SLA) med måltall/ metrikker	
3. Sertifisering i henhold til BS 7799	
4. Egen utviklet metode/ indikatorer	
5. Uavhengig gjennomganger/ ekstern revisjon med forhåndsbestemte indikatorer	
6. Egenevaluering med forhåndsbestemte indikatorer	
7. ISFs Information Security Status Survey	
8. Måling av sikkerhetshendelser og brudd	
9. SBA Check	
10. COBIT fra ISACA	
11. Ingen metoder	
12. Annet (vennligst spesifiser):	

2.6 Er målene/ metrikkene …	
1. Kvantitative (kvantifiserbar informasjon; prosenter, antall, frekvens, gjennomsnitt osv.)	
2. Kvalitativ (skriftlig fremstilling)	
3. Blandet (Noe kvantitativt og noe kvalitativt)	
4. Vet ikke	
5. Annet (vennligst spesifiser):	

3 GENERELT OM MÅLING

Om du måler informasjonssikkerhet eller ikke, vennligst besvar følgende spørsmål:
I hvilken grad er du enig i følgende utsagn? For hvert spørsmål, vennligst kryss av relevante bokser.

3.1 Måling av informasjonssikkerhet kan ha tilleggseffekter, som …	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Bedre holdninger til informasjonssikkerhet						
2. Økt involvering av ledelsen i informasjonssikkerhetssaker						
3. Mer oppmerksomhet på informasjonssikkerhet						
4. Det er lettere å budsjettere informasjonssikkerhet						
5. Det er lettere å prioritere mellom sikkerhetstiltak						
6. Informasjonen blir bedre beskyttet						
7. Det er lettere å lede og styre informasjonssikkerheten						
8. Ingen endring						
9. Annet (vennligst spesifiser):						

3.2 **Formålet med å måle informasjonssikkerhet er…**	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Grunnlag for beslutninger/ ledelses støttesystem						
2. Støtte til beregning av innsparing av investering (ROI)						
3. Å vise til samsvar med lover og forskrifter						
4. Å vise til samsvar med informasjonssikkerhetsstandard						
5. Å informere interessenter om informasjonssikkerhetsstatus						
6. Å kommunisere informasjonssikkerhet status til ledelsen						
7. Annet (vennligst spesifiser):						

3.3 Hvis du IKKE måler informasjonssikkerhet, er årsaken til det at …	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Det ikke er diskutert						
2. Informasjonssikkerhet ikke kan måles						
3. Måling av informasjonssikkerhet er vanskelig						
4. Det er ingen metoder eller verktøy for å måle						
5. Ledelsen spør ikke etter mål for informasjonssikkerhet						
6. virksomheten ikke måler, generelt sett						
7. Det ikke er noen spesiell årsak						
8. Annet (vennligst spesifiser):						

3.4 I min virksomhet blir følgende andre måltall rapportert til ledelsen:	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Økonomi; budsjett, regnskap og lignende						
2. Helse, miljø og sikkerhet (safety)						
3. Samfunnsrelasjoner						
4. Kundetilfredshet						
5. Salgstall						
6. Produksjonstall						
7. Likestilling (kjønn, rase, handikap osv.)						

8. Balansert målstyring (økonomi, kunde, prosess, opplæring)						
9. Vi måler *ikke*						

4 DIN VIRKSOMHET

For hvert spørsmål, vennligst fyll inn eller kryss av i relevant boks.

4.1 Antall ansatte	
Hvor mange ansatte er det i din virksomhet?	

4.2 Informasjonssikkerhetsledelse	
Hvor mange ansatte innen informasjonssikkerhet med konsernansvar?	

4.3 Din stilling	
Min tittel/ stilling er:	

4.4 Til hvilken funksjon rapporterer du? (kryss en boks)

1. IT		5. Risikoledelse	
2. Økonomi		6. Revisjon	
3. Personal (HR)		7. Juridisk	
4. Administrerende direktør/ Styre		8. Annet (vennligst spesifiser):	

4.5 Outsourcing	**JA**	**NEI**
Er deler av virksomhetens IT funksjon utkontraktert/ outsourcet		
Er alle IT funksjoner utkontraktert /outsourcet		

4.6 Hvilken sektor tilhører din virksomhet?

1. Bank, finans, forsikring		7. Offentlig sektor	
2. Kjemikalier, helse		8. Detaljhandel	
3. Energi, kraft		9. Leverandør av IT tjenester	
4. Industri/ produksjon		10. Telekommunikasjon	
5. Media, post		11. Transport	
6. Prosessindustri		12. Annet (vennligst spesifiser):	

5 TILLEGGSINFORMASJON

For å få et mer detaljert syn på måling av informasjonssikkerhet ønsker jeg å foreta noen intervjuer over telefon. Intervjuene vil ikke vare mer enn 20 minutter.

