Yngve Nordby og Christian Waale Hansen

Informasjonssikkerhet
atferd, holdninger og kultur

Nasjonal sikkerhetsmyndighet

Risiko og sårbarhetsstudier ved NTNU

Yngve Nordby og Christian Waale Hansen
Informasjonssikkerhet – atferd, holdninger og kultur

NTNU

Institutt for produksjons- og kvalitetsteknikk

Adresse: N-7491 Trondheim
Besøksadresse: S.P. Andersensvei 5
Telefon: +47 73 59 38 00
Telefaks: +47 73 59 71 17

TITTEL

Informasjonssikkerhet – atferd, holdninger og kultur

FORFATTERE

Yngve Nordby og Christian Waale Hansen

SAMMENDRAG

Denne rapporten presenterer et verktøy for å kartlegge og forbedre informasjonssikkerhetskultur. Verktøyet SjekkIT består av 30 sentrale spørsmål i en basispakke, samt en tilleggspakke med supplerende spørsmål. Arbeidet er en videreføring av et tidligere samarbeidsprosjekt mellom NTNU og NSM. SjekkIT er basert på sentrale teorier som er presentert i rapporten, og er utviklet i samarbeid med fageksperter og brukere av forrige versjon av verktøyet. Det presenteres to ulike tilnærminger for bruk av SjekkIT; en hvor svarene benyttes som grunnlag for statistisk bearbeiding og en hvor spørsmålene brukes til å lede en gruppeprosess. Spørreundersøkelsen er vedlagt bakerst.

ARKIVNØKKEL	RAPPORT NR.
03.2005	ROSS (NTNU) 200504
ISBN	DATO
82-7706-222-2	2005-04-18
SIGNATUR	SIDER/APPEND.
Marvin Rausand	54/51
NØKKELORD NORSK	NØKKELORD ENGELSK
INFORMASJONSSIKKERHET ORGANISASJON MENNESKELIGE FAKTORER SIKKERHETSKULTUR UNDERSØKELSE	INFORMATION SECURITY ORGANISATION HUMAN FACTORS CULTURE QUESTIONNAIRE

INNHOLD

Forord

Denne rapporten er skrevet i tilknytning til prosjektet "Informasjons-sikkerhet – atferd, holdninger og kultur", et samarbeid mellom Nasjonal sikkerhetsmyndighet (NSM) og Norges teknisk-naturvitenskapelige universitet (NTNU). Arbeidet er utført ved Institutt for industriell økonomi og teknologiledelse (IØT), seksjon for helse, miljø og sikkerhet (HMS), med professor Jan Hovden som hovedveileder. Arbeidet har også blitt veiledet fra Institutt for produksjons og kvalitetsteknikk (IPK) ved professor Marvin Rausand.

Bakgrunnen for prosjektet er at NSM og NTNU ønsker å rette fokus mot problemstillinger som har med menneskelige og organisatoriske faktorer ved informasjonssikkerhet å gjøre. Hovedarbeidet i prosjektet har vært å videreutvikle et undersøkelsesverktøy som ble utviklet i et tilsvarende prosjekt høsten 2002 og våren 2003. Videreutviklings-prosessen og det endelige verktøyet, som har fått navnet SjekkIT, presenteres i denne rapporten.

Vi vil takke alle veiledere, samarbeidspartnere og virksomheter som vi har hatt kontakt med i forbindelse utviklingen av SjekkIT. Spesielt gjelder dette for alle deltakerne på arbeidsseminaret i Trondheim 7. og 8. februar 2005, som bidro med verdifulle innspill til utviklingen av SjekkIT. Videre vil vi takke Hans M. Synstnes hos NSM for gode råd og god oppfølging av prosjektet. Vi har i løpet av prosjektet hatt et fruktbart samarbeid med seniorforsker Stig O. Johnsen ved Sintef og stipendiat Eirik Albrechtsen ved NTNU, som begge fortjener en stor takk for alle gode innspill og råd underveis i utviklingsprosessen.

Vi vil til slutt rette en stor takk til Hans M. Synstnes, Eirik Albrechtsen og Stig O. Johnsen som har bidratt med hvert sitt kapittel i rapporten.

Trondheim, 18. april, 2005

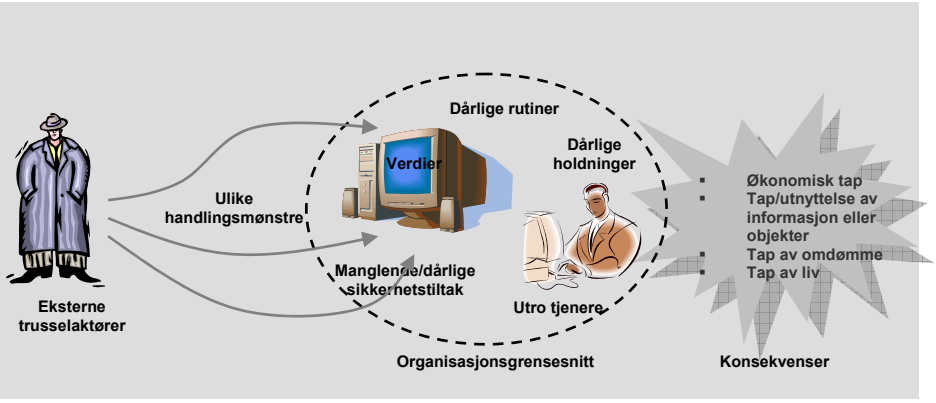
Yngve Nordby
yngven@gmail.com

Christian Waale Hansen
chrishan@samfundet.no

1. Bakgrunn

Innenfor fagfeltet informasjonssikkerhet har man tradisjonelt fokusert på strukturelle og tekniske aspekter som årsak og løsning i forhold til sikkerhetsproblemer. Vellykket sikkerhetsarbeid må imidlertid også sees i sammenheng med menneskelige og organisatoriske faktorer.[1] På bakgrunn av dette ønsker Nasjonal Sikkerhetsmyndighet (NSM) og Norges teknisk-naturvitenskapelige universitet (NTNU) å få et sterkere fokus på ikkestrukturelle aspekter som påvirker informasjonssikkerhet.

Gjennom sikkerhetsloven er alle virksomheter som behandler sikkerhetsgradert informasjon pålagt å drive forebyggende sikkerhetsarbeid. Lovverk og standarder ligger til grunn for dette sikkerhetsarbeidet, og dette har i stor grad ført til at arbeidet har blitt gjennomført med en regelbasert og strukturell tilnærming. I praksis viser det seg at informasjonssikkerhet er et svært komplekst fag-område, som i stor grad også påvirkes av menneskelige og organisatoriske faktorer (Kufås & Mølmann, 2003a). Gode og formaliserte rutiner er ikke nok, man må også fokusere på kunnskap, holdninger og atferd. Trusselbildet og konsekvensene virksomhetene må forholde seg til, er illustrert i Figur 1.

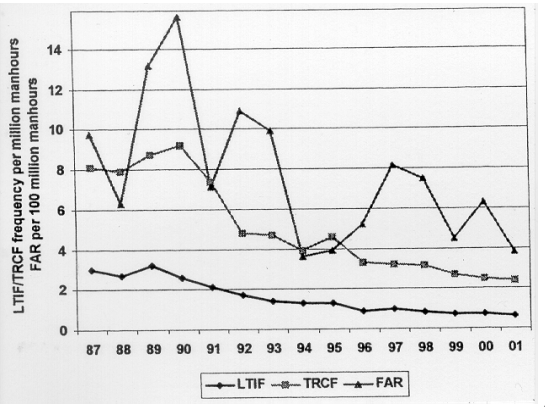


Figur 1: Trusselbilde og konsekvenser (Øksne & Furuseth, 2004)

Fokuset på menneskelige og organisatoriske faktorer innenfor sikkerhetsarbeid er ikke nytt. I 1986 startet oljeselskapet Shell et forskningsprosjekt for å forstå hvorfor uønskede hendelser inntreffer og hva som kan gjøres for å unngå dem. Dette resulterte i verktøyet

[1] For eksempel (Kufås & Mølmann, 2003a)

Hearts and Minds, som ser på sammenhengene mellom organisasjonskultur, individuell atferd og frekvensen av alvorlige uønskede hendelser. Shell har brukt verktøyet siden 1986 med en markant positiv effekt. Dette er illustrert i Figur 2 (Hudson & van der Graaf, 2002).



Figur 2: Shells erfaringer med Hearts and Minds[2]

Metodikken Hearts and Minds var grunnlaget for et tilsvarende samarbeidsprosjekt mellom NSM og NTNU høsten 2002 og våren 2003. Prosjektet "Informasjonssikkerhet og innsideproblematikk" utviklet et verktøy for å kartlegge holdninger, atferd og kultur i forhold til informasjonssikkerhet. Årets prosjekt har blitt gjennomført av Yngve Nordby og Christian Waale Hansen fra NSM/NTNU høsten 2004 og våren 2005, og er en videreføring av dette prosjektet.

Det resulterende verktøyet fokuserer på flere av elementene i organisasjonsgrensesnittet i Figur 1, og kan benyttes både for å måle tilstanden og for å forbedre holdninger, kunnskap, atferd og organisatoriske aspekter relatert til informasjonssikkerhet. Prosjektet er utført som et samarbeid mellom NSM og NTNU.[3] Sintef Teknologi og Samfunn, avdeling for Sikkerhet og Pålitelighet, har i tillegg vært involvert i prosjektet siden november 2004.

---

[2] Shell har hatt en kontinuerlig nedgang i antall uønskede hendelser fra 1987 og frem til 2001. FAR (Fatal Accident Rate) går sporadisk opp og ned, men også denne viser en jevn tendens mot færre ulykker. Det er verdt å merke seg at denne også er i størrelsesorden 100 ganger mindre enn LTIF (Lost Time Injury Frequency) og TRCF (Total Reportable Cases Frequency).

[3] NTNU er involvert gjennom Institutt for produksjons og kvalitetsteknikk (IPK) og Institutt for økonomi og teknologiledelse (IØT), fagseksjon Helse, miljø og sikkerhet (HMS).

2. Etabler en god sikkerhetskultur!

Hans M. Synstnes
Nasjonal sikkerhetsmyndighet
hsynstnes@mil.no

Nasjonal sikkerhetsmyndighet (NSM) ønsker et sterkere fokus på de kulturelle sidene av informasjonssikkerhetsarbeidet. For å sikre en vitenskapelig tilnærming samarbeider NSM med NTNU omkring sikkerhetskultur. Dette samarbeidet har resultert i rapportene *Informasjonssikkerhet og innsiderproblematikk (Kufås & Mølmann, 2003)* og denne oppfølgeren; *Informasjonssikkerhet – atferd, holdninger og kultur (Nordby & Waale Hansen, 2005).*

NSM er tildelt nasjonal fag- og tilsynsmyndighet innen forebyggende sikkerhetstjeneste. I enhver nasjon finnes det en kjerne av informasjon som er av kritisk karakter, og som må beskyttes særlig godt. På grunnlag av verdivurderinger er det viktig at aktuelle offentlige og private virksomheter finner frem til informasjon som har særlig betydning for vår nasjonale sikkerhet. De samme virksomhetene må igjen beskytte den sikkerhetsgraderte informasjonen gjennom hele dens livssyklus, fra den blir utarbeidet til den blir makulert eller avgradert. Hvordan sikkerhetsgradert informasjon skal beskyttes har NSM fastsatt gjennom forskriftene til sikkerhetsloven (se www.nsm.stat.no).

Fokus på sikkerhetskultur gir en mer helhetlig tilnærming til sikkerhetsarbeidet. Sentralt i begrepet sikkerhetskultur inngår begrepene holdning og motivasjon. Tradisjonelt har den forebyggende informasjonsbeskyttelsen hatt fokus på de strukturelle sidene av sikkerhetsarbeidet, og i mindre grad på de kulturelle – dette gjelder i stor grad også sikkerhetsloven med forskrifter. Med de strukturelle sidene menes her detaljerte regler, krav til organisering og fastsatte prosedyrer. Et helhetlig sikkerhetsarbeid fordrer imidlertid at de strukturelle og de kulturelle sidene ses i en sammenheng.

Målsetningene med sikkerhetsarbeidet kan vanskelig nås dersom motivasjon og holdninger svikter. Effekten av de ulike fysiske, personellmessige, IKT-relaterte og administrative tiltakene, som samlet skal beskytte informasjonen, vil bli redusert dersom ledelsen, de foresatte og den enkelte ansatte ikke etablerer en god sikkerhetskultur.

Sagt med andre ord vil effekten av de ressurser som settes inn for å beskytte informasjonen avta dersom forståelsen for, og viljen til å ta sikkerhetshensyn er mangelfull. Dersom ikke de kulturelle sidene av sikkerhetsarbeidet er tilfredsstillende kan dette gi seg flere utslag. For virksomheter underlagt sikkerhetsloven vil dette bety egeneksponering mot trusler som spionasje, sabotasje og i verste fall terrorhandlinger. For en markedsaktør vil mangelfull sikkerhetskultur i tillegg kunne medføre tap av markedsandeler og svekket omdømme.

NSM oppfordrer alle virksomheter til å arbeide målrettet for å oppnå en best mulig sikkerhetskultur. Med *SjekkIT-informasjonssikkerhet* tilbys et konkret verktøy som kan brukes til å måle en virksomhets sikkerhetskultur. NSMs målsetning med verktøyet er at det skal være såpass generelt at det kan benyttes av både offentlige og private virksomheter. Verktøyet kan brukes av alle virksomheter, som av lovpålagte eller andre grunner skal beskytte sensitiv informasjon. Med andre ord er ikke verktøyet avgrenset til bare å omfatte beskyttelse av sikkerhetsgradert informasjon i henhold til sikkerhetsloven

Verktøyet vil ikke fange inn alle sidene av sikkerhetskulturen, men vil likevel gi et godt grunnlag for å bedre bevisstheten rundt mål-setningene med informasjonssikkerhetsarbeidet. Interne målinger av sikkerhetskulturen anbefales gjennomført med jevne mellomrom for å finne endringer. Dels basert på slike målinger bør alle virksomheter utforme og gjennomføre tiltaksplaner for nettopp å bedre den interne sikkerhetskulturen.

Et avsluttende poeng her er at god informasjonssikkerhet er en styrkemultiplikator, som gjør oss mer motstandsdyktige mot uønskede hendelser. Utfordringen er gjerne å formidle dette, og la en slik forståelse avtegne seg gjennom en god sikkerhetskultur.

3. Innledning

Stipendiat Eirik Albrechtsen
Institutt for industriell økonomi og teknologiledelse, NTNU
eirik.albrechtsen@iot.ntnu.no

Perspektiver på informasjonssikkerhetsarbeid

Informasjonssikkerhet er et vidt fagfelt. Tradisjonelt har fagområdet i størst grad fokusert på teknologiske løsninger, kontroll/overvåkning og en mekanisk ledelsesform med dokumenterte policyer for ønsket individuell og gruppemessig atferd.[4] De senere årene har det imidlertid vært en bevegelse mot å også se på holdninger, sikker atferd og sikkerhetskultur. Dette er eksempelvis vist i Nasjonal strategi for IT-sikkerhet og OECDs retningslinjer for IT-sikkerhet. Dette er også illustrert av den gode mottakelsen NSM/NTNU-rapporten "Informasjonssikkerhet og innsideproblematikk"[5] av Kufås og Mølmann har fått, spesielt interessen for undersøkelsesverktøyet for kartlegging av holdninger og sikkerhetskultur. Det kan sies at man i informasjonssikkerhetsarbeidet har beveget seg fra "harde" redskap (teknologi og strukturelle ledelsessystemer) til også å inkludere "myke" sikkerhetshjelpemidler (holdninger, atferd, kultur, med mer). I et harmonisk sikkerhetsarbeid må begge disse prinsippene legges til grunn (se Figur 3)

[4] For mer om dette: se Albrechtsen, E og Grøtan, T.O, 2004. Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner. Kapittel i Lydersen, S. (red) Fra flis i fingeren til ragnarok, Tapir Akademisk Forlag.
[5] Kufås, I og Mølmann, R.A., 2003, *Informasjonssikkerhet og innsideproblematikk*. NTNU, ROSS-rapport nr. 200301.

Figur 3: Komplementære prinsipper i et harmonisk sikkerhetsarbeid

For en helhetlig tilnærming til sikkerhetsarbeider er det viktig å ha både "myke" og "harde/strukturelle" virkemidler tilgjengelig og i bruk:

- Det er selvfølgelig nødvendig med teknologiske løsninger og teknologisk fokus – det er tross alt sikring av IT-systemer og sikker bruk av dem det er snakk om. Informasjonssikkerhet er og blir først og fremst en teknisk gren, men det er også essensielt å fokusere på hvordan mennesker, organisasjon og samfunn bruker og nyttiggjør seg av IT. Informasjons-sikkerhetseksperten Bruce Schneier[6] treffer spikeren på hodet når han sier: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology".
- Det er også nødvendig å ha et dokumentert administrativt ledelsessystem på plass. Policyer, prosedyrer og retningslinjer er viktig å ha som en ledesnor for det praktiske sikkerhetsarbeidet. I flere tilfeller er det er også lovpålagt å ha disse på plass. Å plassere ansvar for operativt sikkerhetsarbeid vil også være viktig.

[6] Schneier, B, 2000:xii, *Secrets & Lies. Digital Security in a Networked World*, John Wiley & Sons

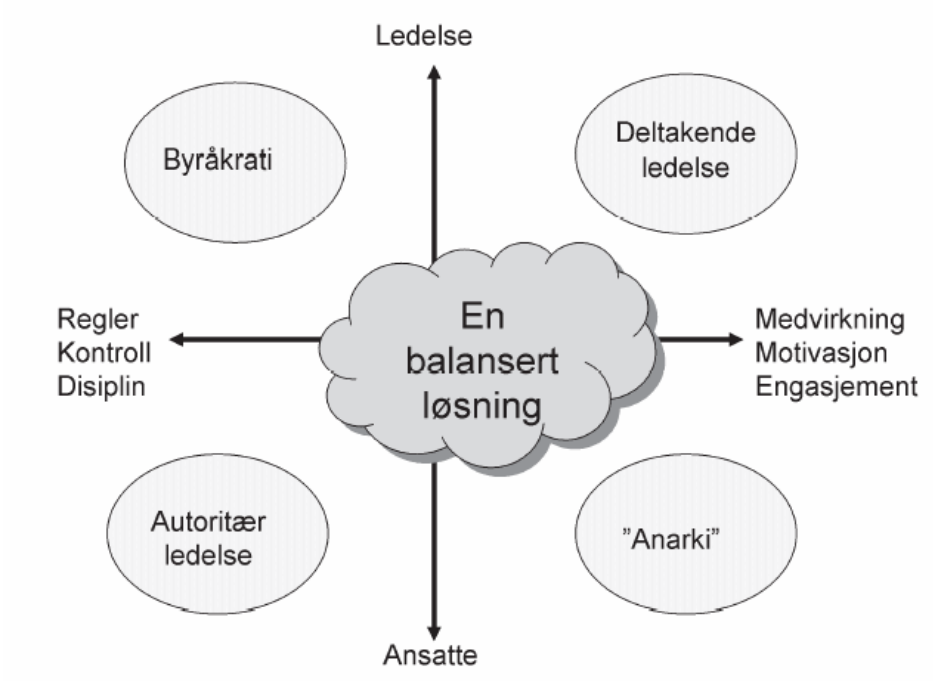
- ”Myk sikkerhet” vil i stor grad handle om hvordan man faktisk gjør sikkerhetsrelaterte ting i det daglige arbeidet. Den myke sikkerheten kan fordeles på individnivå og gruppenivå. På individnivå vil blant annet personlige egenskaper som holdning, kunnskap, kompetanse og erfaring sammen med en rekke omgivelser i virksomheten være viktig for hvor sikker eller usikker atferd den enkelte har.
- På gruppenivå vil den myke sikkerhet dreie seg om sikkerhetskultur. Sikkerhetskultur kan sies å være aspekter ved en kultur som påvirker sikkerheten i en eller annen retning. Det finnes mange forståelser av hva sikkerhetskultur er, et fellestrekk på forståelser er at det er noe som er delt (for eksempel verdier, praksis, oppfatninger, forståelser) av et kollektiv av et slag, som har blitt rotfestet i organisasjonen over tid. Sikkerhetskultur er noe mer enn summen av holdninger, det handler om noe som er rotfestet i organisasjonen og er delt av flere individer. Uavhengig av forståelse er det liten tvil om at en god eller dårlig sikkerhetskultur vil virke inn på sikkerhetsnivået.

Sikkerhetsnivået bestemmes av mange ulike virkemidler og egenskaper i en virksomhet, og samspillet mellom disse. I tillegg til de ovennevnte er det en rekke andre forhold i en virksomhet som påvirker sikkerhetsarbeidet, for eksempel hensynet til økonomi og effektivitet og hvilken kontekst virksomheten arbeider i. Det er derfor viktig å ha forståelse og innsikt i flere prinsipper i sikkerhetsarbeidet.

Det er viktig å få de ulike delene til å spille sammen på en hensiktsmessig måte, noe som kan være en utfordring. Det man faktisk gjør (hverdagsteorien) trenger ikke være i overensstemmelse med det dokumenterte systemet (søndagsteorien). Teori og praksis er som kjent to forskjellige ting. Dette trenger likevel ikke være en svakhet, den faktiske atferden kan være bedre enn den beskrevne ønskete atferden i det dokumenterte systemet.

Det er mange måter å organisere sikkerhetsarbeidet på. I Figur 4 er det vist at det er flere mulige tilnærminger til sikkerhetsledelse. En lokalt tilpasset blanding av å ansvarliggjøre både ledelse og ansatte, og en balansering mellom mål- og regelstyring, kontroll og disiplin på den ene siden og på den andre siden å stimulere til medvirkning og engasjement i sikkerhetsarbeidet vil gi en god balansert løsning for

sikkerhetsledelse. Tradisjonelt sett har informasjonssikkerhetsledelse, for eksempel illustrert av standarden ISO17799[7], plassert seg med et byråkratisk ledelsesfokus.[8] Dette perspektivet innebærer fokus på kontroll og overvåkning, samt en forlangning om at brukere skal følge dokumenterte forventinger om deres atferd.



Figur 4: Alternative tilnærminger til sikkerhetsledelse[9]

Som det går frem av ovenstående er det mange mulige perspektiver på informasjonssikkerhetsledelse og mange prinsipper som kan legges til grunn i sikkerhetsarbeidet. Oversikten som er forsøkt gjort ovenfor må ikke sees på som endelig, det finnes flere perspektiver og prinsipper som også kunne vært inkludert (for eksempel politikk og makt). Hensikten med oversikten har vært å nettopp vise at informasjons-sikkerhet kan og bør sees på med mange forskjellige brillepar.

[7] ISO 17799: Information Technology – Code of practices for information security management

[8] Albrechtsen, E og Grøtan, T.O, 2004. Gammeldags tenkning i moderne organisasjoner? Om IKT-sikkerhet i kunnskapsorganisasjoner. Kapittel i Lydersen, S. (red) Fra flis i fingeren til ragnarok, Tapir Akademisk Forlag.

[9] I Hovden, J, 2004, Sikkerhet i forskning og praksis. Et utfordrende mangfold med Sikkerhetsdagene som arena. Kapittel i Lydersen, S. (red) Fra flis i fingeren til ragnarok, Tapir Akademisk Forlag.

Å se informasjonssikkerhet med flere par briller, og dermed få flere perspektiver, vil gjøre at man 1) er i stand til å være klar over flere sikkerhetsmessige svakheter og dermed også 2) være i stand til å identifisere flere tiltak og virkemidler. Selv om det kan bli mer komplisert og uoversiktlig å ha flere perspektiver, gir det også mer spillerom for tiltak og virkemidler.

Posisjonering av SjekkIT

SjekkIT har i hovedsak fokus på ledelsesstrategier som er plassert oppe til venstre i figur 4. Verktøyet kartlegger hvordan det strukturelle systemet til en virksomhet fungerer, samt hvordan legale brukere (egne organisasjonsmedlemmer og innleid tredjepart) forholder seg til det strukturelle. Dermed får også SjekkIT inn samspillet mellom de to delene i figur 3 – hvordan man faktisk gjør ting (relatert til myke sikkerhetsprinsipper) og hvordan ting er planlagt å bli gjort (det strukturelle/harde sikkerhetsarbeidet). Et slikt perspektiv er et av flere viktige perspektiver på sikkerhetsarbeid.

SjekkIT favner dermed ikke alle perspektiver, men det favner et viktig perspektiv, nemlig forholdet mellom det systematiske, dokumenterte administrative systemet og hvordan man faktisk handler i en virksomhet. Dette er et viktig perspektiv, fordi det er vanlig å organisere sikkerhetsarbeidet på en slik måte at det administrative systemet gir klare retningslinjer for hvordan sikkerhetsarbeidet skal fungere. Det er derfor nyttig å vurdere hvorvidt faktisk atferd på individ og gruppenivå forholder seg til det planlagte systemet.

Med denne bakgrunnen kan man stille seg spørsmålet: er SjekkIT et revisjonsverktøy? En rekke av spørsmålene kan kjennes igjen som tema i en revisjon. I en revisjon forsøker man imidlertid å avdekke avvik i forhold til en norm – det gjør ikke SjekkIT. SjekkIT er mer et diagnoseverktøy som finner ut hvor virksomheten har vondt og hva det skyldes. Det går dermed dypere enn et revisjonsverktøy. I så måte må det sies at verktøyet har en styrke i forhold til tradisjonelle revisjons-verktøy.

Det kan selvfølgelig argumenteres for en rekke andre perspektiver som med fordel kunne vært tatt med i verktøyet. På den annen side ville dette ført til et stort batteri med spørsmål og svaralternativer. Omfanget av undersøkelsen kunne blitt så stort at størrelsen hadde blitt en svakhet ved verktøyet.

Holdninger, atferd og sikkerhetskultur

Disse begrepene har dukket opp som "moteord" innen fagområdet informasjonssikkerhet over de siste årene. Begrepet sikkerhetskultur har spesielt blitt brukt mye de siste årene, og det er nesten fristende å spørre seg hvilke problemer som ikke kan løses ved "å produsere" en ny kultur. Siden SjekkIT legger til grunn at " verktøyet forsøker å gi et bilde av atferd, holdninger og kultur som er relatert til informasjons-sikkerhet", drøftes disse begrepene kort i det videre.

Det legges mange forskjellige forståelser til grunn for holdninger, atferd og kultur, og det er heller ikke at det er så viktig at alle er enige i hva som legges i det forskjellige. Samme hva man mener og tror, er det viktig for sikkerhetsnivået å arbeide med holdninger, atferd og kultur i ulike former.

Holdninger kan defineres som en psykologisk tendens som uttrykkes ved å evaluere et objekt i grader av favør eller disfavør.[10] Holdning til informasjonssikkerhet kan derfor sies å være bestemt ut fra en persons evaluerende reaksjon ovenfor sikkerhetsrelaterte forhold. Holdninger er basert på en trekomponent modell[11], bestående av en kognitiv-, en affeksjons- og en atferds komponent. I SjekkIT har man valgt å vurdere den kognitive komponenten ved å betrakte hvilke tanker og oppfatninger folk har om arbeidet med informasjonssikkerhet.

Atferd er bestemt av mange ulike faktorer. Holdninger er bare en av disse. Andre forhold som påvirker atferd relatert til informasjons-sikkerhet er teknologiske og fysiske beskrankninger, personlige egenskaper, økonomiske rammebetingelser, kulturelle forhold, situasjonelle forhold, oppfatning av risiko og administrative ramme-betingelser. Alle disse forholdene påvirker hverandre gjensidig. I SjekkIT er mange av de atferds relaterte spørsmålene og svar-alternativene rettet mot hvordan de administrative systemene påvirker atferd. I forhold til den posisjoneringen verktøyet har tatt så er dette en

[10] Eagly, A.H & Chaiken, S, 1993, *The psychology of attitudes*. Harcourt Brace Jovaovich College Publishers.

[11] Den kognitive komponenten inneholder tanker og oppfatninger som folk knytter til objektet, og uttrykker positive, negative eller nøytrale evalueringer av objektet. Den affektive komponenten består av følelser, stemninger og emosjoner som folk opplever i relasjon til objektet. Atferdsmessige evaluerende responser av de handlinger og intensjoner om handling som folk utviser overfor objektet. Kilde: Aarø, L.E. og Rise, J: *Den menneskelige faktor*, Skadeforebyggende Forum, SF-rapport 5-96

riktig vinkling. Det er imidlertid viktig å være klar over at atferd også påvirkes av mange andre forhold, spesielt vil atferd i en teknisk gren som informasjonssikkerhet i stor grad kunne påvirkes av teknologiske virkemiddel.

Sikkerhetskultur kan forståes på mange ulike måter. For en god beskrivelse av informasjonssikkerhetskultur anbefales artikkel av Ivar Kufås[12] i NSM/NTNU-rapporten "Innsideproblematikk og informasjonssikkerhet". Sikkerhetskultur kan sies å være aspekter ved en organisasjonskultur, eller subkultur av denne, som påvirker sikkerheten i negativ eller positiv retning. Det kan sies å være to hovedtilnærminger til organisasjonskultur: et fortolkende[13] perspektiv og et funksjonalistisk[14] perspektiv. SjekkIT har basert seg på et funksjonalistisk perspektiv. Dette perspektivet er ofte forstått i tre nivåer[15]: 1) grunnleggende antagelser (implisitte antagelser om hva som faktisk styrer atferd, hvordan folk tenker og føler om ting), 2) uttrykte verdier (holdninger til folk, atferd, potensielle trusler eller regler) og 3) artefakter (konkrete uttrykk, f.eks historier og arbeids-miljø). Ved å benytte SjekkIT får man en indikasjon på kulturelle aspekter ved informasjonssikkerhet i forhold til det administrative systemet, i form av en diagnose basert på enkeltindividers syn på artefakter og uttrykte verdier.

Sikkerhetskultur kan forståes både mer i dybden og bredden enn det SjekkIT gir mulighet til. SjekkIT ser eksempelvis ikke på interaksjon mellom folk (handling, samtale, forståelse av informasjonssikkerhet), ikke på hvordan negative og positive sikkerhetsforhold har blitt sosialisert og legitimert som måten man faktisk handler på uavhengig av det formelle systemet, ikke på hvordan organisasjonen håndterer målkonflikter som berører sikkerhet og ikke på om virksomheten har

---

[12] Kufås, I, 20032: A framework for information security culture; could it help on solving the insider problem". I Kufås, I og Mølmann, R.A., 2003, *Informasjonssikkerhet og innsideproblematikk*. NTNU, ROSS-rapport nr. 200301.

[13] Et fortolkende perspektiv har sine røtter i sosialantropologi, og har som mål å forstå og tolke kulturene, og er ikke opptatt av å "forbedre" kulturen. Sikkerhetskultur og kan sies å være et felles sett av ideer, verdier, holdninger og normer som en gruppe av mennesker føler seg tilknyttet, og som er del av tradisjoner og tidligere sosialisering.

[14] Et funksjonalistisk perspektiv har sine røtter i psykologi-feltet. Dette perspektivet er mer normativt enn det fortolkende, og sier at det finnes en ideal tilstand som man kan tilstrebe. I korte ordelag så er man ute etter å forstå (og måle) i hvilken grad kulturelle aspekter har innflytelse på holdninger som igjen kan lede til konkret atferd.

