CompLex

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Tommy Tranvik

Styring av informasjonssikkerheten i universiteter og høyskoler

Foreløpige resultater

4/2014

CompLex 4/2014

Tommy Tranvik

Styring av informasjonssikkerheten i universiteter og høyskoler

Foreløpige resultater

Senter for rettsinformatikk
Avdeling for forvaltningsinformatikk
Postboks 6706 St Olavs plass
0130 Oslo

Henvendelser om denne bok kan gjøres til:
Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
www. jus.uio.no/iri/

ISBN 978-82-72261-58-9
ISSN 0806-1912

Grafisk produksjon: 07 Media AS – 07.no

Innhold

Sammendrag 5
Skriftliggjorte styringssystemer 5
Innføring og drift. 6
Utfordringer og barrierer 7
Mulige løsninger 9
Internasjonal forskning 10
Problemstillinger og datagrunnlag 11
Innledning 11
Problemstillinger 12
Datagrunnlaget 13
Del I: Informasjonssikkerhet, informasjonsforvaltning og risikostyring . . 17
Konfidensialitet, integritet og tilgjengelighet 17
Informasjonssikkerhet og informasjonsforvaltning 17
Elektronisk sårbarhet 20
Risikostyring 20
Betydning og krav i UH-sektoren. 24
Del II: Skriftliggjøring og dokumentasjon 28
Dokumenter og dokumentomfang. 28
Dokumentstruktur og hovedinnhold 31
Sikkerhetsmål 34
Akseptabel risiko 35
Praktisk betydning. 36
Hovedfokus. 37
Sikkerhetsorganisering. 39
Prinsipper for informasjonssikkerhet 41
IT-sikkerhet og informasjonssikkerhet 42
Nyvinninger og ansvarsplassering 44
Del III: Innføring og drift 47
Fra ord til praksis. 47
Sikkerhetsorganiseringen – dokumenter og realiteter 48

Risikovurderinger – begivenhet eller rutine? 49
Risikovurderinger og sikringstiltak 53
Forebygging og gjenoppretting 54
Datatilsynets kontrollrapporter 55
Del IV: Utfordringer 56
Ressurser 56
Dedikerte stillinger 57
Kompetanseheving og opplæring 59
Tid 60
Tekniske tiltak 61
Virkemidler 62
Egenskaper ved styringssystemene 65
Kommunikasjon og spredning 66
Kommunikasjon av ansvar og oppgaver 68
Egenskaper ved institusjonene 69
Ledelsesforankring 70
Institusjonslandskapet 71
Institusjonskulturen 76
Del V: Mulige løsninger 83
Sikkerhetshendelser 84
Tilpasning av styringssystemene 88
Eksterne aktørers betydning 90
Del VI: Resultatene og forskningen 93
Ledelsesforankring 94
Interne pådrivere 95
Eksternt press eller påvirkning 96
Lokaltilpasning 96
Integrering i daglige aktiviteter 97
Oppsummering 98

Sammendrag

Prosjektet «Informasjonssikkerhet i universitets- og høyskolesektoren» finansieres av UNINETT og gjennomføres i samarbeid mellom Sekretariatet for informasjonssikkerhet i UH-sektoren og Senter for rettsinformatikk (SERI), Universitetet i Oslo.

I denne første rapporten fra prosjektet drøftes fire hovedspørsmål:

1. I hvilken grad hadde universiteter og høyskoler etablert skriftliggjorte styringssystemer for informasjonssikkerhet?
2. I hvilken grad hadde universiteter og høyskoler med skriftliggjorte styringssystemer innført systemene og satt dem i drift?
3. Hvilke utfordringer – hindringer eller barrierer – påvirket innføring og drift av styringssystemene?
4. Hvordan forsøkte institusjonene å håndtere utfordringer de stod overfor ved innføring og drift av styringssystemene?

Rapporten gir foreløpige svar på disse spørsmålene. Rapporten bygger på informasjon – skriftlig dokumentasjon og intervjuer med nøkkelpersonell – innhentet fra 20 av drøyt 30 statlige universiteter og høyskoler som er tilknyttet forskningsnettet i Norge og som betjenes av Sekretariatet for informasjonssikkerhet i UH-sektoren.

Skriftliggjorte styringssystemer

13 av de 20 institusjonene som er kartlagt så langt kan sies å ha etablert eller var i ferd med å etablere skriftliggjorte styringssystemer for informasjonssikkerhet. Med dette menes at disse institusjonene hadde, eller jobbet med å utarbeide, de viktigste styrende, gjennomførende og kontrollerende dokumenter som inngår i et styringssystem for informasjonssikkerhet. Likevel var det mangler ved mange av de skriftliggjorte styringssystemene som gjør at det kan stilles spørsmål med hvor helhetlige og gjennomarbeidede de var. Omfanget av dokumentasjonen varierte en del, men den var likevel relativt lik i struktur og hovedinnhold. De siste sju institusjonene hadde ikke skriftliggjorte styringssystemer selv om noen av dem hadde etablert rutiner/prosedyrer på enkelte områder.

Det virket å være tre hoveddrivkrefter i arbeidet med etablering av skriftliggjorte styringssystemer. For det første Kunnskapsdepartementets nye krav til arbeidet med informasjonssikkerhet. For det andre påvirkning eller assistanse fra UNINETT. For det tredje ønsket om å etterleve rettslige krav, spesielt bestemmelsene om informasjonssikkerhet i personopplysningsloven med forskrift.

Flertallet av institusjoner med skriftliggjorte styringssystemet fokuserte på IT- eller datasikkerhet snarere enn informasjonssikkerhet som sådan. De fokuserte også sterkere på sikring av administrative behandlinger av informasjonsverdier (spesielt personopplysninger) enn på sikring av andre typer behandlinger, for eksempel i forskning, undervisning eller formidling. Arbeidet med sikring av helseopplysninger i medisinske eller helsefaglige forskningsprosjekter representerte i noen grad et unntak fra denne «regelen».

Innføring og drift

I institusjoner hvor styringssystemer eksisterte på papiret var det til dels lang vei å gå før de var innført og satt i drift. Det var derfor, og med delvis unntak av fire institusjoner, store forskjeller mellom dokumentinnhold og praksis. Typiske eksempler på dette var at sikkerhetsorganisasjonen ikke fungerte eller var ukjent for mange av de som inngikk i den; sikkerhetsmål og kriterier for akseptabel risiko hadde liten eller ingen betydning for arbeidet; sentrale aktiviteter, spesielt risikovurderinger, ble ikke gjennomført uten assistanse fra UNINETT; nødvendige sikringstiltak ble i varierende grad iverksatt; ledelsesgjennomganger og sikkerhetsrevisjoner ble ikke utført. Dette forhindret likevel ikke at det var gjennomført enkelte typer sikringstiltak. Spesielt IT-tekniske sikringstiltak var iverksatt. Også andre typer sikringstiltak, for eksempel fysisk tilgangsstyring, var i noen grad etablert. Tiltakene var vanligvis ikke et resultat av risikovurderinger eller at institusjonene hadde innført styringssystemer for informasjonssikkerhet, men ble i de fleste tilfellene etablert på ad hoc-basis.

I flertallet av institusjonene fremstod derfor sikkerhetsdokumentasjonen som en «formalitet», det vil si papirer var laget fordi det var forventet av institusjonene, men som hadde liten eller ingen betydning for det daglige arbeidet. Følgelig var det vanligvis relativt liten forskjell i arbeidet med informasjonssikkerhet mellom institusjoner som hadde etablert (eller var i ferd med å etablere) skriftliggjorte styringssystemer og institusjoner som ikke hadde gjort det.

I enkelte av de fire institusjonene som i noen grad virket å ha fungerende styringssystemer, hadde systemene blitt etablert som følge av konkrete aktiviteter som involverte de ansatte. Igangsetting av og involvering i konkrete aktiviteter fremstod som mer effektivt enn å forlite seg på at instrukser eller signaler «fra toppen» skulle utløse initiativ og innsats nedover i organisasjonshierarkiet.

Utfordringer og barrierer

Det var tre viktige utfordringer eller barrierer som stod i veien for innføring og drift av styringssystemer for informasjonssikkerhet.

Den første utfordringen var knyttet til prioritering av ressurser. Selv om bruken av ressurser på styringssystemer og informasjonssikkerhet hadde økt noe de siste årene, fremstod ressursinnsatsen som utilstrekkelig. Dette handlet om tre forhold. Først begrensede personalressurser, det vil si antallet stillinger som helt eller delvis var dedikert til arbeidet med informasjonssikkerhet og styringssystemer. Dernest mangelfull kompetanse om praktisk informasjonssikkerhetsarbeid blant de som var tildelt sentrale roller i sikkerhetsorganisasjonene. Til slutt mangel på tid til å utføre viktige oppgaver og aktiviteter som ledere og ansatte (ifølge sikkerhetsdokumentasjonen) var pålagt å ivareta. Kombinasjonen av begrensede personalressurser, mangelfull kompetanse og liten tid førte til at mesteparten av innsatsen var konsentrert om IT-avdelingene/seksjonene. I andre deler av institusjonene (med et visst unntak for medisinsk eller helsefaglig forskning) var aktiviteten liten eller ikke-eksisterende.

Den andre utfordringen var knyttet til selve styringssystemene og måten de var utformet på. I flertallet av institusjonene virket styringssystemene i liten grad (men med noen unntak) å være tilpasset hver enkelt institusjons behov og forutsetninger. Isteden var systemene nokså like hverandre og hentet felles inspirasjon fra eksternt veiledningsmateriale. I enkelte institusjoner førte dette til at styringssystemene var for ambisiøse, omfattende og tunge å innføre/drifte sammenliknet med lokale behov og forutsetninger. Samtidig virket som at innholdet i systemdokumentasjonen, spesielt bruken av IT-spesifikk terminologi, gjorde det vanskelig å kommunisere innholdet til ledere og ansatte som manglet IT-teknisk kompetanse. Det var derfor et problem at store deler av de lokale sikkerhetsorganisasjonene hadde utfordringer med å forstå (og i mange tilfeller heller ikke visste om) hvilke roller de var ment å spille i arbeidet med informasjonssikkerhet.

Den tredje utfordringen var knyttet til visse kjennetegn ved institusjonene som kunne vanskeliggjøre innføring og drift av styringssystemene. Dette handlet særlig om tre forhold – ledelsesforankring, organisatoriske utfordringer og kulturelle utfordringer:

- Ledelsesforankring: Toppledelsen i institusjonene virket generelt sett (men med enkelte unntak) å ha et distansert forhold til styringssystemer for informasjonssikkerhet. Styringssystemene var ofte behandlet og vedtatt i universitets- eller høyskolestyrer, men deretter slapp toppledelsen taket i arbeidet. I enkelte institusjoner var mellomledere, for eksempel ledere av avdelinger i sentraladministrasjonen med CSO-ansvar, aktive og viktige pådrivere i arbeidet med informasjonssikkerhet. Men disse lederes pådriverrolle virket primært å være personavhengig og var derfor ikke alltid en indikasjon på at styring av informasjonssikkerheten var institusjonelt forankret på ledelsesnivå.
- Organisatoriske utfordringer: Styringssystemene virket å fungere noe bedre i mindre institusjoner enn i de største institusjonene. Selv om betydningen av dette funnet ikke bør overdrives, tydet det likevel på at innføring og drift var noe enklere i institusjoner med mindre intern oppsplitting (færre underenheter med ulik faglig orientering) og hvor den organisatoriske avstanden mellom ulike aktører ble beskrevet som kort og relativ uformell. I større institusjoner kunne det virke som intern kompleksitet (mange underenheter med svært ulik faglig orientering og relativ stor autonomi), lengre og mer formelle relasjoner forsterket utfordringene med innføring og drift av styringssystemene. Dette til tross for at de største institusjonene brukte relativt flere ressurser (spesielt med hensyn til helt eller delvis dedikerte stillinger) på arbeidet med informasjonssikkerhet enn de mindre institusjonene.
- Kulturelle utfordringer: Åpenheten og forskerfriheten som preger kulturen i akademiske institusjoner kunne i noen grad sies å være en barriere mot innføring og drift av styringssystemene. Enkelte hevdet for eksempel at åpenheten i akademia kunne føre til at hensynet til konfidensialitet ikke ble vektlagt i like stor grad som de mente var nødvendig. Det ble videre hevdet at den individuelle autonomien og selvstendigheten som forskerfriheten innebærer kunne stå i et visst motsetningsforhold til et system basert på sterkere sentralstyring av hvordan informasjonsverdier håndteres i forskning og undervisning. Disse oppfatningene var likevel kontroversielle. Flere mente for eksempel at vitenskapelige ansatte var genuint opptatt av at forskningsdata ble tilfredsstillende sikret, spesielt i prosjekter som var finansiert av eksterne aktører. Men det fremstod som usikkert

om dette også innebar en tilsvarende forståelse for og støtte til innføring og drift av styringssystemer for informasjonssikkerhet.

Barrierene mot innføring og drift av styringssystemer innebar at relativt mange institusjoner mente at de levde med en høyere risiko for brudd på informasjonssikkerheten enn hva ledelsen var oppmerksom på og hva den selv hadde vedtatt. Dette var spesielt (men ikke bare) knyttet til bruken av skytjenester, e-postkommunikasjon i forskningsprosjekter og bærbare dataenheter. Det ble også stilt spørsmål ved om håndteringen av visse typer forskningsdata, spesielt sensitive personopplysninger, var god nok. Graden av risiko som institusjonene utsatte seg for virket derfor å være mangelfullt kartlagt og erkjent.