JA, min virksomhet er villig til å delta I et intervju for å gi mer detaljert informasjon om måling av informasjonssikkerhet.	
Navn på virksomhet:	Navn:
Telefonnummer:	E-post:

JA, jeg ønsker å motta resultater fra denne spørreundersøkelsen. Vennligst send de til (E-post adresse):

Tusen takk for at du fyller ut spørreskjemaet. Vær vennlig og returner det innen **torsdag 10. februar 2005** til **tone.bakaas@norges-bank.no** eller med vanlig post.

Vedlegg B – English questionnaire

Lillehammer, 27.01.2005

MEASURING INFORMATION SECURITY QUESTIONNAIRE

There are numerous theories of measuring information security or security metrics, but no standardised methods. Some organizations have found their practical way of measuring information security status. This survey will contribute to establish 'good practice' for measuring information security status in organizations.

This survey is sent from Tone H Bakaas. I work as a senior adviser in information security in the central bank of Norway. I'm also studying Master of Science in Information Security which is a co-operation between Gjøvik University College in Norway and KTH in Stockholm, Sweden. The topic of my master thesis is "GOOD PRACTICE OF MEASURING INFORMATION SECURITY STATUS". My thesis will be dependent on *your* contribution to this survey. I appreciated if you could spare 15 minutes to complete the questionnaire. I would like you to complete this questionnaire, even if your organisation doesn't measure information security status.

Your responses will be analysed to:

- gain an understanding of how organizations measure their information security status
- indicate why measuring is done and the effects of measuring information security
- give a contribution to establish 'good practice for measuring information security status'

You answer most questions by ticking boxes to the right in the questionnaire. Use of free spaces for additional comments or complementary answers is appreciated.

All responses will be treated in strictest confidence and in the thesis all data will be made anonymous.

Please return this questionnaire before Thursday 10 February 2005 by:

- E-mail at Tone.bakaas@norges-bank.no or
- Mail to Norges Bank, Tone Bakås,
  Stortorget 1, 2609 Lillehammer, NORWAY

THANK YOU in advance for taking part in this survey.

Yours sincerely

Tone H Bakaas

1 INFORMATION SECURITY REQUIREMENTS

For each question, please tick the relevant box(es).

1.3 Which standard/ policy for information security does your organisation use?	
1. ISO 17799/ BS 7799 or national equivalent	
2. Own standard based on ISO 17799	
3. Information Security Forums (ISF) Standard of Good Practice	
4. Own standard based on Standard of Good Practice	
5. COBIT by ISACA	
6. Own standard based on COBIT	
7. The IT baseline Protection Manual (BSI)	
8. Own standard	
9. Other (Please state):	

1.4 Who has approved your organizations information security standard/ policy?	
1. Board of directors/ Executive board level	
2. Chief Executive Officer (CEO)	
3. Security Manager/ Head of security / Person in charge of Information Security	
4. None/ not approved	
5. Other (Please state):	

2 MEASURING INFORMATION SECURITY STATUS

Measures, metrics, performance goals and objectives, indicators or target figures for information security are tools that give relevant information for information security status, which can be used for comparison purposes. It can also be used to manage the effort of information security in the organisation.

For each question, please tick the relevant box(es).

2.1 Does your organisation measure information security?	**YES**	**NO**

IF YOU ANSWER NO, PLEASE SKIP TO QUESTION 3.1

2.2 To which part of the organisation are measures for information security implemented?	
1. To the whole organisation	
2. To some business areas/ departments	
3. To the IT department	
4. To suppliers/ contractors	
5. To critical business processes	
6. To all business processes	
7. To critical infrastructure	
8. Other (Please state):	

2.3 Who has approved your organizations measures for information security?	
1. Board of directors/ Executive board level	
2. Chief Executive Officer (CEO)	
3. Security Manager/ Head of security / Person in charge of Information Security	
4. None/ not approved	
5. Other (Please state):	

2.4 To whom are goals and measures/ metrics for information security reported?	
1. Board of directors/ Executive board level	
2. Chief Executive Officer (CEO)	
3. Security Manager/ Head of security / Person in charge of Information Security	
4. System owners	
5. Head of business areas or equivalent	
6. None	
7. Other (Please state):	

2.5 Which methods do you use to measure your information security status?	
1. Acknowledged indicators/ methods for the industry sector	
2. Service Level Agreements with indicators/ metrics	
3. Certification with BS 7799	
4. Own developed method/ indicators	
5. Independent reviews / external audits with predefined indicators	
6. Self assessment with predefined indicators	
7. ISFs Information Security Status Survey	
8. Measuring of security incidents and breaches	
9. SBA Check	
10. COBIT from ISACA	
11. No methods	
12. Other (Please state):	

2.6 Are the measures / metrics…	
1. Quantitative (quantifiable information; percentage, number, frequency, average e.g.)	
2. Qualitative (written language)	
3. Mixed (Some quantitative and some qualitative)	
4. Don't know	
5. Other (Please state):	

3 MEASURING IN GENERAL

Whether you measure information security or *not*, please answer these questions:

To what extent do you agree in the following statements?