[15] Schein, E, 1992, *Organizational Culture and Leadership.* Jossey-Bass

organisatorisk redundans (evnen til å rådspørre seg med andre, advare, korrigere og holde øye med hverandre).[16]

SjekkIT kartlegger visse deler av en kultur på et høyt nivå uten å gå i dybden på kulturen. Det er viktig å være klar over at dette er et perspektiv på sikkerhetskultur, kultur kan forståes og tolkes på mange andre måter. En organisasjon vil også bestå av mange subkulturer, som hver for seg og måten de samarbeider på kan ha stor innvirkning på sikkerhetsnivået. For eksempel vil en dårlig sikkerhetskultur i IT-driftsavdelingen være langt mer kritisk enn en dårlig sikkerhetskultur blant sluttbrukere, da dette kan føre til at IT-systemene er konfigurert på en sikkerhetsmessig dårlig måte.

Avslutning

SjekkIT er et nyttig diagnoseverktøy for en virksomhet. Ved hjelp av verktøyet kan man stille en diagnose på hvor virksomheten er syk og hvor den er frisk, og kunne sette inn gode virkemiddel for å bli bedre. SjekkIT fokuserer på ett av flere perspektiver ved arbeidet med informasjonssikkerhet. Det er viktig å ikke glemme at informasjons-sikkerhet favner mer enn det perspektivet SjekkIT kan hjelpe med å kartlegge.

Å bruke SjekkIT i en virksomhet vil være positivt for sikkerheten uavhengig av verktøyets resultater. For den enkelte ansatte vil det å besvare skjemaet i seg selv føre til at man gjør seg tanker om og tar lærdom om sikkerhet – og kanskje føre til at den enkelte får en mer sikker atferd.

Da gjenstår det bare å ønske lykke til med bruken av verktøyet. Forhåpentligvis vil det bidra til en sikrere hverdag.

[16] For flere "helseindikatorer" for sikkerhetskultur kan Hale (2000) og Rosness (2001) anbefales.

4. Teoretisk bakgrunn

Organisasjoner kan betraktes fra ulike perspektiver. Noen av disse perspektivene er allerede nevnt i kapittel 3.[17] Bolman & Deal (2004) hevder at man kan betrakte organisasjoner ut fra fire perspektiver. De sentrale elementene er samlet i tabellen under:

	Strukturelt perspektiv	Human Resource perspektiv	Politisk perspektiv	Symbolsk perspektiv
Metafor for organisasjonen	Fabrikk eller maskin	Familie	Jungel	Karneval, tempel, teater
Sentrale begreper	Regler, roller, mål, politikk, teknologi, omgivelser	Behov, ferdigheter, relasjoner	Makt, konflikt, konkurranse, organisasjons-politikk	Kultur, mening, metaforer, ritual, seremoni, historier, helter
Bilde av ledelse	Sosial arkitektur	Myndiggjøring	Advokat eller politiker	Inspirasjon
Grunnleggende ledelses-utfordringer	Å forme strukturen etter oppgaven	Å tilpasse organisasjonen og med-lemmenes behov til hverandre	Å utvikle et makt-grunnlag og bestemme hva som må gjøres	Å skape tro, skjønnhet og mening

Hovedperspektivet i denne rapporten vil være den symbolske fortolkningsrammen, med et fokus på organisasjonskultur og sikker-hetskultur, som presenteres nærmere i de påfølgende underkapitlene.

Organisasjonskultur

Kultur kan defineres på en mengde måter, og organisasjonskultur har blitt et ofte brukt ord for å forklare hvordan ting gjøres i organisasjoner. Det sies at organisasjonskulturen er essensen av en organisasjons uformelle struktur. Men hva er så kultur? Dette kapittelet vil gi en oversikt over sentrale teorier innenfor kulturfeltet. Hofstede (1991) definerer kultur som:

> *Den kollektive programmeringen av hjernen som skiller med-lemmene av en menneskelig gruppe fra en annen.*

[17] De ”myke” og ”harde” aspektene ved sikkerhetsarbeid vises for eksempel i figur 3, ulike tilnærminger til sikkerhetsledelse vises i figur 4.

Schein (1992) definerer kulturen til en gruppe som:

> *Et mønster av antakelser – skapt, oppdaget eller utviklet av en gitt gruppe etter hvert som den lærer å mestre sine problemer med ekstern tilpasning og intern integrasjon – som har fungert tilstrekkelig bra til at det blir betraktet som sant, og som derfor læres bort til nye medlemmer som den rette måten å oppfatte, tenke og føle på i forhold til disse problemene*

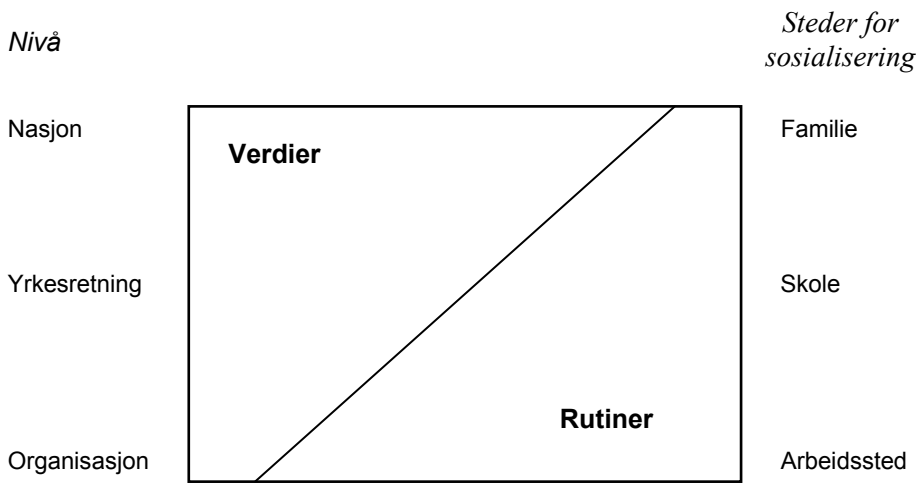
Kulturbegrepet er relatert til et fellesskap og en felles forståelse, og kulturforståelse er i konteksten av denne rapporten viktig av flere grunner (Schein, 1992):

- For å forstå dynamikk mellom ulike subkulturer i organisasjoner.
- For å forstå hvordan teknologi påvirker og påvirkes av organisasjoner.
- Organisasjonslæring, utvikling og planlagt endring kan ikke forstås uten å betrakte kulturen som en primær kilde for motstand.

Schein påpeker at overforenkling er den største faren forbundet med å forstå kultur. *"Måten vi gjør ting på"* og *"våre verdier"* er ofte kun manifestering av kulturen, ikke de grunnleggende antakelsene som kulturen bygger på. Schein har utarbeidet en modell på tre nivåer for å beskrive kultur, og denne modellen vil bli presentert senere i dette kapittelet. I Scheins teori er det et fokus på å identifisere de underliggende verdiene som påvirker atferden i organisasjonen, for deretter å kunne påvirke kulturen i organisasjonen. Dette kan kalles en funksjonalistisk tilnærming, en av to hovedretninger i synet på kultur:

- Det funksjonalistiske perspektivet – har en normativ tilnærming der en ideell tilstand tilstrebes. Det søkes å måle og forstå i hvilken grad kulturelle aspekter har innflytelse på holdninger og atferd, for deretter å kunne påvirke disse.
- Det fortolkende perspektivet – målet er å beskrive og tolke kulturen, og man er ikke opptatt av å forbedre den.

I denne rapporten har vi valgt en funksjonalistisk tilnærming til kulturbegrepet.



Figur 5: Påvirkningsgrad fra verdier kontra rutiner på ulike nivåer i samfunnet (Hofstede, 1991, p.182)

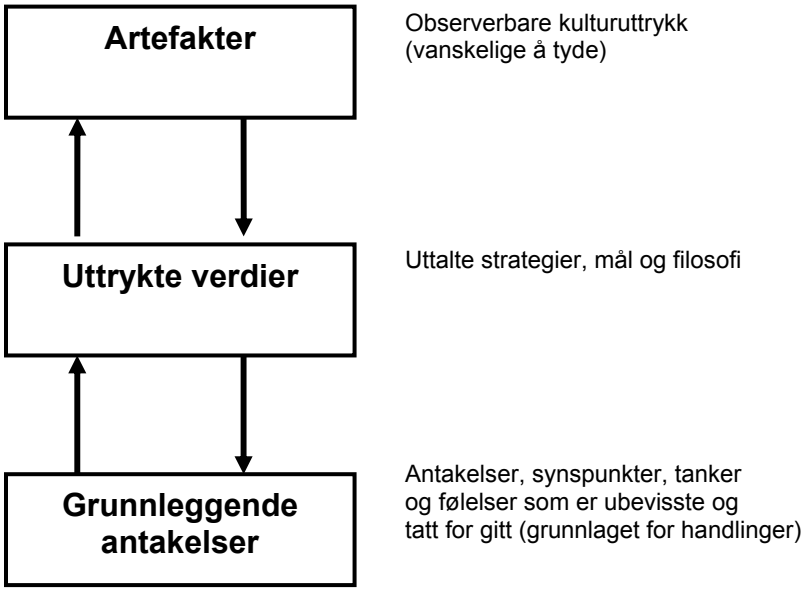
Hofstedes tilnærming til organisasjonskulturbegrepet kan forklares ut fra Figur 5. Denne figuren tar for seg hvilken påvirkning verdier og rutiner har på ulike nivåer i samfunnet. Figuren illustrerer hans syn på at menneskers grunnleggende verdier i større grad stammer fra nasjonal tilhørighet enn fra organisasjonene de jobber i.

Hofstedes undersøkelser har vist at organisasjonskultur hovedsakelig varierer med tanke på symboler, "helter" og ritualer – som han samler i begrepet *rutiner* (practices). Han fokuserer på disse rutinene, ettersom han hevder at *verdiene* til grunnleggerne og lederne *blir til rutiner* hos de ansatte i organisasjonen.

Hofstede anser nasjonal kultur for å være det dominerende grunnlaget for organisasjonskultur, mens Schein mener visjonen, ledelsesstilen og personligheten til grunnleggeren eller andre dominerende ledere er dominerende for organisasjonskulturen. Felles for begge synene er at kulturen synliggjør seg gjennom rutiner og manifestasjoner i organisasjonen. Disse er håndgripelige og enkle å endre, men endringer av rutiner vil ikke automatisk endre kulturen i seg selv. For å endre kulturen må man gå dypere til verks. Man må sette felles mål og arbeide sammen uansett hvilket nivå man er på, og de nye verdiene må ikke være i konflikt med de grunnleggende verdiene de ansatte allerede har med seg fra samfunnet. Interaksjon er i så måte et nøkkelord for endring av kultur.

Scheins trenivåmodell av kultur

Schein (1992) hevder at kultur eksisterer på tre distinkte nivåer. Disse nivåene representerer spennet fra det mest synlige til det usynlige, og muligens også det ukjente, i organisasjoner. Nivåene er illustrert i Figur 6.



Figur 6: Scheins trenivåmodell av kultur (Schein, 1992)

Artefakter

Artefaktene er representert på toppnivået (overflaten) i organisasjonen, og omfatter de synlige manifestasjonene av organisasjonskulturen. Dette er elementene man kan se, høre og føle; som språk, historier, myter, atferdsmønstre, kleskoder, kontorutforming, etc. Artefaktene er enkle å observere, men vanskelige å analysere og tyde – det kan være vanskelig å se relasjonene og mønstrene de representerer. Man må derfor fokusere på de underliggende nivåene for å se artefaktenes betydning.

Uttrykte verdier

De uttrykte verdiene (espoused values) manifesteres ofte i filosofi, mål og strategier. Disse kan identifiseres fra historier, symboler, og hvordan personer forklarer og rettferdiggjør sine handlinger. De

uttrykte verdiene reflekterer hvordan man ønsker å fremstå; ordene som benyttes for å forklare hva man tror man gjør, eller hva man ønsker at andre skal tro man gjør, og kan sees i sammenheng med Argyris & Schöns *espoused theory* og *theories of action.*[18]

Grunnleggende antakelser
Dette nivået omfatter de antakelser som er så dypt forankret i organisasjonen at de, bevisst eller ubevisst, styrer atferden til organisasjonens medlemmer. Dette er grunnlaget og kjernen til organisasjonskulturen. Nivået kan sammenliknes med Argyris & Schöns *theories-in-use*.

Scheins praksisfellesskap

En organisasjonskultur er i stor grad basert på organisasjonens historie og erfaring. Ansatte har gjennom tiden utviklet en rekke antagelser om konteksten de befinner seg i og hvordan man skal oppføre seg i denne. Disse antagelsene læres så videre til nye ansatte i organisasjonen. Antagelsene oppstår ofte i og rundt de funksjonelle enhetene i en organisasjon. Disse funksjonelle enhetene er ofte basert på like arbeidsoppgaver, lik utdannelsesbakgrunn eller lik erfaring i organisasjonen. Det oppstår med dette et internt kulturfellesskap med egne normer og regler i de ulike enhetene. Schein påpeker at det ofte kan oppstå kommunikasjonsproblemer mellom disse kultur-fellesskapene. Dette fordi fellesskapene ofte har ulike mål, og også fordi terminologien som benyttes ofte varierer fra fellesskap til fellesskap. Subkulturene i organisasjonen ofte kan deles i tre grupper, eller *praksisfellesskap* (Schein, 1996; Dybå, 2001):

- **Ingeniørfellesskapet** står for teknologien som ligger til grunn for organisasjonens drift og reglene for hvordan teknologien skal benyttes. Subkulturen baserer seg blant annet på felles erfaringer, utdanning og arbeidsoppgaver. Ingeniørene lager ofte systemer som i liten grad involverer menneskelige aktiviteter. Automatisering og standardisering kommer foran de sosiale aspektene på arbeidsplassen.
- **Ledelsesfellesskapet** er bygget opp rundt felles erfaringer fra å vedlikeholde organisasjonens økonomiske situasjon og å møte kravene fra styret, investorer og kapitalmarked.

[18] For mer, se for eksempel Argyris & Schön (1996)

Ledelsesfellesskapet går i sterkere grad enn de andre fellesskapene på tvers av organisatoriske grenser.

- **Operatørfellesskapet** utvikles lokalt i organisasjonen innenfor ulike operasjonelle enheter, og er den vanskeligste å beskrive av de tre subkulturene. Den baserer seg på menneskelig kontakt, og består typisk av linjeledere og arbeidere som lager og leverer produkter og tjenester som gir grunnlaget for organisasjonen

Hovedproblemet for læring og kunnskapsutvikling i organisasjoner er i følge Schein (1996) manglende erkjennelse av disse tre kulturene, og deres manglende evne til å forstå hverandre.

Sikkerhetskultur

Hva er så god og dårlig sikkerhetskultur? Hale (2000) peker på at en stor grad av forskning må til for å klargjøre hva begrepet sikkerhets-kultur omfatter. Reason (1997) hevder at en god sikkerhetskultur kan karakteriseres slik:

- Den er informert og rettferdig
- Man fokuserer på problemløsning fremfor fordømmelse/straff,
- Betydningen av rapportering og tilbakemelding blir vektlagt

Man kan se på sikkerhetskulturen som en integrert del av den større organisasjonskulturen. Kjennetegnene ved sikkerhetskulturen vil være de elementene i organisasjonskulturen som påvirker sikkerheten i positiv eller negativ retning (Hale, 2000).[19] Rosness (2001) foreslår at sikkerhetskulturbegrepet kan karakteriseres som:

Recurrent patterns of interaction that have an impact on risk

Dette fokuset på atferd og interaksjon stemmer også godt overens med de tidligere presenterte tilnærmingene til kulturbegrepet. Gjentatte atferdsmønstre er representasjoner av de dypere grunnlagene i kulturen. En vedvarende endring av disse atferdsmønstrene, for

[19] Elementene i kulturen vil også påvirke holdninger og atferd som *ikke* er relatert til sikkerhet – og disse vil da også kunne bli påvirket av et økt sikkerhetsfokus. Tilsvarende gjelder for arbeid som påvirker andre delvis overlappende subkulturer innenfor organisasjonskulturen – elementene som påvirker sikkerhetsnivået kan bli påvirket av dette arbeidet.

eksempel ved et sterkere fokus på sikkerhet, vil da kunne påvirke dette grunnlaget, slik at kulturen endres.[20]

Westrum (1993) beskriver tre distinkte typer sikkerhetskulturer som kan forekomme i virksomheter:

- Patologisk kultur – organisasjonen er styrt av et ønske om å bevare status quo. Den fornekter signaler, straffer de som sier ifra og forsøker å unngå rapportering.
- Kalkulerende kultur – organisasjonen forsøker å holde seg til regler og krav fra myndigheter og kunder. De har et begrenset repertoar av virkemidler og tiltak, og fokuserer på enkel avvikshåndtering.[21]
- Generativ kultur – organisasjonen er opptatt av mål og læring, man oppmuntrer ansatte til å si fra dersom de ser noe feil, ser på sikkerhet som en mulighet heller enn som et problem og viser åpenhet for å endre prosessene og systemene.[22]

En god sikkerhetskultur kan sees i sammenheng med sikker atferd. Hovden (2004) påpeker at virkemidlene for å skape sikker atferd er langt flere enn det de fleste benytter seg av:

- Tilrettelegging av de praktiske forutsetningene; for eksempel et godt arbeidsmiljø og god tilrettelegging av arbeidet
- Trusler gjennom lovgivning og straff/sanksjoner
- Sikker atferd må gjøres attraktiv, og man må få belønninger
- Design og fysiske barrierer som tvinger frem sikker atferd
- Overtalelse og overbevisning – god risikokommunikasjon
- Trening for mestring – krisehåndtering og risikobevissthet

Dersom disse virkemidlene kombineres blir effekten forsterket. Det har også blitt gjort arbeid med å identifisere elementer av god sikkerhetskultur, både generelt og direkte relatert til Scheins trenivåmodell.[23] Disse elementene er gjengitt i Vedlegg A.

---

[20] Samtidig vil kulturen kunne gi motstand til disse endrede atferdsmønstrene (Schein, 1992).
[21] Dette kan sees i sammenheng med Argyris & Schöns (1996) enkeltløkkelæring og Senges (1990) adaptiv læring.
[22] Dette kan sees i sammenheng med Argyris & Schöns (1996) dobbeltløkkelæring og Senges (1990) generativ læring.
[23] Dette kan man for eksempel finne i Hale (2000) eller IAEA (2002).

5. Utviklingen av SjekkIT

Forrige versjon av verktøyet

Den teoretiske bakgrunnen for verktøyet ble i hovedsak lagt i prosjektet "Informasjonssikkerhet og innsideproblematikk", der de gikk gjennom en rekke artikler og bøker. Mølmann (2003) identifiserte i dette prosjektet et rammeverk for kategorisering av menneskelige utfordringer i forbindelse med informasjonssikkerhet. Artikkelen tok for seg en rekke utfordringer:

- Interne vs. eksterne aktører
- Tilsiktede vs. utilsiktede handlinger
- Ønskede vs. uønskede konsekvenser av handlinger
- Unnlatelse av pålagte handlinger vs. gjennomføring av forbudte handlinger (i forhold til sikkerhetsbrudd)
- Mellommenneskelig interaksjon vs. interaksjon mellom mennesker og maskiner
- Ulike brukergrupper som representerer ulike typer trusler

Mølmann (2003) peker også på at mange innsidehendelser ligger i gråsonen mellom tilsiktede og utilsiktede handlinger. De er ofte et resultat av manglende kunnskap, manglende forståelse og/eller uansvarlighet. Det pekes også på at en rekke interne sikkerhetsbrudd kan føre til uønskede konsekvenser i seg selv eller i en kombinasjon med eksterne angrep. I prosjektet tok man utgangspunkt i at organisasjonskultur kan være en kilde til god sikkerhet – man kan identifisere og påvirke en *informasjonssikkerhetskultur*.

Den forrige versjonen av verktøyet er basert på en videreutvikling av *Hearts and Minds*, som ble utviklet for å forbedre sikkerheten i Omans oljeindustri. Kufås (2002) diskuterer dette undersøkelsesverktøyet og mener at det er mangelfullt med tanke på å kartlegge grunnleggende ideer, verdier og antagelser, som av mange anses å være de dypeste aspektene ved kultur.[24] En del temaer som var relevante for informasjonssikkerhet ble imidlertid identifisert i Hearts and Minds, og tilpasset til verktøyet. I tillegg til kulturelle aspekter ble også enkeltmenneskelige faktorer inkludert i verktøyet, ettersom forstudiene

[24] Dette blir for eksempel hevdet av Schein (1992) og Hofstede (1991).

viste at disse var viktige i forhold til innsideproblematikk i organisasjoner. Temaene i verktøyet er i tillegg basert på arbeid av Albrechtsen et al. (2002) og *Information Security Forum*.[25] Hovedpunktene fra den førstnevnte, organisatoriske faktorer som påvirker informasjonssikkerhet, er gjengitt i tabellen under:

Kategori	Organisatorisk faktor
Kultur	Normer, felles holdninger og tanker for sikkerhet Villighet til forbedring Arbeidsmiljø Kultur og kunnskap Rapportering Kultur og deltakelse/involvering
Informasjons-sikkerhetsledelse	Kontekst ROS-analyser Kontinuitet Deltakelse/involvering Formalisering av arbeid Beredskap
Organisering	Målkonflikt Ansvar Koblinger/interaksjon Organisasjonslæring Eierskap
Kommunikasjon	Kommunikasjon
Kunnskap og Kompetanse	Teknisk kunnskap & kompetanse Sikkerhetskunnskap Organisasjonskunnskap Opplæring

Verktøyet endte til slutt med 31 spørsmål som ble relatert til følgende åtte temaer:

- Atferd
- Kunnskap og holdninger
- Policy og ledelse
- Inkludering og læring
- Ansvarsfordeling
- Prosedyrer og formalisering
- Analyser, vurderinger og revisjon
- Bevissthet og menneskelige relasjoner

[25] Information Security Forum er en internasjonal forening som fokuserer på forskning på informasjonssikkerhet.

For hvert av spørsmålene er fem skriftlige alternativer presentert, og respondenten skal svare (krysse av) på det alternativet som han/hun føler at gir en mest mulig korrekt beskrivelse av situasjonen spørsmålet omhandler. I tillegg til disse faktorene har man inkludert et sett demografiske variabler, som gir et grunnlag for gruppering og sammenlikning av svar.

Beskrivelse av utviklingsprosessen

Bakgrunnen for videre utvikling er gitt av rapporten fra Kufås og Mølmann som pekte på flere felter som kunne forbedres.[26] Dette har sammen med videre undersøkelser, analyser og en tett dialog med samarbeidende aktører vært grunnlaget for det nye verktøyet.

På bakgrunn av dette ble en ny versjon av verktøyet utarbeidet i januar 2005. Versjonen ble utarbeidet for å ligge til grunn for diskusjoner på et arbeidsseminar i Trondheim 7. og 8. februar der oppdragsgivere, fageksperter, nåværende brukere og potensielt nye brukere av verktøyet var til stede. Fokuset for seminaret var:

- Skape en forståelse av hva sikkerhetskultur er og hvordan man kan arbeide med dette innenfor og på tvers av bransjer
- Gi en oversikt over bakgrunnen for verktøyet, og la samarbeidspartnere komme med innspill til videreutviklingsprosessen

Hovedinnspillene til utviklingsprosessen er samlet i tabellen på neste side. Arbeidet med å sammenfatte et nytt verktøy er utført i etterkant av seminaret, og resultatene er gjengitt i underkapitlene som følger.

[26] For mer om dette, se (Kufås & Mølmann, 2003)

Ønsker til utviklingen av verktøyet	Diskusjonspunkter fra forarbeid og arbeidsseminar
Spissing av spørsmål og alternativer	Spørsmålene og alternativene må være konsistente og relevante for de som skal svare.
Dekning av relevante sikkerhetsproblemer innenfor security og informasjonssikkerhet	Verktøyet må dekke relevante områder innenfor informasjonssikkerhets- og securityfeltene
Dekning av relevante sikkerhetsproblemer i forhold til lovgivning	Verktøyet må være relevant for virksomheter underlagt sikkerhetsloven og dekke relevante felter som loven tar for seg.
Kontinuitet og sporbarhet i verktøyet	Det er ønskelig å kunne sammenlikne resultater fra det nye verktøyet med resultater fra den forrige versjonen av verktøyet. Dårlige spørsmål må fjernes og en mapping mot nytt verktøy utarbeides.
Retningslinjer for analyse av undersøkelsen	Rettet opp mot konkrete spørsmål og gruppering av spørsmål.
Muligheter for implementering av interne målsettinger, tiltak og benchmarking.	Mulighet for å benytte skjemaet i flere faser: • For å definere nivåene man ønsker at organisasjonen skal være på • For å måle status og utarbeide tiltak for å nå målene
Motivasjon for bruk av verktøyet	Spissing av formuleringer, fokus på å rette spørsmålene til de som har grunnlag for å svare, synliggjøring av hvordan god sikkerhetskultur påvirker nivået på sikkerhet.

Resultater av utviklingsprosessen

Innspillene til utviklingsprosessen og de korresponderende resultatene er presentert i de følgende underkapitlene.

Balansen mellom atferd, holdninger og kultur

Forrige verktøy ble utviklet for å se på både enkeltmenneskelige og kulturelle aspekter ved organisasjoner. Noen tilbakemeldinger påpeker at utgangspunktet for undersøkelsene kan være feil; man skal "synse" om hvordan man mener det står til. Disse tilbakemeldingene foreslår at man heller bør fokusere på de enkeltes holdninger og atferd, og ikke ha en gallupundersøkelse om hva folk mener om andre. Disse tilbakemeldingene foreslår at man heller fokuserer på hva enkeltmennesket gjør og mener. Man kan deretter bruke de enkeltes svar for å skape et bilde av virksomheten som helhet. I motsetning har man også fått innspill på at verktøyet i for liten grad har fokusert på kulturelle faktorer i organisasjoner. Disse innspillene har påpekt at kultur ikke kan måles som summen av individuelle holdninger og atferd.

Konkrete resultater:
Det nye verktøyet fokuserer i stor grad på enkeltmennesker og deres syn på hvordan status i virksomheten er. Verktøyet går bredt ut, og forsøker hovedsakelig å måle og påvirke faktorer på de øverste nivåene i Scheins kulturmodell. Ved å endre atferdsmønstre og interaksjons-rutiner kan man så på sikt også endre de mer grunnleggende elementene i kulturen.[27] Vi har i utviklingsprosessen fokusert på at verktøyet *avhengig av hvordan det brukes* skal kunne benyttes for å måle og utvikle sikkerhetskultur i virksomheter. Ved direkte bruk som et revisjons- eller måleverktøy vil man kun se på de overordnede nivåene i sikkerhetskulturen, dvs. rutiner og atferd. Ved bruk som et verktøy i diskusjonsgrupper antas det at man i større grad også kan påvirke sikkerhetskulturen direkte.

Målgrupper for verktøyet

Den forrige versjonen av verktøyet ble også utviklet på oppdrag fra Nasjonal Sikkerhetsmyndighet og NTNU. I utviklingsprosessen var imidlertid også private aktører involvert. Tilbakemeldinger viser at det

[27] Dette kan sees i sammenheng med tilnærmingen til kulturbegrepet som presenteres i Rosness (2001).

revidierte verktøyet bør tilpasses offentlige virksomheter i større grad enn det har vært, samtidig som de private samarbeidspartnernes interesser ivaretas på en hensiktsmessig måte. For å forbedre dette, kan man for eksempel velge én av to strategier:

- Utvikle ett generelt verktøy som kan benyttes av både private og offentlige aktører
- Utvikle to spesifikke verktøy; ett spesielt rettet mot offentlig virksomhet, og ett rettet mot private organisasjoner.

Konkrete resultater:
Man har fokusert på å utvikle ett generelt verktøy som skal være relevant for både offentlige virksomheter og private bedrifter. Det nye verktøyet er utviklet i samarbeid med oppdragsgivere og samarbeidspartnere innenfor både offentlig og privat virksomhet for å sikre anvendbarheten for alle målgrupper.

Antall spørsmål og temaer

Generelt har man fått tilbakemelding på at spredningen og dekningen av spørsmålstemaene i forrige versjon er bra. Undersøkelsesverktøyet omfatter viktige områder innenfor informasjonssikkerhet, med et fokus på IKT-relatert sikkerhet.

Konkrete resultater:
I den nye versjonen har antallet spørsmål økt, for at man skal kunne sette sammen en undersøkelse tilpasset virksomhetens behov. Man har i tillegg fokusert på å knytte spørsmål opp mot felter som er dekket av etablerte lovverk, standarder og policies innenfor informasjons-sikkerhet for å synliggjøre denne bredden i verktøyet. Elementene som beskriver god sikkerhetsledelse, -kultur og -policy er gjengitt i Vedlegg A. Knyttingen av spesifikke spørsmål opp mot disse elementene er gjengitt i Vedlegg B.

Omfanget på verktøyet

Tilbakemeldinger til både denne og forrige utviklingsgruppe har vist at undersøkelsene av mange anses å være for omfattende og tidkrevende. Dette kan resultere i at respondentene går lei underveis, og at kvaliteten i svarene på de seinere spørsmålene kan være dårligere enn på de tidligere spørsmålene. Videre kom det innspill om at undersøkelsen er omfattende med mye tekst som skal leses. Dette kan

føre til at man går lei, og kvaliteten i svarene kan bli dårligere etter hvert.

Konkrete resultater:
Man har i utviklingsarbeidet fokusert på flere temaer for å forenkle verktøyet. For det første er spørsmål og alternativer spissformulert slik at det skal være enklere å ta stilling til de mulige svarene man kan gi. Alternativene er spisset og bedre balansert i forhold til hverandre.

Samtidig som alternativene er spisset har også temaene blitt flere i verktøyet. Dette har resultert i at spørsmålene har blitt fordelt på en basispakke og en tilleggspakke. Basispakken inneholder de mest sentrale spørsmålene i verktøyet, men kan suppleres av spørsmålene i tilleggspakken.

Spørsmålenes relevans for respondentene

Mange respondenter følte at spørsmål i den forrige versjonen ikke var relevante for dem. Tilbakemeldinger påpeker at spørsmål ikke bør blir stilt til de som ikke har forutsetninger til å kunne svare. Svarene fra denne gruppen kan i så fall være verdiløse. Et av de konkrete innspillene fra undersøkelsen påpekte at:

> *"noen av svarene la opp til at jeg som ansatt hadde kunnskap om hva ledelse og sikkerhetsavdelingen foretar seg innen dette fagområdet, men jeg tror at veldig mange ansatte (...) ikke har kunnskap om dette"*.

En rekke respondenter svarer at de ikke har vært fortrolige med de svaralternativene de fikk. Flere tilbakemeldinger fra sluttbrukere har også fokusert på at de savner en mulighet for å svare *"vet ikke"* der spørsmålene ikke føles relevante.

Konkrete resultater:
I arbeidet med det nye verktøyet er det i større grad fokusert på å rette undersøkelsen inn mot vanlige brukere og vanlige brukssituasjoner. De viktigste spørsmålene må kunne besvares av alle, og man bør ikke behøve ekspertkunnskap for å gjennomføre undersøkelsen. Dette er gjort i samarbeid med brukere av verktøyet.