Mulige løsninger

Tre mulige løsninger på utfordringene ble fremhevet at institusjonene selv. For det første at alvorlige sikkerhetshendelser kunne føre til økt oppmerksomhet om behovet for informasjonssikkerhet og utløse flere ressurser til arbeidet. Det var imidlertid langt mellom alvorlige brudd på informasjonssikkerheten: ingen av institusjonene rapporterte om «alvorlige sikkerhetsbrudd» i løpet av de siste 4–5 årene. Datatilsynets kontrollrapporter fra UH-sektoren indikerte likevel at antallet alvorlige sikkerhetsbrudd var noen høyere enn hva institusjonene selv rapporterte. Samtidig mente de fleste institusjonene at de neppe hadde full oversikt over det reelle omfanget av avvik og sikkerhetsbrudd.

For det andre tilpasning av styringssystemer til lokale institusjonsforhold og behov. I de fire institusjonene hvor styringssystemene ble rapportert å fungere (i noen grad) etter hensikten, virket det som styringssystemene i praksis hadde blitt lokaltilpasset selv om dette ikke alltid var synlig i sikkerhetsdokumentasjonen. I de øvrige institusjonene hadde lokaltilpasning enten skjedd i svært begrenset grad eller de manglet skriftliggjorte styringssystemer.

For det tredje økt press eller påvirkning fra eksterne aktører (spesielt Kunnskapsdepartementet og andre myndighetsorganer). Her ble det rapportert at mye av arbeidet med informasjonssikkerhet generelt og styringssystemer spesielt hadde kommet i stand på grunn av denne formen for press eller påvirkning. I noen få og store institusjoner ble det dessuten rapportert at oppslag i media, både lokale studentaviser og regionale eller nasjonale media, hadde bidratt til økt fokus på arbeidet med informasjonssikkerhet.

Internasjonal forskning

Den internasjonale forskningen på innføring og drift av tilsvarende systemer som anvendes til styring av informasjonssikkerheten indikerer at suksess avhenger av fem forhold:

1. Ledelsesforankring.
2. Interne pådrivere (ledere eller ansatte som «brenner for saken»).
3. Press eller påvirkning fra eksterne aktører.
4. Lokaltilpasning av styringssystemene.
5. Integrering av styringssystemet i daglige aktiviteter.

To av disse fem forholdene – eksternt press/påvirkning og interne pådrivere – kan helt eller delvis sies å være til stede i universitets- og høyskolesektoren. De tre siste forholdene – ledelsesforankring, lokaltilpasning og integrering i daglige aktiviteter – virket i langt mindre grad å være til stede.

Hvordan de tre siste forholdene kan realiseres fremstod som den viktigste utfordringen som arbeidet med styring av informasjonssikkerheten i universiteter og høyskoler står overfor i dag.

Problemstillinger og datagrunnlag

Innledning

Dette er første rapport i prosjektet «Informasjonssikkerhet i universitets- og høyskolesektoren». Prosjektet startet i september 2013 og avsluttes i september 2015, og er finansiert av UNINETT.[1] Det praktiske arbeidet i prosjektet gjennomføres i samarbeid mellom UNINETT (Sekretariatet for informasjonssikkerhet i UH-sektoren[2]) og Senter for rettsinformatikk (SERI), Universitetet i Oslo.

Prosjektet har fire hovedmål. For det første å kartlegge praktiske erfaringer og utfordringer med styringssystemer for informasjonssikkerhet i de universitets- og høyskoleinstitusjonene som er medlemmer av UNINETT og tilknyttet det norske forskningsnettet.[3] For det andre å kartlegge hvilke rettslige krav som stilles til – eller er relevante for – arbeidet med styringssystemer for informasjonssikkerhet i UH-sektoren. Resultatene fra begge disse kartleggingene vil, for det tredje, benyttes til å utvikle et forslag til styringssystem for informasjonssikkerhet, basert på ISO/IEC 27001/02: 2013, som er tilpasset universiteter og høyskoler. Siktemålet er at institusjonene skal kunne legge dette forslaget til grunn for sitt eget arbeid med informasjonssikkerhet. For det fjerde å kartlegge erfaringer med innføring og drift av forslaget til styringssystemet hos utvalgte universitets- og høyskoleinstitusjoner (pilotinstitusjoner). Erfaringene fra denne delen av prosjektet vil bli benyttet til ytterligere «skreddersøm» av styringssystemet.

---

1 UNINETT er et konsern som eies av Kunnskapsdepartementet og har sitt hovedkontor (og mesteparten av sin virksomhet) i Trondheim. UNINETT driver nett og nettjenester for universiteter, høyskoler og forskningsinstitusjoner, og ivaretar en rekke andre nasjonale IKT-oppgaver på vegne av UH-sektoren (se https://www.uninett.no/). Se også Bjørn Ness (2013): *Tilkoblet. En fortelling om Internett og Forskningsnettet i Norge*. Trondheim: Akademika forlag.

2 Sekretariatet for informasjonssikkerhet i UH-sektoren ble opprettet av Kunnskapsdepartementet i 2011 og er administrativt underlagt UNINETT. Sekretariatet har to ansatte og skal drive veiledning og rådgiving overfor universiteter og høyskoler i spørsmål om informasjonssikkerhet, beredskap og kontinuitet (se https://www.uninett.no/infosikkerhet/sekretariat).

3 Forskningsnettet er den viktigste IT-løsningen som UNINETT drifter på vegne av UH-sektoren. Dette er et høykapasitetsnett som forbinder de interne datanettverkene til universiteter og høyskoler i Norge med hverandre. Forskningsnettet er forbundet med tilsvarende datanettverk i andre land og med kommersielle datanettverk (se https://www.uninett.no/forskningsnettet). Se også Bjørn Ness (2013): *Tilkoblet. En fortelling om Internett og Forskningsnettet i Norge*. Trondheim: Akademika forlag.

Formålet er at det i størst mulig grad skal bli tilpasset de særegne forhold og utfordringer som gjelder i UH-sektoren.

Denne rapporten vil gi en foreløpig oppsummering av del 1 av prosjektet: praktiske erfaringer og utfordringer knyttet til arbeidet med styringssystemer for informasjonssikkerhet i statlige universitetene og høyskolene som benytter UNINETTs forskningsnettverk og som betjenes av Sekretariatet for informasjonssikkerhet i UH-sektoren. At rapporten inneholder «foreløpige oppsummeringer» innebærer at arbeidet med kartlegging av praktiske erfaringer og utfordringer i alle de drøyt 30 statlige UH-institusjoner som er medlemmer i UNINETT (og som betjenes av Sekretariatet for informasjonssikkerhet) enda ikke er sluttført – så langt er 20 universiteter og høyskoler kartlagt. Hensikten med rapporten er derfor å presentere de viktigste erfaringene og utfordringene slik de avtegner seg i disse 20 institusjonene.

Selv om noen statlige institusjoner fortsatt gjenstår, baserer rapporten seg likevel på et såpass omfattende materiale at den gir et visst grunnlag for å trekke generelle konklusjoner om arbeidet med informasjonssikkerhet i sektoren (se detaljert gjennomgang av datagrunnlaget nedenfor).

Problemstillinger

Fremstillingen i resten av rapporten har til hensikt å gi foreløpige svar på følgende hovedspørsmål:

- **Skriftliggjøring og dokumentasjon**: Hadde de institusjonene som til nå er kartlagt i prosjektet dokumenterte og skriftliggjorte styringssystemer for informasjonssikkerhet? Hvilke systemdokumenter hadde institusjonene laget og hva var hovedinnholdet i den skriftlige dokumentasjonen?
- **Innføring og drift**: I hvilken grad hadde institusjoner med skriftliggjorte styringssystemer innført og satt systemene i drift? Fungerte systemene slik de var beskrevet eller var det store forskjeller mellom innholdet i dokumentene og det praktiske arbeidet?
- **Utfordringer**: Dersom det var forskjeller mellom dokumentinnhold og institusjonspraksis, hva var hovedårsakene til dette? Hvilke utfordringer – hindringer eller barrierer – påvirket i så fall innføring og drift av styringssystemene?
- **Løsninger:** Hvordan forsøkte institusjonene å håndtere de utfordringene de stod ovenfor? Hvilke mulige løsninger pekte institusjonene selv på når det gjaldt innføring og drift av styringssystemer for informasjonssikkerhet?

Problemstillingene diskuteres i den rekkefølgen de er presentert i ovenfor: problemstilling 1 først og deretter problemstilling 2, 3 og 4.

Som allerede antydet, vil rapporten ikke gå i detalj på hvordan problemstillingene skissert ovenfor kan besvares. Det som isteden presenteres er et oversiktsbilde av tilstanden i de delene av sektoren som er kartlagt så langt. Rapporten vil derfor ikke gå inn på hvordan enkeltinstitusjoner arbeider (eller har arbeidet) med etablering og drift av styringssystemer for informasjonssikkerhet. Fokuset vil isteden ligge på hvordan sektoren i stort jobber med denne utfordringen – hva som er gjort, hva som gjenstår og hva som er problematisk.

Helt til slutt diskuteres enkelte forutsetninger som, ifølge forskningen på innføring og drift av virksomhetsinterne styringssystemer, trolig må være til stede for at styringssystemer for informasjonssikkerhet skal bli etablert og satt i drift. Denne avsluttende delen gir en kortfattet oppsummering av (a) tilstanden på informasjonssikkerhetsområdet slik den avtegnet seg i de 20 institusjonene som til nå er kartlagt og (b) hva som eventuelt mangler for at styringssystemer for informasjonssikkerhet skal bli etablert og komme i drift i statlige universiteter og høyskoler.

Før oppmerksomheten vendes mot problemstillingene ovenfor, gis en kort gjennomgang av (a) datagrunnlaget for rapporten, (b) hva styringssystemer for informasjonssikkerhet dreier seg om og (c) hvilke krav som stilles til innføring og drift av styringssystemer i UH-sektoren.

Datagrunnlaget

De 20 statlige universitetene og høyskolene som er kartlagt så langt, er ikke representative for UH-sektoren som sådan. Faglig spesialiserte høyskoler er for eksempel i begrenset grad representert i utvalget mens breddeuniversitetene er representert i noe større grad. Når det gjelder institusjonsstørrelse, kan fem av de 20 institusjonene defineres som store, det vil si at de har flere enn 10 000 studenter og ansatte. De øvrige 15 institusjonene kan defineres som små eller mel-

lomstore, det vil si at de har mindre enn 10 000 studenter og ansatte.[4] Denne fordelingen innebærer at store institusjoner er noe overrepresentert i utvalget, men ikke mer enn at resultatene trolig avdekker visse generelle mønstre når det gjelder arbeidet med etablering og drift av styringssystemer for informasjonssikkerhet i den statlige delen av UH-sektoren. Samtidig fordeler institusjonene seg på andre sentrale kjennetegn som institusjonstype (universiteter vs. høyskoler) og geografisk plassering på en måte som gjør det rimelig å anta at resultatene har en viss gyldighet for sektoren som sådan.

Kartleggingen som ligger til grunn for denne rapporten, baserer seg på følgende metodebruk og datagrunnlag:

Bakgrunnsdokumentasjon: Dette omfatter gjennomgang av sentrale dokumenter som gir allmenne beskriver av eller retningslinjer for hvilke elementer (prosesser og arbeidsoppgaver) som inngår i et styringssystem for informasjonssikkerhet og hvordan styringssystemet skal bygges opp. Gjennomgangen inkluderte blant annet ISO-standarder (ISO/IEC 27001/02: 2013) og beste praksis dokumenter (for eksempel IFS: 2011 Standard of Good Practice for Information Security[5] eller UNINETT UFS 126[6]). Det inkluderte også anbefalinger eller veiledninger fra ulike norske myndighetsorganer, for eksempel Helsedirektoratet («Normen for informasjonssikkerhet i helsesektoren»)[7], Direktoratet for forvaltning og IKT (betaversjonen av forslag til styringssystem for informasjonssikkerhet i offentlig sektor),[8] informasjonsmateriell fra Norsk Senter for Informasjonssikring[9] og Nasjonal Sikkerhetsmyndighet[10] og Datatilsynets veiledninger om internkontroll og informasjonssikkerhet.[11] Til slutt omfattet dokumentgjennomgangen alle Datatilsynets kontrollrapporter fra UH-sektoren i perioden

4 Størrelsesmangfoldet i sektoren (den minste institusjonen har litt over 200 studenter og ansatte, mens den største har omkring 33 000) kunne gitt grunnlag for inndeling av institusjonene i flere enn to kategorier (store og små/mellomstore) (for statistikk over studenter og ansatte ved UH-institusjoner, se Norsk Samfunnsvitenskapelig Datatjeneste, http://dbh.nsd.uib.no/nokkeltall/forholdstall.action, eller Statistisk Sentralbyrå, http://www.ssb.no/utdanning). Når dette likevel ikke er gjort, skyldes det at en mer detaljert kategorisering neppe ville gitt større innsikt i eller kastet sterkere lys over variasjoner i arbeidet med styringssystemer for informasjonssikkerhet. To størrelseskategorier er derfor vurdert som tilstrekkelig for å fange opp de viktigste mønstrene i arbeidet med informasjonssikkerhet i den statlige delen av UH-sektoren.

5 Se https://www.securityforum.org/tools/sogp/.

6 Se https://www.uninett.no/webfm_send/669.

7 Tilgjengelig på http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/Sider/default.aspx.

8 «Betaversjonen» er tilgjengelig på http://internkontroll.infosikkerhet.difi.no/.