3.1 Measuring information security might have additional effects, such as …	In no all case				In case	Don't know
	1	2	3	4	5	
1. Better attitude to information security						
2. Increased management involvement in information security						
3. More attention to information security in the organisation						
4. Budgeting of information security is easier						
5. It is easier to prioritise between inf. security measures						
6. The information is better protected						
7. It is easier to manage and control information security						
8. No change						
9. Other (Please state):						

3.2 **The purpose for measuring information security is…**	In no all case				In case	Don't know
	1	2	3	4	5	
1. It is a basis for decisions/ management support system						
2. It supports return on investment (ROI)						
3. It shows compliance with laws and regulations						
4. It shows compliance with information security standard						
5. To inform stakeholders of the information security status						
6. Communicating inf. security status to the management						
7. Other (Please state):						

3.3 If you do NOT measure information security the reasons are …	In no all case				In case	Don't know
	1	2	3	4	5	
1. It has not been discussed						
2. Information security can not be measured						
3. Measuring information security is difficult						
4. There are no methods or tools for measuring						
5. The management don't ask for it						
6. We generally don't measure						
7. There are no specific reason						
8. Other (Please state):						

3.4 In my organisation these other goal figures are reported to the management:	In no case				In all case	Don't know
	1	2	3	4	5	
1. Economy: budget, annual accounts e.g.						
2. Health, environment and safety						
3. Community Relations						
4. Customer satisfaction						

5. Sales						
6. Production						
7. Equality (gender, race, disability e.g.)						
8. Balanced scorecard (finance, customer, process, learning)						
9. We do *not* measure						

4 YOUR ORGANISATION

For each question, please tick the relevant box(es).

4.1 Number of employees	
How many employees are in your organisation:	

4.2 Information Security Management	
Number of information security staff with enterprise-wide responsibility	

4.3 Your position and organisation	
My occupation/ designation:	

4.4 I report to (organisational level):			
1. IT		5. Risk Management	
2. Finance		6. Audit	
3. Personnel/ Human Relation		7. Legal	
4. CEO/ Board level		8. Other (Please specify):	

4.5 Outsourcing	**YES**	**NO**
Is part of the organisation IT function outsourced		
Is all IT function outsourced		

4.6 In which sector is your organisation?			
1. Banking, Finance, Insurance		7. Governmental Agencies	
2. Chemicals, Healthcare		8. Retail	
3. Energy, power		9. Suppliers of IT services	
4. Manufacturing, engineering		10. Telecommunications	
5. Media, postal services		11. Transportation Services	
6. Process Industries		12. Other (Please specify):	

5 ADDITIONAL INFORMATION

To get a more detailed point of view I would like to interview some organizations by phone. The interviews will take no longer than twenty minutes.

Yes, my organisation is willing to take part in an interview with more detailed questions on measuring information security.	
Name of organisation:	Name:
Phone number:	E-mail:

Yes, I would like to receive the results from this survey. Please, send it to (E-mail):

THANK YOU for completing this questionnaire. Please return it **before Thursday 10 February 2005** to tone.bakaas@norges-bank.no or by mail.

Vedlegg C - Intervjuguide

Du deltok en spørreundersøkelse fra meg tidligere i vinter om måling av informasjonssikkerhet.
Har du tid og anledning til noen ekstra spørsmål, knyttet til samme tema. Det vil ta ca 20 minutter. Det er ikke avgjørende hva du svarte på spørreundersøkelsen.
Er det greit at dine anonymiserte utsagn benyttes i min oppgave?

1. Kan du beskrive din virksomhets prosess for måling?

2. Hvordan settes nivået som det måles mot?

3. Kan du beskrive hva som måles (overordnet - detaljert – bredt – smalt – teknologisk ?)

4. Hva synes du er viktig med en målemetode?

5. Ville det vært enklere å måle om det hadde vært en standard (på samme måte som ISO 17799) for måling som hadde vært tilgjengelig i markedet?

6. Ut fra resultater i min spørreundersøkelse, tyder det på at virksomheter som bruker Balansert Målstyring også måler informasjonssikkerhet mer enn andre – Hvordan påvirkes du av andre målinger i virksomheten?

7. Hvem har initiert måling av informasjonssikkerhet, og hvorfor tror du det har skjedd?

8. Hva mener du er kritiske suksessfaktorer for å måle informasjonssikkerhet?

9. Hva mener du det betyr for styret/ administrerende direktør at måltall for sikkerhet rapporteres?

Vedlegg D - Frekvensanalyser fra spørreundersøkelsen

Frekvensanalyser, som viser antall og prosenter av de ulike alternativene pr variabel i spørreundersøkelsen er i det følgende beskrevet.