Muligheten for å svare "vet ikke" er fortsatt bevisst utelatt av verktøyet, og dette er i samsvar med de involverte aktørenes ønsker:

- Man risikerer å få mange som svarer ”vet ikke” fordi respondentene kan ta en lettvint løsning fremfor å tenke seg godt om på alternativene.
- Man tvinger respondenten til å ta stilling til problemstillingen og kanskje reflektere over egen atferd og holdning i forhold til temaet.
- Man ønsker i stor grad å finne ut hva medlemmene i en organisasjon føler og tror om situasjonen, ikke nødvendigvis å få et fasitsvar på hvordan ting er.

Spørsmålenes og alternativenes konsistens

Det har blitt påpekt at flere av spørsmålene i forrige versjon ikke har vært konsistente i forhold til alternativene som skal vurderes. Det er ikke alltid man kan se noen naturlig kopling verken mellom spørsmålet og alternativene, eller innad blant de ulike alternativene. En mulighet for forbedring ligger i å spisse spørsmålene og alternativene, slik at de er mer konkrete og de hver dekker et smalere område. Dette kan også føre til at målingene kan bli mer presise.

Konkrete resultater:
Man har fokusert på å benytte felles språkbruk i spørsmål og alternativer, samt å sørge for at alternativene er direkte koplet til spørsmålstemaene. Eventuelle overflødige beskrivelser som ikke er direkte relatert til spørsmålsformuleringen er forsøkt fjernet.

Antall skriftlige alternativer

Det bemerkes at det kan være vanskelig å se at svaralternativene ligger på en skala fra 1 til 5. Skillene mellom de fem alternativene er ofte vanskelige å se. Tilbakemeldinger viser at alternativ 3 og 4 ofte oppfattes som mer reelle enn alternativ 5, som ofte anses å beskrive en ideell drømmesituasjon for virksomhetene. Man bør ha en generell vurdering på om nivåene skal beskrive reelle og oppnåelige situasjoner, eller om de skal være ideelle beskrivelser av et nivå med gitte egenskaper.

Konkrete resultater:
Det forrige versjonen av verktøyet hadde fem tekstlige alternativer, den nye versjonen har tre tekstlige alternativer. Det er i den nye versjonen gitt mulighet for å krysse *mellom* alternativene én og tre, og tre og fem for å beholde sporbarhet til forrige versjon, samt gi mulighet

til å vise nyanser mellom de tekstlige alternativene. Alternativene er delvis basert på Westrums nivåer for sikkerhetskultur, samtidig som man har fokusert på å gjøre beskrivelsene så realistiske som mulig.

Konkrete innspill på formulering og innhold

Respondenter har også kommet med direkte kommentarer på innholdet i verktøyet. Enkelte spørsmål har vært satt sammen av to spørsmål (bl.a. spørsmål 15 i det gamle verktøyet). I en slik situasjon kan det være vanskelig å finne et tilfredsstillende svaralternativ som dekker begge temaene, samtidig som det også kan være vanskelig å måle noe konkret da man har to faktorer som blir vurdert og balansert i forhold til hverandre i besvarelsene.

Analysen av spørsmålene identifiserte også en rekke spørsmål der man i prinsippet ville ha respondentene til å svare *ja* eller *nei*. Disse spørsmålene bør omformuleres og alternativene bør nøytraliseres. Undersøkelsene viser også at man har problemer med å svare fordi alternativene ikke er gode nok for å beskrive aspektene som må vurderes når man skal svare på spørsmålet. Et i seg selv enkelt spørsmål om hvorvidt man vil anmelde kolleger som har gjort noe kriminelt kan ha mange aspekter som påvirker beskrivelsene:

- Er handlingen jobbrelatert (lekking av informasjon vs. å kjøre for fort, etc.)?
- Hva motiverte handlingen (stress, tidspress, arbeidspress, etc.)?
- Hva var konsekvensene av handlingen?

Tilbakemeldinger fra pilotvirksomhetene påpeker også at forrige versjon av undersøkelsen tvinger frem gale svar. Dette fordi språket som benyttes ikke er konsistent og presist nok. Dette gjelder for eksempel bruken av ordene sensitiv, gradert, klassifisert, fortrolig og konfidensiell, som brukes om hverandre. Dette bør rettes opp i den reviderte versjonen av verktøyet.

Konkrete resultater:
Spørsmål som dekker flere temaer har blitt splittet opp eller fjernet fra den nye versjonen av verktøyet. Spørsmål som tvinger respondenter til å svare ja eller nei har blitt omformulert slik respondenten skal gi en gradsvurdering. Språket i det nye verktøyet er spissere enn i forrige versjon, slik at det skal være enklere å ta stilling til alternativene.

6. Presentasjon av SjekkIT

Presentasjon av spørsmålsskjemaet

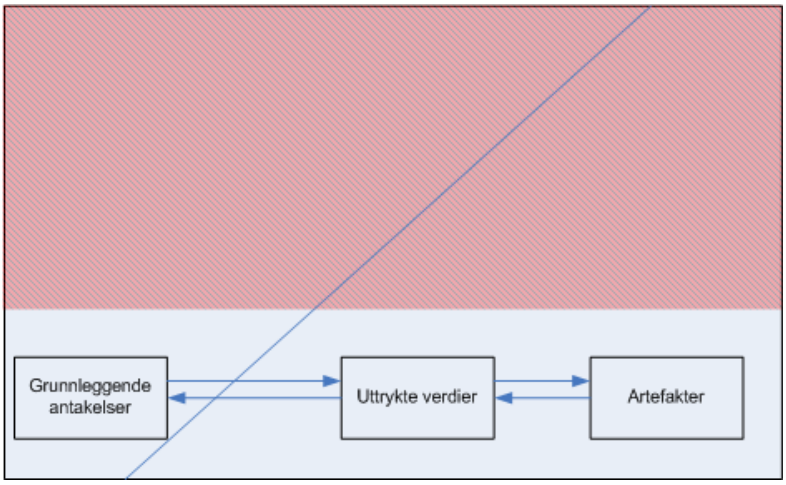
SjekkIT består av en grunnpakke på 30 spørsmål og en tilleggspakke på 34 spørsmål med følgende fordeling:

- **Kunnskap og holdning** – de ansattes kjennskap til sikkerhetsmål, policies og graderingsrutiner er blant spørsmålene i denne kategorien. I basispakken berøres i tillegg ansvarsfordeling, skyldfordeling og åpenhet blant ansatte, samt holdninger i forhold til sikkerhetskrav og brudd på sikkerhetsrutiner. Tilleggspakken omfatter i tillegg holdninger relatert til behandling av sensitiv informasjon og nivået på relevant teknisk kunnskap.
- **Atferd** – denne kategorien ser i basispakken blant annet på atferd relatert til bruk av IT, og hvordan man forholder seg til relevant lovverk. Tilleggspakken tar i tillegg for seg sikkerhetsrutinenes relevans for sluttbrukere, hvordan man oppfører seg dersom uønskede hendelser inntreffer og atferd ved behandling av sensitiv informasjon.
- **Policy og ledelse** – kommunikasjon og involvering av ansatte og samarbeidspartnere, samt virksomhetens prioritering av sikkerhetsarbeid er sentrale aspekter i basispakken. Tilstedeværelsen av gode rutiner for sikkerhet blir også berørt. Tilleggspakken utfyller temaene fra basispakken.
- **Revisjon** – spørsmålene i basispakken ser på risiko- og sårbarhetsanalyser, analyse av hendelser og rutinene for revisjon av informasjonssikkerhet. Tilleggspørsmålene tar også for seg hvorvidt informasjonssikkerhet blir prioritert når relevant utstyr i virksomheten skiftes ut.

De fire kategoriene er et resultat av diskusjoner fra arbeidsseminaret. Spørsmålene som er plassert i grunnpakken utgjør et minstemål for en god undersøkelse. Virksomheter anbefales i tillegg å benytte spørsmål fra tilleggspakken for å supplere på temaer der man ønsker et sterkere fokus. Hvert enkelt spørsmål er presentert og forklart i Vedlegg C.

Teoretisk forankring av verktøyet

I rapporten ser vi på struktur ut fra Mintzbergs tilnærming – utforming og koordinering av aktiviteter. Disse aktivitetene relaterer vi til Hofstedes rutiner og Scheins øverste nivåer av kultur.[28] De representerer den uttalte og praktiske gjennomføringen av aktiviteter. Med hensyn på grunnleggende verdier antar vi at grunnlaget for atferd i stor grad er preget av verdier og holdninger som ligger på et høyere nivå enn organisasjonen. En nordmann vil i stor grad være preget av typisk norske verdier og holdninger. I organisasjoner vil atferden i større grad være preget av rutiner for hvordan ting skal gjøres, og verdiene som ligger til grunn for disse spesifikke handlingene vil tilhøre et lite subsett av det totale antall verdier man besitter.[29] SjekkIT fokuserer på subsettet som er omfattet av Scheins trenivåmodell *innenfor* Hofstedes representasjon av verdier kontra rutiner i samfunnet. Verdiene og rutinene på de overordnede nivåene er ikke direkte omfattet, og det har ikke blitt gjort noen vurdering på i hvilken grad disse påvirker sluttnivået på sikkerhet. Dette kan illustreres som i Figur 7.

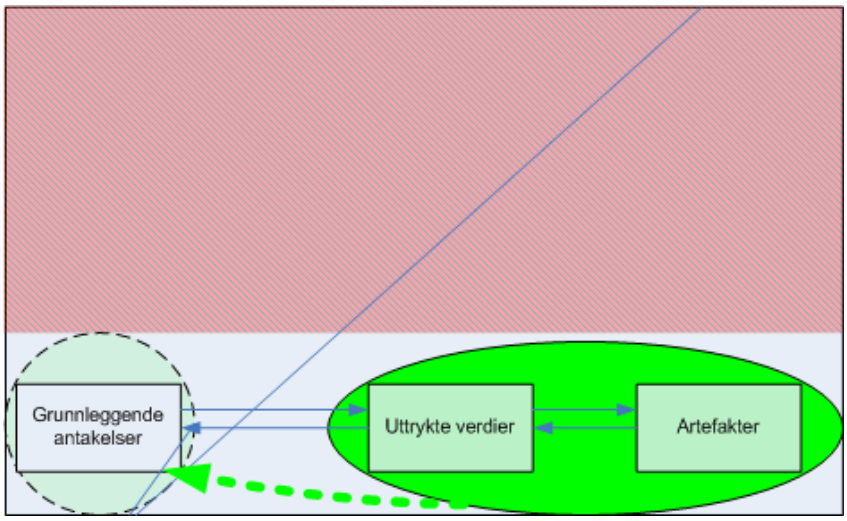


Figur 7: Subsettet av kultur utviklingsprosjektet har rettet seg mot

SjekkIT har i tillegg et fokus på de øverste nivåene i Scheins kulturmodell, det forsøker ikke direkte å avdekke de underliggende verdiene. Man fokuserer på rutiner og atferd. Ved å anta at endring av rutiner og atferd kan påvirke holdninger vil man kunne påvirke de organisasjonsspesifikke verdiene slik at disse på sikt ligger til grunn

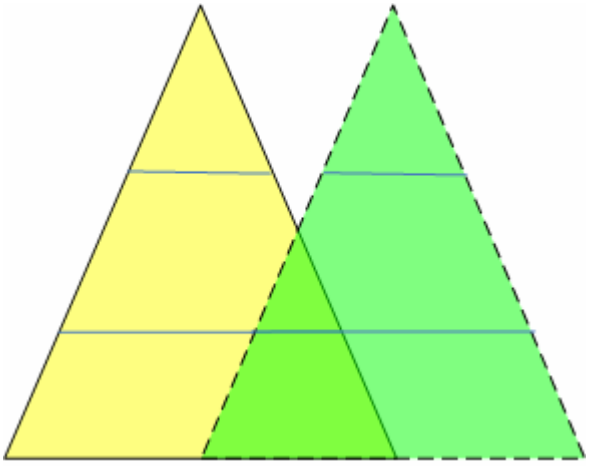
[28] Disse teoriene er presentert i kapittel 3.
[29] Se Figur 5, side 15

for atferden. Denne kulturendringen kommer da som en følge av endrede interaksjons- og atferdsmønstre, som korresponderer med Rosness' (2001) syn på kulturendring. Dette kan da illustreres som i Figur 8.



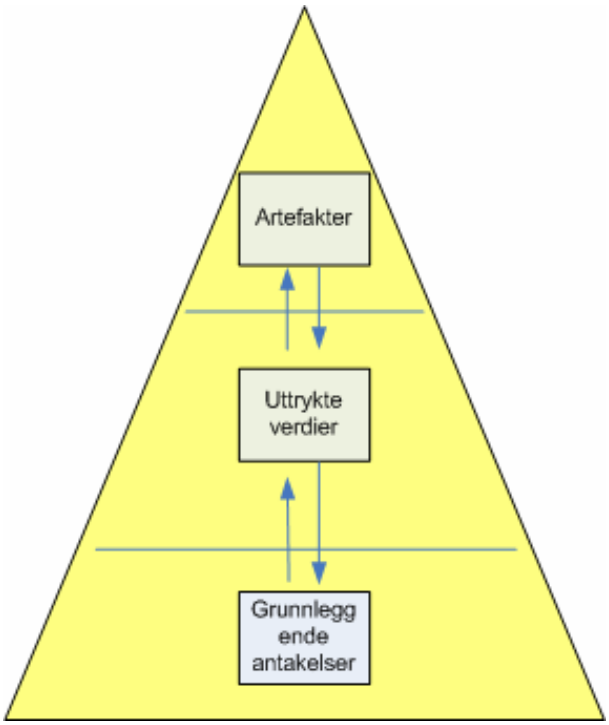
Figur 8: Muligheter for måling og endring av kultur med SjekkIT

Som et diagnostiseringsverktøy er SjekkIT tenkt å kunne identifisere sikkerhetssvakheter i organisasjonen. Dette skal igjen kunne angi grunnlaget for en endring. Den gule trekanten til venstre i Figur 9 representerer sikkerhetskulturen i organisasjonen slik den er på nåværende tidspunkt, og den grønne til høyre en endring mot en bedre sikkerhetskultur.



Figur 9: Nåværende og ønsket sikkerhetskultur i organisasjonen

Trekantene kan sees i sammenheng med Scheins trenivåmodell for kultur. Som vi ser i Figur 10 har man artefakter på toppen, uttrykte verdier i midten og grunnleggende antakelser i bunn. Bredden på pyramiden gir en indikasjon på vanskelighetsgraden av å skulle endre på de spesifikke nivåene.



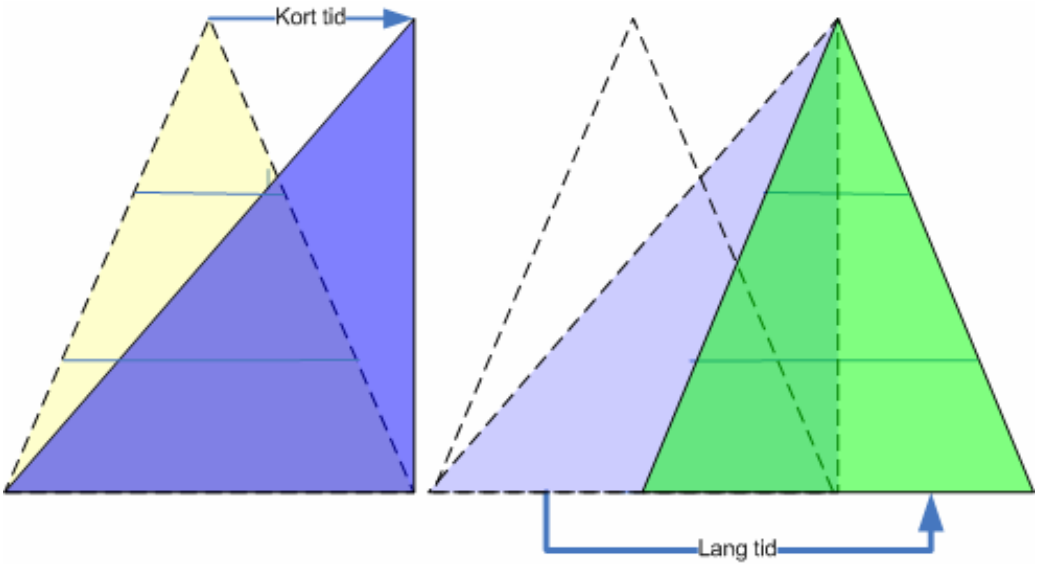
Figur 10: Scheins trenivå kulturmodell

Ofte benyttes en analogi til isfjell om kultur. Man ser bare toppen, noe som gjenspeiles i at man kun forholder seg til rutinene og reglene som preger den synlige atferden i organisasjonen, mens de grunnleggende normene, reglene og verdiene ligger under vannlinjen og er fordekt. Det som er synlig og tilgjengelig kan derfor påvirkes og forskyves i form av endrede rutiner og innføring av nye retningslinjer og prosedyrer. Derimot er det svært vanskelig å endre medarbeideres holdninger og grunnleggende verdier.

Når man målrettet skal endre sikkerhetskulturen i organisasjonen, kan man endre rutiner og prosedyrer og i så måte "flytte" den øvre delen av pyramiden. Grunnleggende antakelser vil fortsatt henge igjen og motsette seg endringen.[30] Det krever lang tid og et kontinuerlig fokus

[30] I henhold til for eksempel (Schein, 1992)

og engasjement fra ledelsen for å endre virksomhetens kultur og oppnå en varig endring i sikkerhetskulturen. SjekkIT kan i denne sammenheng benyttes for å identifisere relevante svakheter i organisasjonen. Det som identifiseres vil ligge på Scheins to øverste nivåer. Ved å så fokusere på endring av atferds- og interaksjonsmønstre vil man kunne forbedre sikkerhetskulturen.[31] Denne prosessen kan illustreres som i Figur 11.



Figur 11: Endringsprosessen for organisasjonskultur

Trekantene i Figur 9 angir nåværende og ønsket sikkerhetskultur. Figur 11 viser hvordan denne endringsprosessen kan foregå.[32] Endring av artefakter og rutiner kan skje på forholdsvis kort tid. De grunnleggende antakelsene vil imidlertid ta mye lenger tid å forandre.[33] Disse vil kun endres når de nye atferdsmønstrene blir tatt for gitt som riktige av organisasjonens medlemmer. Dette krever et kontinuerlig fokus og en bevisst holdning fra ledelsen.

[31] I henhold til (Rosness, 2001)
[32] I henhold til teoriene som benyttes; Schein og Hofstede peker på at det er vanskelig å endre de underliggende verdiene, Rosness peker på at kulturendring foregår gjennom endrede atferdsmønstre og interaksjonsmønstre.
[33] En vellykket endringsprosess kan fort ta minst tre år (Aune, 2000)

Bruksområder for verktøyet

Verktøyet er utarbeidet for to konkrete bruksområder:

- Diagnostiseringsverktøy – som kan måle tilstanden i virksomheten, og angi sterke og svake sider relatert til sikkerhet. Resultatene fra diagnostiseringen kan benyttes videre for å forbedre sikkerheten ved å angi felter der tiltak må settes inn.
- Forbedringsverktøy – kan benyttes i en forbedringsprosess med målsetting og gruppediskusjoner.[34] Målet for verktøyet i en slik kulturendringsprosess er at spørsmålene skal gi grunnlag for diskusjoner rundt sikkerheten og problemområder i virksomheten. Disse diskusjonene må involvere nøkkelpersoner fra et vidt spekter av organisasjonen, og skal igjen føre til konkrete tiltak for å bedre sikkerheten.

Disse to bruksstrategiene er nærmere presentert i de neste kapitlene; diagnostiseringsverktøyet er presentert i kapittel 7, mens kulturbyggingsverktøyet er presentert i kapittel 8. Verktøyet er også utviklet for å ha en opplæringseffekt uavhengig av hvilken bruk man velger. Respondentene vil gjennom undersøkelsen i seg selv måtte ta stilling til både virksomhetens og sitt eget sikkerhetsarbeid.

Hvorfor bruke verktøyet?

Sikkerhetsarbeid har tradisjonelt blitt gjort med en strukturell og regelorientert tilnærming. For å få et mer helhetlig arbeid er det imidlertid viktig å også fokusere på holdninger, kunnskap, atferd og kultur.

Mens de strukturelle tilnærmingene viser hvordan sikkerhetsarbeidet *skal* gjennomføres, vil bruk av SjekkIT gi et bilde av hvordan sikkerhetsarbeidet *faktisk* gjennomføres, samt *synet på* dette arbeidet. Ved å undersøke forholdene mellom det administrative systemet og hvordan folk handler og tenker, kan man få et godt bilde av hvordan sikkerhetsnivået er i virksomheten.

[34] Denne tilnærmingen er benyttet blant annet i SafeTrack-metodikken (Johnsen et al., 2004)

SjekkIT er et verktøy som kan benyttes for å diagnostisere og forbedre sikkerhetskulturen i virksomheter. Denne sikkerhetskulturen vil være de delene av organisasjonskulturen som påvirker sikkerheten i positiv eller negativ retning. Verktøyet fokuserer på sikkerhetsrelatert kunnskap, holdninger, atferd og kultur – en tilnærming som er velkjent og utprøvd i flere tilsvarende verktøy.[35]

Spørsmålsforankring

Spørsmålene i verktøyet er basert på innspill fra brukere, samarbeidspartnere i prosjektet og sentrale teorier. På denne måten har spørsmålenes praktiske relevans blitt sikret. I tillegg har man i utviklingsarbeidet fokusert på å utarbeide spørsmål som er forankret i relevante teorier, standarder og policies for god sikkerhetsledelse og sikkerhetskultur. Dette bakgrunnsstoffet er presentert i Vedlegg A, og omfatter følgende:

- Elementer i god sikkerhetskultur (IAEA, 2002)
- ISO 17799
- Elementer i god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005)

Verktøyet SjekkIT omfatter sentrale elementer i dette bakgrunnsstoffet, enten direkte i spørsmålsbatteriet eller gjennom bruk av verktøyet i virksomheten. Forankringen av spørsmål i forhold til disse teoriene er gjengitt i sin helhet i Vedlegg B, og en presentasjon av hvert enkelt spørsmål er gjengitt i Vedlegg C. Spørsmålene er også relatert til forrige versjon av verktøyet, og koplingene mellom spørsmål i denne og forrige versjon er gjengitt i Vedlegg D.

[35] Blant annet Shells Hearts & Minds (Hudson & van der Graaf, 2002) og Sintefs SafeTrack (Johnsen et al., 2004)

7. SjekkIT som et diagnostiseringsverktøy

Som beskrevet i forrige kapittel vil vi presentere to distinkt forskjellige måter å benytte verktøyet på. Den første, som presenteres i dette kapittelet, tar utgangspunkt i å benytte verktøyet til diagnostisering av virksomheten. Med denne tilnærmingen ønsker man å måle graden av sikkerhet i forhold til flere sentrale temaer, og på grunnlag av dette identifisere problemområder. På denne måten kan man se på verktøyet som et hjelpemiddel for ledelsen som kan rette tiltak på grunnlag av resultatene.

Tilnærmingen baserer seg på å benytte SjekkIT som et undersøkelses-verktøy, og deretter gjøre statistisk analyse av svarene. Sentrale artefakter og uttrykte verdier relatert til god informasjonssikkerhets-kultur blir undersøkt. Hvert enkelt spørsmål er utarbeidet for å belyse sentrale områder innen informasjonssikkerhet, og en slik undersøkelse vil gi gode indikasjoner på forholdene mellom ulike områder. Samtidig vil selve gjennomføringen av en slik undersøkelse kunne bidra til mer bevissthet og oppmerksomhet rundt temaet informasjonssikkerhet.

Den viktigste kritikken mot å gjennomføre en rent statistisk undersøkelse kan knyttes til diskusjonen om kultur; om måling og endring. Det er uenighet om hvorvidt man kan måle holdninger og kultur direkte på denne måten. En større kvantitativ undersøkelse gir tallverdier som forsøker å beskrive abstrakte fenomener. Man kan si at undersøkelsen gir svar på konkrete uttrykk for underliggende kulturelle faktorer. Det er derfor viktig at man er forsiktig og ikke drar for bastante slutninger dersom man har en ensidig kvantitativ tilnærming.

Definering av sikkerhetsmål

Selv om verktøyet i utgangspunktet er lagt opp med svaralternativer som fra venstre mot høyre gir en gradvis økning mot bedre score, er det viktig for virksomheten å gjøre seg opp en mening om det er ønskelig å oppnå høyeste score på alle spørsmål. Det er viktig å se på hvilken sammenheng hvert enkelt spørsmål har i virksomheten.

Som nevnt tidligere kan ulike virksomheter karakteriseres ved hjelp av Mintzbergs organisasjonsformer. Graden av strukturering og sentralisering vil påvirke hvordan arbeid skal og bør gjennomføres, og dette vil kunne påvirke hvor organisasjoner ønsker å ligge på skalaen. For svært byråkratiske og regelorienterte organisasjoner vil det for eksempel kunne være ønskelig å ligge på nivå 3 på en rekke temaer. Dette kan også sees i sammenheng med at man i dette tilfellet ligger på Westrums tredje nivå; en kalkulerende kultur.

Om man setter seg som mål å oppnå nivå tre eller fire i noen kategorier, så bør også dette taes hensyn til når man analyserer resultatene. Det kan derfor være akseptabelt at noen spørsmål gir en tilsynelatende lavere gjennomsnittsscore enn det kan være for andre spørsmål.

Datainnsamling

I hovedsak ønsker man så mange respondenter som mulig ved en slik kvantitativ tilnærming. Dette er både for å få et godt statistisk grunnlag, men også for å sette fokus på informasjonssikkerhet i virksomheten.

Når man skal motivere arbeidere til å delta i undersøkelsen er det viktig at man ikke gjør tiltak som favoriserer en type respondenter i større grad enn andre. Man må også sørge for å ikke å stille krav til respondentene som har negativ innvirkning på kvaliteten av besvarelsen. Et eksempel på dette vil være et belønningssystem som tilgodeser de som svarer nærmest opp til et ønsket svarmønster eller høyeste poengscore. Det må tilstrebes at hver enkelt respondent svarer så ærlig som mulig, slik at man får et reelt bilde av virksomheten. To ulike måter å samle respondenter er beskrevet i tabellen under:

Bruk av gulrot	Bruk av tvang
Respondenten motiveres til å delta ved bruk av belønning.	Respondenten tvinges til å delta – for eksempel gjennom at undersøkelsen gjøres obligatorisk.
Kan gi motivasjon til å ta seg tid til å delta i undersøkelsen, men man kan risikere at respondentene krysser i full fart for å sikre seg belønning eller lodd	Kan medføre at respondenten krysser fort for å bli ferdig og kunne fortsette med vanlig arbeid, ettersom man ikke får noe tilbake for å delta.

Begge disse tilnærmingene har blitt benyttet i ved bruk av forrige versjon av verktøyet.[36] Disse metodene er imidlertid ikke nok i seg selv. Synliggjøring av resultater er en svært viktig motivasjonsfaktor for deltakelse; det må komme frem at det å delta fører til noe. Det må komme frem hvor virksomheten gjør det bra og dårlig, og hvilke forbedringstiltak undersøkelsene har ført til. Dette kan gi arbeiderne motivasjon til å påvirke egen hverdag. Det er da viktig at:

- Det kommuniseres i god tid i forveien at ledelsen stiller seg bak undersøkelsen.
- Det må vises resultater og synliggjøres tiltak som en konsekvens av hva respondentene har svart.
- Det må vises at tiltak som tilsynelatende medfører merarbeid er viktig, verdsettes fra ledelseshold og at virksomheten som helhet er tjent ved å legge ned ressurser i informasjons-sikkerhet.

Vi har identifisert tre enkle fremgangsmåter for hvordan man kan samle inn statistiske data. Hver enkelt metode er kort presentert og deretter er det gitt en oppsummering av styrker og svakheter ved hver enkelt tilnærming

[36] Tvang (obligatorisk deltakelse) ble benyttet i forbindelse med en intervjubasert tilnærming, gulrot ble benyttet i sammenheng med en webbasert undersøkelse. I tillegg har man også benyttet en tilnærming med frivillig deltakelse uten gulrot i en tredje virksomhet. Sistnevnte førte til relativt lav svarprosent.

Webbasert spørreundersøkelse

Dette vil være en enkel metode større virksomheter kan benytte for å distribuere og samle informasjon. Man kan lage egne dedikerte applikasjoner som enten spres internt, eller som kjører gjennom et webgrensesnitt. Denne datainnsamlingsmetoden har blitt benyttet av en av samarbeidspartnerne i prosjektet, og erfaringene har vært gode.[37]

Med en slik tilnærming kan man enkelt lage fleksible løsninger som gjør det lettvint å legge til og/eller fjerne spørsmål fra basispakken og tilleggspakken. Det vil også være enkelt å samle resultatene fra undersøkelsen for videre statistisk bearbeidelse. De viktigste fordelene og ulempene ved bruk av webbaserte undersøkelser er gjengitt i tabellen under:

Webbasert undersøkelse	
Fordeler	**Ulemper**
• Enkel å distribuere og enkelt å samle inn resultater. • Større statistisk materiale som gir godt grunnlag for å sammenligne grupper og kan også gi grunnlag for hypotesetesting. • Man kan nå større deler av organisasjonen og lettere få et bilde av organisasjonen som helhet.	• Nyanser fra avdeling til avdeling kan fort bli borte ved analysen da en massiv spredt respons fort setter et større fokus på organisasjonen som helhet. • Man mister nyanser i besvarelsene som kan komme frem om respondenten kan henvende seg til ansvarlige for undersøkelsen. • Det vil være vanskeligere å få respondenten til å reflektere over sammenhengen mellom spørsmålene og hvordan disse gir en indikasjon på ønsket atferd og bevissthetsgrad ved behandling av sensitiv informasjon. • Man har mindre kontroll med kvaliteten i besvarelsene. Det kan herske ulike motiver for å svare på undersøkelsen.

Ved bruk av en internettbasert undersøkelse er det viktig å sørge for å gjøre verktøyet godt kjent i organisasjonen. Dette kan for eksempel gjøres ved å skrive en kort introduksjon på intranettet.

[37] Den webbaserte datainnsamlingsmetoden ble i denne virksomheten kombinert med gulrotpolitikk for å få ansatte til å delta.