9 https://norsis.no/.

10 Se spesielt https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/.

11 Tilgjengelig på http://datatilsynet.no/Sikkerhet-internkontroll/.

2001-2013,[12] og internasjonal forskningslitteratur om innføring og drift av virksomhetsinterne styringssystemer.

Skriftlig dokumentasjon fra universiteter og høyskoler: Dette omfattet interne dokumenter (og annet skriftlig materiale) fra de 20 statlige universitetene og høyskolene som er kartlagt så langt. Den skriftlige dokumentasjonen inkluderte policyer og prinsipper for arbeidet med informasjonssikkerhet, beskrivelser av rutiner for sikker håndtering av informasjon, interne system- og informasjonskartlegginger,[13] dokumenter utarbeidet i forbindelse med utførelsen av konkrete arbeidsoppgaver og interne rapporter eller prosjektnotater i forbindelse med innføring og drift av styringssystemer for informasjonssikkerhet. Dokumentasjonen inkluderte også opplysningsmateriell om informasjonssikkerhet til studenter og ansatte som institusjonene hadde utarbeidet og distribuert. Enkelte deler av den skriftlige dokumentasjonen var offentlig tilgjengelig, blant annet på institusjonenes hjemmesider, mens andre deler av dokumentasjonen var konfidensiell.

Intervjuer med nøkkelpersonell i universiteter og høyskoler: Dette omfattet intervjuer med ansatte i de statlige 20 institusjonene som jobbet med informasjonssikkerhet. De som ble intervjuet på institusjonsnivå kan inndeles i tre grupper: (1) daglig ansvarlig for informasjonssikkerheten (CSO/CISO eller informasjonssikkerhetsrådgivere[14]), (2) IT-ledere og (3) ikke-teknisk personell med viktige informasjonssikkerhetsoppgaver (for eksempel jurister som arbeidet med internkontroll på informasjonssikkerhetsområdet). I enkelte av de største institusjonene ble det gjennomført 3-5 intervjuer, mens i de mindre institusjonene ble det gjennomført 1 eller 2 intervjuer. I intervjuene ble det stilt spørsmål om følgende forhold: Dagens tilstand med hensyn til etablering eller drift av styringssystemer for informasjonssikkerhet (hva var gjort, hva gjenstod), hvilke tiltak/initiativ som tidligere var initiert på dette området (og resul-

12 Kontrollrapportene dekker derfor hele perioden personopplysningsloven med forskrift har vært gjeldende (loven og forskriften trådte i kraft 1. januar 2001).

13 System- og informasjonskartlegginger omfatter skjematiske oversikter over hvilke informasjonssystemer som institusjonene benyttet og hvilke typer informasjon som systemene forvaltet.

14 Chief Security Officer har et generelt ansvar for sikkerheten og beredskapen i institusjonene, mens Chief Information Security Officer har et særlig ansvar for informasjonssikkerheten. Oppgavene til CSO og CISO kunne derfor (i noen grad) være overlappende. Flertallet av institusjonene benyttet imidlertid ikke CSO eller CISO som benevnelser på den daglig ansvarlige for informasjonssikkerheten. Isteden hadde rollen fått benevnelsen informasjonssikkerhetsrådgiver, eventuelt også informasjonssikkerhetsleder. Uansett hvilken benevnelse som ble anvendt, var hovedoppgavene til CSO, CISO eller informasjonssikkerhetsrådgiver å bistå toppledelsen i informasjonssikkerhetsspørsmål og å koordinere og lede det operative arbeidet med informasjonssikkerhet i institusjonene.

tatene av eller erfaringene med disse), hindringer eller utfordringer som etablering og drift av styringssystemer for informasjonssikkerhet stod overfor, nye utfordringer for arbeidet med informasjonssikkerhet som institusjonene oppfattet som viktige og vanskelige, og institusjonenes egenopplevde behov for ekstern assistanse, spesielt fra UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren.

Ut over dette er det gjennomført enkelte intervjuer med representanter for Kunnskapsdepartementet og ansatte i myndighetsorganer som arbeider med informasjonssikkerhet på andre områder enn i UH-sektoren. Dette gjaldt blant annet ansatte i Helsedirektoratet som jobber med «Normen for informasjonssikkerhet i helsesektoren»). Hensikten med disse intervjuene var å få innsikt i erfaringer med informasjonssikkerhetsarbeid fra andre sektorområder og å kontrastere disse med tilsvarende erfaringer fra statlige universiteter og høyskoler. Resultater fra disse intervjuene vil imidlertid ikke bli viet spesiell oppmerksomhet i denne rapporten.

Del I: Informasjonssikkerhet, informasjonsforvaltning og risikostyring

Før vi ser nærmere på hvordan universiteter og høyskoler har jobbet med styringssystemer for informasjonssikkerhet, er det hensiktsmessig å gi en kort oversikt over hva dette handler om. Denne delen av rapporten vil derfor (kort) drøfte tre grunnleggende spørsmål: (1) Hva handler informasjonssikkerhet om? (2) Hvordan er et internt styringssystem for informasjonssikkerhet ment å fungere? (3) Hvilke krav stilles til etablering og drift av slike styringssystemer i universiteter og høyskoler?

Konfidensialitet, integritet og tilgjengelighet

Informasjonssikkerhet defineres som virksomheters eller organisasjoners behov for å beskytte informasjon mot tre typer uønskede hendelser. Dette er hendelser som kan føre til brudd på:

a) informasjonens konfidensialitet: hindre at uvedkommende får tilgang til informasjon de ikke skal ha tilgang til,
b) informasjonens integritet: hindre at uvedkommende endrer, sletter eller på andre måte manipulerer informasjonen og
c) informasjonens tilgjengelighet: sørge for at informasjonen er tilgjengelig for de som har behov for den når behovet oppstår.

Uønskede hendelser som fører til brudd på konfidensialiteten kan for eksempel være at taushetsbelagt informasjon offentliggjøres på internettet, mens brudd på integriteten kan oppstå ved at de samme opplysningene endres på utilsiktede måter. Uønskede hendelser som fører til brudd på tilgjengeligheten kan være at de ansatte ikke får tak i informasjon de har behov for fordi datasystemets kjøleanlegg er ute av drift.

Informasjonssikkerhet og informasjonsforvaltning

Informasjonssikkerhet – beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet – kan sies å handle om informasjonsforvaltning. Med dette menes at informasjonssikkerhet påvirker hvordan organisasjoner håndte-

rer informasjon som de er avhengige av for å gjøre jobben sin.[15] Informasjonssikkerhet dreier seg derfor ikke bare om å beskytte informasjonsverdier mot uønskede hendelser. Det dreier seg også om at informasjonssikkerhet har betydning for hvordan organisasjoner kommuniserer, fordeler, bevarer, gjenfinner, sammenstiller og publiserer informasjon.

Koblingen mellom informasjonssikkerhet og informasjonsforvaltning kommer til uttrykk i rettslige reguleringer som gjelder for universiteter og høyskoler. Bestemmelsene i forvaltningsloven om saksbehandlingen i offentlige forvaltningsorganer inneholder for eksempel egne regler om informasjonssikkerhet. Det samme er tilfelle for reglene i arkivloven om oppbevaring av dokumentasjon i forvaltningen. Informasjonssikkerhet er derfor en virksomhetsomspennende oppgave – den griper inn i alle deler av offentlige (og private) organisasjoner hvor informasjon håndteres og forvaltes.

At informasjonssikkerhet er en virksomhetsomspennende oppgave innebærer at nedslagsfeltet til arbeidet med informasjonssikkerhet er svært bredt og begrenser seg ikke til hva som skjer innenfor organisasjonenes «fire vegger». Arbeidet med informasjonssikkerhet kan for eksempel strekke seg fra IT-løsninger som hver enkelt medarbeider holder i hånden (bærbare dataenheter) og helt til internasjonale selskaper som leverer programvare/applikasjoner til de samme IT-løsningene. I en slik situasjon handler informasjonssikkerhet om hva som skjer med informasjonen i hele kjeden – fra den enkelte medarbeider til internasjonale selskaper – og under hele informasjonens «livssyklus» (fra den registreres til den slettes). Spørsmålet er hvordan man kan hindre at informasjon som

15 Dette perspektivet på informasjonssikkerhet kommer blant annet til uttrykk i Direktoratet for forvaltning og IKT (2013): *Informasjonsforvaltning i offentlig sektor.* Rapport nr. 10, tilgjengelig på http://www.difi.no/filearchive/rapport-informasjonsforvaltning-i-offentleg-sektor-2013-10-10.pdf. Perspektivet har særlig basis i deler av «den klassiske» organisasjonsforskningen. Her rettes fokuset mot hvordan begrenset kapasitet til å håndtere informasjon blir forsøkt løst gjennom måten organisasjonene bygges opp på, for eksempel ved utstrakt arbeidsdeling/spesialisering eller prosedyrer og retningslinjer for håndtering av ulike typer saker/situasjoner. Se for eksempel W. Richard Scott og Gerald F. Davis (2014): *Organizations and Organizing. Rational, Natural and Open System Perspectives*. Upper Saddle River: Pearson Education; Herbert A. Simon (1993): *Models of Bounded Rationality*. Cambridge, Mass.: The MIT Press; Mairead Browne (1993): *Organizational Decision-making and Information*. Norwood, NJ: Ablex Publishing; Herbert A. Simon (1976): *Administrative Behavior. A Study of Decision-Making Processes in Administrative Organizations*. New York: The Free Press. Liknende perspektiver har også preget e-forvaltningsforskningen. Se for eksempel Ig Snellen, Marcel Thaens og Wim van de Donk (2012): *Public Administration in the Information Age: Revisited*. Amsterdam: IOS Press; Christopher G. Reddick (2012): *Public Administration and Information Technology*. Burlington: Jones & Bartlett Learning; Christopher Hood og Helen Z. Margetts (2007): *The Tools of Government in the Digital Age*. Basingstoke: Palgrave Macmillan.

håndteres på forskjellige måter og av aktører innenfor og utenfor organisasjonsgrensene kommer uvedkommende i hende, blir skadet/ødelagt eller simpelthen forsvinner?

Etter som informasjonssikkerhet er en virksomhetsspennende oppgave som også strekker seg ut i organisasjonsomgivelsene, forutsetter både litteraturen og de rettslige reguleringene som gjelder på området at organisasjonene etablerer styringssystemer for informasjonssikkerhet. Dermed handler informasjonssikkerhet også om virksomhetsstyring. Styringen av informasjonssikkerhet skal i prinsippet skje på tilsvarende måte som når det for eksempel gjelder helse, miljø og sikkerhet. Det er derfor ikke uvanlig at arbeidet med informasjonssikkerhet beskrives som en form for internkontroll.

Virksomhetsstyring for informasjonsforvaltning og informasjonssikkerhet krever at organisasjoner besvarer en rekke spørsmål om hvordan de håndterer informasjonsverdier. Spørsmålene dreier seg blant annet om oppgaver som informasjonsoversikt, verdiprioriteringer og informasjonsbehov:

- Informasjonsoversikt: «hvilke typer informasjon har vi behov for og hvordan får vi tak i den informasjonen vi trenger?»
- Verdiprioritering: «hvilke typer informasjon er spesielt viktig for oss og hvilke typer informasjon er ikke like viktig?»
- Informasjonsbehov:
  - «Hvem skal ha tilgang til hvilke typer informasjon og hvor lenge skal tilgangene vare?»
  - «Hvordan sørge for at rett informasjon er tilgjengelig for de rette medarbeiderne til rett tid?»
  - «Hvordan unngå at informasjonen endres eller slettes av personer som ikke har rett til å gjøre dette?»

Alle disse spørsmålene – informasjonsoversikt, verdiprioritering og informasjonsbehov – handler om informasjonssikkerhet, for eksempel å ta stilling til hvilken informasjon det er spesielt viktig å beskytte og å sørge for at informasjonen ikke endres eller slettes av uvedkommende (beskytte informasjonens integritet). Men spørsmålene handler også om informasjonsforvaltning. Tiltak for beskyttelse av konfidensialiteten og tilgjengeligheten er for eksempel direkte koblet til fordelingen av ansvar, myndighet og oppgaver mellom forskjellige ledere og medarbeidere: hvem trenger å vite hva og hvordan sørge for at alle får tilgang til den informasjonen de til enhver tid har behov for i arbeidet sitt?

På denne måten handler informasjonssikkerhet om noe mer enn beskyttelse av konfidensialitet, integritet og tilgjengelighet. Det handler om hvordan organisasjonene er oppbygd og fungerer, og hvordan de samhandler med aktører i sine omgivelser (samarbeidsparter, leverandører, databehandlere, osv.).

Elektronisk sårbarhet

Koblingen mellom informasjonssikkerhet og informasjonsforvaltning kan hevdes å være spesielt sterk når informasjonen foreligger i elektronisk form og behandles ved bruk av elektroniske hjelpemidler (datamaskiner, programvare og datanettverk).[16] Dette skyldes at informasjon i elektronisk form har visse egenskaper som informasjon i papirform ikke har i samme grad, blant annet at stadig større mengder informasjonen kan distribueres, endres, manipuleres og gjenfinnes på enkle og lite kostnadskrevende måter. Elektronisk informasjon er derfor mer sårbar enn papirbasert informasjon og dermed øker utfordringene knyttet til sikring av viktig eller virksomhetskritisk informasjon.[17]

Konsekvensene av overgangen fra papirbasert til elektronisk (eller digital) informasjonsforvaltning kan sies å være todelt. For det første, og som allerede nevnt, at informasjonssikkerhet blir et sentralt element i den generelle virksomhetsstyringen og informasjonsforvaltningen i offentlig (og privat) sektor. For det andre at manglende informasjonssikkerhet kan føre til at organisasjoner i offentlig (og privat) sektor får problemer med å ivareta sine lovpålagte oppgaver eller realisere sine selvvalgte målsettinger. Informasjonssikkerhet er derfor ment å bidra til at sårbar elektronisk informasjon beskyttes mot trusler – eksterne og interne – som kan forstyrre organisasjonenes evne til å fungere på en hensiktsmessig og relativt effektiv måte.