1 Informasjonssikkerhetskrav

Hvilken standard for informasjonssikkerhet bruker din virksomhet?	Antall	Prosent
1. ISO 17799/ BS 7799 eller nasjonal variant	20	40,8
2. Egen standard basert på ISO 17799	18	36,7
3. Information Security Forums (ISF) Standard of Good Practice	17	34,7
4. Egen standard basert på Standard of Good Practice	9	18,4
5. COBIT fra ISACA	5	10,2
6. Egen standard basert på COBIT	3	6,1
7. The IT baseline Protection Manual (BSI)	2	4,1
7. Egen standard	15	30,6

Hvem har godkjent din virksomhets standard for informasjonssikkerhet?	Antall	Prosent
1. Styre/ Styrenivå	25	51,0
2. Administrerende direktør	10	20,4
3. Sikkerhetsleder/ Person med ansvar for informasjonssikkerhet	11	22,4
4. Ingen/ ikke godkjent	3	6,1

2 Måling av informasjonssikkerhetsnivå

Er det satt mål for eller måler virksomheten informasjonssikkerhet?	Antall	Prosent
JA	33	67,3
NEI	16	32,7

I hvilken del av virksomheten er måling av informasjonssikkerhet iverksatt?	Antall	Prosent
1. I hele virksomheten	17	51,5
2. I enkelte forretningsområder/ avdelinger	10	30,3
3. I IT avdelingen	15	45,5
4. Mot leverandører	9	27,3
5. I kritiske forretningsprosesser	7	21,2
6. I alle forretningsprosesser	1	3
7. I kritisk infrastruktur	12	36,4

Hvem har godkjent virksomhetens mål for informasjonssikkerhet?	Antall	Prosent
1. Styre/ Styrenivå	9	27,3
2. Administrerende direktør	8	24,2
3. Sikkerhetsleder/ Ansvarlig for informasjonssikkerhet	19	57,6

Hvem blir mål for og måling av informasjonssikkerhet rapportert til?	Antall	Prosent
1. Styre/ Styrenivå	11	33,3
2. Administrerende direktør	14	42,4
3. Sikkerhetsleder/ Ansvarlig for informasjonssikkerhet	22	66,7
4. Systemeiere	16	48,5
5. Leder for forretningsområde eller lignende	18	54,5

I hvilken del av virksomheten er måling av informasjonssikkerhet iverksatt?	Antall	Prosent
1. Anerkjente indikatorer/ metoder innen indistrisektoren	2	6,7
2. Tjenesteleverandøravtaler (SLA) med måltall/ metrikker	9	30,0
3. Sertifisering i henhold til BS 7799	4	13,3
4. Egen utviklet metode/ indikatorer	12	40,0
5. Uavhengig gjennomganger/ekstern revisjon med forhåndsbestemte indikatorer	13	43,3
6. Egenevaluering med forhåndsbestemte indikatorer	7	23,3
7. ISFs Information Security Status Survey	17	56,7
8. Måling av sikkerhetshendelser og brudd	12	40,0
9. SBA Check	1	3,3
10. COBIT fra ISACA	3	10,0

Er målene/ metrikkene ...	Antall	Prosent
1. Kvantitative	9	26,5
2. Kvalitativ	5	14,7
3. Blandet	20	58,8

3 Generelt om måling

I det følgende er antall besvarelser for hver gradering summert.

Måling av informasjonssikkerhet kan ha tilleggseffekter, som ...	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Bedre holdninger til informasjonssikkerhet		1	8	23	15	1
2. Økt involvering av ledelsen i informasjonssikkerhetssaker		1	6	26	15	
3. Mer oppmerksomhet på informasjonssikkerhet		3	6	28	10	
4. Det er lettere å budsjettere informasjonssikkerhet		4	20	14	9	1
5. Det er lettere å prioritere mellom sikkerhetstiltak		3	9	24	12	
6. Informasjonen blir bedre beskyttet	3	6	15	18	5	1
7. Det er lettere å lede og styre informasjonssikkerheten		5	7	20	14	1

Formålet med å måle informasjonssikkerhet er...	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Grunnlag for beslutninger/ ledelses støttesystem		5	7	19	16	1
2. Støtte til beregning av innsparing av investering (ROI)	1	15	14	12	3	
3. Å vise til samsvar med lover og forskrifter	1	7	9	20	9	1
4. Å vise til samsvar med informasjonssikkerhetsstandard		4	7	16	18	1
5. Å informere interessenter om informasjonssikkerhetsstatus	1	4	8	21	13	
6. Å kommunisere informasjonssikkerhet status til ledelsen		1	3	20	23	

Hvis du IKKE måler informasjonssikkerhet, er årsaken til det at ...	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Det ikke er diskutert	6	5	5	6	2	
2. Informasjonssikkerhet ikke kan måles	10	4	3	6	0	
3. Måling av informasjonssikkerhet er vanskelig	1	3	4	13	3	
4. Det er ingen metoder eller verktøy for å måle	2	6	9	5	1	
5. Ledelsen spør ikke etter mål for informasjonssikkerhet	3	2	1	11	5	
6. virksomheten ikke måler, generelt sett	8	2	5	7	1	

I min virksomhet blir følgende andre måltall rapportert til ledelsen:	I lite grad				I stor grad	Vet ikke
	1	2	3	4	5	
1. Økonomi; budsjett, regnskap og lignende				4	44	
2. Helse, miljø og sikkerhet (safety)	2	1	2	16	23	3
3. Samfunnsrelasjoner	5	5	5	10	7	11
4. Kundetilfredshet	3	1	7	9	24	2
5. Salgstall	6			6	26	4
6. Produksjonstall	2	4	1	8	24	4
7. Likestilling (kjønn, rase, handikap osv.)	4	8	8	9	4	12
8. Balansert målstyring (økonomi, kunde, prosess, opplæring)	5	5	4	12	13	7