Papirbasert spørreundersøkelse

Den papirbaserte undersøkelsen baserer seg på å trykke opp undersøkelsen på papir og distribuere disse i organisasjonen. Skjemaene samles deretter inn og skrives inn eller skannes for videre statistisk bearbeiding. Også denne datainnsamlingsmetoden har blitt benyttet i en av de samarbeidende virksomhetene.[38] De viktigste fordelene og ulempene er gjengitt i tabellen under:

Papirbasert undersøkelse	
Fordeler	**Ulemper**
• Enkelt å distribuere i organisasjoner hvor ikke alle bruker PC • Lettere å få folk til å konsentrere seg om undersøkelsen og ikke noe annet ved gjennomføring. • Gjør det lettere for respondentene å ta med seg undersøkelsen andre steder og å legge undersøkelsen fra seg om man trenger mer tid eller det dukker opp oppgaver som krever øyeblikkelig oppfølging. • Gjør det lettere for respondentene å gi kommentarer til uklare spørsmål rett på skjemaet. • Ovennevnte fordeler gir ofte resultat i høyere svarprosent, som igjen gir bedre grunnlag for å identifisere problemområder som gjelder hele avdelingen. • Gjennomføring av mindre, papirbaserte undersøkelser gjør det lettere å fange opp individuelle nyansene mellom avdelingene.	• Det er mer etterarbeid med å skrive inn svarene • Respondenten må ta kontakt med undersøkelsesteamet for å få avklart spørsmål som er uklare. • Det vil være vanskeligere å få respondenten til å reflektere over sammenhengen mellom spørsmålene og hvordan disse gir en indikasjon på ønsket atferd og bevissthetsgrad ved behandling av sensitiv informasjon. • Man har mindre kontroll med kvaliteten i besvarelsene. Det kan herske ulike motiver for å svare på undersøkelsen.

[38] Erfaringene fra denne datainnsamlingsmetoden er ikke like gode som på de andre to, men dette er i hovedsak fordi man gjorde deltakelsen frivillig; verken gulrot eller tvang ble benyttet. Erfaringene går i hovedsak på at man burde kombinert datainnsamlingsmetoden med en av disse metodene for å øke svarprosenten.

Intervjuundersøkelse

Den tredje datainnsamlingsmetoden baserer seg på at respondentene intervjues én etter én, og at resultatene noteres og tas med tilbake for statistisk analyse. Denne tilnærmingen har blitt benyttet av en tredje samarbeidende virksomhet, med gode erfaringer.

Under intervjuundersøkelser er det viktig at intervjuer er godt forberedt og har med seg undersøkelsen til både seg selv og til respondenten. Det kan også være nyttig å lage seg en liten intervjuguide på forhånd, som inneholder eksempler som illustrerer hva som menes og legges i de ulike spørsmålene dersom respondenten skulle være i tvil ved enkelte spørsmål. Viktige fordeler og ulemper ved intervjuundersøkelser er gjengitt i tabellen under:

Intervjuundersøkelse	
Fordeler	**Ulemper**
• Gir bedre mulighet til å kvalitetssikre besvarelsen ved å stille oppfølgingsspørsmål og be respondenten utdype der svaret virker uklart. • Gir mulighet til å bruke verktøyet til å vise sammenhenger mellom ulike aspekter ved sikkerhetskultur ved å lede respondenten inn i refleksjon over sammenhengen mellom spørsmålsstillingene og en økt bevissthet rundt sikkerhetskultur. • Respondenten får mulighet til å komme med tilleggsopplysninger og betraktninger som ikke er omhandlet direkte i spørsmålsbatteriet.	• Ressurskrevende • Gir lite statistisk grunnlag med mindre man gjennomfører intervjuene i massivt omfang. • Respondenten mister anonymitet og kan være ukomfortabel med situasjonen. Dette kan igjen medføre at respondenten ikke svarer ærlig.

Analyse av resultatene

I dette kapittelet vil vi belyse hvordan man skal tolke og analysere resultatene fra undersøkelsen. Det er i denne sammenheng nødvendig å ta hensyn til *hvordan* undersøkelsen er gjennomført, da dette vil ha innvirkning på hvilke resultater man kan forvente av undersøkelsen. Antallet respondenter som har deltatt er et eksempel på dette.

Tolkning av spørsmål og resultater

Spørsmålene i SjekkIT er delt inn i fire hovedkategorier; (1) kunnskap og holdning, (2) atferd, (3) policy og ledelse og (4) revisjon. Disse kategoriene omfatter sentrale spørsmål som i hovedsak skal analyseres og behandles selvstendig. Intensjonen for verktøyet er at hvert enkelt spørsmål skal bidra til å belyse et viktig emne i seg selv, kategoriene skal bidra til å gi respondenten et overordnet fokus. Det er derfor viktig å identifisere konkrete spørsmål og felter som er sterke og svake i en analyse.

I forrige versjon av verktøyet var spørsmålene delt opp i kategorier, identifisert fra sentrale faktorer innen arbeid med informasjons-sikkerhet. Spørsmålene i SjekkIT er i utviklingsprosessen blitt koplet opp mot sentrale elementer i god sikkerhetskultur og IKT-sikkerhetspolicy. Disse elementene er beskrevet i Vedlegg A, og koplinger mot spørsmål er gjengitt i Vedlegg B. Spørsmål som ikke er koplet opp er basert på innspill i utviklingsprosessen. En beskrivelse av hvert enkelt spørsmål er gitt i Vedlegg C.

Koplinger mellom spørsmålene i denne og forrige versjon av verktøyet er gjengitt i Vedlegg D, slik at virksomheter som ønsker det kan sammenlikne med tidligere resultater. Det anbefales imidlertid at hvert spørsmål behandles mest mulig selvstendig, eller eventuelt relatert til felles temaer som for eksempel IT-sikkerhet og rapporteringskultur der dette er aktuelt.

Ved å analysere ut i fra de demografiske dataene kan man finne ut hvilke deler av organisasjonen hvor det er sprik og deretter rette spesifikke, målrettede forbedringsplaner mot disse. Dette kan anses å

være en sammenlikning av ulike praksisfelleskap[39] i virksomheten der oppfattelser og meninger kan variere stort.

Ettersom man selv kan konfigurere verkøyet til å dekke de mest relevante feltene i virksomhetene, vil dette også ha en innvirkning på analysen av resultatene. Noen spørsmål kan være i relevante i større og mindre grad i deler av virksomheten, og resultatene kan gi større spredning, eller indikere en lavere eller høyere verdi enn det som er reelt for virksomheten. Det er derfor viktig at man er forsiktig med å tolke resultatet som strengt positive eller negative på disse spørsmålene. Her må hver enkelt virksomhet benytte skjønn for å avgjøre hvilke spørsmål man kan forvente hva fra.

Statistisk analyse

Når det gjelder tolkning av resultatene, er det flere muligheter for statiske analyser. Den enkleste er å måle gjennomsnittsverdier på hvert enkelt spørsmål og sammenligne disse mot et ønsket nivå i virksomheten, samt mot de øvrige spørsmålene man har valgt å inkludere. Ved å sammenligne resultater fra de forskjellige demografiske grupperingene som er gjort kan man identifisere og rette tiltak mot spesifikke målgrupper i organisasjonen.

For å kunne behandle svarene og samtidig kunne si noe om resultatet for hver enkelte demografiske oppdeling, er det en enkel tommelfingerregel for hvor mange besvarelser man bør ha. Den sier at du bør ha minst like mange besvarelser per oppdeling, som antall spørsmål som er med i undersøkelsen. Skal man analysere resultatene per avdeling, bør man med andre ord helst ha like mange besvarelser per avdeling som det er antall spørsmål i undersøkelsen.

Verktøyet kan også benyttes til å måle endringer i organisasjonen over tid, ved å gjennomføre undersøkelsen jevnlig og se på resultatene fra periode til periode. Om man gjennomfører denne tilnærmingen er det viktig å være klar over forutsetningene som kreves for å kunne hevde at endringene i målingene er av statistisk signifikans.[40] I utgangs-

[39] I henhold til Scheins (1992) beskrivelse av begrepet.

[40] For statistiske analyser anbefales det å lese relevant litteratur på området, for eksempel læreboken i statistikk som benyttes ved NTNU: R. E. Walpole, R. H. Myers, S. L. Myers and K. Ye (2002): Probability and Statistics for Engineers and Scientists, Prentice Hall.

punktet kreves det at man har uavhengig datamateriale, noe som forutsetter at man ikke kan benytte samme respondenter flere år på rad, eller at de er upåvirket av forrige undersøkelse når de gjennomfører neste. I praksis er dette meget vanskelig å gjennomføre og man skal derfor være forsiktig med å hevde at man har et statistisk grunnlag som viser endringen. Resultatene kan allikevel benyttes til å vise en trend om man kan se en endring over flere perioder, samt å identifisere områder for videre analyse.

8. Bruk av SjekkIT for å bygge IKT-sikkerhetskultur

Seniorforsker Stig O. Johnsen
Sintef Teknologi og Samfunn, avdeling Sikkerhet og Pålitelighet
stig.o.johnsen@sintef.no

I Stortingsmelding 7 (2001-2002) står det: "det ledelsen systematisk gir oppmerksomhet og prioritet, blir kultur" – og slik er det også med IKT-sikkerhetskultur. Utvikling og forbedring av sikkerhetskulturen er en aktivitet som krever tid, oppmerksomhet og innsats både fra ledelsen og selvsagt de enkelte ansatte. Forbedring og utvikling av sikkerhetskultur er ikke ett enkelt skippertak, men en kontinuerlig forbedringsprosess som må gå over lengre tid.

SjekkIT kan benyttes til å evaluere dagens status, men også benyttes til å videreutvikle IKT sikkerhetskulturen. Når en skal ta i bruk skjemaet har vi anbefalt at følgende tre hovedaktiviteter gjennomføres:

1. **Planlegg bruken av SjekkIT:**
2. **Gjennomfør SjekkIT-undersøkelsen (bruk workshop/søkekonferanse)**
3. **Følg opp resultatene fra SjekkIT og forbered neste SjekkIT undersøkelse**

Disse aktivitetene er beskrevet mer fullstendig i avsnittet som følger. En slik fremgangsmåte er en vanlig prosess i forbindelse med organisasjonsutvikling og organisasjonslæring.[41]

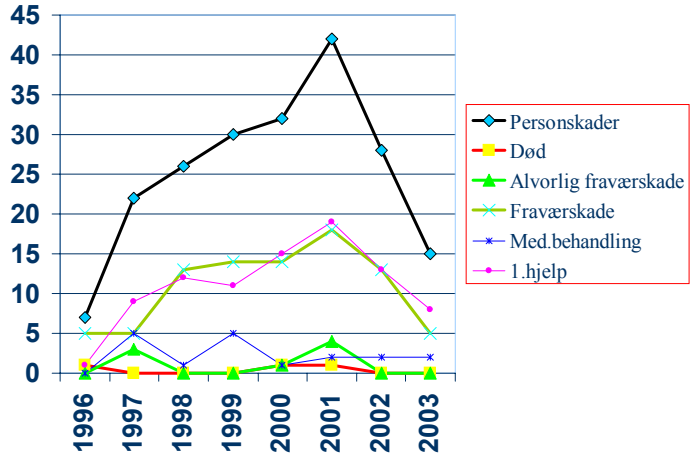
Organisasjonsutvikling som samskapt læring, hvor skjemaet SjekkIT brukes som basis for å videreutvikle holdninger og etablere tiltak, har vist seg å fungere. Spesielt det å diskutere holdninger og tiltak i en fellesarena mellom ledelsen og de ansatte har vist seg å være konstruktivt. Sjansen for å gjennomføre noe øker hvis folk får være med å bestemme selv.

Eksempler på områder som vanligvis evalueres og videreutvikles i forbindelse med sikkerhetskultur er:

[41] Se eksempelvis M. Levin "Ledelse og Teknologi" – Universitetsforlaget 1999

- Lederengasjement
- Rapporteringskultur og løpende læring av hendelser
- Løpende tilpasning av rutiner/prosedyrer og regler i samarbeid
- Opplæring og utvikling av felles verdier

NTNU/SINTEF har bygd opp erfaring på kulturverktøy og vi har etablert et faglig nettverk knyttet til dette, basert også på verktøy som er inspirert av Hearts and Minds utviklet av Shell International fra 1986. Hearts and Minds synes å ha redusert antall ulykker og hendelser i Shell. De prosjektene av SINTEF og NTNU som har basert seg på en bred tilnærming av sikkerhetskultur har vært vellykket. Et eksempel på et slikt prosjekt vises i Figur 12, hvor resultatet av en tilsvarende prosess igangsatt i 2001 ga meget positive resultater av utvikling av ulykkesfrekvensen i de påfølgende årene.



Figur 12: Utvikling av ulykker etter igangsetting av sikkerhetstiltak i 2001

Som tidligere nevnt vil vi foreslå tre hovedaktiviteter for å videre-utvikle IKT-sikkerheten og IKT-sikkerhetskulturen. Omfanget av disse aktivitetene vil vi anslå slik:

1. **Planlegg bruken av SjekkIT** **- ca ½ dag**
2. **Gjennomfør SjekkIT undersøkelsen** **- ca ½ til 1 dag**
3. **Følg opp** **- ca ½ dag**

Hovedaktivitetene kan beskrives slik:

1. **Planlegg bruken av SjekkIT:**
   - Avklar hvem skal eie forbedringsprosessen knyttet til å fylle ut skjemaet. Vårt råd er at ledelsen, sjefene må eie prosessen knyttet til å fylle ut skjemaet og behandle resultatet.
   - Avklar hva som er fokusområdet som skal forbedres ved å fylle ut skjemaet og hvem er målgruppe for skjemaet. Det kan være uønskede hendelser og spesielle områder som en ønsker forbedret.
   - Identifiser indikatorer som skal følges opp og forbedres i forbindelse med undersøkelsen. Indikatorer kan eksempelvis være tid og resurser brukt til å behandle uønskede hendelser.
   - Tilpass skjemaet til målgruppe og fokusområde, ved å velge ut spørsmål som du synes er relevante.

2. **Gjennomfør SjekkIT undersøkelsen (bruk workshop/søkekonferanse):**
   - Send ut skjemaet til målgruppen og sørg for at skjemaet fylles ut.
   - Diskuter svarene i en gruppe bestående av ledelse, ansatte/målgruppe. Prioriter de 4-5 viktigste forbedrings-områdene i samarbeid i gruppen. Identifiser tiltak med ansvarlige og måldato som kan forbedre sikkerhetskulturen for de utvalgte områdene. Gjennomfør dette i en god gruppe-prosess, slik at både de ansatte og ledelsen opplever at de har eierskap til prosessen og resultatet.

3. **Følg opp resultatene fra SjekkIT og forbered neste SjekkIT undersøkelse:**
   - Følg opp tiltakene periodisk, slik at barrierer og forsinkelser ikke setter en stopper for tiltakene.
   - Følg opp utvikling av holdninger. Gjennomfør forbedringstiltak som også innebærer endringer av interne regler og rutiner.
   - Gjennomfør spørreundersøkelsen etter ca 1 år for å følge opp utvikling av svar som gis.
   - Følg opp indikatorene som er valgt ut, og sjekk at tiltakene leder til en positiv utvikling.

Vi foreslår at skjemaet tas i bruk ut fra et reelt behov for å kunne videreutvikle sikkerheten og sikkerhetskulturen. Lykke til!

9. Videre arbeid

Denne rapporten har presentert versjon to av verktøyet. I og med at verktøyet i helhet er utviklet av vernepliktige som avtjener ettårig førstegangstjeneste, vil utviklingen av verktøyet være iterativ. Hvert nytt kull vil ta for seg ulike aspekter for deretter å sette seg inn relevant teori i forhold til dette.

I den første rapporten ble det gjort rede for hvorfor kulturaspektet og innsideproblematikk er et relevant tema innen sikkerhetsarbeid. Utfordringer i forhold til å måle virkning av myke verdier, samt en taksonomi for klassifisering av menneskelige utfordringer til informasjonssikkerhet ble også undersøkt.

Resultatet fra forrige kull ble et verktøy med utgangspunkt i Hearts and Minds fra Shell. I denne rapporten har det blitt fokusert på å videreutvikle dette verktøyet i tett samarbeid med brukere av forrige utgave, samt å gi den nye versjonen et godt teoretisk fundament. Under vil vi presentere noen av de problemstillingene vi ikke har rukket å jobbe med, men som er aspekter som er relevante i forhold til neste iterasjon i evolusjonen av verktøyet.

Kobling mot andre relevante metoder og teorier

Vi anser SjekkIT som et godt diagnostiseringsverktøy som kan identifisere problemområder i organisasjonen. Det ville være hensiktsmessig om man etterpå kunne benytte andre relevante verktøy eller metodegrunnlag til å gjøre videre analyser av problemene. Tiltaksverktøy vil også være relevante i den videre analysen.

Lage en brosjyreversjon av verktøyet

Det kan være hensiktsmessig å lage en enklere presentasjon av verktøyet, for eksempel i form av en brosjyre eller utbrettskart.[42] Denne brosjyren bør kun presentere informasjon som er relevant for gjennomføring av undersøkelser. Dette vil forenkle spredning og bruk av verktøyet. De som er interessert i teorien bak vil fortsatt ha mulighet til å finne denne i den fulle rapporten.

[42] Dette ble gjort med Hearts and Minds; Shell International Exploration and Production B.V (2001).

Utvikling av en engelskspråklig versjon

I forhold til å benytte verktøyet i multinasjonale, eller flerspråklige virksomheter, vil det være nyttig om verktøyet er oversatt fra norsk. Dette har vært et konkret ønske fra flere samarbeidspartnere, men kan også være interessant for seg selv dersom rapporten skal brukes i internasjonal forskning.

Engelsk er verdensspråket og det vil være mest hensiktsmessig å begynne med å lage en engelskspråklig utgave. På sikt kan det også være aktuelt med andre språk. Det er viktig at man kvalitetssikrer oversettelsesarbeidet slik at man beholder utvetydige spiss-formuleringer som gir respondenten en klar formening om hva han svarer på. Dette også for å sikre kvaliteten i besvarelsene i forhold til å sammenligne med respons fra andre utgaver med andre språk.

Utvikling av et internettbasert verktøy

Når verktøyet benyttes til diagnostisering er kvaliteten på diagnosen avhengig av antall respondenter. En hensiktsmessig tilnærming i forhold til å nå flest mulig respondenter vil være å utvikle en gjennomtenkt internettløsning. Her kan man benytte seg av flere fordeler i mediet for å sikre kvalitet på besvarelsene:

- Multimedia i form av bilder, video og lyd.
- Hjelpetekst som kommer frem ved behov.
- Visning av ett og ett spørsmål, så undersøkelsen virker mindre massiv.
- Gi respondenten mulighet til å gå ut av undersøkelsen, for så å fortsette på et senere tidspunkt.
- Gi øyeblikkelig grafisk tilbakemelding til brukeren på besvarelsen og hvilke kategorier som scorer lavt og kanskje litt om hvordan dette leses i ettertid – om brukeren skulle ønske å legge ved en tilleggskommentar til besvarelsen.

Det vil ut ifra en slik undersøkelse være lettvint å samle besvarelsene rett i et analyseverktøy for videre behandling.

Videreutvikling av spørsmålsbatteriet

Det vil også være viktig å ta for seg spørsmålsproblemstillingene og se til at man har dekket inn sentrale problemområder. Andre felter som er vesentlige i forhold til informasjonssikkerhet kan ha kommet til.

En revisjon av spørsmålsformuleringer og svaralternativer i tråd med utviklingen innen områdene man tar opp vil også være nødvendig. På denne måten kan man sikre at spørsmålene er fortsatt er aktuelle i tråd med teknologisk utvikling og endrede organiserings- og atferds-mønstre.

I forhold til spørsmålene kan det være hensiktsmessig å gjøre statistiske analyser av erfaringsdata fra gjennomførte analyser. Ved hjelp av forskjellige statistiske metoder kan man identifisere eventuell kovarians mellom spørsmålene. Der man identifiserer avhengigheter bør man se om spørsmålene er overflødige beskrivelser av samme problemstilling, eller om spørsmålene utfyller hverandre. Det finnes flere kjente statistiske metoder for å vise sammenheng mellom spørsmål. Under følger et lite knippe med de mest sentrale i forhold til SjekkIT.

Statiske analysemetoder	
Faktorgruppering	Det vil være interessant og se om man kan finne en faktorinndeling for spørsmålsgruppene. Her vil man kunne identifisere kovarians mellom spørsmålene og vurdere hvorvidt det er av verdi å ta med alle spørsmålene per gruppe. Det vil også være av interesse å se om man har samme gruppering på spørsmålene rent statistisk som den kategoriseringen man har gjort nå.
Regresjonsanalyser	Det vil også være av interesse å gjøre regresjonsanalyser av hvert spørsmål mot en målbar parameter i forhold til det spørsmålet eller gruppen av spørsmål ønsker å påvirke, for eksempel antall uønskede hendelser mot atferdsspørsmål relatert til bestemte uønskede hendelser. Om vi kan vise en sammenheng mellom svarene og parameteren kan det på-vises en sammenheng mellom spørsmålet og atferden man ønsker å identifisere.
Principal Component analyse	Det vil være av interesse å sammenligne grupperinger av spørsmål mot hverandre i et mangedimensjonalt koordinat-system for å se om vi kan identifisere kovarians mellom svarene og se på mulige tolkninger av spørsmål med høy varians. Kanskje kan svar fra forskjellige spørsmål belyse problemstillingene fra forskjellig vinkel, og i så måte senke den relative spredningen innen det vi ønsker å måle.
Annovaanalyse	Kan vi dele datasettet opp i grupper slik at det er mindre variasjon innenfor gruppene enn det er mellom gruppene? I så fall kan spørsmål som har vært vanskelige å trekke entydige meninger ut av være slåes sammen med andre spørsmål og være med å bidra til en mer entydig tolkning av spørsmålet.

Referanser

Albrechtsen, E. Kufås, I. & Tobiassen, J. (2002), *Organisatoriske faktorer i informasjonssikkerhet,* Fordypningsprosjekt ved Institutt for industriell økonomi og teknologiledelse, NTNU.

Albrechtsen, E., Grøtan, T.O., Johnsen, S.O. (2005), *IKT-sikkerhets-politikk for SMB*, Sintefrapport.

Argyris, C. & Schön, D. (1996), *Organizational learning II: Theory, method and practice*. Addison-Wesley, Reading, Mass.

Aune, A. (2000), *Kvalitetsdrevet ledelse – kvalitetsstyrte bedrifter*, tredje utgave, Gyldendal Akademisk, Oslo.

Bolman, L.G. & Deal, T.E (2004), *Nytt perspektiv på organisasjon og ledelse*, tredje utgave, Gyldendal Akademisk, Oslo

Dybå, T. (2001), *Enabling Software Process Improvement: An Investigation of the Importance of Organizational Issues*, IDI Report 7/2001, Ph.D. Thesis, Norwegian University of Science and Technology, Trondheim.

Garvin, D. (1993), Building a Learning Organization*, Harvard Business Review*, **71**(4):78-91.

Hale, A. (2000), Editorial – Culture's confusion, *Safety Science*, **34**:1-14.

Hofstede, G. (1991), *Cultures and Organisations: Software of the Mind*, McGraw-Hill.

Hovden, J. (2004), *Sikkerhetsledelse og sikkerhetskultur – moteord uten reelt innhold eller forutsetning for god sikkerhet?,* Foredrag ved NSMs Sikkerhetskonferanse, Kolsås leir 17.-18. november 2004.

Hudson, P. & van der Graaf, G. C. (2002), *Hearts and Minds: The status after 15 years Research*, Society of Petroleum Engineers (SPE 73941) International conference on HSE in Oil and Gas Exploration and production, Kuala Lumpur 20.-22. mars 2002.

IAEA (2002), *Safety Culture in Nuclear Installations: Guidance for use in the enhancement of safety culture*, IAEA, Vienna, 2002, ISBN 92–0–119102–2.

Johnsen, S.O., Herrera, I.A., Jersin, E., Rosness, R., Vatn, J., Veiseth, M., Tungland, M., Bergersen, C.E.B. (2004), *The Track to Safety Culture (SafeTrack), a toolkit for operability analysis of cross border rail traffic, focusing on safety culture*, Sintefrapport STF38 A04414, ISBN 82-14-02731-4.

Kufås, I. (2002), *A framework for information security culture; could it help on solving the insider problem?* Artikkel i: Kufås, I. & Mølmann, R. A. (2003), *Informasjonssikkerhet og innsideproblematikk*, ROSS (NTNU) 200301, Nasjonal Sikkerhetsmyndighet og NTNU.

Kufås, I. & Mølmann, R. A. (2003a), *Informasjonssikkerhet, mennesker og kultur; diskusjon av verktøyet*, Artikkel i: Kufås, I. & Mølmann, R. A. (2003), *Informasjonssikkerhet og innside-problematikk*, ROSS (NTNU) 200301, Nasjonal Sikkerhetsmyndighet og NTNU.

Mintzberg, H. (1989), *Mintzberg on management: Inside our strange world of organizations*, The Free Press.

Mølmann, R. A. (2003), *The human factor: Taxonomy for classifying human challenges to information security*, Artikkel i: Kufås, I. & Mølmann, R. A. (2003), *Informasjonssikkerhet og innside-problematikk*, ROSS (NTNU) 200301, Nasjonal Sikkerhetsmyndighet og NTNU.

Nonaka, I. & Takeuchi, H. (1995), *The Knowledge-Creating Company,* Oxford University Press.

Rosness, R. (2001), *Safety Culture: Yet another buzzword to hide our confusion?*. SINTEF-notat. Tilgjengelig på www.risikoforsk.no/Publikasjoner/Safety%20culture.pdf

Schein, E.H. (1992), *Organizational Culture and Leadership*, Jossey-Bass, San Francisco.

Schein, E.H. (1996), Three Cultures of Management: The Key to Organizational Learning, *Sloan Management Review*, **38**(1).

Senge, P. (1990), *The Fifth Discipline: The Art & Practice of the Learning Organization,* Doubleday/Currency Books, New York.

Shell International Exploration and Production B.V (2001), *Hearts and Minds*, *HSE, Understanding your Culture*, brosjyre med undersøkelsesverktøyet fra SIEP.

Westrum, R. J. (1993), Cultures with Requisite Imagination, i: Wise, Stager and Hopkin (Eds.) *Verification and Validation of Complex Systems: Human Factors Issues*, Springer, Heidelberg.

Øksne, A. & Furuseth, H.R. (2004), *Risikohåndtering – bruk av risiko- og sårbarhetsanalyser i det kontinuerlige sikkerhetsarbeidet*, ROSS (NTNU) 200402, Nasjonal Sikkerhetsmyndighet og NTNU.

Vedlegg A: Bakgrunnsteori for spørsmål

Det finnes en rekke standarder og policies som angir hvordan sikkerhetsledelse og informasjonssikkerhetsledelse bør utføres. Tabellene under tar for seg sentrale deler fra IAEAs beskrivelse av god sikkerhetskultur, den internasjonale standarden ISO 17799, samt retningslinjer utarbeidet av Sintef for god IKT-sikkerhetspolitikk.

Viktige artefakter og/eller uttrykte verdier	
Karakteristikk	**Beskrivelse**
Forpliktelse fra toppledelsen	Toppledere må demonstrere forpliktelse til sikkerhet gjennom oppførsel, innstilling og ressursallokering.
Synlig lederskap	Lederne må gå foran som forbilder i sikkerhetsrelaterte saker.
Systematisk forpliktelse	Synliggjort gjennom kvaliteten på prosedyrer og dokumentasjon i sikkerhetsledelsessystemet, samt i kvaliteten på risikovurderinger og risikokontroll.
Selvvurdering	For å fremme ytelsen blant de ansatte ved å involvere de direkte i vurdering og forbedring av arbeidsrutiner.
Sikkerhetsfokus i strategiske planer	Sikkerhetsmål må spesifiseres, måles og følges opp.
Sikkerhet vs. Produksjon	Ingen konflikter mellom fokus og prioritering av sikkerhet kontra produksjon.
Tilsynsorganer og eksterne grupper	Felles nivå av respekt mellom ansatte i virksomheten, tilsynsorganer og andre eksterne grupper.
Proaktivt og langsiktig perspektiv	Planer må ha korte, middels lange og langsiktige målsettinger for å vise at virksomheten aktivt forbereder seg til fremtiden.
Endringsledelse	Virksomheten må kjenne til utfordringene relatert til endring, og må ha kjennskap til implikasjonene for sikkerhet.
Dokumentasjon og rutiner	Virksomhetens rutiner og dokumentasjon må være lettfattelig og lett tilgjengelig, og må benyttes både til opplæring og i arbeidssituasjoner.
Forskrifter og prosedyrer	Prosedyrene må ta høyde hva man skal gjøre dersom uventede hendelser inntreffer.
Tilstrekkelig kompetent personale	Både kvaliteten og kvantiteten på personalet er viktig for å kunne opprettholde et godt sikkerhetsnivå.
Utforskende holdning	Ansatte må ha en utforskende holdning for å kunne identifisere svakheter, og ikke bare følge rutinene blindt.
MTO-perspektiv	Kunnskap om interaksjonen mellom menneske, organisasjon og teknologi, og hvordan dette påvirker sikkerhet.

Klare roller	Ansvarsforholdene og rollene relatert til sikkerhet må være klart definerte, og ansvaret for sikkerhetsrelaterte oppgaver.
Motivasjon og tilfredsstillelse	Atferden til ansatte er i stor grad preget av graden av motivasjon de har og tilfredsstillelsen de får av arbeidet.
Involvering	Ansatte vil ikke ha et eierskap for sikkerhet hvis de ikke er involvert i å identifisere og løse sikkerhetsproblemer.
Gode arbeidsforhold	Sikkerhet kan kompromitteres på bakgrunn av tidspress, arbeidsbelastning og stress.
Måling	Sikkerhetsytelsen må måles, og trender og resultater må formidles til alle ansatte.
Ressursallokering	Allokering av ressurser til rutine- og ikkerutinearbeid må vurderes opp mot sikkerhetsperspektiver.
Samarbeid	Gruppearbeid og kryssfunksjonelt samarbeid må være effektivt og bør belønnes.
Konflikthåndtering	Det må være enkelt å kunne ta opp problemer, slik at mistro og syndebukker unngås.
Åpent forhold	Ledere og ansatte må ha et åpent og respektfullt forhold.
Forståelse for samspill	Ansatte må ha forståelse for sine arbeidsprosesser og samspillet mellom de ulike arbeidsprosessene i virksomheten.
God orden og fysisk stand	Den fysiske standen på virksomheten, og ordenen i lokalene påvirker moralen, og dermed også nivået på sikkerheten.

Uttrykte verdier	
Karakteristikk	**Beskrivelse**
"Sikkerhet prioriteres høyt"	Uttrykket må følges opp med handlinger og atferd, for eksempel gjennom ressursallokering og klare ansvarsforhold.
"Sikkerheten kan alltid forbedres"	Organisasjoner må ha et kontinuerlig fokus på å forbedre sikkerheten – dette er tett relatert til selvvurdering blant ansatte.
Åpenhet og kommunikasjon	Ansatte må være sikre på at de kan tiltros kunnskap, og også ha muligheten til å individuelt eller som en gruppe kommunisere eventuelle bekymringer.
Organisasjonslæring	Det er en villighet til å lære og på å dele sine erfaringer med andre.
Grunnleggende antakelser	
Karakteristikk	**Beskrivelse**
Tidsfokus	Det må være en balanse mellom fortid, nåtid og fremtid. Denne balansen må være tydelig i plan-legging av aktiviteter og i de ansattes arbeid.
Synet på feil	Feil kan ses på noe man kan lære av eller noe man må straffe. I et sikkerhetsperspektiv er det viktig å kunne påpeke sikkerhetsfeil uten å frykte straff – ellers vil kunnskapen bli holdt tilbake.