Risikostyring

I tillegg til virksomhetsstyring og informasjonsforvaltning, handler informasjonssikkerhet om risikostyring. Med risikostyring menes at organisasjoner etablerer virksomhetsinterne styringssystemer for identifisering, vurdering og

16 Se for eksempel Malcolm Harkins (2013): *Managing Risk and Information Security: Protect to Enable*. New York: Apress Media; Torgeir Daler et al. (2010): *Håndbok i datasikkerhet. Informasjonsteknologi og risikostyring.* Trondheim: Tapir Akademisk Forlag; Jan T. Bjørnsen (2012): *Slik får de IT-styring og kontroll. Håndbok for ledere, styremedlemmer og IT-ansvarlige.* Oslo: Universitetsforlaget.

17 Se for eksempel Rolf S. Normann og Tommy Tranvik (2012): *Personvern og informasjonssikkerhet i kommunen*. Oslo: Kommuneforlaget.

håndtering av trusler mot informasjonens konfidensialitet, integritet og tilgjengelighet (uønskede hendelser).[18]

Risikoen for at uønskede hendelser skal skje defineres som hendelsenes sannsynlighet multiplisert med den potensielle skadevirkningen (konsekvens). Vurderinger av sannsynlighet skjer vanligvis ved å anslå hvor mange ganger de aktuelle hendelsene kan tenkes å inntreffe i løpet av en bestemt tidsperiode (for eksempel ett år). Vurderinger av hendelsenes skadevirkning baserer seg vanligvis på antagelser om de mulige negative effektene hendelsene kan innebære for organisasjonen, dens samarbeidspartnere eller kundene/brukerne. Negative effekter kan blant annet omfatte økonomisk skade, fare for liv og helse, omdømmetap eller krenkelser av personvernet.

Logikken som ligger til grunn for risikostyrt informasjonssikkerhet kan sies å være todelt. For det første å forutse uønskede hendelser (brudd på konfidensialiteten, integriteten og tilgjengeligheten). For det andre å iverksette tiltak mot uønskede hendelser før de oppstår.[19] Dette skal gjøres ved bruk av risikovurderinger, hvor uønskede hendelser først identifiseres og deretter vurderes i relasjon til sannsynlige og skadevirkning (konsekvens). Deretter er tanken at det skal det iverksettes tiltak mot de uønskede hendelser som vurderes å ha størst risiko.

Dette innebærer at risikostyrt informasjonssikkerhet skal føre til at institusjoner og organisasjoner er forberedt på og er i forkant av eventuelle problemer: uønskede hendelser skal forutsees og forebyggende tiltak skal etableres slik at hendelsene enten avverges eller at effekten av dem reduseres dersom de likevel skulle inntreffe. Forebyggende (eller risikoreduserende) tiltak skal dermed minske behovet for gjenopprettende tiltak – skaden skal (så langt det lar seg gjøre) forhindres istedenfor å utbedres etter at den er oppstått.[20] Fokuset på forebygging fremfor gjenoppretting har paralleller til arbeidet med helse, miljø og sikkerhet. Også her er målet å unngå eller avverge skade, ikke primært å behandle skaden etter at den er oppstått (selv om dette selvsagt vil være en viktig oppgave når «ulykken er ute»). I en informasjonssikkerhetssammenheng kan eksempler på forebyggende (eller risikoreduserende) tiltak kan være at informasjon som

18 Selv om risikostyring kan sies å være en viktig del av digital informasjonsforvaltning i offentlig sektor, blir risikostyring sjelden drøftet i e-forvaltningslitteraturen. Dette til tross for at styringsutfordringer som oppstår i forbindelse med digital informasjonsforvaltning (og bruk av informasjons- og kommunikasjonsteknologi), er en gjennomgående tematikk i litteraturen.

19 Se for eksempel Richard O'Hanley og James S. Tiller (2014): *Information Security Management Handbook*. Boca Raton: CRC Press.

20 Se for eksempel Christopher Hood og David Jones (red.) (2001): *Accident and Design. Contemporary Debates in Risk Management*. London: Routledge.

sendes over usikre kommunikasjonskanaler (internettet) krypteres for å unngå at den snappes opp og leses av uvedkommende, eller at viktig informasjon lagres i ulike datasystemer slik at den likevel er tilgjengelig selv om ett av systemene er ute av drift.

I tillegg innebærer risikostyrt informasjonssikkerhet et tydelig fokus på prioritering av tiltak og økonomisering av ressursbruken.[21] Også dette skal gjøres ved bruk av risikovurderinger. Her er tanken at risikovurderinger skal resultere i en prioritert liste over uønskede hendelser: hendelser med størst risiko kommer øverst på listen, mens hendelser med minst risiko havner nederst. Rangering av uønskede hendelser med hensyn til risiko skal føre til at bruken av knappe ressurser blir mest mulig målrettet og effektiv, det vil si at forebyggende tiltak iverksettes for å unngå (eller redusere skadevirkningene av) de uønskede hendelsene som kommer høyest på prioriteringslisten (har en uakseptabel høy risiko). Det betyr for eksempel at dersom sannsynligheten for og skadevirkningene av at datasystemer er ute av drift vurderes som langt større enn at informasjon formidlet over internettet snappes opp av uvedkommende, skal ressursene primært brukes på å forbedre/sikre driften av datasystemene. Knappe ressurser skal altså brukes der hvor de kan gjøre størst forskjell – på å forebygge de mest alvorlige utfordringene – og ikke «smøres tynt ut over» en lang rekke mer eller mindre uviktige problemer.[22]

Organiseringen av arbeidet med å forutse, forebygge og prioritere uønskede hendelser og tiltak er ment å ha en tydelig hierarkisk oppbygning, det vil si at arbeidet skal styres fra toppen av organisasjonspyramiden. I all litteratur om informasjonssikkerhet beskrives derfor informasjonssikkerhet som et topplederansvar.[23] Meningen er at toppledelsen skal sette informasjonssikkerhet på agen-

21 Se for eksempel Rainer Böhme (red.) (2013): *The Economics of Information Security and Privacy*. Berlin: Springer.

22 Den samme prioriterings- og økonomiseringslogikken ligger for eksempel til grunn for økonomiregelverket i staten. Et grunnleggende styringsprinsipp er, ifølge dette regelverket, at risikovurderinger skal bidra til at statlige midler brukes på en mest mulig målrettet og effektiv måte (se økonomiregelverket § 4, tilgjengelig på http://www.dfo.no/no/Forvaltning/Okonomiregelverket/). Dette viser at risikostyring er en generell styringsteknikk, tett koblet til New Public Management-reformer. For nærmere diskusjoner, se spesielt Michael Power (2007): *Organized Uncertainty. Designing a World of Risk Management*. Oxford: Oxford University Press og Christopher Hood et al. (2001): *The Government of Risk. Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

23 Standarder og beste praksis på området understreker at styring av informasjonssikkerheten er et ledelsesansvar. Ledelsens involvering i arbeidet beskrives derfor som en avgjørende forutsetning for at informasjonssikkerheten skal bli tatt på alvor på alle nivåer i organisasjonen. Se spesielt ISO/IEC 27001: 2013: *Information Technology – Security Techniques – Information Security Management Systems – Requirements* eller IFS: 2011 *Standard of Good Practice for Information Security*.

daen gjennom klare styringssignaler og prioriteringer: den skal tilkjennegi viktigheten av informasjonssikkerhet overfor resten av organisasjonen; bestemme hvor mye sikkerhet som er nødvendig i organisasjonen; avsette tilstrekkelige ressurser til sikring av informasjon; og kontrollere, følge opp og stille nye krav til arbeidet med informasjonssikkerheten. Vektleggingen av hierarkisk styring forutsettes samtidig at toppledelsen (og organisasjonen) formaliserer arbeidet med informasjonssikkerhet. Det mest avgjørende i denne sammenheng er at det opprettes en egen sikkerhetsorganisasjon.

Formalisering av informasjonssikkerhetsarbeidet gjennom opprettelsen av en sikkerhetsorganisasjon innebærer at myndighet, ansvar og oppgaver skal fordeles mellom ledere og medarbeidere. Sikkerhetsorganisasjonen skal derfor beskrive hvem som har myndighet til å fatte hvilke beslutninger og hvem som skal utføre hvilke arbeidsoppgaver (eventuelt også når eller hvor ofte ulike oppgaver skal utføres). I tillegg skal det vedtas egne mål og strategier for sikkerhetsorganisasjonens arbeid som blant annet skisserer hvilke krav toppledelsen setter til informasjonssikkerheten og hvilke hovedprioriteringer som ligger til grunn for arbeidet. Det forutsettes også at toppledelsen sørger for at sikkerhetsorganisasjonen er tilstrekkelig bemannet og at den har kompetanse i risikostyrt arbeidsmetodikk, for eksempel når det gjelder oppgaver som kartlegging og klassifisering av informasjonsverdier, gjennomføring av risikovurderinger, etablering av sikringstiltak eller intern revisjon av informasjonssikkerheten. Til slutt forutsettes det at ledelsen jevnlig (vanligvis årlig) gjennomgår arbeidet med informasjonssikkerhet (ledelsens gjennomgang). På denne måten skal innsatsen preges av ledelsesstyrt planmessighet og forutsigbarhet istedenfor av lokale eller individuelle ad hoc-initiativ eller periodiske skippertak (eller ingen innsats i det hele tatt).[24]

Planmessighet og forutsigbarhet innebærer samtidig at arbeidet med informasjonssikkerhet skal byråkratiseres. I dette ligger at hovedelementene i arbeidet – styring/organisering, gjennomføringen av konkrete aktiviteter og etterfølgende kontroll – ikke bare skal iverksettes, men at de også skal dokumenteres skriftlig. Skriftliggjøring av hovedelementene – styring/organisering, gjennomføring og kontroll – er derfor en viktig del av etablering og drift av styringssystemer for informasjonssikkerhet. Hensikten med skriftliggjøringen er dels å dokumentere at organisasjonene ivaretar de rettslige kravene som stilles til informasjonssikkerheten og dels å bidra til egen læring og kontinuerlig forbedring av informasjonssikkerheten. Tanken er altså at institusjonene skal kunne demonstrere graden av regeletterlevelse, ta vare på viktig kunnskap og erfaringer og benytte dette som grunnlag for videreutvikling av arbeidet med informasjonssikkerhet.

24 Se for eksempel Steve G. Watkins (2013): *An Introduction to Information Security and ISO 27001: 2013: A Pocket Guide*. Ely, UK: IT Governance Pub.

Betydning og krav i UH-sektoren

Ovenfor har vi sett at betydningen av informasjonssikkerhet øker etter hvert som informasjonen (og de informasjonssystemene som anvendes) blir mer sårbar, det vil si når organisasjoner helt eller delvis går over fra papirbasert og manuell informasjonsbehandling til elektronisk og automatisert informasjonsbehandling. Det er derfor ingen tilfeldighet at informasjonssikkerhet vokste frem som et eget fagområde samtidig med utbredelsen av datamaskiner og datanettverk,[25] og at fokuset rettet seg særlig mot «kunnskapsvirksomheter» i offentlig og privat sektor.[26]

«Kunnskapsvirksomheter» defineres som institusjoner eller organisasjoner som i hovedsak beskjeftiger seg med verdiskaping gjennom forvaltning eller foredling av informasjon/data.[27] Universiteter og høyskoler er kanskje de fremste eksemplene på slike «kunnskapsvirksomheter». Det skyldes at en sentral del av samfunnsmandatet til universiteter og høyskoler er (a) å innsamle og analysere informasjon/data ved bruk av vitenskapelige metoder og (b) produsere og formidle kunnskap av høy internasjonal kvalitet.[28] Det kan derfor hevdes at heller ikke i UH-sektoren er informasjonssikkerhet «en teknisk øvelse for spesielt interesserte». Isteden handler det om hvordan organiseringen og styringen av selve kjernevirksomheten – kunnskapsproduksjon og formidling – skal foregå.

Universiteters og høyskolers status som samfunnets fremste «kunnskapsvirksomheter» har ført til økt prioritering av arbeidet med informasjonssikkerhet, spesielt (men ikke bare) som følge av rapporten og anbefalingene fra 22. ju-

25 Se for eksempel Karl de Leeuw og Jan Bergstra (red.) (2007): *The History of Information Security*. Amsterdam: Elsevier; James Martin (1973): *Security, Accuracy and Privacy in Computer Systems*. Englewood Cliffs: Prentice-Hall; eller Peter Hamilton (1972): *Computer Security*. London: Cassell/Associated Business Programmes.