4 Uavhengige variable i spørreundersøkelsen

I det følgende er uavhengige variable og data om virksomheten presentert

Antall ansatte	Antall	Prosent
0 – 999 ansatte	14	28,6
1.000 – 4.999 ansatte	10	20,4
5.000 - 19.999 ansatte	10	20,4
Mer enn 20.000 ansatte	15	30,6

Antall ansatte innen informasjonssikkerhet	Antall	Prosent
Ingen ansatte	4	8,7
1 ansatt	16	34,8
Fra 2 – 3 ansatte	9	19,6
Fra 4 – 6 ansatte	7	15,2
Fra 7 – 10 ansatte	5	10,9
Fler enn 10 ansatte	7	15,2

Stilling/ tittel til respondent	Antall	Prosent
Sikkerhetsleder eller lignende	25	52,1
Leder av annen enhet, f eks IT-avdeling	6	12,5
Rådgiver eller konsulent	17	35,4

Respondent rapporterer til	Antall	Prosent
1. IT	25	52,1
2. Økonomi	2	4,2
3. Personal (HR)	2	4,2
4. Administrerende direktør/ Styre	17	35,4
5. Risikoledelse	6	12,5
6. Revisjon	2	4,2
7. Juridisk	1	2,1

Outsourcing	Antall	Prosent
Alle IT-funksjoner outsourcet	5	10,4
Deler av IT-funksjonene er outsourcet	29	60,4
Ikke outsourcet IT-funksjoner	14	29,2

Information Security Forum (ISF)	Antall	Prosent
Medlem	30	61,2
Ikke medlem	19	38,8

Bransjetilknytning	Antall	Prosent
1. Bank, finans, forsikring	9	18,4
2. Kjemikalier, helse	1	2,0
3. Energi, kraft	5	10,2
4. Industri/ produksjon	9	18,4
5. Media, post	3	6,1
6. Prosessindustri	3	6,1
7. Offentlig sektor	9	18,4
8. Detaljhandel	1	2,0
9. Leverandør av IT tjenester	5	10,2
10. Telekommunikasjon	2	4,0
11. Transport	2	4,0
12. Sentralbanker	8	16,3

Land	Antall	Prosent
Norge	23	46,9
Sverige	6	12,2
Danmark	5	10,2
Finland	5	10,2
Storbritannia	4	8,1
Andre europeiske	6	12,2

Vedlegg E – Utkast til «paper» basert på oppgaven

Why and how is information security measured?

Tone Hoddø Bakås, tohobak@online.no
Frode Volden, frode.volden@hig.no
Gjøvik University College/Høgskolen i Gjøvik

Abstract

This paper describes what is considered to be good practice for measuring Information Security (IS) level in organisations. Which methods are used to measure IS, what characterizes organizations that measure information security, and what effects the measurements are considered to have, are among the questions addressed in the study.

A survey was sent to a strategic selection of organisations that is considered to be among the leading within information security. They were asked whether they measure their level of information security, how they do it, and why. The survey got replies from 49 European organizations. For all the organizations, Information Technology is considered to be an important part of, or closely attached to their business. The organizations are mainly from the Nordic region and a few are from other European countries. They are mostly large organizations in a Nordic perspective, with employees working on information security.

Results from the survey shows that measurements primarily is considered to be a way to involve the organization's management on the importance of IS rather than a tool to actually improve security.

Keywords

Security Metrics, Information Security Status, Security Measurement, Benchmarking.

Introduction

Research and theories describe the need for, the benefit of, and methods for measuring information security level. It is however unclear to what degree IS actually is measured, and if measured; how and why it is done.

"Common practice" for measuring information security is not established. It's therefore a challenge to find practical methods for complying with security requirements and to be able to communicate the organisation's security level. This report seeks to describe good practice for measuring information security level in organizations that both clearly have a need for good IS, and that acknowledges this need.

This study aims to get a better picture of how IS measurements actually is performed today, what characterises organizations that have a measurement practice, and what motivates them to do so.

Related work

Why information security should be measured

A good number of works states that measurements of IS is important, but the theories do not describe practical use of measuring IS. Payne [1] focuses on qualities of good metrics and sketches a program for security metrics to improve the superiority of the security, and with that contribute to develop the organization as a whole. Geisler [2] means that measurement instruments can be characterized with different attributes by how good they are and describes steps in the construction of metrics. Solms looks at measuring information security as one of many dimensions [3]. Wang and Wulf emphasise the importance of having a clear definition of what is to be measured [4]. Knowledge of what is to be measured and the choice of security indicator is the beginning of the measuring process. Frost [5] describes the use and definition of metrics at a security management level. He implies that security metrics, framework and models for security measuring are in an early phase of development and that best practice has not yet been established for this area.