Synet på sikkerhet	Alle ansatte må føle et ansvar for å ha god sikkerhet i virksomheten.
Systemtenking	Man må ha en forståelse for samhandlingen mellom ulike deler og systemer.
Lederens rolle	Ledelsesfilosofien påvirker hvordan man opptrer i en virksomhet, men dette hemmer ikke muligheten for å opptre som en instruktør og lagleder for å bidra med sikkerhetsrelatert kunnskap.
Synet på mennesker	Menneskesynet påvirker hvordan ansatte behandles i en organisasjon. Ansatte kan ses på som udisiplinerte og selvinnrettet, eller som interesserte i å oppnå sitt potensial gjennom utvikling. Det sist-nevnte synet har flest fordeler for sikkerhet på lang sikt.

Sikkerhetspolitikk basert på ISO 17799	
Karakteristikk	**Beskrivelse**
Begrepet IKT-sikkerhet må være avklart	Begrepet må være avklart og satt inn i en mer generell sikkerhetssammenheng
Styret og ledelsen må ha et tydelig og forpliktende engasjement	Virksomhetens styre og ledelse skal ha et tydelig og forpliktende engasjement i forhold til IKT-sikkerhet, og skal aktivt bidra til profilering og legitimering av det daglige arbeidet med IKT-sikkerhet og gjennom praksis vise at hensynet til IKT-sikkerhet gjennomsyrer mål, strategier og beslutninger.
Behovet må være klarlagt, og tydelige målsettinger utledet	Behovet for IKT-sikkerhet skal være klarlagt, og mål-settinger for arbeidet med IKT-sikkerhet må være utledet.
Sikkerhetspolicyen må ha en klar hensikt mot målgruppen	Målgruppen for policyen er egne ansatte og eksterne samarbeidspartnere.
Sentrale, relevante IKT-sikkerhetsprinsipper må være beskrevet	Virksomheten skal føre en oversikt over hvilke generelle og spesifikke utfordringer som er særlig viktige og som skal prioriteres. IKT-brukere ved virksomheten skal gis veiledning og opplæring som sikrer korrekt atferd i forhold til relevante systemer og brukergrensesnitt.
Roller og ansvar må for ledelse og ansatte må være beskrevet	Det skal utarbeides stillingsinstrukser med beskrivelse av ansvar og oppgaver for IKT-sikkerhetspersonell. Daglig leder skal ha ansvar for organisering og gjennomføring av sikkerhetsarbeid.
Konsekvenser av brudd på sikkerhetspolitikk og regler må være beskrevet	Alle vesentlige regelbrudd skal påtales og følges opp internt. Relevante hendelser som har interesser for andre skal rapporteres til dertil egnede organer.
Sikkerhetspolitikken skal evalueres løpende, og være en del av den løpende intern-kontrollen	Sikkerhetspolitikken skal endres jevnlig og oppdateres i takt med endrede rammebetingelser og teknologiutvikling. Gjennomføring av det organiserte sikkerhetsarbeidet skal evalueres jevnlig på grunnlag av beskrivelser av oppgavens ansvar. Det skal utarbeides regelmessige rapporter som skal benyttes til revisjon.

Sentrale IKT-sikkerhetsprinsipper	
Karakteristikk	**Beskrivelse**
Sikkerhetsledelse	En uttalelse fra ledelsen om dennes engasjement er en viktig del av en IKT-sikkerhetspolitikk. Ledelsens uttalelse kan øke de ansattes oppmerksomhet mot IKT-sikkerhet. Herunder anbefales at øverste leder signerer dokumentet.
Samsvar med lovpålagte krav	Alt IKT-sikkerhetsarbeid i organisasjonen skal være i samsvar med de lovpålagte krav virksomheten må forholde seg til. IKT-sikkerhetsledelse skal koordineres med HMS og internkontroll.
Etiske hensyn	Virksomheten skal respektere andres rettmessige interesser. Virksomhetens handling eller mangel på handling kan skade andre. Det etiske aspektet skal også vektlegges ved risikovurdering. Risiko skal derfor ikke bedømmes ene og alene ut fra virksomhetens egne behov, men også ut fra de ringvirkninger sikkerhetsbrudd hos kan påføre andre virksomheter.
Risikobasert tilnærming	Virksomheten skal gjennomføre risikovurderinger for å systematisk identifisere trusler og sårbarhetsfaktorer, slik at den kan vite hvilke handlinger og prioriteringer som må gjøres og dermed implementere egnede tiltak for å håndtere uakseptable risikoer.
Klassifisering av informasjon og IKT-systemer	Informasjon og IKT-systemer skal være klassifisert for å indikere behov, prioritet og grad av beskyttelse. Klassifiseringer identifiseres gjennom lover/regler og risikovurderingen, og samordnes så langt som praktisk mulig med tilsvarende kategoriseringer hos samarbeidspartnere.
Håndtering av eksterne brukere og samarbeidspartnere	IKT-sikkerhet skal ivaretaes hvis Virksomheten setter ut (outsourcer) drift av sine IKT-systemer til en ekstern part. En kontrakt skal inngåes for å klarlegge ansvar for risikovurdering, sikkerhetstiltak og -prosedyrer for IKT-systemer. Viktige momenter er definisjon og håndtering av avvik, rapportering av driftsavbrudd, opplisting av autoriserte personer hos leverandør, begrensinger i bruk av tilgjengelige tjenester, mv
Fysiske tiltak	Utstyr og informasjon skal sikres mot farer i omgivelsene (eks. brann, vann, støv), spionasje, sabotasje og tyveri vha både bygningsmessige tiltak og bruk av automatiske overvåknings-, kontroll- og varslingssystemer. Kritiske elementer i IKT-systemer og sensitiv informasjon skal befinne seg i sikre områder, beskyttet av barrierer og inngangskontroll. Beskyttelsesbehovet skal være bestemt ut fra fastsatt risiko, ref risikovurderingen.
Innføring av nye systemer og vedlikehold av eksisterende	Planlegging og forberedelse av innføring av nye systemer skal gjennomføres slik at man tar hensyn til relevante sikkerhetsmessige krav som

	tilgjengelighet, behov for kapasitet /ytelse og behov for ressurser med sikkerhetsmessig kompetanse. Sikkerhet skal være designet inn i alle systemer og vedlikeholdt deretter.
Nettverk- og internettbeskyttelse	For å hindre sikkerhetsbrudd i nettverkstjenester skal tilgang til både interne og eksterne nett kontrolleres ved barrierer og autentiseringsmekanismer for brukere og utstyr ved tilgang til informasjon og i grensesnitt mellom Virksomheten sitt nettverk, andre virksomheters nettverk og offentlige nett.
Beskyttelse mot og oppdagelse av ondsinnet kode (”vern mot infeksjonssykdommer”) og uønsket reklame (spam)	Det skal etableres tiltak for å forhindre og oppdage ondsinnet kode (for eksempel virus, ormer, trojanere og logiske bomber). Bevissthet og riktig atferd fra den enkelte IKT-bruker kombinert med teknologiske installasjoner skal forhindre og oppdage ondsinnet kode hos organisasjonen.
E-post og spam	Det anbefales å bruke oppdaterte spamfilter. Samtidig må brukerne ha mulighet til å inspisere hvilke meldinger som er stoppet, og ha muligheter for å påvirke filtreringskriteriene.
Basis IKT-forvaltning	Her beskrives forvaltning av IKT som ikke nødvendigvis er spesifikt sikkerhetsrelevant, men som må ligge i bunnen for en sikkerhetspolitikk.
Tilgangsstyring/Brukertilgang	Formelle prosedyrer skal etableres for å kontrollere fordeling av tilgangsrettigheter til IKT-systemer og servicer. Prosedyrene skal dekke alle faser av brukertilgang, fra første registrering til de-registrering av brukere som ikke lenger trenger tilgang til systemene.
Anskaffelse og avskaffelse	Ved anskaffelse av utstyr og programvare skal sikkerhet være integrert. Service og vedlikehold skal inngå ved anskaffelse. Det skal kontrolleres at sensitiv informasjon og lisensiert programvare er fjernet eller overskrevet på alt utstyr med lagringskapasitet før avhending.
Hendelses- og krisehåndtering	Det skal etableres kanaler som aktører (ansatte, kunder, outsourcing, tredjepart) snarest mulig skal rapportere til om uønskede hendelser. Et beredskapssystem skal etableres for å redusere forstyrrelser fra sikkerhetshendelser ved å kombinere preventive- og gjenopprettingstiltak.
Behandling av ny teknologi	I dag er trenden at man "tar det man får" i form av ferdigpakkede standardkomponenter. Dette innebærer at sikkerhetskompetansen forskyves fra brukersiden til leverandørsiden. Så langt det er praktisk mulig skal det utarbeides forholdsregler før slikt utstyr tas i bruk
Brukermedvirkning	De ansattes forståelser og forslag skal benyttes i planleggingen av både teknologiske og administrative IKT-sikkerhetssystemer. Dette innebærer at policydokumentet må utarbeides og implementeres sammen med de ansatte.
Formelle og uformelle individrettede tiltak og	Det skal etableres prosedyrer (regler, arbeidsinstrukser) for bruk av informasjon og IKT-

bevisstgjøring	systemer for å støtte opp under politikken. Prosedyrene skal være dokumenterte og vedlikeholdes, og skal sørge for riktig og sikker bruk av informasjon og IKT.
Konsekvenser av brudd på policyen og disiplinære handlinger	Alle vesentlige sikkerhetsbrudd skal påtales og følges opp internt. Alle ulovligheter skal anmeldes. God atferd i sikkerhetsspørsmål bør også profileres.

Vedlegg B: Kopling mellom spørsmål og teori

Viktige artefakter og/eller uttrykte verdier (IAEA, 2002)	
Karakteristikk	**Dekning i verktøyet**
Forpliktelse fra toppledelsen	Dekket av spørsmål 16, 17 og 21, som ser på kommunikasjon, lederens rolle og ressursallokering.
Synlig lederskap	Dekket av spørsmål 16 og 17, som omfatter kommunikasjon og lederens rolle.
Systematisk forpliktelse	Dekket av spørsmål 26, 27 28 og 30, som omfatter rutiner og revisjon.
Selvvurdering	Dekket av spørsmål 18, som omfatter involvering av ansatte
Sikkerhetsfokus i strategiske planer	Dekket av spørsmål 1; tilstedeværelse av og kjennskap til målsettinger og en klar sikkerhetspolicy.
Sikkerhet vs. Produksjon	Dekket av spørsmål 3 og 21, som ser på prioritering av ressurser og holdningene til sikkerhetsregelbrudd.
Tilsynsorganer og eksterne grupper	Dekket av spørsmål 19 og T.30, som omhandler erfaringsdeling med andre virksomheter og myndigheter.
Proaktivt og langsiktig perspektiv	Dekket av spørsmål 1 og T.26, som omfatter tilstedeværelsen av policy og målsettinger, og tilstedeværelse av en proaktiv tankegang hos ansatte.
Endringsledelse	Kan dekkes inn gjennom bruk av verktøyet, ved å formidle målingsresultatene, samt benytte verktøyet for kontroll av sikkerhetskritiske områder i en endringsprosess.
Dokumentasjon og rutiner	Dekket av spørsmål 2, T.13 og T.18 som ser på kjennskap og bruk av rutiner og prosedyrer, og hvordan dette påvirker hverdagen i virksomheten.
Forskrifter og prosedyrer	Dekket av spørsmål 23, 27 og 28, som ser på beredskap og rapportering av uønskede hendelser.
Tilstrekkelig kompetent personale	Opplæringsaspektene er dekket av spørsmål 6 og T.29. Kunnskapsnivået måles også gjennom kjennskapen til mål, regler og lovverk; det vil si spørsmål 1, 14 (pluss T.31 og T.32) og T.13.
Utforskende holdning	Ikke direkte dekket av spørsmålene. Spørsmål 4, 7, T.12 og T.16 kan antas å være relatert til disse holdningene. Disse spørsmålene dekker feltene om noen får skyld ved en uønsket hendelse, om det er akseptert å innrømme feil og å peke på feil hos andre.

MTO-perspektiv	Dekkes gjennom bruk av verktøyet, som dekker MTO-perspektivene. Kunnskapen kan bygges gjennom formidling av resultatene fra undersøkelsen.
Klare roller	Dekket av spørsmål 5, som omhandler ansvarsforhold, samt spørsmål 18 som omfatter involvering av ansatte.
Motivasjon og tilfredsstillelse	Dekkes i demografidelen av undersøkelsen.
Involvering	Dekkes direkte i spørsmål 18.
Gode arbeidsforhold	Dekkes i demografidelen av undersøkelsen, samt av spørsmål 15.
Måling	Kan dekkes gjennom jevnlig bruk av verktøyet. Resultatene må formidles. Kommunikasjon dekkes i tillegg av spørsmål 16.
Ressursallokering	Dekkes av spørsmål 21, som omhandler prioritering av sikkerhetsoppgaver i forhold til regulære driftsoppgaver.
Samarbeid	Ikke direkte dekket. Kan dekkes gjennom bruk av verktøyet i en gruppesesjon for å identifisere virksomhetens status og vurdere tiltak.
Konflikthåndtering	Dekkes inn av spørsmål 7, T.14, T.16, T.19 og T.20.
Åpent forhold	Dekkes inn av spørsmål 4, 16, 17, T.12, T.16, T.19 og T.20.
Forståelse for samspill	Dekkes inn av spørsmål T.15
God orden og fysisk stand	Dekkes inn av spørsmål 25 og 15, som henholdsvis omfatter fysisk sikring av virksomheten, og den enkeltes ryddighet på kontorplassen.

Uttrykte verdier (IAEA, 2002)	
Karakteristikk	**Dekning i verktøyet**
"Sikkerhet prioriteres høyt"	Dekkes inn av spørsmål 1, men må også følges opp gjennom andre handlinger, som for eksempel gjennom spørsmål 3 og 21.
"Sikkerheten kan alltid forbedres"	Berøres av spørsmål 1 og 18.
Åpenhet og kommunikasjon	Berøres av spørsmål 4, 16, 18, 23, T.12, T.20 og T.21.
Organisasjonslæring	Berøres av spørsmål 18, 19, 20, 29 og T.30.

Grunnleggende antakelser (IAEA, 2002)	
Karakteristikk	**Dekning i verktøyet**
Tidsfokus	Blir berørt av spørsmål 1, gjennom policy og målsettinger.
Synet på feil	Blir berørt av spørsmål 4, 7, T.12, T.16, T.19 og T.20
Synet på sikkerhet	Blir berørt av spørsmål 2 og T.18.
Systemtenking	Blir berørt av spørsmål T.15
Lederens rolle	Blir berørt av spørsmål 16, 17 og T.12.
Synet på mennesker	Menneskesyn er ikke direkte dekket i verktøyet.

Sikkerhetspolitikk basert på ISO 17799	
Karakteristikk	**Dekning i verktøyet**
Begrepet IKT-sikkerhet må være avklart	Dekkes av spørsmål 1
Styret og ledelsen må ha et tydelig og forpliktende engasjement	Dekkes av spørsmål 1, 16, 17 og 21
Behovet for IKT-sikkerhet må være klarlagt, og tydelige målsettinger utledet	Dekkes av spørsmål 1 og 14
Sikkerhetspolicyen må ha en klar hensikt mot målgruppen	Dekkes av spørsmål 1, 2 og T.13
Sentrale, relevante IKT-sikkerhetsprinsipper må være beskrevet	Dekkes av spørsmål 1, T.13
Roller og ansvar må for ledelse og ansatte må være beskrevet	Dekkes av spørsmål 4 og 17
Konsekvenser av brudd på sikkerhetspolitikk og regler må være beskrevet	Dekkes av spørsmål 7, T.16
Sikkerhetspolitikken skal evalueres løpende, og være en del av den løpende internkontrollen	Spørsmål 26 og 28

Sentrale IKT-sikkerhetsprinsipper (Albrechtsen et al. 2005)	
Karakteristikk	**Dekning i verktøyet**
Sikkerhetsledelse	Dekket av spørsmål 1, 16, 17
Samsvar med lovpålagte krav	Dekket av spørsmål 14 + T.31 og T.32
Etiske hensyn	Ikke dekket
Risikobasert tilnærming	Dekket av spørsmål 30
Klassifisering av informasjon og IKT-systemer	Dekket av spørsmål 8 og 26
Håndtering av eksterne brukere og samarbeidspartnere	Dekket av spørsmål 19, 20 og T.30
Fysiske tiltak	Dekket av spørsmål 25
Innføring av nye systemer og vedlikehold av eksisterende systemer	Dekket av spørsmål 26, samt T.27 og T.33
Nettverk- og internettbeskyttelse	Dekket av spørsmål 10, 11, 12, 13 og 24
Beskyttelse mot og oppdagelse av ondsinnet kode	Dekket av spørsmål T.1, T.3 og T.21
E-post og spam	Dekket av spørsmål 11, T.1
Basis IKT-forvaltning	Ikke dekket
Tilgangsstyring/Brukertilgang	Dekket av spørsmål 10
Anskaffelse og avskaffelse	Dekket av spørsmål T.33
Hendelses- og krisehåndtering	Dekket av spørsmål 23, 27, 29
Behandling av ny teknologi	Dekket av spørsmål 26 og T.33
Brukermedvirkning	Dekket av spørsmål 18
Formelle og uformelle individrettede tiltak og bevisstgjøring	Dekket av spørsmål 5, 16, 17, T.29
Konsekvenser av brudd på policyen og disiplinære handlinger	Dekket av spørsmål 7

Vedlegg C: Beskrivelse av spørsmålene

Basisspørsmål – kunnskap og holdning

1	B/L	I hvilken grad kjenner du til om virksomheten klare målsettinger og en etablert policy for informasjonssikkerhet?	Jeg er ikke kjent med at virksomheten har mål-settinger eller policy for informasjonssikkerhet.		Jeg er kjent med at virksomheten har mål-settinger for informasjons-sikkerhet, men kjenner ikke til noen egen policy for informasjonssikkerhet.		Jeg kjenner til policyen for informasjonssikkerhet og kjenner målsettingene i denne. Vet at denne følges opp på en god måte.

Spørsmål 1 er sentralt for alt som er relatert til sikkerhetsmål og sikkerhetspolitikk, og er relevant for flere kategorier i både (Albrechtsen et al., 2005) og (IAEA, 2002). Er disse formulert og gjort kjent i organisasjonen? Spørsmålet stilles til både ledere og ansatte – ettersom disse kan ha ulik oppfatning om hvorvidt disse målene er gjort kjent.

Spørsmålet kan også indikere om informasjonssikkerhet prioriteres i virksomheten, og om sikkerhetsfokuset er tilstede i den langsiktige og strategiske planleggingen.

2	B/L	Hvordan synes du kravene til informasjonssikkerhet påvirker deg i ditt daglige arbeid?	Jeg ser på informasjons-sikkerhet som hemmende for mitt daglige gjøremål i virksomheten.		Jeg følger lover og regler, og reflekterer ikke videre over det. Merarbeid med informasjonssikkerhet er nødvendig og jeg har forståelse for dette.		Kravene til informasjons-sikkerhet hjelper meg å gjøre jobben min på en forsvarlig og hensiktsmessig måte i forhold til de lover og regelverk jeg forholder meg til.

Spørsmål 2 undersøker den enkeltes holdning ovenfor informasjons-sikkerhet, og hvordan den enkelte føler at kravene påvirker arbeidet han/hun gjør. Svarene på dette spørsmålet kan også gi en indikasjon på hvorvidt virksomhetens rutiner og dokumentasjon er lettfattelig og tilgjengelig, som er viktig i en god sikkerhetskultur (IAEA, 2002). Temaet ble også dekket i forrige versjon av verktøyet.

3	B/L	I hvilken grad oppfatter du at det er akseptabelt å bryte sikkerhetsreglene for å øke effektiviteten?	Det er akseptert å bryte sikkerhetsreglene for å kunne levere resultater raskere.		Jeg prøver å følge regel-verket, men hvis det er mye press for å levere hender det at reglene brytes.		Det er ikke akseptert å bryte sikkerhetsreglene og det forekommer ikke.

Dette spørsmålet gir en viktig indikasjon på om sikkerhet virkelig prioriteres, eller om dette kun er noe som blir hevdet[43]. Balansen mellom fokusene på sikkerhet og produksjon er også et viktig aspekt ved en god sikkerhetskultur (IAEA, 2002), som blir belyst av dette spørsmålet. Dersom reglene brytes under press vil dette være et viktig område å jobbe videre med for virksomheten. Det vil også være interessant å se om det er skjevheter i forhold til hva ledere og ansatte svarer på spørsmålet.

4	B/L	Hvordan opplever du det er å påpeke feil hos kolleger?	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet, sier man ifra. Folk tar til seg rettledning, men er også ekstra nøye med å se etter feil hos andre en periode etterpå.		Det er ikke så ofte det trengs, men folk er lydhøre overfor egne feil. Den enkelte tar til seg bemerkninger, og systemet revideres ofte for å fange opp uønsket atferd.

Spørsmål 4 er en viktig indikasjon på hvorvidt det er et åpent forhold mellom ansatte i virksomheten. Et åpent forhold er et viktig element i en god sikkerhetskultur (Reason, 1997; Hale, 2000; IAEA, 2002) og er også en viktig forutsetning for organisasjonslæring (Senge, 1990; Garvin 1993). Temaet ble også delvis dekket i forrige versjon av verktøyet.

5	B/L	Hvem oppfatter du har ansvaret for informasjonssikkerheten i virksomheten din?	Ledelsen har det over-ordnede ansvaret. Ansvaret er ikke fordelt videre i organisasjonen.		Det eksisterer en sikkerhetsavdeling eller sikkerhetsansvarlig med fullt ansvar for informasjonssikkerhet. Ansatte får pålegg og retningslinjer fra sikkerhetsavdelingen.		Ansatte på alle nivå har ansvar for informasjons-sikkerhet, og fokuset på sikkerhet er forankret i ledelsen. Oppgavene løses og følges opp lokalt.

En god ansvarsfordeling og en klar definering av roller er viktige elementer i en god sikkerhetskultur (IAEA, 2002). Det er også viktig at dette er formidlet ut til alle ansatte, så de er klar over hvordan dette gjøres. Det vil også på dette spørsmålet være interessant å se om det er ulik oppfatning av ansvarsfordelingen blant ledere og ansatte. Temaet ble også dekket i forrige versjon av verktøyet.

[43] Dette kan relateres til Scheins (1992) beskrivelse av uttrykte verdier – uttalte mål om hvor virksomheten *ønsker å være* eller *tror de er*.

6	B/L	Opplever du at du har fått tilstrekkelig opplæring rundt informasjonssikkerhet og sikker bruk av IT-systemer?	Jeg har ikke fått opplæring i sikker bruk av IT.		Jeg har fått opplæring i gjeldende regelverk og rutiner for sikker bruk av virksomhetens informasjonssystemer. Opplæringen dekker tiltak og beredskap mot uønskede hendelser		Ledelsen følger opp gjennom kontinuerlig informasjon og opplæring blant alle brukergrupper. Alle bidrar aktivt i opplæringen.

Et godt kunnskapsnivå er et sentralt aspekt av en god sikkerhetskultur, og gode opplæringsprogrammer er i så måte viktig for virksomheter. Dette spørsmålet undersøker om de ansatte føler de har fått god opplæring, samt hvilke overordnede felter opplæringen har dekket. Forrige versjon av verktøyet tok også opp dette temaet.

7	B/L	I hvilken grad får noen skylden dersom en uønsket hendelse inntreffer?	Enkeltansatte eller samarbeidspartnere blir trukket fram som syndebukker dersom det skjer et sikkerhetsbrudd.		En kombinasjon av tekniske eller personlige feil sees på som årsaker til at hendelser skjer. Systemet i seg selv får ofte skylden for sikkerhetsproblemene.		Verken personer eller samarbeidende virksomheter blir syndebukker. Beskyldninger er sjelden noe tema.

Skyldspørsmålet er relevant for et godt sikkerhetsnivå og læring av feil. Sistnevnte er et viktig element både relatert til sikkerhet (Reason, 1997; IAEA, 2002; Albrechtsen et al., 2005) og organisasjonslæring (Senge, 1990; Garvin, 1993).

Dette spørsmålet ser på hvem eller hva som skylden dersom en uønsket hendelse inntreffer, noe som vil være viktig for å se på hvilke hendelser som rapporteres og hva som blir gjort for å lære av dem. I virksomheter med en syndebukkultur vil det være vanskelig å innføre metoder for organisasjonslæring, noe dette spørsmålet kan identifisere. Temaet ble også dekket i forrige versjon av verktøyet.

8	B/L	Hvordan oppfatter du at informasjon i virksomheten graderes?	Det finnes ikke, eller jeg kjenner ikke, rutiner for å skille sensitiv og åpen informasjon. Det gjøres ingen verdivurdering av informasjonen.		Det finnes regelverk for å skille mellom sensitiv og åpen informasjon, men jeg kjenner ikke til hvordan de fungerer.		Det finnes graderingssystemer og de ansatte kjenner disse godt slik at ikke informasjon blir feilgradert. Kriterier og rutiner for verdivurdering av informasjon følges av de ansatte og videreutvikles og tilpasses løpende.

Spørsmål 8 omfatter kjennskapen til rutiner for gradering av informasjon, et viktig aspekt i en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Temaet ble også dekket i forrige versjon av verktøyet.

9	B/L	Hvordan behandler du sensitiv informasjon?	Tenker sjelden over at sensitiv informasjon skal behandles med forsiktighet.		Er klar over restriksjonene knyttet til sensitivt og sikkerhetsgradert materiale.		Er kjent med utstederen av informasjonen (eierskapet), kjenner hvem som har tilgang og forstår hvorfor informasjonen er sensitiv. Er "føre var" når jeg kommer i kontakt med sensitiv informasjon.

Den enkeltes behandling av sensitiv informasjon er et viktig aspekt ved en god sikkerhetskultur. Tenker man godt nok over at informasjon må behandles forsiktig? Har bevisstgjøringen på dette feltet vært god nok? Temaet kan relateres Kufås & Mølmanns (2003) diskusjoner rundt innsideproblematikk, og ble også dekket i forrige versjon av verktøyet.

Basisspørsmål - atferd

10	B/L	Hvilke vaner har du for valg og bruk av brukernavn og passord?	Skifter aldri passord. Enkelhet prioriteres framfor sikkerhe		Bruker samme passord på forskjellige tjenester. Skifter passord av og til.		Skifter passord ut fra en risikovurdering. Benytter passord som er en kombinasjon av tall og store/små bokstaver som er over 7 tegn.

Vaner for valg og bruk av passord er viktige deler av en god IKT-sikkerhetspolitikk, blant annet i forbindelse med nettverksbeskyttelse og tilgangsstyring (Albrechtsen et al., 2005).

11	B/L	Hvilke e-postvaner har du?	Åpner og videresender e-post med vedlegg uten å tenke på sikkerheten. Tenker aldri over at e-post kan komme uvedkommende i hende.		Det er laget regler for god e- post skikk som beskriver hvordan e-post skal benyttes.		Er klar over at e-post er et usikkert medium. Avsender kan forfalskes, og vedlegg og lenker kan være skadelige eller feilaktige. Det er laget regler som beskriver hvordan e-post kan brukes sikkert for å sikre at bare rett person får korrekt informasjon uten at andre får innsyn i det.

Dårlige e-postvaner kan føre til sikkerhetshull og uønskede hendelser. Spørsmål 11 er på bakgrunn av dette viktig for å undersøke hvor godt ansatte kjenner til problemer som kan oppstå rundt bruk av e-post. Atferden på dette feltet kan påvirke nettverksbeskyttelsen og håndteringen av e-post og spam, som begge er deler av en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Temaet ble også dekket i forrige versjon av verktøyet.

12	B/L	Hvordan ivaretar du sikkerheten når du surfer på internett?	Klikker som regel "OK" på spørsmål. Synes det er vanskelig å vite hva som er rett. Oppgir sensitiv informasjon ukritisk uten å sjekke at nettadressen er ufarlig.		Forsøker å være forsiktig, kontrollerer web-adresser jeg benytter. Det vil si, oppgir ikke personlige opplysninger som bruker-identitet, passord eller annen informasjon uten å være sikker på at web-adressen er ekte. Klikker etter magefølelsen.		Oppgir bare sensitiv opplysning på web-adresser jeg har kontrollert eller hvor sertifikater benyttes.

Spørsmål 12 er relatert til surfing på internett, og er som spørsmål 11 relevant for en god nettverksbeskyttelse. Spørsmålet undersøker hvilke vaner de ansatte har når de bruker nettlesere. Temaet ble også dekket i forrige versjon av verktøyet.

13	B/L	Hvordan ivaretar du sikkerheten ved arbeid hjemmefra på egen PC?	Tenker lite på informasjons-sikkerhet. Andre personer (f.eks. familie), har full adgang til min PC. Lagrer arbeidet på egen PC uten å kryptere. Enkelhet prioriteres framfor sikkerhet.		Følger etablerte rutiner. Er klar over restriksjonene knyttet til gradert materiale. Det er etablert gode rutiner for å arbeide sikkert med PC som skal koples opp utenfra i virksomhetens interne nett.		Tar alle forholdsregler og er oppmerksom på at å arbeide på denne måten øker faren for virus og lekkasje av informasjon. Hjemme-PC har samme sikkerhetsnivå som jobb-PC. Bruker kryptert forbindelse til jobben, og lagrer filene mine på en sikker server på jobb.

Holdninger og atferd relatert til fjernarbeid er relevant for god nett-verksbeskyttelse i virksomheter, som spørsmål 11 og 12. Spørsmålet kan også sees i sammenheng med spørsmål 24 som tar for seg virksomhetens tilrettelegging for fjernarbeid. Dersom rutinene og vanene ved fjernarbeid er gode, vil dette ha en positiv effekt på nettverksbeskyttelsen. Temaet ble også dekket i forrige versjon av verktøyet.

14	L	Hvordan forholder du deg til lovpålagte regler, som for eksempel Sikkerhetsloven og Personopplysningsloven i virksomheten?	Relevant lovverk er ikke kommunisert ut i virksomheten. Ledelsen eller sikkerhets-ansvarlige har noe kjennskap til lovverket. Det er sannsynlig at virksomheten ikke oppfyller alle kravene fordi disse ikke er godt kjent.		Interne prosedyrer blir periodisk sammenlignet med kravene i loven slik at lovverket blir oppfylt.		Vi har jevnlig intern opplæring, og interne rutiner blir løpende oppdatert når lovverket justeres og oppdateres. Det er god forståelse for lovverket, og alle ser nødvendigheten av et lovpålagt regelverk i virksomheten

Spørsmål 14 er rettet mot ledelsen, og undersøker hvor god kjennskap de har til de relevante lovverkene de må forholde seg til. I alternativene undersøkes det blant annet hvordan opplæring og prosedyrer påvirkes av endringer i lovverkene, noe som er en del av en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Spørsmålet er også en del av forrige versjon av verktøyet.

15	B/L	Hvordan vil du beskrive kontorplassen din når du går fra den?	Fortrolige papirer ligger åpent og tilgjengelig for hvem som helst. Jeg låser eller stenger PCen sjelden når jeg forlater den.		Følger de etablerte reglene, fortrolige papirer gjøres utilgjengelig for ikke autoriserte. Låser/stenger som regel PCen, men ikke når jeg skal ta en kjapp tur bort fra den (ca 5-15 minutter).		Fortrolige papirer gjøres utilgjengelig for ikke-autoriserte personer, og jeg låser alltid PC når jeg forlater den.