26 Informasjonssikkerhet er en aktivitet som til alle tider har vært praktisert av personer eller institusjoner som har hatt behov for hemmelighold, se for eksempel Karl de Leeuw og Jan Bergstra (red.) (2007): *The History of Information Security*. Amsterdam: Elsevier. Men siden midten/slutten av 1960-tallet har informasjonssikkerhet fått en langt større allmenn betydning og utbredelse enn tidligere – og blitt gjort til en egen fagdisiplin. Dette kommer blant annet til uttrykk gjennom at bøker om datateknologi begynte å behandle spørsmål om datasikkerhet, og at det utover på 1970- og 1980-tallet dukket opp stadig flere publikasjoner om datasikkerhet spesielt og informasjonssikkerhet generelt. Etter hvert ble data- og informasjonssikkerhet også etablert som egne fag på universiteter og høyskoler, både i Norge og i utlandet.

27 Se for eksempel Daniel Bell (1974): *The Coming of the Post-Industrial Society*. New York: Basic Books.

28 Se for eksempel kapittel 1 i lov om universiteter og høyskoler (http://lovdata.no/dokument/NL/lov/2005-04-01-15).

li-kommisjonen.[29] Dette kommer blant annet til uttrykk gjennom Kunnskapsdepartementets (KD) tildelingsbrev til institusjonene. I tildelingsbrevet for 2013 kreves det blant annet at institusjonene innfører «(…) et styringssystem for informasjonssikkerhet (SSIS) bygget på grunnprinsippene i anerkjente sikkerhetsstandarder.»[30] I det samme tildelingsbrevet vises det til punkt 1.7 i Digitaliseringsrundskrivet fra Fornyings-, administrasjons- og kirkedepartementet,[31] som viser videre til referansekatalogen til Direktoratet for forvaltning og IKT (DIFI).[32] I direktoratets referansekatalog fremgår det at «anerkjente sikkerhetsstandarder» skal forstås som ISO/IEC 27001: 2013 og ISO/IEC 27002: 2013, det vil si de to mest brukte «oppskriftene» på hvordan risikostyrt informasjonssikkerhetsarbeid skal organiseres og utføres. I henhold til referansekatalogen har ISO/IEC 27001: 2013 og ISO/IEC 27002: 2013 status som «anbefalte standarder» i all offentlig (statlig) forvaltning.

Skjerpede krav fra Kunnskapsdepartementet må også sees i sammenheng med at universiteter og høyskoler omfattes av en rekke lover og forskrifter hvor det stilles krav til arbeidet med informasjonssikkerhet. De viktigste av disse er personopplysningsloven med forskrift og forvaltningsloven med forskrift (e-forvaltningsforskriften).[33] I disse lovene og forskriftene pålegges universiteter og høyskoler blant annet å innføre risikobaserte styringssystemer for informasjonssikkerhet når det gjelder (a) elektronisk behandling av opplysninger om enkeltpersoner (personopplysninger) og (b) når det gjelder elektronisk kommunikasjon med og i offentlige forvaltningsorganer.[34] I tillegg inneholder offentlig-

29 Se http://www.regjeringen.no/smk/html/22julikommisjonen/22JULIKOMMISJONEN_NO/RAPPORT.HTM. En gjennomgang av de siste årenes stortingsmeldinger om høyere utdanning – Meld. St. 18 (2012-2013), Meld. St. 13 (2011-2012), St. meld. nr. 44 (2008-2009) og St. meld. nr. 30 (2008-2009) – viser at digital teknologi vies økende oppmerksomhet både når det gjelder undervisning og forsking. Informasjonssikkerhet behandles imidlertid i svært liten grad. Faktisk nevnes informasjonssikkerhet eksplisitt bare én gang i de fire siste stortingsmeldingene om høyere utdanning. Informasjonssikkerhet får imidlertid noe større oppmerksomhet i faglige utredninger om organisering og styring av IT-systemer i UH-sektoren. Se spesielt Universitets- og Høyskolerådet (2009): Strategi, organisering og styring av felles administrative IT-systemer i universitets- og høyskolesektoren. Tilgjengelig på http://www.uhr.no/documents/UHR_utvalg_strategi_organisering_og_styring_av_felles_IT__2_.pdf.

30 Tildelingsbrevet til institusjonene 2013 (tilgjengelig på http://www.regjeringen.no/nb/dep/kd/dok/andre/brev/utvalgte_brev/2013/tildelingsbrev-til-universiteter-og-hoys.html?id=715914).

31 Se http://www.regjeringen.no/nb/dep/kmd/dok/rundskriv/2012/digitaliseringsrundskrivet.html?id=706462.

32 Se http://standard.difi.no/forvaltningsstandarder/referansekatalogen-html-versjon.

33 Se spesielt Arild Jansen og Dag W. Schartum (red.) (2005): *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Bergen: Fagbokforlaget.

34 Dessuten inneholder forvaltningsloven en rekke andre bestemmelser som har betydning for arbeidet med informasjonssikkerhet, for eksempel når det gjelder taushetsplikt (konfidensialitet) og partsinnsyn (tilgangsstyring).

hetslova med forskrift og arkivloven med forskrifter bestemmelser som har betydning for UH-institusjoners arbeid med informasjonssikkerhet.[35] Det samme gjelder enkelte bestemmelser i deler av særlovgivningen, for eksempel helseforskningsloven. Til slutt vil bestemmelsene om vern av informasjon og informasjonsutveksling i den nye straffeloven ha betydning også for universiteter og høyskoler.[36]

I tillegg til Kunnskapsdepartementets krav i tildelingsbrevene og lovpålagte krav, har vurderingene til andre offentlige aktører bidratt til økt fokus på informasjonssikkerhet i UH-sektoren. I den åpne delen av sin trusselvurdering for 2014 nevner for eksempel Politiets Sikkerhetstjeneste (PST) at den er særlig bekymret for at fremmede staters etterretningstjenester forsøker å rekruttere studenter ved norske universiteter og høyskoler. I den samme trusselvurderingen nevner PST at høyteknologiske utdannings- og forskningsmiljøer kan bli – eller har allerede vært – utsatt for forsøk på ulovlig kunnskapsoverføring til utenlandske stater (primært Iran), spesielt med tanke på utvikling av komponenter til masseødeleggelsesvåpen.[37] Til sist har Riksrevisjonen styrket sin revisjonsvirksomhet på informasjonssikkerhetsområdet de siste 3-4 årene, noe også institusjoner i UH-sektoren har erfart.[38]

For å bistå institusjonene med å følge opp kravene til informasjonssikkerhet, har Kunnskapsdepartementet gitt UNINETT i mandat å opprette Sekretariatet for informasjonssikkerhet i UH-sektoren.[39] Sekretariatet skal blant annet bidra med rådgiving ved innføring av styringssystemer for informasjonssikkerhet og bistå institusjonene i arbeidet med «(…) å styrke risikoerkjennelse, sikkerhetskultur, holdninger og lederskap mv.»[40] Departementet sier videre at tiltaket – opprettelsen av Sekretariatet for informasjonssikkerhet – vil bli fulgt opp

35 Dette gjelder for eksempel allmennhetens rett til innsyn i offentlige dokumenter (tilgjengelighet) og unntak fra denne retten (konfidensialitet). Det gjelder også kravene til fysisk sikring av arkivlokaler og sikring av integriteten og autentisiteten til elektroniske dokumenter. Se for eksempel Jan F. Bernt og Harald Hove (2009): *Offentlighetslova med kommentarer*. Bergen: Fagbokforlaget; Ivar Fonnes (2010): *Arkivhåndboken for offentlig forvaltning*. Oslo: Kommuneforlaget.

36 Den nye straffeloven er vedtatt av Stortinget, men den er enda ikke trådt i kraft (medio 2014). Lovens kapittel 21 inneholder blant annet bestemmelser om identitetskrenkelser, innbrudd i datasystemer, krenkelser av privat kommunikasjon, hindring av driften av datasystemer og uberettiget bruk av tilgangsdata (for eksempel passord) og fremstilling, besittelse eller tilgjengeliggjøring av dataprogram som er ment brukt for å begå straffbare handlinger.

37 Se Åpen trusselvurdering 2014 (Politiets Sikkerhetstjeneste), tilgjengelig på http://www.pst.no/media/67044/PSTs_tv2014.pdf.

38 Se for eksempel Riksrevisjonen dokument 1: 2012-2013, s. 147 ff (tilgjengelig på https://www.riksrevisjonen.no/rapporter/Documents/2012-2013/Dokument_1/Hele.pdf).

39 Se https://www.uninett.no/infosikkerhet.

40 Tildelingsbrevet til institusjonene 2013.

gjennom rapportering på hvordan institusjonene gjør bruk av «(…) denne interne tjenesten.»[41] Samtidig har Kunnskapsdepartementet styrket kontrollvirksomheten overfor institusjonene på andre måter, for eksempel ved å be om å få tilsendt dokumentasjon på gjennomførte risikovurderinger av hvordan informasjonsverdier, spesielt personopplysninger, håndteres.

Tydeligere formelle krav til institusjonene, økt vektlegging av rapportering/kontroll og større satsning på rådgiving/bistand innebærer at fokuset på informasjonssikkerhet generelt, og styringssystemer spesielt, er skjerpet sammenliknet med hva som var tilfelle tidligere.

I den neste og de påfølgende delene av rapporten gjøres det rede for hvordan lovpålagte og andre krav til informasjonssikkerheten følges opp av 20 statlige universiteter og høyskoler.

41 Tildelingsbrevet til institusjonene 2013.

Del II: Skriftliggjøring og dokumentasjon

I del I har vi sett at byråkratisering – skriftliggjøring og dokumentasjon – er en viktig del av arbeidet med etablering og drift av styringssystemer for informasjonssikkerhet. Den første problemstillingen som drøftes er derfor graden av dokumentasjon på institusjonsnivå: I hvilken utstrekning hadde de 20 statlige universitetene og høyskolene dokumenterte og skriftliggjorte styringssystemer for informasjonssikkerhet? Hva var hovedinnholdet i den systemdokumentasjonen som fantes?

Dokumenter og dokumentomfang

Gjennomgang av de 20 institusjonenes sikkerhetsdokumentasjon viste at flertallet av dem hadde jobbet med skriftliggjøring av styringssystemer for informasjonssikkerhet. 2/3 av institusjonene (13 av 20 universiteter og høyskoler) hadde derfor utarbeidet (eller var i ferd med å utarbeide) skriftliggjorte styringssystemer (med tilhørende arbeidsrutiner). I tillegg hadde én av de øvrige institusjonene laget flere forskjellige utkast til styringssystem (med tilhørende arbeidsrutiner) for noen år tilbake. Utkastene hadde imidlertid ikke blitt vedtatt av ledelsen og styringssystemet var derfor formelt sett ikke trådt i kraft.

Denne konklusjonen, det vil si at 2/3 av de kartlagte institusjonene hadde eller var i ferd med å utarbeide skriftliggjorte styringssystemer for informasjonssikkerhet, er basert på en nokså liberal og romslig definisjon av hva som inngår i et helhetlig og fullverdig styringssystem. Utgangspunktet er at et helhetlig og fullverdig styringssystem krever at tre hovedtyper systemdokumenter er på plass. For det første styrende dokumenter. De styrende dokumentene trekker opp rammene for arbeidet med informasjonssikkerhet, spesielt sikkerhetsmål, kriterier for akseptabel risiko, sikkerhetsstrategi, sikkerhetsorganisering og konfigurasjonskart (oversikt over hvordan den elektroniske behandlingen av informasjon er bygd opp og fungerer). For det andre gjennomførende dokumenter. De gjennomførende dokumentene forteller hvordan institusjonene skal utføre ulike sikkerhetsoppgaver, og inneholder blant annet maler og rutiner for risikovurderinger, iverksetting av sikringstiltak og retningslinjer for sikker håndtering av ulike typer informasjon. For det tredje kontrollerende dokumenter. De kontrollerende dokumentene spesifiserer hvordan informasjonssikkerheten skal sjek-

kes og arbeidet følges opp, og inneholder rutiner for avvikshåndtering, sikkerhetsrevisjon og ledelsens gjennomgang.[42]

Det viste seg at svært få av de 13 institusjonene hadde skriftliggjort samtlige elementer som inngår i den styrende, gjennomførende og kontrollerende dokumentasjonen. Mange av dem manglet for eksempel kriterier for akseptabel risiko og flere institusjoner hadde ikke laget oversikter over informasjonssystemer og teknisk infrastruktur (konfigurasjonskart) eller rutiner for sikkerhetsrevisjoner. Nedenfor skal vi dessuten se at det knyttet seg usikkerhet til andre elementer i styringssystemene, blant annet når det gjaldt oppbyggingen av institusjonenes sikkerhetsorganisasjoner.

Disse manglene gjorde det problematisk å snakke om helhetlige og fullverdige styringssystemer i de fleste av institusjonene. Likevel omfattet systemdokumentasjonen flere av de sentrale elementene som er ment å inngå i et styringssystem for informasjonssikkerhet. De fleste institusjonene hadde for eksempel beskrevet sine sikkerhetsorganisasjoner og sikkerhetsmål, rutiner for risikovurdering, avvikshåndtering og ledelsens gjennomgang. På denne bakgrunn kan det derfor (med noen forbehold) hevdes at disse 13 institusjonene hadde skriftliggjort (eller var i ferd med å skriftliggjøre) hovedstrukturen i et styringssystem for informasjonssikkerhet.