National Institute of Standards and Technology (NIST) has formulated guidelines to assist management in deciding where security initiatives should be implemented by use of security metrics and quantitative supported information [6]. KITH[5] has utilised security metrics from NIST [7] to practical use through indicators for information security for The Ministry of Health in Norway [8]. This is to enable the communication of status to management and public officials, follow the development within security areas and to implement measures within the health system. Bakås, Hagen and Orderløkken [9] have implemented the guidelines from NIST to develop security metrics for outsourcing of IT services. Deisz, Ingebrigtsen og Nilsen [10] have evaluated through a practical case, how one can measure information security in a contract from an outsourced environment.

Risk analyses [11] consider threats and vulnerabilities, and can be based on quantified and detailed numbers and cost/benefit assessments. Broder implies that risk analysis adds to quantitative possibilities and costs are an advantageous management tool [12]. Nygård [13] describes possible security metrics for a control system through use of risk analyses.

Methods from security organizations, trade and industry

Documentation and analysis, based on methods found in trade and industry can contribute to valuable information as to what is practicable and effective.

Independent reviews and security audits, for example, a penetration test [14], is recognized and practical methods. A penetration test can, to some degree, be compared to theories related to an Adversary Work Factor [15]. Many organizations use ISO 17799 [16] as a standard for information security and some chose to certify themselves against BS 7799, part 2. Stamland [17] means that organizations certified against BS7799-2 have a higher degree of maturity than organizations that have chosen the method in a more informal way. ISF [6]have established the standard «Standard of Good Practice» [18]] jointly with an own electronic questionnaire and benchmarking tool Status Survey [19]. A simplified version of the Status Survey, Health check, is

[5] Kompetansesenter for informasjonsteknologi for helse og velferd
6 Information Security Forum

under development. ISF also have methods for risk analyses [20] [21] [22]. The methods from ISF are only for members, but the standard is freely available. SBA Check, [23] is a checklist based software, with the objective of supporting the evaluation of information security in organizations. Björk [24] describes experiences of the methodical use of the tool. COBIT [25] is an accepted international standard for IT security from the audit organization ISACA and provides a framework and possibilities to measure information security.

General measuring methods

Etzioni [26] describes the function of measuring and setting the aim for organizations. An aim gives an orientation when describing a future condition and gives the possibility to judge proceed in relation to competence and effectiveness. Such future conditions have considerable sociological powers that influence actions and reactions.
The management also follow up different key numbers for IT through e.g. service level agreements [27]. Balanced scorecard is a management system for controlling to certain aims. [28-31].

Choice of methodology

A survey was sent to a strategic selection of organisations that were considered to be among the leading within information security. The studied population is meant to be a sample of "the best" organisations when it comes to information security, and is not meant to be a general representative sample. Therefore, the results from the study can not be generalised to organisations in general. The surveys population are large organisations where IT is considered to be an important part of, or is closely integrated to the business, and that acknowledge that IS is an important issue by having employees working with IS and having an IS policy.

The surveys population consists of organizations from different branches and different countries, but mainly from the Nordic region. They are mostly large organizations in a Nordic perspective, with employees working on information security issues. The average number of employees for the organizations is 16.250, with a median of 6.000. Many of them are member of Information Security Forum (ISF), an independent security organization and authority on information security. It is also expected that members of ISF are concerned on information security.

The questionnaires were sent to information security employees in 78 organizations, in most cases to IS managers. We received answers from 49 organizations, giving us a reply-rate of 63 %.

Data was analyzed using the statistical package SPSS ver 12. For all the statistical calculations a significance level (p-value) of 0.05 was accepted as satisfactory.

How is information security measured?

Which organizations measure information security?

33 of the 49 organizations (67%) in the study say they measure IS. Somewhat surprisingly, neither size of the organization nor the security standards in use have significant effect on whether IS is measured or not. Table 1 show that organizations in the financial sector or within the service branch are more likely than others to measure IS. Organizations that have outsourced parts (73%) of their IT functions are more likely to measure IS than those that have

not (43%). Organizations that have employed a security manager measure more (80%) than those that do not (52%). Measuring IS is time consuming and organizations that have five or more employees in a central security unit are more likely to measure (87%) than organizations with less than five employees (57%). Organizations that measure also seems to be more occupied with measurements in general and especially they which use balanced scorecard. These results are all satisfactorily significant ($p<0.05$).

Table 1 Measurements divided into different branches

Business branches	Total number	Numbers that measure	Parts that measure
Banking, finance, insurance	9	8	89 %
Service and trade	13	11	85 %
Production, industry	12	8	67 %
National banks	8	4	50 %
Public sector	7	2	29 %

Methods for measuring information security

Quantitative or qualitative measuring?

Literature concentrate on the use of quantitative measuring [1,6].Expectations are that practical solutions to a larger degree are based on qualitative methods. 85% of the respondents say they to some degree use quantitative measurements, and sustain the theories.

The survey indicates with satisfactory significance ($p<0.05$) that respondents that are not members of ISF, to a larger degree utilize only qualitative methods (33%). ISF members hardly use only qualitative methods (5%).