En beskrivelse av hvordan kontorplassen ser ut når man forlater den kan gi en god indikasjon på hvordan man behandler sensitiv informasjon. Dersom man generelt lar ting ligge åpent vil dette også kunne medføre at sensitiv informasjon er tilgjengelig for folk som ikke har tilgang. Spørsmålet kan også gi en indikasjon på om det er gode arbeidsforhold og god orden og fysisk stand, som er aspekter av en god sikkerhetskultur (IAEA, 2002).

Basisspørsmål – policy og ledelse

16	B/L	I hvilken grad er ledelsen opptatt av å kommunisere informasjonssikkerhet til ansatte og sam-arbeidspartnere?	Ledelsen synes ikke å være spesielt opptatt av informasjonssikkerhet, ansatte får lite informasjon om informasjonssikkerhet.		Ledelsen bryr seg når det har vært en hendelse. Ledelsen informerer, men det er mye enveis-kommunikasjon.		Ledelsen er løpende opptatt av informasjons-sikkerhet og gir ut relevant informasjon til med-arbeidere og samarbeids-partnere, samtidig som det er god dialog.

Kommunikasjon av informasjonssikkerhet er et viktig aspekt av en sikkerhetskultur. Temaet kan relateres til flere elementer i IAEA (2002); forpliktelse fra toppledelsen, synlig lederskap og åpent forhold. Disse aspektene er også identifisert som viktige elementer i en god sikkerhetskultur av blant annet Reason (1997) og Hale (2000). Temaet ble også dekket i forrige versjon av verktøyet.

17	B/L	I hvilken grad oppfatter du at lederne i virksomheten går foran som gode eksempler når det gjelder informasjonssikkerhet?	Oppfatter ikke at lederne går foran som gode eksempler.		Lederne går til en viss grad foran som gode eksempler, men i enkelte situasjoner, som f.eks for å nå tids-frister, bryter de reglene for å nå målene		Lederne går alltid foran som gode eksempler og viser hvordan ting bør gjøres.

Synlig lederskap er en viktig del av en god sikkerhetskultur (Hale, 2000; IAEA, 2002). Ledernes atferd vil påvirke ansattes atferd, da disse kan anses å være forbilder for sine underordnede. Dette kan sees i sammenheng med formelle og uformelle individrettede tiltak og bevisstgjøring, deler av en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Spørsmålet kan også relateres til ledelsens forpliktelse til informasjonssikkerhet, som vil påvirke sikkerhetskulturen (IAEA, 2002).

18	B/L	I hvilken grad oppfatter du at ansatte inkluderes i arbeidet med informasjonssikkerhet?	Ledelsen og sikkerhets-ansvarlige utreder og kommer med retningslinjer og generelle tiltak uten innspill fra ansatte.		Rapporter og erfaringer fra de ansatte benyttes i utformingen av prosedyrer og regler.		Ansatte blir rådført og deltar i utforming av tiltak, og blir sett på som en viktig ressurs i arbeidet for informasjonssikkerhet. Enkelte ansatte får konkrete oppgaver innen informasjonssikkerhet.

Inkludering av ansatte er en sentral del av en god sikkerhetskultur (Hale, 2000) og en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Ved involvering vil ansatte få et eierskap til arbeidet med informasjonssikkerhet, samtidig som dette kan sikre at tiltakene som utarbeides er tilpasset det daglige arbeidet til de ansatte. Samtidig så vil inkludering gjøre at flere aspekter tas i betrakting når arbeidet skal gjøres. Temaet ble også dekket i forrige versjon av verktøyet.

19	L	I hvilken grad utveksles erfaringer med informasjonssikkerhet med andre virksomheter?	Det hentes lite erfaringer fra andre. Sikkerhetsarbeidet er lukket og internt.		Det fokuseres på å måle informasjonssikkerhet for å kunne sammenligne med andre virksomheter.		Virksomheten deltar aktivt i fagnettverk relatert til informasjonssikkerhet. Virksomheten undersøker stadig hvordan sam-arbeidspartnere og andre virksomheter, også i andre bransjer og sektorer, jobber med informasjonssikkerhet.

Forholdet til tilsynsorganer og andre eksterne grupper er et aspekt som påvirker sikkerhetskultur (IAEA, 2002) og IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Spørsmål 19 undersøker hvorvidt arbeidet med informasjonssikkerhet er lukket/internt eller åpent. Dersom organisasjonen har en god evne til å dele erfaringer med og ta til seg erfaringer fra omverdenen, vil dette være et eksempel på en generativ kultur (Westrum, 1993). Dette er i tillegg et viktig aspekt ved en lærende organisasjon (Garvin, 1993).

20	L	I hvilken grad oppfatter du at samarbeids-partnere inkluderes i arbeidet med informasjonssikkerhet?	Samarbeidspartnere er ikke involvert i utarbeidelse av retningslinjer.		Samarbeidspartnere skal følge virksomhetens prosedyrer, regler og relevant lovverk.		Samarbeidspartnere skal følge virksomhetens prosedyrer, regler og relevant lovverk, men blir også rådført og deltar aktivt i arbeidet for å sikre god informasjonssikkerhet.

Spørsmål 19 retter seg mot ledelsen, og undersøker i hvilken grad samarbeidspartnere er involvert i arbeidet med informasjonssikkerhet. Som for spørsmål 19 er dette et tema som kan benyttes til å identifisere hvorvidt organisasjonen er en generativ (Westrum, 1993) eller lærende organisasjon (Garvin, 1993), samtidig som god håndtering av sam-arbeidspartnere er en del av en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Temaet ble også dekket i forrige versjon av verktøyet.

21	B/L	Blir informasjons-sikkerhet prioritert i forhold til de vanlige daglige gjøremål?	Det fokuseres kun på å få unna virksomhetens primæroppgaver. Informasjonssikkerhet sees utelukkende på som en ekstra belastning og utgiftspost.		Primæroppgavene er i fokus, men det settes av tilstrekkelige ressurser til å imøtekomme pålegg, bestemmelser og kjente trusler. Det settes av nok ressurser til å gjøre regler kjent. Ved hendelser settes det inn nok ressurser til å opprette stabil drift.		Ressurser prioriteres ut fra en risikovurdering og en kost-/nyttevurdering. Man forsøker å ligge i forkant for å unngå uønskede hendelser. Informasjonssikkerhet er integrert i daglig drift og i utvikling av primæroppgavene.

Virksomhetens prioritering av sikkerhetsoppgaver i forhold til regulære driftoppgaver vil ha en påvirkning på sikkerhetskulturen (IAEA, 2002). Spørsmålet kan også benyttes til å undersøke hvorvidt sikkerhet faktisk prioriteres høyt, eller om dette kun er noe man hevder. Ved slik bruk kan resultatene sees i sammenheng med Scheins (1992) beskrivelse av uttrykte verdier. Temaet ble også dekket i forrige versjon av verktøyet.

22	L	Hvordan håndteres informasjonssikkerhet i prosjekter?	Informasjonssikkerhet er ikke et tema når nye prosjekter planlegges. Eventuelle problemer knyttet til informasjons-sikkerhet blir utsatt til gjennomføringsfasene av prosjekter og løses etter hvert.		Informasjonssikkerhet blir tatt hensyn til i prosjekter, og deltakerne er alle autoriserte til å kunne gjøre jobben. Prosjektene skal følge etablerte prosedyrer, regler og relevant lovverk.		Når nye prosjekter planlegges blir informasjonssikkerhet vurdert i startfasen. Risiko- og sårbarhets-analyser gjennomføres og informasjonssikkerhet testes løpende underveis. Prosjektgruppene har forståelse for at informasjonssikkerhet er av kritisk betydning.

Spørsmål 22 kan relateres til systematisk forpliktelse, dokumentasjon og rutiner, som påvirker sikkerhetskulturen (IAEA, 2002). Spørsmålet var også en del av forrige versjon av verktøyet, og håndtering av informasjonssikkerhet i prosjekter ble identifisert som et viktig område gjennom arbeidsseminaret i Trondheim 7. og 8. februar 2005.

23	B/L	I hvilken grad verdsettes rapportering av uønskede hendelser i virksomheten?	Jeg får ingen tilbakemelding fra noen om hvordan det går med saken når jeg rapportere videre internt. Jeg velger heller å prøve å løse problemet selv.		Dersom hendelsen er av såpass omfang at den har direkte konsekvenser for mitt daglige arbeid, rapporterer jeg den. Min nærmeste overordnede er den jeg rapporterer til og jeg får tilbakemelding om at min rapportering er mottatt og at noen vil se på saken.		Jeg rapporterer alltid dersom jeg opplever en sikkerhetsrelatert, uønsket hendelse. Jeg kjenner til hvem i virksomheten jeg skal rapportere ulike typer hendelser til. Jeg opplever at henvendelsen blir tatt på alvor og at det skjer noe. Jeg blir informert om løsningen dersom det er nødvendig og/eller relevant.

Spørsmål 23 omfatter hvorvidt rapportering verdsettes av virksom-heten, samt hvordan rapporter følges opp. Dette kan sees i sammen-

heng med aspektene forskrifter og prosedyrer (IAEA, 2002) og hendelses- og krisehåndtering (Albrechtsen et al., 2005). Temaet ble også dekket i forrige versjon av verktøyet.

24	B/L	I hvilken grad oppfatter du at virksomheten prioriterer sikkerheten ved fjernarbeid, for eksempel ved oppkopling mot virksomhetens nett?	Enkelhet prioriteres framfor sikkerhet. Det viktigste er å kunne koble opp utstyr til virksomhetens nett på en enkel måte.		Det er etablert regler for sikkert arbeid med PC som skal kobles opp utenfra i virksomhetens interne nett.		Virksomheten har gode rutiner for fjernarbeid. Jeg er likevel oppmerksom på at fjernarbeid øker faren for virus og lekkasje av informasjon.

Spørsmål 24 undersøker hvordan de ansatte oppfatter at virksomheten prioriterer sikkerhet ved fjernarbeid. Temaet kan relateres til aspektet nettverks- og internettbeskyttelse som er en viktig del av en god IKT-sikkerhetspolitikk (Albrechtsen). Spørsmålet kan også sees i sammenheng med spørsmål 13 som ser mer på den enkeltes atferd ved fjernarbeid.

25	L	I hvor stor grad er fysiske sikkerhetstiltak etablert?	Det er få fysiske tiltak for å sikre sensitiv informasjon og systemer. Utenforstående har fri adgang til lokalene.		Virksomheten har adgangskontroll i bygget og virksomhetskritiske informasjonssystemer er fysisk sikret.		Virksomheten er godt sikret med flere nivåer av adgangskontroll på forskjellige områder og lokaler. Ingen besøkende går uten følge uten at dette er avklart med sikkerhets-ansvarlig. Kontorer låses, PCer med sensitivt materiell er låst fast og lagringsenhet fjernes og låses vekk.

Gode fysiske sikkerhetstiltak kan sees i sammenheng med god sikkerhetskultur (IAEA, 2002) og god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Fysiske sikkerhetstiltak vil også påvirke tilgjengeligheten av sensitiv informasjon, slik at det kan bli vanskelig for utenforstående å få tak i dette.

26	L	I hvilken grad er det gode kriterier eller rutiner for å velge ut hvilke IT-systemer som skal beskyttes?	Det er ikke etablerte rutiner for å velge ut hvilke IT-systemer som skal beskyttes.		Sikkerhetsavdelingen har ansvaret for utvelgelse av hvilke IT-systemer som skal beskyttes.		Det eksisterer gode rutiner for å fange opp hvilke IT-systemer som skal beskyttes, og hovedansvaret ligger på sikkerhetsavdelingen.

Gode rutiner for å velge er en del av en god IKT-sikkerhetspolitikk. Spørsmålet kan sees i sammenheng med systematisk forpliktelse (IAEA, 2002) og rutiner for behandling av ny teknologi, innføring av nye systemer og vedlikehold av eksisterende systemer (Albrechtsen et al., 2005).

27	L	I hvilken grad har virksomheten gode rutiner for å sikre kontinuerlig drift?	Det er ikke etablert beredskapsplaner. Det fokuseres ikke mye på å unngå uønskede hendelser.		Virksomheten har regler, rutiner og løsninger som trer i kraft ved alvorlige hendelser. Rutinene sikrer kontinuitet ved forventede uønskede hendelser.		Man kjører ofte risiko- og sårbarhetsanalyser, slik at virksomheten til enhver tid har et oppdatert risikobilde. Ved hendelser trer et beredskapsapparat med nødvendige tiltak i kraft, slik at driften kan opprettholdes mens feilen rettes. I ettertid analyseres hendelsen for å kunne unngå tilsvarende hendelser i fremtiden.

Gode rutiner for kontinuerlig drift kan sees i sammenheng med god hendelses og krisehåndtering (Albrechtsen et al., 2005) og systematisk forpliktelse, forskrifter og prosedyrer (IAEA, 2002). Spørsmålet retter seg kun mot ledere, ettersom disse vil ha mest kunnskap innenfor dette området.

Basisspørsmål – revisjon

28	L	Hvordan revideres informasjonssikkerhet?	Revisjon av informasjons-sikkerhet skjer kun ved eksternt press og større hendelser.		Det gjennomføres revisjoner for å påse at regler og prosedyrer for informasjonssikkerhet eksisterer og blir fulgt.		Jevnlige revisjoner fokuserer både på kunnskap, atferd og holdninger. Revisjon brukes aktivt for å forbedre virksomhetens rutiner og prosedyrer.

Spørsmål 28 kan relateres til at sikkerhetspolitikken skal være en del av internkontrollen og evalueres løpende (Albrechtsen et al., 2005), samt systematisk forpliktelse, forskrifter og prosedyrer (IAEA, 2002). Jevnlig revisjon av informasjonssikkerhet er viktig for å opprettholde et godt sikkerhetsnivå, og er derfor et viktig spørmål i undersøkelses-verktøyet. Temaet ble også dekket i forrige versjon av verktøyet.

29	L	I hvilken grad analyseres inntrufne uønskede hendelser?	Det gjøres lite analyser av hendelser. Kun større hendelser som rammer betydelige deler av virksomheten følges opp.		Hendelsen analyseres med fokus på etablere en rutine for å unngå samme hendelse igjen. Det gjøres lite oppfølgingsarbeid for å se sammenhenger og få oversikt.		Hendelsen analyseres slik at organisasjonen kan lære og unngå tilsvarende hendelser og ringvirkninger av slike.

Analyse av inntrufne hendelser og feil er en viktig oppgave i en lærende organisasjon (Garvin, 1993; Westrum, 1993; IAEA, 2002), og spørsmål 29 undersøker i hvilken grad dette gjøres. Analyse av inn-trufne hendelser er også et element i god hendelses- og krise-håndtering, som er en del av en god IKT-sikkerhetspolitikk.

30	L	Hvordan gjennomføres risiko- og sårbarhets-analyser?	De eneste analysene som foregår, er de sikkerhets-ansvarliges egne vurderinger som gjøres i det daglige arbeidet. Ledelsen har liten oversikt over risiko.		Det gjennomføres til tider risiko- og sårbarhets-analyser. Det settes grenser og eventuelle minimums-standarder for akseptabel risiko, og tiltak settes i verk der risikoen er større enn de fastsatte grensene.		Det gjennomføres ofte risiko- og sårbarhets-analyser, og virksomheten har løpende fokus på risiko og sårbarheter. Tiltak settes i verk med det samme behovet oppstår.

God systematisk forpliktelse er en del av en god sikkerhetskultur (IAEA, 2002), og risikobasert tilnærming er en del av en god IKT-sikkerhetspolitikk (Albrechtsen et al., 2005). Spørsmål 30 kan relateres til disse temaene, og et viktig aspekt som dekkes i verktøyet. Temaet ble også dekket i forrige versjon av verktøyet.

Tilleggsspørsmål – kunnskap og holdning

T.1	B/L	Hvor god kunnskap har du om følgende teknologier: ad-ware, spy-ware og virus?	Jeg har liten eller ingen kjennskap til dette, og har i liten grad en formening om hvilken skade disse kan forårsake.		Vet hva de vanligste truslene representerer, og er i stand til å beskytte meg mot disse.		Har inngående kunnskap på området, kjenner til de vanligste sikkerhetshullene truslene benytter seg av, og er i stand til å beskytte min PC og nettverket den er tilkoblet.

I dagens komplekse IT-hverdag kan ukyndig bruk av datamaskiner utgjøre alvorlige sikkerhetstrusler. Det er vanskelig å hele tiden være i forkant for å bygge barrierer og de ansattes bevissthet i forhold til trusselbildet kan være med å dempe sannsynligheten for sikkerhetshull. Spørsmålet gir en indikasjon på bevissthetsnivå i forhold til de mest vanlige truslene; virus, spionprogrammer og programmer som samler informasjon om deg.

T.2	B/L	I hvilken grad oppfatter du at man er opp-merksom på ukjente personer på arbeids-plassen din?	Man vil sannsynligvis ikke legge merke til om ukjente personer er på arbeidsplassen.		Ukjente personer som ser viktige ut vil sannsynligvis få gå rundt, andre vil bli sjekket for hvorfor de er der.		Alle ukjente personer blir lagt merke til, og man undersøker hva de har der å gjøre.

Dette spørsmålet tar for seg hvor bevist man er uvedkommende som er inne i virksomheten. Om man håndterer sensitiv informasjon ønsker man ikke at uvedkommende skal kunne gå fritt rundt, og man bør være på vakt ovenfor mistenkelige, ukjente personer.

T.3	B/L	Hvor godt kjenner du til kryptering?	Jeg har liten eller ingen kjennskap til kryptering.		Har en formening om nødvendigheten av kryptering og er i stand til å skru på kryptering i applikasjoner der dette er mulig. Vet hvilke systemer rundt meg som er kryptert.		Kjenner godt til kryptering. Kan anslå hvor sikker krypteringen er. Er i stand til å sette opp sikker kryptering av medier jeg bruker.

Spørsmålet tar for seg kunnskapsnivå i forhold til kryptering. Dette vil ikke være aktuelt for alle virksomheter, men kan være et relevant spørsmål i avdelinger som håndterer sensitiv informasjon og hvor det ikke er etablert rutiner og systemer som håndterer kryptering. Eksempler på dette kan være i avdelinger hvor man benytter mye ny teknologi og hvor den teknologiske utskiftningen skjer fort.

T.4	B/L	I hvilken grad bruker du intranettet til å finne informasjon om sikkerhet (regler osv.)?	Jeg vet ikke om det finnes noe, og det tar for lang tid å lete etter det.		Jeg vet det finnes, men må lete fordi jeg ikke vet hvor det ligger.		Jeg vet hvor det finnes og bruker nettet ofte for å holde meg oppdatert.

Spørsmålet er aktuelt i virksomheter hvor man baserer seg på intranettet til å oppdatere sikkerhetsreglementet og legge ut rutiner i forhold til sikker atferd. Spørsmålet er ment å gi en indikasjon på i hvilken grad de ansatte benytter intranettet til å finne informasjon om sikkerhetsregler og rutiner.

T.5	B/L	Hvordan er de vanlige rutinene for bruk av telefaks?	Sender faks til angitt nummer uten å kontrollere at faksen kommer frem, og uten å undersøke om rett person får den.		Sender faks til angitt nummer og venter på bekreftelse på at den er kommet frem. Undersøker ikke alltid om rett mottaker har fått faksen på faksnummeret som har blitt benyttet.		Er alltid sikker på at rett faksnummer benyttes og forsikrer meg om at rett informasjon har kommet frem til rett mottaker.

I enkelte bransjer er det aktuelt med sensitiv informasjon over faks. I forhold til dette kan spørsmålet være med på å avdekke hvor bevist de ansatte er informasjonen de håndterer og hvilke implikasjoner som er forbundet med å oppgi informasjon over telefaks. Spørsmålet er ment å kunne gi en indikasjon på hvorvidt dette er noe man bør se nærmere på i virksomheten.

T.6	B/L	Hvordan forholder du deg til sensitiv informasjon på telefon?	Jeg er ikke videre kritisk til hva folk spør om, og svarer så mye jeg vet om tema på forespørsel.		Jeg vet hva slags innfor-masjon som er sensitiv og som ikke skal oppgis på telefon.		Jeg er fullt inneforstått med hva slags informasjon jeg har lov å oppgi og hva jeg ikke har lov å oppgi. Når jeg blir forespurt om informasjon tenker jeg alltid nøye gjennom om informasjonen kan brukes til andre formål enn det den opprinnelig er tiltenkt.

I enkelte bransjer er det aktuelt med sensitiv informasjon over telefon. I forhold til dette kan spørsmålet være med på å avdekke hvor bevist de ansatte er informasjonen de håndterer og hvilke implikasjoner som er forbundet med å oppgi informasjon over telefon og problematikk forbundet med dette. Spørsmålet er ment å kunne gi en indikasjon på hvorvidt dette er noe man bør se nærmere på i virksomheten.

T.7	B/L	Hvordan håndterer du sensitiv informasjon når du mottar skrevne dokumenter?	Jeg har ikke noe forhold til om informasjonen som er gitt meg er sensitiv eller ikke. Papirene er åpne og tilgjengelige for andre.		Jeg vet hva slags innfor-masjon som er sensitiv og som ikke kan vises til andre. Jeg er som regel nøye med å låse unna dokumenter for uvedkommende.		Jeg tenker over hvem som kan få se dokumentene avhengig av hvor jeg gjør av dem og sørger for at ingen uvedkommende får tilgang. Jeg er fullt inneforstått med hva slags informasjon jeg kan og ikke kan oppgi innenfor graderingen dokumentet har. Når jeg får dokumenter, tenker jeg alltid nøye gjennom om informasjonen kan brukes til andre formål enn det den opprinnelig er tenkt til.

Spørsmålet kan være med på å avdekke hvor bevist de ansatte er informasjonen de håndterer i skrevne dokumenter og hvilke implikasjoner som er forbundet med nedskrevet sensitiv informasjon. En lav poengsum på dette spørsmålet kan gi en indikasjon på hvorvidt dette er noe man bør se nærmere på i virksomheten.

T.8	B/L	Hvordan håndterer du sensitiv informasjon når du skriver dokumenter?	Jeg tar med all den informasjonen som kan være nyttig i dokumenter. Enkel tilgang på nødvendig informasjon er viktigere for meg enn å sjekke hva det er lov å oppgi.		Jeg vet hva slags innfor-masjon som er sensitiv og som ikke skal oppgis i dokumenter med forskjellig klareringsnivå.		Jeg er fullt inneforstått med hva slags informasjon jeg kan og ikke kan oppgi innenfor graderingen dokumentet har og tenker igjennom hvem som kan ha tilgang på dokumentet. Når jeg blir forespurt om informasjon, tenker jeg alltid nøye gjennom om informasjonen kan brukes til andre formål enn det den opprinnelig er tenkt til.

I enkelte bransjer er det aktuelt med sensitiv informasjon i dokumenter. I forhold til dette kan spørsmålet være med på å avdekke hvor bevist de ansatte er informasjonen de håndterer og hvilke implikasjoner som er forbundet med å oppgi informasjon og problematikk forbundet med dette. Spørsmålet er ment å kunne gi en indikasjon på hvorvidt dette er noe man bør se nærmere på i virksomheten.

T.9	B/L	Hvordan ivaretar du sikkerheten ved bruk av mobilt utstyr som eksempelvis bærbar PC, telefon, lomme-PC eller minnepinne?	Enkelhet prioriteres framfor sikkerhet. Lagrer sensitiv informasjon på mobilt utstyr uten å kryptere eller å ta sikkerhetskopi. Tenker lite på informasjonssikkerhet. Andre personer har tilgang til mitt mobile utstyr.		Jeg følger etablerte rutiner og er klar over restrik-sjonene knyttet til sensitiv informasjon på mobilt utstyr. Utstyret er beskyttet med passord og informasjon er kryptert.		Informasjon på mobilt utstyr er alltid kryptert og jeg har sikkerhetskopi. Informasjon lagres i utgangspunktet på en sikker server på jobben. Bruker kryptert forbindelse med autentisering ved utveksling av data. Hva man får tilgang på ved arbeid utenfra, er bestemt ut fra en risikovurdering.

Det blir mer og mer vanlig å ta med seg elektronisk informasjon ut av virksomheten, på mobiltelefon, bærbar datamaskin, håndholdt data-maskin, minnepinner og liknende. Det er viktig at man da klarer å beskytte informasjonen på en hensiktsmessig måte, slik at denne ikke kommer på avveie. Spørsmålet vil ikke være aktuelt for alle deler av virksomheten og det er viktig at respondentene har en enhetlig oppfatning av hva som regnes som sensitiv informasjon.

T.10	B/L	I hvilken grad oppfatter du at det er akseptabelt å laste ned og dele opphavsbeskyttet materiale (musikk, film, dokumenter, programvare, bøker, lyd)?	Fildeling er akseptert og det forekommer. Materiale lagres av og til på lokale filtjenere og på egen PC. Når materiale er tilgjengelig så kopieres og spres det. Det er en utbredt holdning at dette er helt greit.		Det er etablert regler som forbyr lagring og bruk av opphavsbeskyttet materiale, men det forekommer.		Det er god forståelse for at man ikke kopierer og videreformidler opphavsbeskyttet materiale, og det forekommer heller ikke.

Spørsmålet er ment å identifisere om det forekommer fildeling og kopiering av opphavsrettighetsbeskyttet materiale. Dette er et stadig økende problem og det illustrerer en dårlig sikkerhetsmessig holdning da mange av programmene som benyttes til fildeling representerer en sikkerhetsrisiko og potensielt kan åpne virksomhetens nettverk for utenforstående.

T.11	B/L	I hvilken grad oppfatter du at det er akseptabelt å teste ut sikkerhetsbarrierer i IT-systemene?	Testing av systemenes sikkerhetsgrenser og sikkerhetshull er akseptert og det forekommer.		Dette er ikke lov i henhold til regelverket, men kan forekomme.		Det er ikke akseptabelt og forekommer ikke.

I dette spørsmålet ønsker man å se på om det råder en kultur for å forsøke å trenge igjennom sikkerhetsbarrierene i virksomheten. Ansatte kan ha forskjellig motivasjon for å ønske å trenge igjennom barrierene (fildeling, programvare for instant messenging, ftp servere, med mer). Spørsmålet gir en indikasjon på hvorvidt dette forekommer og er med etter ønske fra samarbeidspartner.

T.12	B	Hvordan opplever du det er å påpeke feil hos ledere?	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet sier man i fra. Lederen tar til seg rettledning, men er også ekstra nøye med å se etter feil og svakheter hos andre en periode etterpå.		Det er ikke så ofte det trengs, men lederne er lydhøre overfor egne feil og oppfordrer ansatte til å passe på at de går foran som gode eksempler.

Det er av interesse å se til at de medarbeiderne ikke er redde for å gi beskjed til lederne om de slurver med sikkerheten. Det er viktig at lederne går foran som gode eksempler og sørger for å være gode rollemodeller for de ansatte (Hale, 2000). Dette temaet ble også delvis dekket i forrige versjon av verktøyet. Åpent forhold, Åpenhet og kommunikasjon og Lederens rolle er alle sentrale områder som blir berørt i dette spørsmålet (IAEA, 2002).

T.13	B/L	Er du kjent med virksomhetens prosedyrer og regler for informasjonssikkerhet?	Jeg har ikke kjennskap til hvordan virksomheten tar hånd om informasjons-sikkerhet. Det finnes muligens noen dokumenter om dette, men disse har jeg ikke sett på.		Jeg vet hvor jeg kan finne dokumentasjon om hvordan virksomheten tar hånd om informasjons-sikkerhet. Jeg har ikke fått noen særlig innføring i virksomhetens arbeid på dette området.		Jeg føler at jeg har god kjennskap til hvordan virksomheten tenker om informasjonssikkerhet. Informasjon om prosedyrer og regler er lett tilgjengelig, og jeg får alltid vite om endringer og oppdateringer på området.

Spørsmålet tar for seg tilgjengelighet på prosedyrer og regler. Det er viktig at medarbeidere ikke må lete etter reglene når det er noe de lurer på og at det gis informasjon om når regelverket er blitt oppdatert slik at de ansatte kan lære seg de nye rutinene. Temaet var dekket i forrige versjon av verktøyet og er relevant i forhold til dokumentasjon og rutiner, tilstrekkelig kompetent personale (IAEA, 2002), samt at sikkerhetspolicyen må ha en klar hensikt mot målgruppen og at sentrale, relevante IKT-sikkerhetsprinsipper må være beskrevet (Albrechtsen et al., 2005).

T.14	B/L	Hvordan mener du kravene til informasjons-sikkerhet påvirker forholdet mellom de ansatte?	Fokus på informasjons-sikkerhet fører til et dårlig forhold mellom de ansatte.		Fokus på informasjons-sikkerhet påvirker ikke forholdet mellom de ansatte.		Fokus på informasjons-sikkerhet har en positiv innvirkning på forholdet mellom de ansatte. Alle ansatte jobber for at virksomheten som helhet skal ha så god informasjonssikkerhet som mulig.

Spørsmålet kan gi en indikasjon på hvordan de ansatte mener kravet til informasjonssikkerhet påvirker mellommenneskelige forhold i organisasjonen. Om de ansatte føler at fokuset er en belastning er de også mer negative til å følge de rutinene de er pålagt. Temaet kan også belyse aspekter i forhold til konflikthåndtering (IAEA, 2002) og var også dekket i forrige versjon av verktøyet.

T.15	L/B	I hvilken grad har du oversikt over virksom-hetens arbeidsrutiner, informasjonssystemer og samspillet mellom disse?	Jeg har liten oversikt over hvordan rutiner og sys-temer påvirker hverandre, og vet lite om hvilke konse-kvenser en feil i en rutine eller system kan ha for andre systemer.		Jeg har en viss forståelse av sammenhengen mellom rutinene og systemene i virksomheten. Stort sett kan jeg si hvilke konsekvenser mine handlinger har for enkelt-systemer, men har liten oversikt over konsekvenser for tilstøtende systemer.		Jeg kjenner sammen-hengen mellom rutiner og systemer godt, og har god forståelse for hvordan feil kan forårsake sikkerhets-brister i andre systemer.

Spørsmålet skal fange opp hvor bevist brukerne er sine handlinger og hvilke konsekvenser feil bruk kan ha for tilstøtende systemer. I dagens arbeidsmiljø med stadig med kompleks teknologi og avanserte nettverksorganisasjoner er det nødvendig at ansatte kjenner til følgene av sine gjerninger. Forståelse for samspill og evnen til systemtenking (Senge, 1990; IAEA, 2002) er viktige momenter som blir tatt opp.

T.16	B/L	I hvilken grad oppfatter du at det er akseptert å innrømme egne feil?	I liten grad, ansatte ønsker ikke å si fra dersom man har forårsaket en feil, ettersom dette bare har negative konsekvenser for den ansatte selv.		Til en viss grad, ansatte sier i fra ved alvorlige hendelser. Dårlige eller manglende rutiner får skylden.		I stor grad, man har ikke noe problem med å si ifra. Ansatte sier alltid fra dersom de gjør feil, og dette blir brukt til å lære av feilen.