Dateringen av systemdokumentasjonen viste at den i hovedsak var «ferskvare»: i de aller fleste av de 13 institusjonene var den 2-4 år gammel. I noen få institusjoner var dokumentasjonen av eldre noe dato enn dette, det vil si at den hadde blitt utarbeidet og vedtatt før 2009/10. Et par institusjoner rapporterte for eksempel at de hadde laget mesteparten av sin systemdokumentasjon helt på begynnelsen av 2000-tallet (og at den siden ikke hadde blitt revidert i særlig grad). Også noen institusjoner med «ferskvare» hadde utarbeidet enkelte deler av sin systemdokumentasjon, for eksempel oversikt over informasjonssystemer og informasjonsverdier, sikkerhetsmål eller rutiner for sikker håndtering av personopplysninger, i perioden før 2009/10. Dette gjaldt i særlig grad institusjoner som hadde vært gjenstand for kontrollbesøk fra Datatilsynet. Den systemdokumentasjonen som da ble utarbeidet (etter pålegg fra Datatilsynet) virket imidlertid å ha blitt vurdert som utilstrekkelig sett i lys av Kunnskapsdepartementets (og Riksrevisjonens) økte fokus på og krav til arbeidet med informa-

42 I informasjonssikkerhetslitteraturen og blant myndighetsorganer finnes det noe ulike oppfatninger om hvilke dokumenter som er styrende, gjennomførende og kontrollerende. Enkelte mener for eksempel at rutiner for ledelsens gjennomgang er kontrollerende fremfor styrende dokumenter, mens andre mener at rutiner for risikovurderinger er styrende fremfor gjennomførende dokumenter. Hvordan ulike dokumenter klassifiseres, er likevel av akademisk interesse. Det avgjørende er om institusjonene hadde utarbeidet og vedtatt dokumentene eller ikke.

sjonssikkerhet i UH-sektoren. I noen av disse institusjonene var det derfor iverksatt nye runder med «papirarbeid» og ny sikkerhetsdokumentasjon var (eller var i ferd med å bli) utarbeidet og vedtatt.

Systemdokumentasjonen – styrende, gjennomførende og kontrollerende dokumenter – var i enkelte av 13 institusjonene til dels betydelig i omfang. De styrende dokumentene (som institusjonene selv vanligvis omtalte som sikkerhetspolicy og prinsipper for informasjonssikkerhet, se nedenfor) var normalt på mellom 20 og 30 sider, men kunne i noen institusjoner være mer omfattende enn dette (50-60 sider). I tillegg kom de gjennomførende og kontrollerende dokumentene. Spesielt de gjennomførende dokumentene kunne være omfattende og spenne over et vidt spekter av aktiviteter, for eksempel regler for bruk av håndholdte dataenheter; e-post eller sosiale medier; tildeling av brukernavn og passord; avslutting av brukerkontoer; håndtering av sensitive personopplysninger i forbindelse med helseforskning; rutiner for anvendelse av ulike IT-systemer, osv. De kontrollerende dokumentene omfattet rutiner for egenkontroll, for eksempel gjennomføring av sikkerhetsrevisjoner eller prosedyrer for melding og håndtering av avvik.

I tillegg hadde flere institusjoner egne skriftliggjorte styringssystemer for ivaretakelsen av informasjonssikkerheten og andre rettslige forpliktelser i medisinske eller helsefaglige forskningsprosjekter.[43] I flere av disse institusjonene var styringssystemet for informasjonssikkerhet i praksis delt i to: en del som spesifikt omhandlet medisinsk og helsefaglig forskning og en annen del som omfattet resten av virksomheten. Det innebar at systemdokumentasjonen ikke var samlet på én plass, men var fordelt mellom ulike typer «håndbøker» eller internkontrollsystemer. Til sammen kunne styrende, gjennomførende og kontrollerende dokumenter i enkelte av de 13 institusjonene som hadde dette utgjøre mellom 100 og 200 sider tekst. Det mest typiske var imidlertid at det totale dokumentomfanget var noe mindre – mellom 30 og 100 sider (og i enkelte institusjoner også litt mindre enn dette).

43 Medisinsk og helsefaglig forskning reguleres i hovedsak av helseforskningsloven, personopplysningsloven og forskningsetikkloven. Dette innebærer blant annet at medisinske eller helsefaglige prosjekter skal godkjennes av Regionale komiteer for medisinsk og helsefaglig forskningsetikk (se spesielt https://helseforskning.etikkom.no). Når det gjelder informasjonssikkerhet, er det reglene i personopplysningsloven med forskrift som kommer til anvendelse. Under *Normen for informasjonssikkerhet i helsesektoren* har derfor *Veileder i personvern og informasjonssikkerhet i forskningsprosjekter* blitt laget (se http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/dokumenter/veiledere/Documents/veileder_personvern-og-informasjonssikkerhet-i-forskningsprosjekter-v11.pdf). Veilederen skal sikre at personopplysningslovgivningens regler om informasjonssikkerhet blir overholdt i medisinske og helsefaglige forskningsprosjekter.

I de resterende sju institusjonene var styrende, gjennomførende og kontrollerende dokumenter enten ikke utformet eller det var laget enkelte typer gjennomførende dokumenter. Her var det for eksempel snakk om enkelte rutiner for bruk av bærbare dataenheter og sosiale medier eller retningslinjer for tildeling av brukernavn og passord. Ut over dette kunne det finnes enkelte driftsrutiner for IT-avdelingen/seksjonen som berørte informasjonssikkerheten, for eksempel retningslinjer for sikkerhetsoppdateringer av programvare. Den klareste mangelen i disse institusjonene var at den styrende og kontrollerende dokumentasjonen var tilnærmet fraværende. De sju institusjonene manglet derfor sentrale elementer som sikkerhetsmål, sikkerhetsstrategi, kriterier for akseptabel risiko, sikkerhetsorganisasjon og rutiner for egenkontroll (revisjoner, avvikshåndtering og ledelsesgjennomganger). Når det gjelder disse institusjonene synes det derfor riktig å si at de ikke hadde et skriftliggjort styringssystem for informasjonssikkerhet. Systemdokumentasjonen fremstod som fragmentert og lite systematisk, og det virket noe tilfeldig hvorfor enkelte typer dokumenter var utarbeidet mens andre typer dokumenter ikke var det.

Nedenfor skal vi se at forskjeller i systemdokumentasjon mellom institusjonene ikke alltid skjulte tilsvarende forskjeller i det praktiske arbeidet med informasjonssikkerhet. Det var altså ikke nødvendigvis slik at institusjoner med omfattende dokumentasjon av sine styringssystemer hadde et mer omfattende informasjonssikkerhetsarbeid, eller jobbet mer systematisk med sikring av informasjonsverdier, enn institusjoner som i mindre grad hadde skriftliggjorte styringssystemer.

Dokumentstruktur og hovedinnhold

Hvordan var strukturen på og hovedinnholdet i sikkerhetsdokumentasjonen i de 20 institusjonene som ble kartlagt?

Flertallet av de 13 institusjonene som hadde utarbeidet (eller var i ferd med å utarbeide) skriftliggjorte styringssystemer for informasjonssikkerhet, baserte oppbyggingen av sin systemdokumentasjon på anbefalinger, veiledninger og dokumentmaler publisert av UNINETT. Her dreide det seg i særlig grad på UNINETTs styringssystemforslaget publisert i UFS 126.[44] Unntaket var de institusjonene som også hadde utarbeidet styrende, gjennomførende og kontrollerende dokumenter for ivaretakelsen av informasjonssikkerheten i medisinsk eller helsefaglig forskning. Disse institusjonene hadde enten laget sine egne

44 Tilgjengelig på https://www.UNINETT.no/ferdige-ufs. UFS 126 kan beskrives som en konsentrert og bearbeidet versjon av ISO/IEC 27001/02: 2005.

systemdokumenter, noe som innebar til dels betydelige forskjeller i dokumentstruktur (og innhold) på tvers av institusjonene, eller de hadde basert seg på veiledninger og anbefalinger publisert i *Norm for informasjonssikkerhet i helsesektoren*[45] (spesielt *Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren*[46]). Til slutt var det noen få institusjoner som hadde laget sine egne styringssystemer, helt eller delvis uavhengig av UFS 126. Her ble det rapportert at årsaken til uavhengigheten var at institusjonene ønsket å ha mest mulig egenkontroll med organiseringen og utførelsen av arbeidet med informasjonssikkerhet.

Resultatet av UNINETTs innflytelse på institusjonenes systemdokumentasjon var at mesteparten av den var forholdsvis lik på tvers av institusjoner. I enkelte tilfeller hadde innflytelsen vært så stor at det stort sett bare var navnet på institusjonene og mindre ulikheter i beskrivelsene av sikkerhetsorganiseringen som skilte systemdokumentasjonen tilhørende forskjellige institusjoner fra hverandre. Det virker derfor riktig å si at UNINETTs anbefalinger, veiledninger og dokumentmaler (spesielt UFS 126) hadde hatt betydelig gjennomslagskraft på institusjonsnivå. Uten UNINETTs veiledninger og anbefalinger er det følgelig trolig at flertallet av de 13 institusjonene ville manglet skriftliggjorte styringssystemer for informasjonssikkerhet. Det samme kan i noen grad sies om *Norm for informasjonssikkerhet i helsesektoren*. Uten denne normen virker det tvilsomt om det ville eksistert egne styringssystemer for behandling av personopplysninger i medisinsk og helsefaglig forskning.

Baksiden av medaljen var, som allerede indikert, at UNINETTs gjennomslagskraft førte til betydelig standardisering av institusjonenes styringssystemer. De var derfor i liten grad (og i de fleste institusjonene) ikke «gjort lokale», det vil si at de i begrenset utstrekning var forsøkt tilpasset lokale institusjonsforhold eller behov. Dette er et viktig poeng som diskuteres nærmere i kommende deler av rapporten.

UNINETTs standardiserende innflytelse innebar at flertallet av institusjonene hadde en todelt dokumentstrukturen. Den første delen ble omtalt som «informasjonssikkerhetspolicy» og den andre delen ble omtalt som «prinsipper for informasjonssikkerhet». Strukturen på og hovedinnholdet i flertallet av de 13 institusjonenes systemdokumentasjon kan derfor presenteres på følgende måte:

45 Se http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/Sider/default.aspx.

46 Tilgjengelig på http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/dokumenter/veiledere/Documents/veileder_personvern-og-informasjonssikkerhet-i-forskningsprosjekter-v11.pdf.

Del I: Informasjonssikkerhetspolicy

- Sikkerhetsmål og strategi
- Sikkerhetsorganisering
  - policyeier (vanligvis universitets- eller høyskoledirektør)
  - informasjonssikkerhetsleder (CISO/CSO eller informasjonssikkerhetsrådgiver)
  - linjeansvar (fordeling av oppgaver mellom administrative ledere sentralt og fakulteter, institutter eller andre enheter)
  - systemeiere (administrative eller faglige enheter)
  - systemansvarlige (IT-avdelingen)
  - brukere (spesielt ansatte og studenter)
  - eksterne aktører (konsulenter, kontraktsparter, databehandlere)

Del II: Prinsipper for informasjonssikkerhet

- Gjennomførende og kontrollerende rutiner
- Pålegg om gjennomføring av konkrete sikringstiltak
- Fordeling av ansvar innenfor en rekke spesifikke områder (for eksempel verdiklassifisering av informasjon, risikovurderinger, fysisk soneinndeling, tilgangsstyring, avvikshåndtering, beredskap og kontinuitet, osv.)
- Samsvar
  - oversikt over relevante lover og forskrifter
- Dokumentstruktur
  - forklaringer til systematikken i sikkerhetsdokumentasjonen

Selv om hovedstrukturen og innholdet i systemdokumentasjonen var relativt standardisert, var det (som nevnt ovenfor) enkelte deler av dokumentasjonen som likevel var forsøkt tilpasset lokale institusjonsforhold. Dette gjaldt i første rekke oppbygningen av sikkerhetsorganiseringen. Her kom lokale tilpasninger blant annet til uttrykk ved at noen av de aller største institusjonene hadde opprettet såkalte CERT, det vil si en IT-teknisk sikkerhetsgruppe.[47] CERT var derfor en gruppe ansatte i IT-avdelingene som hadde i oppgave å overvåke sikkerhetstilstanden og varsle om sikkerhetsproblemer knyttet til IT-systemer og teknisk infrastruktur (for eksempel identitetstyveri, virusangrep eller datainnbrudd). De fleste institusjonene hadde imidlertid ikke en egen IT-teknisk sikkerhetsgruppe, men benyttet seg isteden av UNINETTs CERT-tjeneste.[48]

47 Computer Emergency Response Team.

48 For beskrivelse, se https://www.uninett.no/tjenester/cert.

En del flere institusjoner hadde dessuten opprettet et eget informasjonssikkerhetsforum,[49] mens andre institusjoner ikke hadde etablert denne typen koordinerende og rådgivende organer for arbeidet med informasjonssikkerhet. Der hvor denne typen møteplasser/forum eksisterte, var beskrivelsene av oppgaver og myndighet basert på anbefalingene til UNINETT (UFS 126). I flere institusjoner hvor informasjonssikkerhetsforum eksisterte på papiret ble det rapportert at forumene enten var «sovende» eller spilte liten rolle i planleggingen og gjennomføringen av arbeidet med informasjonssikkerhet. Bare i noen få institusjoner ble det rapportert at informasjonssikkerhetsforumet hadde relativt regelmessige møter og at det ivaretok sine oppgaver slik som beskrevet i systemdokumentasjonen.