Methods used

Results from the survey shows that organizations that measure IS use more than one method to do so. The average number of methods is 2.5. This may be explained by the fact that there are no established method for IS measurement today, and that organizations therefore use a variety of methods. More than 50% of the respondents thought that IS is difficult to measure, but only a few mean this implies that information security cannot be measured.

Table 2 show that own developed methods, measuring of security incidents and independent reviews are frequently in use in organizations from the survey. The survey encompasses many organizations with ISF membership and 74% utilize methods and tools from ISF for measuring their information security status. ISF Status Survey [33] is the most used tool. The results indicate that few industrial standards can be found related to measuring information security.

Table 2 The methods for measuring information security

Which methods do you use to measure your information security status?	
ISFs Information Security Status Survey	55,9 %
Undependent reviews/ external audits with predefined indicators	38,2 %
Own developed methods/ indicators	41,2 %
MEasuring of security incidents and breaches	38,2 %

Service Level Agreements with indicators / metrics	29,4 %
Self assessment with predefined indicators	23,5 %
Other methods from ISF	16,0 %
Certification within BS 7799	11,8 %
COBIT from ISACA	8,8 %
Acknowledged indicator/ methods from the industri sector	5,9 %
SBA Check	2,9 %

Where does measurement take place?

The surveys results show that of the 33 organizations that does measure, approximately half of them focus on general measurements that cover the whole organization. They also measure the information security in the IT-departments, but not details in the business processes. Only 27% measure IS for suppliers and only 3% measure all business processes. Most organization (67%) report IS status to top management. This indicates that the measuring of information security happens to be a management tool.

Why is information security measured?

In the questionnaire, we asked the respondents to mark on a scale from 1 to 5, where 1 is ”in no cases” and 5 is “in all cases”, the purpose and effect of IS measurements.

Purpose for measuring

Based on theory we expected that showing compliance to laws, regulations and standard was the primary purpose for measuring IS. Table 3 shows what the survey population consider to be the most important purpose of IS measurements. The results from the survey indicate that measuring information security is regarded a management tool, more than a tool to directly improve IS. This is also confirmed by those who do not measure, as they state that the reason they don’t measure IS is that the management don’t ask for it.

Table 3 Purpose of measuring information security

(The figures show the average values on a scale from 1 to 5, whereby 5 is the highest)

The purpose of measuring information security is ...	Average value
To communicate information security status to the management	4.56
It shows compliance with information security standards	4.32
It is a basis for decisions/ management support system	4.13
To inform stakeholders of information security status	3.88
It shows compliance with laws and regulations	3.66
To support calculations of return of investments (ROI)	2.94

The survey results show that 67% of the organizations reports status to CEO or the board level in the organization. 23% reports to the system owner and the business areas. Only 10% say that reports stops at the security manager level.

The survey also shows that IS measurements are used for managing agreements for IT-functions that have been outsourced. These are often large economical agreements, and IS measurements are often included in the contracts with the service providers [10].

Effects of measuring

Based on theory, a hypothesis is that IS measurements directly improve IS. Personnel will improve in areas that are measured [5,26], and wish to be seen as capable in the eyes of their superiors and in their surroundings [37] [38].

Table 4The effects of IS measurements

(The figures show the average values on a scale from 1 to 5, whereby 5 is the highest)

The effects of measuring information security are:	Average value
Increased management involvement in information security	4.25
Better attitude to information security	4.19
It is easier to manage and control information security	4.16
More attention to information security in the organisation	4.06
It is easier to prioritise between information security measures	3.91
Budgeting of information security is easier	3.56
The information is better protected	3.47

The results from our study (table 4) show that direct effects on IS was rated the least important effect of measuring IS. This is somewhat a surprise, but supports the finding that IS measurements primarily is considered a management tool and an important awareness tool within information security.

A statistical analysis was performed in the form of a factor analysis for organizations that measure information security and for variables where the respondents have given their subjective opinions. The factor analysis shows that, all together, three components clarify 47% of the variation, whereby component 1 clarifies a whole 24%. The variables in this factor are all variables connected to management and confirm that IS measurements are a management tool.

Summary and conclusions

In our study, organizations that actually measure information security is mainly in the financial and service branches, and they have to a larger degree than other organizations outsourced their IT functions. They have employed security managers, have five or more employees in a central security unit and are more engaged in the use of balanced scorecard. The results from the survey shows that membership of ISF or geographical belonging does not influence to what degree organizations measure information security. Neither does the security standards the company say they follow.

The survey shows that quantitative methods are widely used for IS measurements. Well over half the organizations combine quantitative and qualitative measurements. Members of ISF, for the most, use quantitative methods and also, to a large degree, utilise the method Status Survey from ISF. Many organizations make use of several methods for measuring, which enhance that there seems to be few recognised methods for IS measurements. In addition to the methods of ISF, independent reviews and auditing, own developed methods and measuring of security incidents are most commonly used. IS measurements, occurs on a broad basis in the

organizations and in the IT-department, which indicates that measuring is a management tool. This is confirmed by the fact that a total of 67% report the status of information security to their board or CEO.