Spørsmålet tar for seg hvorvidt organisasjonen forsøker å lære av hendelser og fokuserer på å forbedre rutiner i motsetning til å finne syndebukker og fordele skyld. Temaet ble også delvis dekket i forrige versjon av verktøyet og er sentralt i forhold til en utforskende holdning, hvor åpent forhold man har i organisasjonen og synet på feil (IAEA, 2002). I tillegg må konsekvenser av brudd på sikkerhetspolitikk og regler være beskrevet i sikkerhetspolicyen i virksomheten (Albrechtsen et al., 2005).

T.17	B/L	I hvilken grad kjenner du til hvem som har tilgang på sensitiv informasjon?	Jeg har ingen formening om hvem som har rett til å se sensitiv informasjon.		Jeg er klar over hvilken autorisasjon som kreves for å få se informasjonen.		Jeg vet alltid hvilken autorisasjon som kreves for å få innsyn i informasjonen og hvem i omgivelsene mine som har rett til å se informasjonen.

Det er viktig at de som håndterer informasjon også er klar over hvem som kan se informasjonen de håndterer, og ikke minst hvem som ikke skal se den. Uvitenhet er gjerne en årsak til regelbrudd, og en lav score her blant de som håndterer sikkerhetsgradert informasjon kan fort gi grunnlag for å mistenke mørketall i forhold til brudd på forskrifter.

T.18	B/L	Hvordan synes du kravene til informasjonssikkerhet påvirker det daglige arbeidet i virksomheten?	Informasjonssikkerhet er bare nødvendig pga lovverk, og sees ute-lukkende på som en ekstra belastning og utgiftspost.		De fleste forstår at informasjonssikkerhet er viktig i forhold til daglig arbeid/drift, regler og lovverk.		Informasjonssikkerhet går hånd i hånd med arbeidet/driften, og er nødvendig for å kunne drive på en hensiktsmessig og forsvarlig måte

Spørsmålet skal gi en indikasjon på hva slags oppfatning respondenten har om organisasjonen og sine medarbeideres holdning i forhold til å prioritere informasjonssikkerhet. Man vet at folk generelt har høyere tanker om egne ferdigheter og prestasjoner, og dette bør man også ta høyde for når man skal tolke svarene.
Spørsmålet oppfattes som relevant i forhold til synet på sikkerhet og i forhold til dokumentasjon og rutiner (IAEA, 2002).

Tilleggspørsmål – atferd

T.19	B/L	Hvordan reagerer du hvis du oppdager en feil eller et problem innen ditt ansvarsområde?	Retter opp feilen så raskt som mulig. Informerer ingen om dette.		Sier fra til linjeleder om det som har skjedd.		Informerer relevante personer i organisasjonen om det som har skjedd, slik at de kan lære av det.

Det er relevant å se hvorvidt medarbeidere selv er komfortable med å ta tak i feil og mangler i rutiner og atferd i organisasjonen. Det er viktig for organisasjonen at det er gode kommunikasjonslinjer og at disse benyttes. Aspekter ved dette kan også sees i sammenheng med konflikthåndtering åpenhet og kommunikasjon, og i synet på feil (IAEA, 2002).

T.20	B/L	Hvordan reagerer du hvis du oppdager en feil eller et problem innen andre sitt ansvarsområde?	Vil ikke skape problemer, så jeg sier ikke i fra, dette er ikke mitt bord.		Tar det opp med ved-kommende som har ansvaret. Regner med at ansvarlig følger opp.		Informerer relevante personer i organisasjonen om det som har skjedd, slik at virksomheten kan lære av det.

Det er relevant å se hvorvidt medarbeidere også er i stand til å ta tak i feil og mangler i andres rutiner og deres atferd. Det er viktig for organisasjonen at det er gode kommunikasjonslinjer og at disse benyttes. Aspekter ved dette kan også sees i sammenheng med konflikthåndtering åpenhet og kommunikasjon, og i synet på feil (IAEA, 2002).

T.21	B/L	I hvilken grad passer du på å kryptere sensitiv informasjon du håndterer?	Kjenner ikke til kryptering, og krypterer aldri noe som helst.		Krypterer det jeg vurderer til å være strengt nødvendig.		Krypterer alltid all sensitiv informasjon. Krypterer heller for mye enn for lite.

Kryptering er ikke relevant for alle virksomheter og spørsmålet er kun med for at man enkelt skal kunne sjekke at de som er pålagt å kryptere følger gjeldende prosedyrer.

T.22	B/L	Hvor nøye er du på skjerming av innsyn når du håndterer sensitiv informasjon?	Jeg tenker sjelden på at andre kan se eller høre hva jeg holder på med når jeg håndterer sensitiv informasjon. Jeg diskuterer sensitiv informasjon på mobil og/eller leser sensitive dokumenter på offentlige steder.		Jeg prøver som regel å sørge for at ingen har direkte innsyn i det jeg holder på med. Jeg må likevel ta samtaler og se på dokumenter der jeg er når jeg mottar dem, og tidvis kan dette skje i omgivelser jeg ikke har full kontroll over.		Jeg passer på at ingen har innsyn i det jeg holder på med. Jeg behandler aldri sensitiv informasjon utenfor skjermede omgivelser, verken i papirform, elektronisk eller muntlig.

Spørsmålet forsøker å identifisere hvorvidt respondentene reflekterer over omgivelsene når de skal behandle konfidensiell informasjon. Dette spørsmålet er ikke nødvendigvis like relevant for alle

virksomheter, eller i alle avdelinger i virksomheten og det kan derfor være hensiktsmessig å ta ekstra hensyn til dette når man tolker svarene.

T.23	B/L	Hvordan benytter du virksomhetens prosedyrer og regler for informasjonssikkerhet i ditt daglige arbeid?	Ser i hovedsak bort fra reglene, de er mer til hinder enn til hjelp i arbeidet.		Reglene og prosedyrene er alltid den riktige måten å gjøre jobben på. Jeg har ikke satt meg inn i hvorfor prosedyrene og reglene er som de er.		Reglene som benyttes gir en god beskrivelse av hvordan arbeid bør gjøres og er nyttige i mitt daglige arbeid.

Spørsmålet tar for seg holdningen til prosedyrer og regler i virksomheten og er tenkt å kunne gi en indikasjon på hvorvidt disse faktisk benyttes i det daglige arbeidet. Temaet ble også dekket i forrige versjon av verktøyet.

T.24	B/L	I hvilken grad kjenner du til utsteder av informasjon (eierskap) når du håndterer sensitive informasjon?	Jeg har ingen formening om hvem som har ansvaret for og hvem som er utsteder av informasjonen.		Jeg vet hvem som er ansvarlig for innholdet, og vet stort sett hvem som har utstedt informasjonen jeg håndterer.		Jeg vet alltid hvor informasjonen kommer fra og hvem som har utstedt den.

Spørsmålet er kommet til som et ønske fra brukere for å kunne gjøre målinger på organisasjonen av hvor bevisst respondenten er eierskap av informasjonen som håndteres. Dette kan ha konsekvenser for hvordan informasjonen skal leses og sikres.

Tilleggsspørsmål – policy og ledelse

T.25	L	I hvilken grad er ledelsen opptatt av å kommunisere informasjonssikkerhet til underleverandører og samarbeidspartnere?	Ledelsen synes ikke å være spesielt opptatt av informasjonssikkerhet, underleverandører og samarbeidspartnere får lite informasjon om informasjonssikkerhet.		Ledelsen bryr seg når det har vært en hendelse. Ledelsen informerer, men det er mye enveis-kommunikasjon.		Ledelsen er løpende opptatt av informasjons-sikkerhet og gir ut relevant informasjon til under-leverandører og samarbeidspartnere, samtidig som det er god dialog.

I dette spørsmålet tas det opp hvorvidt ledelsen er opptatt av dialog med underleverandører og å gi ut informasjon og rettledninger som sørger for at sikkerheten blir ivaretatt også i forhold til disse. Dette må regnes som relevant i forhold til håndtering av eksterne brukere og samarbeidspartnere (Albrechtsen et al., 2005).

T.26	B	I hvilken grad arbeider alle bevisst for å unngå uønskede sikkerhets-relaterte hendelser?	Vi ligger i etterkant. Det repareres når hendelser har inntruffet.		Vi prøver å ta vare på sikkerheten, men kommer av og til på etterskudd, for eksempel ved innføring av ny teknologi.		Vi forsøker alltid å ligge i forkant, og jobber systematisk for å forhindre uønskede hendelser. Målet er at det aldri skal fore-komme feil i forbindelse med informasjonssikkerhet.

Her forsøkes det å måle hva slags oppfatning medarbeiderne har av organisasjonen som helhet; om man føler at organisasjonen har gode

nok rutiner til å ta vare på sikkerheten. Dette kan relateres til et proaktivt og langsiktig perspektiv (IAEA, 2002).

T.27	⊥	I hvilken grad er informasjonssystemene godt sikret mot feil?	Robusthet og redundans for systemene vurderes sjelden. Enkeltfeil i ett system kan føre til følgefeil i andre systemer.		Det hender informasjons-systemene går ned, men bare i korte perioder. Vanlig drift kan gjenopptas etter kort tid.		Informasjonssystemene er satt opp etter beste praksis og er testet for robusthet. Kritiske komponenter er satt opp med redundans, slik at nedetiden på systemene er neglisjerbar og har ingen innvirkning på drift.

Det er viktig at virksomheten ikke risikerer at informasjonssystemene går ned som en følge av feil i enkeltsystemer. Dette nevnes i forhold til innføring av nye systemer og vedlikehold av eksisterende systemer (Albrechtsen et al., 2005)

T.28	⊥	Hvordan håndteres informasjonssikkerhet ved outsourcing?	Informasjonssikkerhet er ikke et tema ved outsourcing. Det legges kun vekt på at jobben gjøres til lavest mulig pris. Ved feil eller hendelser skyves skyld over på tjeneste- eller under-leverandør.		Potensielle tjeneste- eller underleverandører vurderes i forhold til hvordan de ivaretar informasjonssikkerhet. Leverandøren skal følge virksomhetens prosedyrer, regler og relevant lovverk og dette er kontraktsfestet.		Informasjonssikkerhet er et fokusområde ved outsourcing og er kontraktsfestet. Virksomheten samarbeider med leverandørene for å sikre god informasjons-sikkerhet på den outsourcede oppgaven. Leverandøren får bare tilgang til den informasjonen som er nødvendig og har god forståelse for dette.

Outsourcing blir en stadig mer aktuell problemstilling i forhold til informasjonssikkerhet og det er viktig virksomheten har en gjennomtenkt policy til hvordan man skal forholde seg til eksterne samarbeidspartnere. Temaet ble dekket i forrige versjon av verktøyet og er også sentralt i forhold til håndtering av eksterne brukere og samarbeidspartnere (Albrechtsen et al., 2005).

T.29	⊥	I hvilken grad mener du det gis gode tilbud for å heve kompetansen på informasjonssikkerhet?	Kurs og opplæring ses på som nødvendig, men det stjeler tid fra det vi egentlig jobber med.		Systematisk opplæring blir gitt. Det lages systematiske kursplaner. Opplæringen dekker tiltak og beredskap mot uønskede hendelser.		Utvikling av kompetanse blir sett på som en kontinuerlig prosess. Opplæring tilpasses risikobildet og virksomhetens behov.

Hva respondenten anser som gode tilbud vil være individuelt, men kan allikevel være en temperaturmåling på i hvilken grad medarbeidere er fornøyd med de tilbudene til kompetanseheving innen informasjons-sikkerhet som tilbys. Dette anses som relevant i forhold til tilstrekkelig kompetent personale (IAEA, 2002) og formelle og uformelle individrettede tiltak og bevisstgjøring (Albrechtsen et al., 2005)

T.30	L	I hvilken grad utveksles erfaringer med informasjonssikkerhet med myndighetene?	Vi rapporterer i forhold til minstekravet i lovgivning dersom det følges opp av myndighetene.		Vi rapporterer i forhold til lovgivning og har en dialog med myndighetene.		Det er etablert fagnettverk og læringsarena mellom myndigheter og virksomhet. Virksomheten og myndighetene deltar aktivt.

Her er det et ønske å identifisere i hvilken grad virksomheten samarbeider med tilsynsorganer og benytter myndighetenes erfaringsdatabaser. Dette er i samsvar med kategoriene tilsynsorganer og eksterne grupper, organisasjonslæring (IAEA, 2002) og håndtering av eksterne brukere og samarbeidspartnere (Albrechtsen et al., 2005).

Tilleggsspørsmål – revisjon

T.31	B/L	Hvordan forholder du deg til Sikkerhetsloven?	Jeg kjenner ikke til lovverket.		Jeg kjenner til de deler av lovverket som er relevant for mitt arbeid.		Jeg har god kjennskap til lovverket og hvilke felter det omfatter.

I dette spørsmålet ønsker man å undersøke hvorvidt respondenten har tilstrekkelig kunnskap om lovpålagte regler og krav. Dette er i samsvar med lovpålagte krav (Albrechtsen et al., 2005) og i forhold til tilstrekkelig kompetent personale (IAEA, 2002).

T.32	B/L	Hvordan forholder du deg til Personopplysningsloven?	Jeg kjenner ikke til lovverket.		Jeg kjenner til de deler av lovverket som er relevant for mitt arbeid.		Jeg har god kjennskap til lovverket og hvilke felter det omfatter.

I dette spørsmålet ønsker man å undersøke hvorvidt respondenten har tilstrekkelig kunnskap om lovpålagte regler og krav. Dette er i samsvar med lovpålagte krav (Albrechtsen et al., 2005) og i forhold til tilstrekkelig kompetent personale (IAEA, 2002).

T.33	L	I hvilken grad fokuseres det på informasjonssikkerhet ved anskaffelse og avhending av utstyr som benyttes til behandling eller lagring av sensitiv informasjon?	I liten grad, andre forhold legges til grunn ved avgjørelse av hvilke systemer som skal anskaffes. Systemer som skiftes ut destrueres ikke.		Informasjonssikkerhet er ett av flere kriterier som legges til grunn ved valg av nytt system. Det er faste rutiner for avhending av gammelt utstyr.		Informasjonssikkerhet er det viktigste kriteriet som legges til grunn ved valg av nytt system. Det er faste rutiner for avhending av gammelt utstyr slik at man sikrer at informasjon ikke kommer på avveie.

I dette spørsmålet ønsker man å identifisere i hvilken grad virksomheten har etablerte rutiner for avhending og avskaffelse av IT-utstyr. Dette er et viktig aspekt relatert til innføring av nye systemer og vedlikehold av eksisterende systemer, anskaffelse og avskaffelse og behandling av ny teknologi (Albrechtsen et al., 2005).

T.34	B/L	I hvor stor grad har du tillit til sikkerheten i virksomhetens IT-systemer?	Jeg har ingen tillit til sikkerheten i IT-systemene.		Jeg regner med at det meste håndteres forsvarlig av systemene.		Jeg har full tillit til at systemene siler ut de viktigste truslene, men passer også på å være oppdatert på de viktigste områdene selv.

Dette spørsmålet er sentralt i forhold til hvilket utgangspunkt respondenten har når vedkommende svarer på IT-relaterte spørsmål. Har man blind tro på IT-systemet, så oppleves man kanskje som uforsiktig og skjødesløs i oppførselen innen IKT.

Vedlegg D: Koplinger til forrige versjon

Kopling mellom spørsmål og forrige og nåværende versjon av verktøyet	
Gammelt spørsmål	**Nytt spørsmål**
1	12
2	11
3	9
4	13
5	Fjernet
6	T.13
7	Fjernet
8	T.14
9	2
10	16
11	21
12	T.28
13	22
14	27
15	6 og T.29
16	18
17	7
18	5 (overlappende tema)
19	5 (overlappende tema)
20	T.23
21	23
22	23
23	14
24	30
25	8
26	28
27	19
28	Kan relateres til T.16, T.19, T.20
29	Fjernet
30	Kan relateres til 4, T.12, T.16
31	2

SjekkIT – informasjonssikkerhet

Av Christian Waale Hansen (NTNU/NSM), Stig Ole Johnsen (SINTEF) og Yngve Nordby (NTNU/NSM)

Mennesker, som enkeltpersoner eller i grupper, har stor betydning for informasjonssikkerhet. Holdninger og organisasjonskultur er noe av grunnlaget for hvordan man forholder seg til sensitiv informasjon. Dette verktøyet forsøker å gi et bilde av atferd, holdninger og kultur som er relatert til informasjonssikkerhet. Verktøyet er utviklet som et samarbeid mellom Nasjonal Sikkerhetsmyndighet, NTNU og SINTEF.

Sentrale definisjoner

Informasjonssikkerhet (IS): Beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet. Informasjonen kan finnes muntlig, skriftlig eller på elektronisk form.

- **Konfidensialitet;** sikring av at bare de som er autorisert til å ha tilgang til informasjon har tilgang til den.
- **Integritet;** verning av nøyaktigheten og full-stendigheten av informasjon og behandlingsmetoder.
- **Tilgjengelighet;** sikring av at autoriserte brukere har tilgang til informasjon og tilknyttet utstyr når det er påkrevd.
- I tillegg nevnes ofte **autentisering**, som dreier seg om å få visshet om at en part virkelig er den han utgir seg for. Når man bruker et passord eller en PIN-kode er dette en del av en autentisering.

Uønsket hendelse: en hendelse som *har* eller *kan ha* forårsaket materielle, immaterielle eller menneskelige tap, eller brudd på informasjonssikkerhet, dvs. brudd på konfidensialitet, integritet eller tilgjengelighet.

Risiko er en funksjon av *Sannsynlighet* og *Konsekvens*.

Sårbarhet Et utrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med
å gjenoppta sin virksomhet etter at hendelsen har inntruffet.

Gradering: Påføring av en beskyttelsesgrad eller sikkerhetsgrad i henhold til sikkerhetsloven og/eller påføring av en beskyttelsesgrad eller sikkerhetsgrad i henhold til andre lover og instrukser, som eksempelvis beskyttelsesinstruksen eller på bakgrunn av en vurdering av virksomhetskritisk informasjon. Uttrykket *gradering* brukes gjennomgående for å dekke disse aspektene i verktøyet.

SjekkIT – informasjonssikkerhet

Legg merke til følgende!

Besvarelsen skal være anonym.
Alle spørsmålene må besvares.
For hvert spørsmål kan det kun krysses av i en rute.
Hensikten er at du skal svare det som du føler og tror er riktig.
B/L angir hvem som skal svare – B er alle ansatte, L er ledere på alle nivå.

Spørsmål	Brukere/Ledere	Spørsmål:					
		Kunnskap og holdning					
1	B/L	I hvilken grad kjenner du til om virksomheten klare målsettinger og en etablert policy for informasjonssikkerhet?	Jeg er ikke kjent med at virksomheten har målsettinger eller policy for informasjonssikkerhet.		Jeg er kjent med at virksomheten har målsettinger for informasjonssikkerhet, men kjenner ikke til noen egen policy for informasjonssikkerhet.	X	Jeg kjenner til policyen for informasjonssikkerhet og kjenner målsettingene i denne. Vet at denne følges opp på en god måte.
2	B/L	Hvordan synes du kravene til informasjonssikkerhet påvirker deg i ditt daglige arbeid?	Jeg ser på informasjonssikkerhet som hemmende for mitt daglige gjøremål i virksomheten.	X	Jeg følger lover og regler, og reflekterer ikke videre over det. Merarbeid med informasjonssikkerhet er nødvendig og jeg har forståelse for dette.		Kravene til informasjonssikkerhet hjelper meg å gjøre jobben min på en forsvarlig og hensiktsmessig måte i forhold til de lover og regelverk jeg forholder meg til.
3	B/L	I hvilken grad oppfatter du at det er akseptabelt å bryte sikkerhetsreglene for å øke effektiviteten?	Det er akseptert å bryte sikkerhetsreglene for å kunne levere resultater raskere.		Jeg prøver å følge regelverket, men hvis det er nødvendig for å levere hender det at reglene brytes.		Det er ikke akseptert å bryte sikkerhetsreglene og det forekommer ikke.
4	B/L	Hvordan opplever du det er å påpeke feil hos kolleger?	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet, sier man ifra. Folk tar til seg rettledning, men er også ekstra nøye med å se etter feil hos andre en periode etterpå.		Det er ikke så ofte det trengs, men folk er lydhøre overfor egne feil. Den enkelte tar til seg bemerkninger, og systemet revideres ofte for å fange opp uønsket atferd.
5	/L	Hvem oppfatter du har ansvaret for informasjonssikkerheten i virksomheten din?	Ledelsen har det overordnede ansvaret. Ansvaret er ikke fordelt videre i organisasjonen.		Det eksisterer en sikkerhetsavdeling eller sikkerhetsansvarlig med fullt ansvar for informasjonssikkerhet.		Ansatte på alle nivå har ansvar for Informasjonssikkerhet, og fokuset på sikkerhet er forankret i ledelsen.

Hvordan skal skjemaet besvares?

For hver kategori skal du sette kryss for det svaralternativet som du synes best beskriver situasjonen i virksomheten. Det er ikke meningen at du skal lese alle rutene – det tar fort for lang tid! Gjør i stedet følgende:

1. Les spørsmålet og gjør deg opp en mening om virksomheten er bra eller dårlig på dette punktet.
2. Start og lese der du mener virksomheten befinner seg.
3. Juster svaret ditt til høyre eller venstre for å finne den beskrivelsen som passer best.

Hver kategori måles på en femtrinns skala, der tre av alternativene er beskrevet. Du vil kanskje ikke finne en rute/beskrivelse som stemmer 100 % overens med det du mener er situasjonen i virksomheten. I så fall velger du den som du mener passer best, eller krysser midt imellom (på rute 2 eller 4) der du mener at dette er riktig.

Når du er ferdig med undersøkelsen skal svarkortet på siste side fylles inn.

Personlige opplysninger og opplysninger om forholdet til virksomheten

Alder:
- ☐ Under 18
- ☐ 18 - 25
- ☐ 26 - 35
- ☐ 36 - 50
- ☐ 51 - 60
- ☐ Over 60

Kjønn:
- ☐ Mann
- ☐ Kvinne

Nivå i organisasjonen:
- ☐ Leder
- ☐ Medarbeider

Fagområde:
- ☐ Administrasjon
- ☐ Teknisk / drift
- ☐ Sikkerhet
- ☐ Salg og kundebehandling
- ☐ Forskning og utvikling
- ☐ Annet

Ansettelsesforhold?
- ☐ Fast ansatt
- ☐ Deltidsansatt
- ☐ Innleid konsulent

Hvor mange virksomheter har du jobbet i, inkludert denne?
- ☐ 1
- ☐ 2
- ☐ 3 - 5
- ☐ 6 eller flere

Høyeste utdannelse:
- ☐ Universitet (lavere grad, 1-3 år)
- ☐ Universitet (høyere grad, > 3 år)
- ☐ Høyskole (1-3 år)
- ☐ Høyskole (>3 år)
- ☐ Videregående
- ☐ Annet

Totalt antall år i virksomheten:
- ☐ 0 - 1 år
- ☐ 1 - 5 år
- ☐ 6 - 10 år
- ☐ 11 - 25 år
- ☐ Over 25 år

Trives du i jobben din og med arbeidsoppgavene?
- ☐ Ja
- ☐ Nei

Hva slags erfaring har du med bruk av datamaskiner:
- ☐ Lang erfaring med bruk og programmering av datamaskiner
- ☐ Erfaren, avansert bruker
- ☐ Kan de programmene jeg bruker oftest, men ikke så mye mer
- ☐ Ustø på det meste som har med data å gjøre
- ☐ Ingen erfaring (bruker ikke datamaskiner i jobben)

Mener du at IT-systemene håndterer sikkerheten for deg?
- ☐ Ja
- ☐ Nei

Har du noen gang brutt sikkerhetsreglene?
- ☐ Ja, bevisst (en eller flere ganger)
- ☐ Ja, men det var før jeg visste at det jeg gjorde var mot reglementet
- ☐ Ja, men jeg ble presset til å gjøre det:
  - ☐ På grunn av tidspress/arbeids-press, men jeg valgte det selv
  - ☐ Jeg ble instruert til å gjøre det
- ☐ Ja, ved en forglemmelse/slurv
- ☐ Vet ikke
- ☐ Nei

Hvis ja, har du brutt et påbud eller et forbud? (kan krysse i begge):
- ☐ Påbud
- ☐ Forbud

Ble det oppdaget?
- ☐ Ja
- ☐ Nei

Dersom du oppdaget at en kollega gjorde noe kriminelt på arbeidsplassen (f.eks. tyveri eller svindel), ville du rapportert dette?
- ☐ Ja, i alle tilfeller
- ☐ Det kommer an på situasjonen og hvem det er
- ☐ Nei

Spørsmål	Brukere/Ledere	Spørsmål:					
		Kunnskap og holdning					
1	B/L	I hvilken grad kjenner du til om virksomheten har klare målsettinger og en etablert policy for informasjons-sikkerhet?	Jeg er ikke kjent med at virksomheten har målsettinger eller policy for informasjonssikkerhet.		Jeg er kjent med at virksomheten har målsettinger for informasjonssikkerhet, men kjenner ikke til noen egen policy for informasjonssikkerhet.		Jeg kjenner til policyen for informasjonssikkerhet og kjenner målsettingene i denne. Vet at denne følges opp på en god måte.
2	B/L	Hvordan synes du kravene til informasjonssikkerhet påvirker deg i ditt daglige arbeid?	Jeg ser på informasjonssikkerhet som hemmende for mitt daglige gjøremål i virksomheten.		Jeg følger lover og regler, og reflekterer ikke videre over det. Merarbeid med informasjons-sikkerhet er nødvendig og jeg har forståelse for dette.		Kravene til informasjonssikkerhet hjelper meg å gjøre jobben min på en forsvarlig og hensiktsmessig måte i forhold til de lover og regel-verk jeg forholder meg til.
3	B/L	I hvilken grad oppfatter du at det er akseptabelt å bryte sikkerhetsreglene for å øke effektiviteten?	Det er akseptert å bryte sikkerhetsreglene for å kunne levere resultater raskere.		Jeg prøver å følge regelverket, men hvis det er mye press for å levere hender det at reglene brytes.		Det er ikke akseptert å bryte sikkerhetsreglene og det forekommer ikke.
4	B/L	Hvordan opplever du det er å påpeke feil hos kolleger?	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet, sier man ifra. Folk tar til seg rettledning, men er også ekstra nøye med å se etter feil hos andre en periode etterpå.		Det er ikke så ofte det trengs, men folk er lydhøre overfor egne feil. Den enkelte tar til seg bemerkninger, og systemet revideres ofte for å fange opp uønsket atferd.
5	B/L	Hvem oppfatter du har ansvaret for informasjonssikkerheten i virksomheten din?	Ledelsen har det overordnede ansvaret. Ansvaret er ikke fordelt videre i organisasjonen.		Det eksisterer en sikkerhetsavdeling eller sikkerhetsansvarlig med fullt ansvar for informasjonssikkerhet. Ansatte får pålegg og retningslinjer fra sikkerhetsavdelingen.		Ansatte på alle nivå har ansvar for Informasjonssikkerhet, og fokuset på sikkerhet er forankret i ledelsen. Oppgavene løses og følges opp lokalt.

6	B/L	Opplever du at du har fått tilstrekkelig opplæring rundt informasjonssikkerhet og sikker bruk av IT-systemer?	Jeg har ikke fått opplæring i sikker bruk av IT.		Jeg har fått opplæring i gjeldende regelverk og rutiner for sikker bruk av virksomhetens informasjonssystemer. Opplæringen dekker tiltak og beredskap mot uønskede hendelser.		Ledelsen følger opp gjennom kontinuerlig informasjon og opplæring blant alle brukergrupper. Alle bidrar aktivt i opplæringen.
7	B/L	I hvilken grad får noen skylden dersom en uønsket hendelse inntreffer?	Enkeltansatte eller samarbeidspartnere blir trukket fram som syndebukker dersom det skjer et sikkerhetsbrudd.		En kombinasjon av tekniske eller personlige feil sees på som årsaker til at hendelser skjer. Systemet i seg selv får ofte skylden for sikkerhetsproblemene.		Verken personer eller samarbeidende virksomheter blir syndebukker. Beskyldninger er sjelden noe tema.
8	B/L	Hvordan oppfatter du at informasjon i virksomheten graderes?	Det finnes ikke, eller jeg kjenner ikke, rutiner for å skille sensitiv og åpen informasjon. Det gjøres ingen verdivurdering av informasjonen.		Det finnes regelverk for å skille mellom sensitiv og åpen informasjon, men jeg kjenner ikke til hvordan de fungerer.		Det finnes graderingssystemer og de ansatte kjenner disse godt slik at ikke informasjon blir feilgradert. Kriterier og rutiner for verdivurdering av informasjon følges av de ansatte og videreutvikles og tilpasses løpende.
9	B/L	Hvordan behandler du sensitiv informasjon?	Tenker sjelden over at sensitiv informasjon skal behandles med forsiktighet.		Er klar over restriksjonene knyttet til sensitivt og sikkerhetsgradert materiale.		Er kjent med utstederen av informasjonen (eierskapet), kjenner hvem som har tilgang og forstår hvorfor informasjonen er sensitiv. Er ”føre var” når jeg kommer i kontakt med sensitiv informasjon.

		Atferd					
10	B/L	Hvilke vaner har du for valg og bruk av brukernavn og passord?	Skifter aldri passord. Enkelhet prioriteres framfor sikkerhet.		Bruker samme passord på forskjellige tjenester. Skifter passord av og til.		Skifter passord ut fra en risikovurdering. Benytter passord som er en kombinasjon av tall og store/små bokstaver som er over 7 tegn.
11	B/L	Hvilke e-postvaner har du?	Åpner og videresender e-post med vedlegg uten å tenke på sikkerheten. Tenker aldri over at e-post kan komme uvedkommende i hende.		Det er laget regler for god e- post skikk som beskriver hvordan e-post skal benyttes.		Er klar over at e-post er et usikkert medium. Avsender kan forfalskes, og vedlegg og lenker kan være skadelige eller feilaktige. Det er laget regler som beskriver hvordan e-post kan brukes sikkert for å sikre at bare rett person får korrekt informasjon uten at andre får innsyn i det.
12	B/L	Hvordan ivaretar du sikkerheten når du surfer på internett?	Klikker som regel ”OK” på spørsmål. Synes det er vanskelig å vite hva som er rett. Oppgir sensitiv informasjon ukritisk uten å sjekke at nettadressen er ufarlig.		Forsøker å være forsiktig, kontrollerer web-adresser jeg benytter. Det vil si, oppgir ikke personlige opplysninger som brukeridentitet, passord eller annen informasjon uten å være sikker på at web-adressen er ekte. Klikker etter magefølelsen.		Oppgir bare sensitiv opplysning på web-adresser jeg har kontrollert eller hvor sertifikater benyttes.
13	B/L	Hvordan ivaretar du sikkerheten ved arbeid hjemmefra på egen PC?	Tenker lite på informasjonssikkerhet. Andre personer (f.eks. familie), har full adgang til min PC. Lagrer arbeidet på egen PC uten å kryptere. Enkelhet prioriteres framfor sikkerhet.		Følger etablerte rutiner. Er klar over restriksjonene knyttet til gradert materiale. Det er etablert gode rutiner for å arbeide sikkert med PC som skal koples opp utenfra i virksomhetens interne nett.		Tar alle forholdsregler og er oppmerksom på at å arbeide på denne måten øker faren for virus og lekkasje av informasjon. Hjemme-PC har samme sikkerhetsnivå som jobb-PC. Bruker kryptert forbindelse til jobben, og lagrer filene mine på en sikker server på jobb.