Et mindretall av institusjonene hadde laget sine egne versjoner av UNINETTs anbefalinger og veiledninger for styringssystemer i informasjonssikkerhet (UFS 126). Her dreide det seg enten om institusjoner som daterte sine styringssystemer til perioden før UNINETT publiserte sine anbefalinger og veiledninger (2010), eller institusjoner som bevisst hadde «kjørt sitt eget løp» (og derfor hadde liten eller ingen kontakt med UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren). Likevel hadde også disse institusjonene en dokumentstruktur som i hovedtrekk speilte den oppbyggingen som er skissert ovenfor. Dette kom særlig til uttrykk gjennom todelingen av de styrende, gjennomførende og kontrollerende dokumentene («informasjonssikkerhetspolicy» og «prinsipper for informasjonssikkerhet»).

Når det gjelder det mer detaljerte innholdet i systemdokumentasjonen i de 13 institusjonene som hadde fått – eller var i ferd med å få – dette på plass, er følgende forhold spesielt verdt å kommentere:

Sikkerhetsmål

Hensikten med sikkerhetsmål er at de (på overordnet nivå) skal angi hva institusjonene ønsker å oppnå med beskyttelsen av den informasjonen de håndterer og begrunne hvorfor informasjonssikkerhet er viktig. Sammen med sikkerhetsstrategien,[50] skal sikkerhetsmålene være retningsgivende for arbeidet med informasjonssikkerhet.

---

49 Informasjonssikkerhetsforum er ment å være et rådgivende organ for ledelsen når det gjelder arbeidet med informasjonssikkerhet. Forumene består av utvalgte ledere/medarbeidere i institusjonene og ledes vanligvis av CISO, CSO eller informasjonssikkerhetsrådgiver.

50 Sikkerhetsstrategien skal beskrive de viktigste prioriteringene som ligger til grunn for arbeidet med informasjonssikkerhet, for eksempel ved å gi retningslinjer for hvilke datasystemer eller andre deler av informasjonshåndteringen som kan settes ut til eksterne tjenesteleverandører.

I de institusjonene som er kartlagt, var sikkerhetsmål til dels svært mange og sammensatte. Enkelte institusjoner opererte for eksempel med 12-15 forskjellige sikkerhetsmål av ulik karakter. Det var vanlig at sikkerhetsmålene blant annet omfattet følgende forhold:

- Sørge for at institusjonen overholdt regler om informasjonssikkerhet i de lover og forskrifter som gjaldt for institusjonen.
- Sørge for at personvernet til studenter, medarbeidere og forskningsdeltakere ble ivaretatt.
- Sørge for at informasjonsverdier ble sikret i henhold til verdienes betydning for institusjonen (eller for de personene opplysningene gjaldt).
- Motivere ledere og ansatte til å ivareta sitt ansvar for informasjonssikkerheten i institusjonen.
- Sørge for at eksterne tjenesteleverandører rettet seg etter institusjonenes krav til informasjonssikkerhet.

Som allerede indikert, var det typiske at disse (og andre) sikkerhetsmål var hentet fra veiledninger og anbefalinger publisert av UNINETT. Likevel opererte enkelte institusjoner, spesielt de som hadde et «fritt og uavhengig» forhold til UNINETTs anbefalinger og veiledninger, med en del færre sikkerhetsmål enn hva som var tilfelle i de øvrige institusjonene. Men også disse institusjonene hadde hentet flere av sine sikkerhetsmål fra UNINETTs anbefalinger og veiledninger.

UNINETTs innflytelse på utformingen av sikkerhetsmål var ikke like sterk i styringsdokumenter for informasjonssikkerhet i medisinske og helsefaglige forskningsprosjekter. Her var det isteden normen for informasjonssikkerhet i helsesektoren som spilte førstefiolin. Målene var likevel ikke vesensforskjellige fra de som UNINETT anbefaler, men kunne omfatte enkelte tilleggsmomenter, for eksempel ivaretakelse av hensynet til meroffentlighet eller sikring av forskningsdeltakernes rettigheter i henhold til bestemmelser i personopplysningsloven, helseforskningsloven og forvaltningsloven.

Akseptabel risiko

Definisjoner av kriterier for akseptabel risiko (akseptkriterier) fremstod som en utfordring i de kartlagte institusjonene. Slike kriterier er ment å angi hvor stor grad av informasjonssikkerhet institusjonene mener er nødvendig for at sikkerheten skal være tilfredsstillende: «Hvor mye sikkerhet har vi behov for her hos oss?» Det er videre meningen at akseptkriteriene skal brukes ved risikovurderinger for å avgjøre om risikoen for uønskede hendelser er større enn hva institusjonen har definert som akseptabel.

Det vanligste var at institusjonene hadde definert det som kan oppfattes som akseptkriterier når det gjaldt brudd på informasjonens tilgjengelighet, typisk hvor lang nedetid som var akseptabelt for IT-systemer med høy, middels eller lav kritikalitet. Det var også vanlig at akseptkriterier for tilgjengelighet ikke ble spesifisert i de innledende og styrende dokumentene, men var ofte «gjemt bort» i andre deler av systemdokumentasjonen. Dermed kunne kriteriene for tilgjengelighet være krevende å finne.

Tilsvarende kriterier var vanligvis ikke utformet når det gjaldt informasjonens konfidensialitet og integritet. I enkelte institusjoner kunne akseptabel risiko for konfidensialitet og integritet likevel være formulert i forbindelse med medisinsk og helsefaglig forskning. Men disse akseptkriteriene gjaldt bare for denne delen av forskningsaktiviteten og ikke for andre typer forskning eller oppgaver (administrasjon, undervisning, formidling, osv.).

Praktisk betydning

Det var derfor ikke overraskende at intervjuene antydet at både kriterier for akseptabel risiko og sikkerhetsmålene generelt sett virket å ha liten betydning for det operative sikkerhetsarbeidet. Verken sikkerhetsmålene eller de kriteriene for akseptabel risiko som eksisterte virket å være kjent blant vitenskapelige og administrativt ansatte. Samtidig kunne de daglig ansvarlige for informasjonssikkerheten (CISO, CSO eller informasjonssikkerhetsrådgiver) ha problemer med å huske hvilke sikkerhetsmål og kriterier for akseptabel risiko som eventuelt var definert.

Med hensyn til sikkerhetsmål, var det likevel to målsettinger som virket å være kjent og som ble tillagt betydelig vekt. For det første målet om å overholde relevante lover og forskrifter. For det andre målet om å ivareta personvernet til studenter, medarbeidere eller forskningsdeltakere ved elektronisk behandling av personopplysninger (de to målsetningene var i noen grad overlappende: ivaretakelse av personvernet var nært knyttet til overholdelse av reglene om informasjonssikkerhet i personopplysningsloven med forskrift).[51] Begge disse målene fremstod som spesielt viktige for institusjonene i den forstand at de ble rapportert å være retningsgivende for det operative informasjonssikkerhetsarbeidet.

51 Fokuset på personvern og behandling av personopplysninger skyldes trolig også at Riksrevisjonen hadde vært spesielt opptatt av hvordan UH-institusjoner fulgte opp bestemmelsene om informasjonssikkerhet i personopplysningsloven § 13 og personopplysningsforskriften kapittel to. Se for eksempel Riksrevisjonen Dokument 1 (2012-2013). Tilgjengelig på https://www.riksrevisjonen.no/Rapporter/Sider/Dokument1for2011.aspx.

Hovedfokus

I flertallet av institusjonene ble det altså rapportert at personvern – og rettslige regler om elektronisk behandling av personopplysninger – var hovedfokuset for arbeidet med informasjonssikkerhet. Dette gjaldt for eksempel i forbindelse med personal- og studentadministrasjon, eksamensplanlegging og sensur, administrasjon av medisinsk eller helsefaglig forskning eller generell forskningsadministrasjon. Personopplysningsloven med forskrift var derfor den viktigste rettslige reguleringen som institusjonene forholdt seg til på informasjonssikkerhetsområdet. Ut over dette ble det rapportert at forvaltningsloven (særlig bestemmelsene om taushetsplikt), offentlighetsloven, arkivloven med forskrifter og helseforskningsloven med forskrift hadde betydning for arbeidet med informasjonssikkerhet.

Til tross for at alle disse regelverkene ble hevdet å påvirke styringen av informasjonssikkerheten, var det liten tvil om at personopplysningslovgivningen dominerte tenkningen i de fleste institusjonene. Betydningen av de andre regelverkene som ble nevnt i systemdokumentasjonen fremstod som noe mer uklar. Samtidig ble det ikke rapportert om at andre enn de nevnte regelverkene hadde betydning for institusjonenes styring av arbeid med informasjonssikkerhet. E-forvaltningsforskriften, som inneholder grunnleggende krav til informasjonssikkerheten i elektronisk kommunikasjon med og innenfor forvaltningsorganer (inkludert universiteter og høyskoler), ble for eksempel ikke nevnt som viktig i annet enn et par institusjoner.

I flere av institusjoner virket det som fokuset på personvern og personopplysninger var nært knyttet til et tilsvarende fokus på (a) administrative behandlinger av opplysninger om enkeltpersoner (ansatte og studenter) og (b) behandling av helseopplysninger i medisinske eller helsefaglige forskningsprosjekter. Det kunne derfor synes som behandling og sikring av personopplysninger ble assosiert med en bestemte arbeidsprosesser: administrasjon og visse deler av forskningsvirksomheten.[52] Bevisstheten om at personopplysninger også ble behandlet i andre typer arbeidsprosesser, spesielt i andre deler av forskningsvirksomheten

52 Med administrasjon menes ikke bare arbeid som utføres av administrative ansatte i sentraladministrasjonen, på fakulteter og institutter eller i fagavdelinger og andre organisatoriske enheter. Som indikert ovenfor, inkluderer det også en rekke oppgaver som helt eller delvis utføres av vitenskapelig ansatte og annet undervisningspersonell, blant annet undervisnings- og eksamensplanlegging og -gjennomføring, sensur og klagebehandling, disiplinærsaker (annullering av eksamen, utestengning eller bortvisning av studenter), rapportering av vitenskapelig produksjon, planlegging og gjennomføring av seminarer, konferanser eller workshops, søknadsprosesser (for eksempel til Norges Forskningsråd, EU eller andre finansieringskilder), administrasjon av innvilgede forskningsprosjekter, utarbeidelse av forskningsstrategier, osv.

enn den medisinske og helsefaglige, fremstod ikke som like sterk.[53] Dette kom til uttrykk på to måter:

For det første ved at enkelte institusjoner virket å ha relativt høy bevissthet omkring behandling og sikring av helseforskningsdata – og hadde laget egne systemer og rutiner for dette. Selv om tilsvarende systemer og rutiner i noen grad kunne finnes for behandling og sikring av personopplysninger i andre typer forskningsprosjekter, var likevel inntrykket at bevisstheten om behovet for beskyttelse av ikke-medisinsk forskningsdata ikke var like stor. For det andre ved at personopplysninger som ikke ble behandlet i administrasjon og medisinsk forskning virket å bli oppfattet som «noe annet.» Dette handlet om at personopplysningslovens bestemmelser om informasjonssikkerhet ble beskrevet som særlig relevante når det gjaldt administrasjon og medisinsk forskning. De samme bestemmelsene virket ikke å bli forstått som like relevante når det gjaldt håndtering av personopplysninger i andre sammenhenger, for eksempel i ikke-medisinske forskningsprosjekter. Dette til tross for at ikke-medisinske forskningsprosjekter også kunne behandle personopplysninger og derfor var underlagt personopplysningsloven. Konsekvensen virket å være at det hadde oppstått en viss skjevhet i arbeidet med informasjonssikkerhet: mesteparten av arbeidet var rettet inn mot beskyttelse av administrative behandlinger av personopplysninger og helseforskningsdata. Behovet for informasjonssikkerhet i de øvrige delene av virksomheten som behandlet personopplysninger, spesielt i ikke-medisinske forskningsprosjekter, virket det å være mindre bevissthet omkring.[54]

Bare én institusjon rapportert at arbeidet med informasjonssikkerhet hadde et annet hovedfokus enn personvern og personopplysninger. Her ble beskyttelse av konfidensielle forskningsdata (som ikke inneholdt personopplysninger) prioritert høyest (eller i alle fall like høyt som personvern og sikring av personopplysninger). I et par andre institusjoner ble det understreket at selv om personvern og personopplysninger var hovedfokuset, var det også viktig å sikre andre typer informasjonsverdier, spesielt innenfor forsknings- eller undervisnings-

53 I personopplysningsloven er alle typer informasjon og vurderinger som kan knyttes til en bestemt enkeltperson definert som personopplysninger. Hva personopplysningene brukes til – administrasjon eller forskning – har ingen betydning for hva som i rettslig forstand er å forstå som personopplysninger. Det innebærer at regelverket stiller de samme kravene til sikring av personopplysninger uavhengig av om de benyttes til administrative eller forskningsmessige formål, og uavhengig av hvilken type administrasjon eller forskning det er snakk om.

54 Datatilsynets kontrollrapporter fra UH-sektoren indikerte at når personopplysninger ble brukt til forskningsformål ble de ikke sikret på samme måten som når personopplysninger ble brukt til administrative formål. Det kan tenkes at noe av årsaken til dette var at institusjonene assosierte behandlingen av personopplysninger sterkere til administrative prosesser enn til deler av forskningsvirksomheten.

delen av virksomheten. Samtidig ble det rapportert at arbeidet med beskyttelse av disse informasjonsverdier ikke var kommet like langt som når det gjaldt administrasjonens behandling av personopplysninger.

Sikkerhetsorganisering

Ovenfor har vi nevnt at hensikten med en sikkerhetsorganisasjon er å fordele myndighet, ansvar og konkrete arbeidsoppgaver mellom aktørene på institusjonsnivå (ledere, administrativt og vitenskapelige ansatte, osv.). Sikkerhetsorganisasjonen er derfor bærebjelken i det praktiske og daglige arbeidet med informasjonssikkerhet.