Results from the survey and interviews show that the most important purposes of measuring are to communicate the status of information security to management, to show conformity of information security standards and at the same time give management the basis for decision making. Those that do not measure state that the main reason they don't, is that the management does not ask for it. The conclusion based on this, is that IS measurements primarily is seen as a management tool. Positive effects on IS comes as secondary effect in the form of increased involvement by management in information security issues.

References

[1] Payne SC.2001; A Guide to Security Metrics. SANS Security Essentials GSEC Practical Assignment.

[2] Geisler E. 2000. The metrics of science and technology. Westport: Quorum books,

[3] Solms BV.2001; Information Security - A multidimensional Discipline. Computers Security:504-8.

[4] Wang C.1997; A framework for security measurement. (NISSC).

[5] Frost B. 2000. Measuring Performance - Using new metrics to deploy strategy and improve performance.

[6] Swanson M, Bartol, Nadya, Sabato, John, Hash, Graffo, Laurie.2003; Security Metrics Guide for Information Technology Systems. NIST publication 800-55 (USA: US Department of Commerce).

[7] Andersen B, Pettersen, Per-Gaute. 1995. Benchmarking. Otta: Tano AS,

[8] KITH. 2004. Indikatorer for informasjonssikkerhet.

[9] Bakås-Hagen-Orderløkken. 2003. Sikkerhetsmetrikker for outsourcing av driftstjenester. Gjøvik: Gjøvik University College, pp. 35.

[10] Deisz-Ingebrigstsen-Nilsen. 2004. An evaluation of a practical case of measuring security in an outsourced environment. Gjøvik: Gjøvik University College, pp. 27.

[11] Norsk standardiseringsforbund N. 1991. Norsk Standard: Risikoanalyse NS 5814.

[12] Broder JF. 2000. Risk Analysis and the security survey: Elsevier Science,

[13] Nygård A-R. 2004. Risikostyrt informasjonssikkerhet i driftskontrollsystem. IT. Gjøvik: Høgskolen i Gjøvik.

[14] ACSA. 2001. Information System Security Attribute Quantification or Ordering. In: Associates ACS, editor. Workshop on Information Security System Scoring and Ranking. Williamsburg, Virginia: ACSA and MITRE, pp. 70.

[15] Wood BJ, Bouchard, Julie F. Red Team Work Factor as a Security Measurement. (Cyber Defence Research Centre).

[16] ISO. 2001. ISO Standard ISO/IEC 17799: Code of practice for information security management.

[17] Stamland F-A. 2004. Is BS7799 worth the effort? Gjøvik: Høgskolen i Gjøvik, pp. 80.

[18] ISF. 2003. The Forums Standard of Good Practice. Information Security Forum.

[19] Information Security Forum I. 2005. Information Security Status Survey 2005: Running the Survey. London: ISF.

[20] Information Security Forum I. 2000. FIRM: Implementation Guide. London.

[21] Information Security Forum I. 1993. SARA: Simple to Apply Risk Analysis for Information Systems. London.
[22] Information Security Forum I. 1997. SPRINT: Directory of Controls. London.
[23] Dataföreningen. 1999. SBA Check. Stockholm: Dataföreningen.
[24] Björk F. 2001. Security Scandinavian Style. Royal Institute of Technology. Stockholm: Stockholm University, pp. 120.
[25] ISACA, CobiT - Control Objectives for Information and related Technology, CobiT, www.isaca.org, Visited 30.03.2005
[26] Etzioni A. 1964. Modern Organizations. New York/Oslo: Tanum - Norli,
[27] Holt J. 2004. Getting the Right Service Level Agreement. Computing Magazine.
[28] Lindøe P. 1988. Målstyring - en flerfaglig tilnærming. Stavanger: Rogalandsforkning, pp. 10.
[29] Hoff KG, Holving, Per Aksel. 2001. Balansert målstyring, Balanced Scorecard på norsk. Oslo: Universitetsforlaget,
[30] Ladegård G. 1993. Kriterier for effektiv målstyring. Bergen: Norges Handelsshøgskole, pp. 19.
[31] Wincentsen T, Strategiimplementering ved hjelp av balansert målstyring, http://www.umb.no/sevu/fap/foredrag/trond_wincentsen.pdf, Visited 17.03.2005
[32] Creswell JW. 2003. Research Design: Qualitative, quantitative, and mixed method approaches: SAGE Publications,
[33] Booth WC, Colomb, Greogory G, Williams, Joseph M. 2003. The craft of research. Chicago: The University of Chicago Press.,
[34] Holme IM, Solvang, Bernt Krohn. 2004. Metodevalg og metodebruk. Otta: Tano Aschehoug,
[35] Haraldsen G. 1999. Spørreskjemametodikk etter kokebokmetoden. Oslo: ad Notam Gyldendal AS,
[36] Information Security Forum I. 2005. The Forums Standard of Good Practice. Information Security Forum.
[37] Snekkenes E.2004; Security Reporting. (Søknadsnummer ES98333).
[38] Wold G. 2004. Key factors in making Information Security Policies effective. Gjøvik: Gjøvik University College, pp. 89.