14	L	Hvordan forholder du deg til lovpålagte regler, som for eksempel Sikkerhetsloven og Personopplysningsloven i virksomheten?	Relevant lovverk er ikke kommunisert ut i virksomheten. Ledelsen eller sikkerhetsansvarlige har noe kjennskap til lovverket. Det er sannsynlig at virksomheten ikke oppfyller alle kravene fordi disse ikke er godt kjent.		Interne prosedyrer blir periodisk sammenlignet med kravene i loven slik at lovverket blir oppfylt.		Vi har jevnlig intern opplæring, og interne rutiner blir løpende oppdatert når lovverket justeres og oppdateres. Det er god forståelse for lovverket, og alle ser nødvendigheten av et lovpålagt regelverk i virksomheten
15	B/L	Hvordan vil du beskrive kontorplassen din når du går fra den?	Fortrolige papirer ligger åpent og tilgjengelig for hvem som helst. Jeg låser eller stenger PCen sjelden når jeg forlater den.		Følger de etablerte reglene, fortrolige papirer gjøres utilgjengelig for ikke autoriserte. Låser/stenger som regel PCen, men ikke når jeg skal ta en kjapp tur bort fra den (ca 5-15 minutter).		Fortrolige papirer gjøres utilgjengelig for ikke autoriserte personer, og jeg låser alltid PC når jeg forlater den.
		Policy og ledelse					
16	B/L	I hvilken grad er ledelsen opptatt av å kommunisere informasjonssikkerhet til ansatte og samarbeidspartnere?	Ledelsen synes ikke å være spesielt opptatt av informasjons-sikkerhet, ansatte får lite informasjon om informasjonssikkerhet.		Ledelsen bryr seg når det har vært en hendelse. Ledelsen informerer, men det er mye enveiskommunikasjon.		Ledelsen er løpende opptatt av informasjonssikkerhet og gir ut relevant informasjon til medarbeidere og samarbeidspartnere, samtidig som det er god dialog.
17	B/L	I hvilken grad oppfatter du at lederne i virksomheten går foran som gode eksempler når det gjelder informasjonssikkerhet?	Oppfatter ikke at lederne går foran som gode eksempler.		Lederne går til en viss grad foran som gode eksempler, men i enkelte situasjoner, som f.eks for å nå tidsfrister, bryter de reglene for å nå målene		Lederne går alltid foran som gode eksempler og viser hvordan ting bør gjøres.
18	B/L	I hvilken grad oppfatter du at ansatte inkluderes i arbeidet med informasjonssikkerhet?	Ledelsen og sikkerhetsansvarlige utreder og kommer med retningslinjer og generelle tiltak uten innspill fra ansatte.		Rapporter og erfaringer fra de ansatte benyttes i utformingen av prosedyrer og regler.		Ansatte blir rådført og deltar i utforming av tiltak, og blir sett på som en viktig ressurs i arbeidet for informasjonssikkerhet. Enkelte ansatte får konkrete oppgaver innen informasjons-sikkerhet.

19	L	I hvilken grad utveksles erfaringer med informasjonssikkerhet med andre virksomheter?	Det hentes lite erfaringer fra andre. Sikkerhetsarbeidet er lukket og internt.		Det fokuseres på å måle informasjonssikkerhet for å kunne sammenligne med andre virksomheter.		Virksomheten deltar aktivt i fagnettverk relatert til informasjonssikkerhet. Virksomheten undersøker stadig hvordan samarbeidspartnere og andre virksomheter, også i andre bransjer og sektorer, jobber med informasjonssikkerhet.
20	L	I hvilken grad oppfatter du at samarbeidspartnere inkluderes i arbeidet med informasjonssikkerhet?	Samarbeidspartnere er ikke involvert i utarbeidelse av retningslinjer.		Samarbeidspartnere skal følge virksomhetens prosedyrer, regler og relevant lovverk.		Samarbeidspartnere skal følge virksomhetens prosedyrer, regler og relevant lovverk, men blir også rådført og deltar aktivt i arbeidet for å sikre god informasjonssikkerhet.
21	B/L	Blir informasjonssikkerhet prioritert i forhold til de vanlige daglige gjøremål?	Det fokuseres kun på å få unna virksomhetens primæroppgaver. Informasjonssikkerhet sees utelukkende på som en ekstra belastning og utgiftspost.		Primæroppgavene er i fokus, men det settes av tilstrekkelige ressurser til å imøtekomme pålegg, bestemmelser og kjente trusler. Det settes av nok ressurser til å gjøre regler kjent. Ved hendelser settes det inn nok ressurser til å opprette stabil drift.		Ressurser prioriteres ut fra en risikovurdering og en kost-/nyttevurdering. Man forsøker å ligge i forkant for å unngå uønskede hendelser. Informasjonssikkerhet er integrert i daglig drift og i utvikling av primæroppgavene.
22	L	Hvordan håndteres informasjonssikkerhet i prosjekter?	Informasjonssikkerhet er ikke et tema når nye prosjekter planlegges. Eventuelle problemer knyttet til informasjonssikkerhet blir utsatt til gjennomføringsfasene av prosjekter og løses etter hvert.		Informasjonssikkerhet blir tatt hensyn til i prosjekter, og deltakerne er alle autoriserte til å kunne gjøre jobben. Prosjektene skal følge etablerte prosedyrer, regler og relevant lovverk.		Når nye prosjekter planlegges blir informasjonssikkerhet vurdert i startfasen. Risiko- og sårbarhetsanalyser gjennomføres og informasjons-sikkerhet testes løpende underveis. Prosjektgruppene har forståelse for at informasjonssikkerhet er av kritisk betydning.

23	B/L	I hvilken grad verdsettes rapportering av uønskede hendelser i virksomheten?	Jeg får ingen tilbakemelding fra noen om hvordan det går med saken når jeg rapportere videre internt. Jeg velger heller å prøve å løse problemet selv.		Dersom hendelsen er av såpass omfang at den har direkte konsekvenser for mitt daglige arbeid, rapporterer jeg den. Min nærmeste overordnede er den jeg rapporterer til og jeg får tilbakemelding om at min rapportering er mottatt og at noen vil se på saken.		Jeg rapporterer alltid dersom jeg opplever en sikkerhetsrelatert, uønsket hendelse. Jeg kjenner til hvem i virksomheten jeg skal rapportere ulike typer hendelser til. Jeg opplever at henvendelsen blir tatt på alvor og at det skjer noe. Jeg blir informert om løsningen dersom det er nødvendig og/eller relevant.
24	B/L	I hvilken grad oppfatter du at virksomheten prioriterer sikkerheten ved fjernarbeid, for eksempel ved oppkopling mot virksomhetens nett?	Enkelhet prioriteres framfor sikkerhet. Det er viktigste er å kunne koble opp utstyr til virksomhetens nett på en enkel måte.		Det er etablert regler for sikkert arbeid med PC som skal kobles opp utenfra i virksomhetens interne nett.		Virksomheten har gode rutiner for fjernarbeid. Jeg er likevel oppmerksom på at fjernarbeid øker faren for virus og lekkasje av informasjon.
25	L	I hvor stor grad er fysiske sikkerhetstiltak etablert?	Det er få fysiske tiltak for å sikre sensitiv informasjon og systemer. Utenforstående har fri adgang til lokalene.		Virksomheten har adgangskontroll i bygget og virksomhetskritiske informasjonssystemer er fysisk sikret.		Virksomheten er godt sikret med flere nivåer av adgangskontroll på forskjellige områder og lokaler. Ingen besøkende går uten følge uten at dette er avklart med sikkerhetsansvarlig. Kontorer låses, PCer med sensitivt materiell er låst fast og lagringsenhet fjernes og låses vekk.
26	L	I hvilken grad er det gode kriterier eller rutiner for å velge ut hvilke IT-systemer som skal beskyttes?	Det er ikke etablerte rutiner for å velge ut hvilke IT-systemer som skal beskyttes.		Sikkerhetsavdelingen har ansvaret for utvelgelse av hvilke IT-systemer som skal beskyttes.		Det eksisterer gode rutiner for å fange opp hvilke IT-systemer som skal beskyttes, og hovedansvaret ligger på sikkerhetsavdelingen.

27	L	I hvilken grad har virksomheten gode rutiner for å sikre kontinuerlig drift?	Det er ikke etablert beredskapsplaner. Det fokuseres ikke mye på å unngå uønskede hendelser.		Virksomheten har regler, rutiner og løsninger som trer i kraft ved alvorlige hendelser. Rutinene sikrer kontinuitet ved forventede uønskede hendelser.		Man kjører ofte risiko- og sårbarhetsanalyser, slik at virksomheten til enhver tid har et oppdatert risikobilde. Ved hendelser trer et beredskapsapparat med nødvendige tiltak i kraft, slik at driften kan opprettholdes mens feilen rettes. I ettertid analyseres hendelsen for å kunne unngå tilsvarende hendelser i fremtiden.
		Revisjon					
28	L	Hvordan revideres informasjonssikkerhet?	Revisjon av informasjonssikkerhet skjer kun ved eksternt press og større hendelser.		Det gjennomføres revisjoner for å påse at regler og prosedyrer for informasjonssikkerhet eksisterer og blir fulgt.		Jevnlige revisjoner fokuserer både på kunnskap, atferd og holdninger. Revisjon brukes aktivt for å forbedre virksomhetens rutiner og prosedyrer.
29	L	I hvilken grad analyseres inntrufne uønskede hendelser?	Det gjøres lite analyser av hendelser. Kun større hendelser som rammer betydelige deler av virksomheten følges opp.		Hendelsen analyseres med fokus på etablere en rutine for å unngå samme hendelse igjen. Det gjøres lite oppfølgingsarbeid for å se sammenhenger og få oversikt.		Hendelsen analyseres slik at organisasjonen kan lære og unngå tilsvarende hendelser og ringvirkninger av slike.
30	L	Hvordan gjennomføres risiko- og sårbarhetsanalyser?	De eneste analysene som foregår, er de sikkerhetsansvarliges egne vurderinger som gjøres i det daglige arbeidet. Ledelsen har liten oversikt over risiko.		Det gjennomføres til tider risiko- og sårbarhetsanalyser. Det settes grenser og eventuelle minimumsstandarder for akseptabel risiko, og tiltak settes i verk der risikoen er større enn de fastsatte grensene.		Det gjennomføres ofte risiko- og sårbarhetsanalyser, og virksomheten har løpende fokus på risiko og sårbarheter. Tiltak settes i verk med det samme behovet oppstår.
31	B/L	Hvordan oppfattet du denne undersøkelsen?	Tidkrevende og unødvendig, ikke relevant.		Helt OK.		Spennende, satte ny fokus og tilførte meg ny kunnskap.

Tilleggsspørsmål							
		Kunnskap og holdning					
Spørsmål	Brukere/Ledere	Spørsmål:					
T.1	B/L	Hvor god kunnskap har du om følgende teknologier: ad-ware, spy-ware og virus?	Jeg har liten eller ingen kjennskap til dette, og har i liten grad en formening om hvilken skade disse kan forårsake.		Vet hva de vanligste truslene representerer, og er i stand til å beskytte meg mot disse.		Har inngående kunnskap på området, kjenner til de vanligste sikkerhetshullene truslene benytter seg av, og er i stand til å beskytte min PC og nettverket den er tilkoblet.
T.2	B/L	I hvilken grad oppfatter du at man er oppmerksom på ukjente personer på arbeidsplassen din?	Man vil sannsynligvis ikke legge merke til om ukjente personer er på arbeidsplassen.		Ukjente personer som ser viktige ut vil sannsynligvis få gå rundt, andre vil bli sjekket for hvorfor de er der.		Alle ukjente personer blir lagt merke til, og man undersøker hva de har der å gjøre.
T.3	B/L	Hvor godt kjenner du til kryptering?	Jeg har liten eller ingen kjennskap til kryptering.		Har en formening om nødvendigheten av kryptering og er i stand til å skru på kryptering i applikasjoner der dette er mulig. Vet hvilke systemer rundt meg som er kryptert.		Kjenner godt til kryptering. Kan anslå hvor sikker krypteringen er. Er i stand til å sette opp sikker kryptering av medier jeg bruker.
T.4	B/L	I hvilken grad bruker du intranettet til å finne informasjon om sikkerhet (regler osv.)?	Jeg vet ikke om det finnes noe, og det tar for lang tid å lete etter det.		Jeg vet det finnes, men må lete fordi jeg ikke vet hvor det ligger.		Jeg vet hvor det finnes og bruker nettet ofte for å holde meg oppdatert.
T.5	B/L	Hvordan er de vanlige rutinene for bruk av telefaks?	Sender faks til angitt nummer uten å kontrollere at faksen kommer frem, og uten å undersøke om rett person får den.		Sender faks til angitt nummer og venter på bekreftelse på at den er kommet frem. Undersøker ikke alltid om rett mottaker har fått faksen på faksnummeret som har blitt benyttet.		Er alltid sikker på at rett faksnummer benyttes og forsikrer meg om at rett informasjon har kommet frem til rett mottaker.

T.6	B/L	Hvordan forholder du deg til sensitiv informasjon på telefon?	Jeg er ikke videre kritisk til hva folk spør om, og svarer så mye jeg vet om tema på forespørsel.		Jeg vet hva slags informasjon som er sensitiv og som ikke skal oppgis på telefon.		Jeg er fullt inneforstått med hva slags informasjon jeg har lov å oppgi og hva jeg ikke har lov å oppgi. Når jeg blir forespurt om informasjon tenker jeg alltid nøye gjennom om informasjonen kan brukes til andre formål enn det den opprinnelig er tiltenkt.
T.7	B/L	Hvordan håndterer du sensitiv informasjon når du mottar skrevne dokumenter?	Jeg har ikke noe forhold til om informasjonen som er gitt meg er sensitiv eller ikke. Papirene er åpne og tilgjengelige for andre.		Jeg vet hva slags informasjon som er sensitiv og som ikke kan vises til andre. Jeg er som regel nøye med å låse unna dokumenter for uvedkommende.		Jeg tenker over hvem som kan få se dokumentene avhengig av hvor jeg gjør av dem og sørger for at ingen uvedkommende får tilgang. Jeg er fullt inneforstått med hva slags informasjon jeg kan og ikke kan oppgi innenfor graderingen dokumentet har. Når jeg får dokumenter, tenker jeg alltid nøye gjennom om informasjonen kan brukes til andre formål enn det den opprinnelig er tenkt til.
T.8	B/L	Hvordan håndterer du sensitiv informasjon når du skriver dokumenter?	Jeg tar med all den informasjonen som kan være nyttig i dokumenter. Enkel tilgang på nødvendig informasjon er viktigere for meg enn å sjekke hva det er lov å oppgi.		Jeg vet hva slags informasjon som er sensitiv og som ikke skal oppgis i dokumenter med forskjellig klareringsnivå.		Jeg er fullt inneforstått med hva slags informasjon jeg kan og ikke kan oppgi innenfor graderingen dokumentet har og tenker igjennom hvem som kan ha tilgang på dokumentet. Når jeg blir forespurt om informasjon, tenker jeg alltid nøye gjennom om informasjonen kan brukes til andre formål enn det den opprinnelig er tenkt til.

T.9	B/L	Hvordan ivaretar du sikkerheten ved bruk av mobilt utstyr som eksempelvis bærbar PC, telefon, lomme-PC eller minnepinne?	Enkelhet prioriteres framfor sikkerhet. Lagrer sensitiv informasjon på mobilt utstyr uten å kryptere eller å ta sikkerhetskopi. Tenker lite på informasjonssikkerhet. Andre personer har tilgang til mitt mobile utstyr.		Jeg følger etablerte rutiner og er klar over restriksjonene knyttet til sensitiv informasjon på mobilt utstyr. Utstyret er beskyttet med passord og informasjon er kryptert.		Informasjon på mobilt utstyr er alltid kryptert og jeg har sikkerhetskopi. Informasjon lagres i utgangspunktet på en sikker server på jobben. Bruker kryptert forbindelse med autentisering ved utveksling av data. Hva man får tilgang på ved arbeid utenfra, er bestemt ut fra en risikovurdering.
T.10	B/L	I hvilken grad oppfatter du at det er akseptabelt å laste ned og dele opphavsbeskyttet materiale (musikk, film, dokumenter, programvare, bøker, lyd)?	Fildeling er akseptert og det forekommer. Materiale lagres av og til på lokale filtjenere og på egen PC. Når materiale er tilgjengelig så kopieres og spres det. Det er en utbredt holdning at dette er helt greit.		Det er etablert regler som forbyr lagring og bruk av opphavs-beskyttet materiale, men det forekommer.		Det er god forståelse for at man ikke kopierer og videreformidler opphavsbeskyttet materiale, og det forekommer heller ikke.
T.11	B/L	I hvilken grad oppfatter du at det er akseptabelt å teste ut sikkerhetsbarrierer i IT-systemene?	Testing av systemenes sikkerhetsgrenser og sikkerhetshull er akseptert og det forekommer.		Dette er ikke lov i henhold til regelverket, men kan forekomme.		Det er ikke akseptabelt og forekommer ikke.
T.12	B	Hvordan opplever du det er å påpeke feil hos ledere?	Forekommer ikke. Det skaper bare misnøye og dårlig arbeidsklima.		Skjer det gjentatte brudd på reglementet sier man i fra. Lederen tar til seg rettledning, men er også ekstra nøye med å se etter feil og svakheter hos andre en periode etterpå.		Det er ikke så ofte det trengs, men lederne er lydhøre overfor egne feil og oppfordrer ansatte til å passe på at de går foran som gode eksempler.

T.13	B/L	Er du kjent med virksomhetens prosedyrer og regler for informasjonssikkerhet?	Jeg har ikke kjennskap til hvordan virksomheten tar hånd om informasjonssikkerhet. Det finnes muligens noen dokumenter om dette, men disse har jeg ikke sett på.		Jeg vet hvor jeg kan finne dokumentasjon om hvordan virksomheten tar hånd om informasjonssikkerhet. Jeg har ikke fått noen særlig innføring i virksomhetens arbeid på dette området.		Jeg føler at jeg har god kjennskap til hvordan virksomheten tenker om informasjonssikkerhet. Informasjon om prosedyrer og regler er lett tilgjengelig, og jeg får alltid vite om endringer og oppdateringer på området.
T.14	B/L	Hvordan mener du kravene til informasjonssikkerhet påvirker forholdet mellom de ansatte?	Fokus på informasjonssikkerhet fører til et dårlig forhold mellom de ansatte.		Fokus på informasjonssikkerhet påvirker ikke forholdet mellom de ansatte.		Fokus på informasjonssikkerhet har en positiv innvirkning på forholdet mellom de ansatte. Alle ansatte jobber for at virksomheten som helhet skal ha så god informasjonssikkerhet som mulig.
T.15	L/B	I hvilken grad har du oversikt over virksomhetens arbeidsrutiner, informasjonssystemer og samspillet mellom disse?	Jeg har liten oversikt over hvordan rutiner og systemer påvirker hverandre, og vet lite om hvilke konsekvenser en feil i en rutine eller system kan ha for andre systemer.		Jeg har en viss forståelse av sammenhengen mellom rutinene og systemene i virksomheten. Stort sett kan jeg si hvilke konsekvenser mine handlinger har for enkeltsystemer, men har liten oversikt over konsekvenser for tilstøtende systemer.		Jeg kjenner sammenhengen mellom rutiner og systemer godt, og har god forståelse for hvordan feil kan forårsake sikkerhets-brister i andre systemer.
T.16	B/L	I hvilken grad oppfatter du at det er akseptert å innrømme egne feil?	I liten grad, ansatte ønsker ikke å si fra dersom man har forårsaket en feil, ettersom dette bare har negative konsekvenser for den ansatte selv.		Til en viss grad, ansatte sier i fra ved alvorlige hendelser. Dårlige eller manglende rutiner får skylden.		I stor grad, man har ikke noe problem med å si ifra. Ansatte sier alltid fra dersom de gjør feil, og dette blir brukt til å lære av feilen.
T.17	B/L	I hvilken grad kjenner du til hvem som har tilgang på sensitiv informasjon?	Jeg har ingen formening om hvem som har rett til å se sensitiv informasjon.		Jeg er klar over hvilken autorisasjon som kreves for å få se informasjonen.		Jeg vet alltid hvilken autorisasjon som kreves for å få innsyn i informasjonen og hvem i omgivelsene mine som har rett til å se informasjonen.
T.18	B/L	Hvordan synes du kravene til informasjonssikkerhet påvirker det daglige arbeidet i virksomheten?	Informasjonssikkerhet er bare nødvendig pga lovverk, og sees utelukkende på som en ekstra belastning og utgiftspost.		De fleste forstår at informasjonssikkerhet er viktig i forhold til daglig arbeid/drift, regler og lovverk.		Informasjonssikkerhet går hånd i hånd med arbeidet/driften og er nødvendig for å kunne drive på en hensiktsmessig og forsvarlig måte

		Atferd					
T.19	B/L	Hvordan reagerer du hvis du oppdager en feil eller et problem innen ditt ansvarsområde?	Retter opp feilen så raskt som mulig. Informerer ingen om dette.		Sier fra til linjeleder om det som har skjedd.		Informerer relevante personer i organisasjonen om det som har skjedd, slik at de kan lære av det.
T.20	B/L	Hvordan reagerer du hvis du oppdager en feil eller et problem innen andre sitt ansvarsområde?	Vil ikke skape problemer, så jeg sier ikke i fra, dette er ikke mitt bord.		Tar det opp med vedkommende som har ansvaret. Regner med at ansvarlig følger opp.		Informerer relevante personer i organisasjonen om det som har skjedd, slik at virksomheten kan lære av det.
T.21	B/L	I hvilken grad passer du på å kryptere sensitiv informasjon du håndterer?	Kjenner ikke til kryptering, og krypterer aldri noe som helst.		Krypterer det jeg vurderer til å være strengt nødvendig.		Krypterer alltid all sensitiv informasjon. Krypterer heller for mye enn for lite.
T.22	B/L	Hvor nøye er du på skjerming av innsyn når du håndterer sensitiv informasjon?	Jeg tenker sjelden på at andre kan se eller høre hva jeg holder på med når jeg håndterer sensitiv informasjon. Jeg diskuterer sensitiv informasjon på mobil og/eller leser sensitive dokumenter på offentlige steder.		Jeg prøver som regel å sørge for at ingen har direkte innsyn i det jeg holder på med. Jeg må likevel ta samtaler og se på dokumenter der jeg er når jeg mottar dem, og tidvis kan dette skje i omgivelser jeg ikke har full kontroll over.		Jeg passer på at ingen har innsyn i det jeg holder på med. Jeg behandler aldri sensitiv informasjon utenfor skjermede omgivelser, verken i papirform, elektronisk eller muntlig.
T.23	B/L	Hvordan benytter du virksomhetens prosedyrer og regler for informasjonssikkerhet i ditt daglige arbeid?	Ser i hovedsak bort fra reglene, de er mer til hinder enn til hjelp i arbeidet.		Reglene og prosedyrene er alltid den riktige måten å gjøre jobben på. Jeg har ikke satt meg inn i hvorfor prosedyrene og reglene er som de er.		Reglene som benyttes gir en god beskrivelse av hvordan arbeid bør gjøres og er nyttige i mitt daglige arbeid.
T.24	B/L	I hvilken grad kjenner du til utsteder av informasjon (eierskap) når du håndterer sensitive informasjon?	Jeg har ingen formening om hvem som har ansvaret for og hvem som er utsteder av informasjonen.		Jeg vet hvem som er ansvarlig for innholdet, og vet stort sett hvem som har utstedt informasjonen jeg håndterer.		Jeg vet alltid hvor informasjonen kommer fra og hvem som har utstedt den.

		Policy og ledelse					
T.25	L	I hvilken grad er ledelsen opptatt av å kommunisere informasjonssikkerhet til Underleverandører og samarbeidspartnere?	Ledelsen synes ikke å være spesielt opptatt av informasjons-sikkerhet, underleverandører og samarbeidspartnere får lite informasjon om informasjonssikkerhet.		Ledelsen bryr seg når det har vært en hendelse. Ledelsen informerer, men det er mye enveiskommunikasjon.		Ledelsen er løpende opptatt av informasjonssikkerhet og gir ut relevant informasjon til underleverandører og samarbeidspartnere, samtidig som det er god dialog.
T.26	B	I hvilken grad arbeider alle bevisst for å unngå uønskede sikkerhetsrelaterte hendelser?	Vi ligger i etterkant. Det repareres når hendelser har inntruffet.		Vi prøver å ta vare på sikkerheten, men kommer av og til på etterskudd, for eksempel ved innføring av ny teknologi.		Vi forsøker alltid å ligge i forkant, og jobber systematisk for å forhindre uønskede hendelser. Målet er at det aldri skal forekomme feil i forbindelse med informasjonssikkerhet.
T.27	L	I hvilken grad er informasjonssystemene godt sikret mot feil?	Robusthet og redundans for systemene vurderes sjelden. Enkeltfeil i ett system kan føre til følgefeil i andre systemer.		Det hender informasjonssystemene går ned, men bare i korte perioder. Vanlig drift kan gjenopptas etter kort tid.		Informasjonssystemene er satt opp etter beste praksis og er testet for robusthet. Kritiske komponenter er satt opp med redundans, slik at nedetiden på systemene er neglisjerbar og har ingen innvirkning på drift.
T.28	L	Hvordan håndteres informasjonssikkerhet ved outsourcing?	Informasjonssikkerhet er ikke et tema ved outsourcing. Det legges kun vekt på at jobben gjøres til lavest mulig pris. Ved feil eller hendelser skyves skyld over på tjeneste- eller underleverandør.		Potensielle tjeneste- eller under-leverandører vurderes i forhold til hvordan de ivaretar informasjons-sikkerhet. Leverandøren skal følge virksomhetens prosedyrer, regler og relevant lovverk og dette er kontraktsfestet.		Informasjonssikkerhet er et fokusområde ved outsourcing og er kontraktsfestet. Virksomheten samarbeider med leverandørene for å sikre god informasjonssikkerhet på den outsourcede oppgaven. Leverandøren får bare tilgang til den informasjonen som er nødvendig og har god forståelse for dette.
T.29	L	I hvilken grad mener du det gis gode tilbud for å heve kompetansen på informasjonssikkerhet?	Kurs og opplæring ses på som nødvendig, men det stjeler tid fra det vi egentlig jobber med.		Systematisk opplæring blir gitt. Det lages systematiske kursplaner. Opplæringen dekker tiltak og beredskap mot uønskede hendelser.		Utvikling av kompetanse blir sett på som en kontinuerlig prosess. Opplæring tilpasses risikobildet og virksomhetens behov.

T.30	L	I hvilken grad utveksles erfaringer med informasjonssikkerhet med myndighetene?	Vi rapporterer i forhold til minstekravet i lovgivning dersom det følges opp av myndighetene.		Vi rapporterer i forhold til lovgivning og har en dialog med myndighetene.		Det er etablert fagnettverk og læringsarena mellom myndigheter og virksomhet. Virksomheten og myndighetene deltar aktivt.
		Revisjon					
T.31	B/L	Hvordan forholder du deg til Sikkerhetsloven?	Jeg kjenner ikke til lovverket.		Jeg kjenner til de deler av lovverket som er relevant for mitt arbeid.		Jeg har god kjennskap til lovverket og hvilke felter det omfatter.
T.32	B/L	Hvordan forholder du deg til Personopplysningsloven?	Jeg kjenner ikke til lovverket.		Jeg kjenner til de deler av lovverket som er relevant for mitt arbeid.		Jeg har god kjennskap til lovverket og hvilke felter det omfatter.
T.33	L	I hvilken grad fokuseres det på informasjonssikkerhet ved anskaffelse og avhending av utstyr som benyttes til behandling eller lagring av sensitiv informasjon?	I liten grad, andre forhold legges til grunn ved avgjørelse av hvilke systemer som skal anskaffes. Systemer som skiftes ut destrueres ikke.		Informasjonssikkerhet er ett av flere kriterier som legges til grunn ved valg av nytt system. Det er faste rutiner for avhending av gammelt utstyr.		Informasjonssikkerhet er det viktigste kriteriet som legges til grunn ved valg av nytt system. Det er faste rutiner for avhending av gammelt utstyr slik at man sikrer at informasjon ikke kommer på avveie.
T.34	B/L	I hvor stor grad har du tillit til sikkerheten i virksomhetens IT-systemer?	Jeg har ingen tillit til sikkerheten i IT-systemene.		Jeg regner med at det meste håndteres forsvarlig av systemene.		Jeg har full tillit til at systemene siler ut de viktigste truslene, men passer også på å være oppdatert på de viktigste områdene selv.

NR:	Spørsmål:	1	2	3	4	5
	Kunnskap og holdning					
1	Klare målsettinger og etablert sikkerhetspolicy					
2	Krav til informasjonssikkerhet påvirker daglig arbeid					
3	Bryte reglene for å øke effektiviteten					
4	Påpeke feil ovenfor kolleger					
5	Ansvar for informasjonssikkerhet i virksomheten					
6	Tilstrekkelig opplæring i bruk av IT-systemene					
7	Skyldspørsmål ved hendelser					
8	Gradering av informasjon					
9	Behandling av sensitiv informasjon					
	Atferd					
10	Brukernavn og Passordvaner					
11	E-postvaner					
12	Sikkerhet ved surfing					
13	Arbeid hjemmefra på egen PC					
14	Lovpålagte regler					
15	Kontorplassen din					
	Policy og ledelse					
16	Kommunisere sikkerhet					
17	Ledere går foran som gode eksempler					
18	Ansatte inkluderes i arbeid med informasjonssikkerhet					
19	Utveksling av erfaring med andre virksomheter					
20	Inkludering av samarbeidspartnere i arbeid med i.s.					
21	Prioritering av informasjonssikkerhet					
22	Håndtering av informasjonssikkerhet i prosjekter					
23	Verdsetting av rapportering i virksomheten					
24	Prioritering av sikkerhet ved fjernarbeid					
25	Fysiske sikkerhetstiltak					
26	Rutiner for valg av IT-systemer som skal beskyttes					
27	Rutinre for å sikre kontinuerlig drift					
	Revisjon					
28	Revisjon av informasjonssikkerhet					
29	Analyse av inntrufne hendelser					
30	Gjennomføring av risiko og sårbarhetsanalyser					
31	Hva synes du om undersøkelsen (telles ikke med)					
	(Summer antall enere, toere, osv..) SUM					
		*	*	*	*	*
		1	**2**	**3**	**4**	**5**
		=	**=**	**=**	**=**	**=**
	Score pr svar nummer					

SUM

/ 30

Gjennomsnittscore =

ROSS-programmet ved NTNU støttes av Vesta Forsikring AS. I samarbeid med Vesta Forsikring AS arrangerer NTNU hvert år (siden 1985) konferansen "Sikkerhetsdagene".

R O S S

Informasjon om aktivitetene ved NTNU innenfor risiko- og sårbarhetsstudier (ROSS) finnes på Web-adressen:
http://www.ntnu.no/ross

ISBN: 82-7706-222-2