Beskrivelsene av sikkerhetsorganiseringen i institusjonenes systemdokumentasjon var vanligvis to- eller tredelt. Den første delen bestod av en beskrivelse av oppgave- og ansvarsfordeling mellom ledere i linjen: administrative ledere i sentraladministrasjonen og ledere (faglige eller administrative) på fakultets eller grunnenhetsnivå (institutter, biblioteker, museer, forskningssentre, osv.). Den andre delen bestod av en beskrivelse av oppgave- og ansvarsfordeling mellom systemeiere (forvaltere av ulike IT-systemer, spesielt avdelinger i sentraladministrasjonen) og systemansvarlig (IT-avdelingen/seksjonen). Som nevnt flere ganger allerede, var det i enkelte institusjoner også en tredje og siste del. Den bestod av egne og utdypende beskrivelser av fordelingen av ansvar og oppgaver i medisinske og helsefaglige forskningsprosjekter (hvor oppgavene til roller som «forskningsansvarlig», «prosjektledere» og «prosjektdeltakere» vanligvis var definert og spesifisert).[55] Av intervjuene fremgikk det at forholdet mellom systemeiere og systemansvarlige virket å være noe uklart: hvordan var det meningen at relasjonen mellom disse to rollene i praksis skulle fungere? De fleste forstod likevel relasjonen med utgangspunkt i en bestiller-utfører-modell: systemeierne «bestilte» teknisk sikringstiltak fra systemansvarlig, som deretter «utførte» hva systemeierne hadde «bestilt».

Til tross for at alle de 13 institusjonene med sikkerhetsdokumentasjon hadde (på papiret) en to- eller tredelte sikkerhetsorganiseringen, var det til dels vanskelig å få svar på hvordan institusjonene så for hvordan helheten i organisasjonsmodellen skulle fungere. Det kunne for eksempel være noe uklart hvem

55 Beskrivelser av roller og oppgaver i medisinsk og helsefaglig forskning var vanligvis en del av disse institusjonenes generelle interkontroll. Årsaken til dette var at beskrivelsene ikke bare dreide seg om informasjonssikkerhet, men inneholdt i tillegg rutiner for overholdelse av en rekke andre juridiske plikter (med særlig henvisning til helseforsknings- og personopplysningsloven), for eksempel når det gjaldt ulike søknads- og godkjenningsprosesser, utarbeidelse av samtykkeskjema, endringsmeldinger til REK, informasjon til forskningsdeltakere, osv.

som skulle ivareta hvilke oppgaver og når (eventuelt også hvor ofte) de ulike oppgavene skulle utføres. Én av årsakene til dette var trolig at arbeidsfordelingen mellom aktørene/rollene i sikkerhetsorganisasjonen var noe fragmentert, det vil si at institusjonene manglet en samlet og uttømmende oversikt over hvem som skulle gjøre hva. Det typiske var at noen oppgaver (og fordelingen av dem) var beskrevet i policydokumentene (under overskriften «sikkerhetsorganisering»), mens andre oppgaver (og fordelingen av dem) ble beskrevet i andre deler av sikkerhetsdokumentasjonen, for eksempel under «prinsipper for informasjonssikkerhet».

I tillegg kunne atter andre oppgaver være beskrevet i egne retningslinjer for behandling og sikring av personopplysninger i forskningsprosjekter, spesielt medisinsk og helsefaglig forskning. I disse retningslinjene kunne det også dukke opp roller (med tilhørende ansvar og oppgaver) som ikke var nevnt i de generelle policydokumentene («forskningsansvarlig», «prosjektledere» og «prosjektdeltakere»). Dermed fremstod det som noe uklart hvordan sammenhengen mellom den generelle og de mer fagspesifikke delene av sikkerhetsorganiseringen i praksis var tenkt å fungere.

Dessuten, og som allerede antydet, problematiserte enkelte institusjoner forholdet mellom systemeiere og systemansvarlige. Systemeiere var i stor grad ikke-teknisk personell, spesielt ledere i sentraladministrasjonen eller administrativ/faglig ledelse på fakultets- og instituttnivå. Spørsmålet som ble stilt var i hvilken grad disse lederne hadde den nødvendige spesialistkompetansen til «å bestille» IT-teknisk sikkerhet fra de systemansvarlige, det vil si teknologene i IT-avdelingene/seksjonene? Dersom systemeierne manglet den IT-tekniske bestillerkompetansen, samtidig som den var sentralisert hos de systemansvarlige, ville ikke det bety at ansvarsforholdet i praksis ble snudd på hodet? Ville ikke de systemansvarlige da måtte påse at systemeierne «bestilte» den nødvendige IT-teknisk sikkerhet slik at «utførerne» (de systemansvarlige) i realiteten ble «bestillere»?

Dette var en problemstilling som ble satt på spissen ved anskaffelser av nye IT-løsninger. Her var det de systemansvarlige (IT-avdelingene/seksjonene) som, ifølge sikkerhetsdokumentasjonen, skulle godkjenne innkjøp og installasjon av IT-systemer/utstyr i sentraladministrasjonen eller på fakultets-/instituttnivå. Men det ble hevdet at dette førte til at de systemansvarlige måtte ta et større ansvar for IT-teknisk sikkerhet enn hva bestiller-utfører-modellen la opp til. Dermed kunne de systemansvarlige havne i en vanskelig dobbeltrolle: På den ene siden skulle de være relativ passive «utførere» av systemeiernes bestillinger,

men på den andre siden skulle de også være aktive «godkjenner» av bestillinger de var ment å utføre på vegne av systemeierne.

Enkelte av de som ble intervjuet uttrykt også usikkerhet knyttet til beskrivelsene av forholdet mellom linjeansvaret og systemeierskapet. Hvem var eiere av de ulike IT-løsningene? Var det meningen av linjeledere og systemeiere skulle ivareta de samme eller forskjellige oppgaver? Hva skulle man i så fall gjøre i rollen som linjeleder og hva skulle man gjøre i rollen som systemeier, spesielt dersom man både var systemeier og linjeleder? Andre oppfattet ikke disse spørsmålene som vanskelige å besvare, men rapporterte at forholdet mellom linjeansvar og systemeierskap var uproblematisk. De som hevdet dette synspunktet var i første rekke nøkkelpersonell i institusjoner hvor «systemeierskap» ble hevdet å være – eller var i ferd med å bli – et innarbeidet begrep blant ledere og ansatte.

I én av institusjonene ble det rapportert at man hadde gått bort fra systemeierrollen og bestemt at ansvaret for informasjonssikkerheten isteden skulle knyttes til «tjenesteeiere». Dette indikerte at arbeidet med informasjonssikkerhet ble frikoblet fra forvaltning av konkrete IT-tekniske løsninger (IT-systemer) og at fokuset i større grad ble rettet mot de tjenestene – eller de arbeidsprosessene – som IT-systemene ble brukt til å utføre. Introduksjon av tjenesteeierrollen hadde imidlertid skapt noe forvirring – hva var en «tjeneste» og hvem var eiere av de ulike «tjenestene»? Rollen som tjenesteeier hadde derfor ikke blitt innarbeidet – forstått og akseptert – i institusjonen enda.

Prinsipper for informasjonssikkerhet

Innholdet i systemdokumenter med tittelen «Prinsipper for informasjonssikkerhet» var noe uensartet og fremstod i de fleste institusjonene som en sammensetning av tre elementer. For det første pålegg om iverksetting av konkrete oppgaver eller tiltak, for eksempel beskrivelser av hvilke rutiner eller retningslinjer som måtte utformes eller spesifisering av konkrete sikringstiltak som skulle iverksettes. For det andre beskrivelser av enkelte typer arbeidsverktøy som skulle benyttes i informasjonssikkerhetsarbeidet, for eksempel risikomatriser eller soneinndelingsmatriser (inndeling av bygninger/rom i ulike «sikkerhetskategorier» – typisk markert med forskjellige farger: grønn, gul og rød – og med tilhørende angivelser av løsninger for tilgangsstyring[56]). For det tredje beskrivelser av hvem som skulle utføre eller hadde ansvaret for konkrete arbeidsoppgaver (altså

56 Grønne soner var ment å være allment tilgjengelige, gule soner innebar begrenset tilgjengelighet (for eksempel at bare personer med student- eller ansattkort kom inn) og røde soner innebar strengt begrenset tilgjengelighet (for eksempel at bare utvalgte ansatte hadde tilgang).

en delvis utdyping eller presisering av sikkerhetsorganisering beskrevet i policydokumentene).

Enkelte av de som ble intervjuet rapportert om en viss usikkerhet når det gjaldt håndteringen av de konkrete sikringstiltakene som prinsippdokumentene beskrev eller krevde. Dette hang sammen med at policy- eller prinsippdokumentene (eller begge deler) normalt understreket at alle beslutninger om iverksetting av sikringstiltak skulle basere seg på risikovurderinger. Risikovurderinger skulle altså danne grunnlaget for beslutninger om etablering av nødvendige tiltak for beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet. Spørsmålet var da hvilken status sikringstiltakene som ble beskrevet i prinsippdokumentene faktisk hadde. Skulle de forstås som en form for «grunnsikring», altså tiltak som var så basale og nødvendige at de skulle gjennomføres uavhengig av om det var gjennomført risikovurderinger eller ikke? Var det i så fall meningen at sikringstiltak basert på risikovurderinger skulle komme «på toppen av» kravene om «grunnsikring» skissert i prinsippdokumentene? Eller skulle risikovurderinger (og resultatene fra disse) være bestemmende for (a) om beskrevne sikringstiltak i prinsippdokumentene var nødvendig å gjennomføre eller ikke, og (b) hvordan tiltakene eventuelt skulle utformes? Kort sagt, hva hadde førsteprioritet? Sikringstiltakene beskrevet i prinsippdokumentene eller sikringstiltak basert på risikovurderinger?

Selv om enkelte ga uttrykk for usikkerhet om hvordan disse spørsmålene skulle besvares, rapporterte andre at de enten ikke hadde reflektert over problemstillingen, eller at de oppfattet sikringstiltakene i prinsippdokumentene som en form for «grunnsikring» (og at risikobaserte tiltak var noe som kom i tillegg). Likevel virket statusen til prinsippene, særlig sett i relasjon til bruken av risikovurderinger, å være uavklart i flertallet av institusjonene.

IT-sikkerhet og informasjonssikkerhet

Både i institusjoner med og uten skriftliggjorte styringssystemer, utgjorde de IT-ansatte – eller utvalgte deler av IT-avdelingene/seksjonene – «krumtappen» i arbeidet med informasjonssikkerhet: det var denne gruppen medarbeidere som vanligvis ga arbeidet innhold og retning (også der hvor omfanget av arbeidet var av beskjeden karakter).

Dominansen til og avhengigheten av de IT-ansatte kom klart til uttrykk i den skriftlige styringsdokumentasjonen i de 13 institusjoner hvor dette fantes. Her var det en tendens til at informasjonssikkerhet ble forstått som data- eller IT-sik-

kerhet. Styringsdokumentasjonen avspeilte derfor en bestemt oppfatning av hva som er kjernen i arbeidet med informasjonssikkerhet, det vil si teknisk sikkerhet ved anskaffelser og bruk av IT-systemer eller ved oppgraderinger og drift av teknisk infrastruktur. Oppmerksomheten var følgelig (og med noen få unntak) rettet mot (a) IT-systemer og teknisk infrastruktur snarere enn institusjonenes arbeidsprosesser og (b) det tekniske miljøet informasjonsverdiene befant seg i snarere enn informasjonens «livssyklus» (hvordan informasjon ble håndtert fra første gangs registrering og helt frem til den enten ble slettet, anonymisert, arkivert eller liggende ubrukt).

Vektleggingen av teknisk sikkerhet og IT-løsninger kom også til uttrykk i sikkerhetsorganiseringen, spesielt gjennom fokuset på systemeiere og systemansvarlige. Som nevnt ovenfor, innebar dette stor oppmerksomhet omkring sikring av de viktigste administrative IT-systemene. Også dette avspeilte seg vanligvis i sikkerhetsorganiseringen, for eksempel ved at ledere i sentraladministrasjonen ofte ble eksplisitt utpekt som eiere av fellesadministrative IT-systemer eller dataregistre. Vitenskapelige ledere eller ansatte ble i langt mindre grad tildelt tilsvarende roller og ansvar (men med et visst unntak for medisinske eller helsefaglige forskningsprosjekter).

For mange av de som ble intervjuet var prioriteringen av IT-løsninger og teknisk sikkerhet enten et bevisst valg eller, dersom valget ikke var bevisst, noe som likevel ble oppfattet som hensiktsmessig med tanke på deres faglige ekspertise. Poenget her er at arbeidets forankring i IT-avdelingene/seksjonene førte til at kompetanse og interesser var intimt knyttet til de tekniske sidene av informasjonssikkerheten. Enkelte var for eksempel helt tydelige på at de jobbet med data- eller IT-sikkerhet spesielt og ikke med informasjonssikkerhet generelt. Disse personene oppfattet derfor forskjellen mellom IT-sikkerhet og informasjonssikkerhet som en avgjørende distinksjon – IT-sikkerhet ble fremstilt som noe prinsipielt annet enn informasjonssikkerhet. IT-sikkerhet ble dermed beskrevet som en datafaglig spesialitet, noe som førte til at arbeidet ble plassert innenfor «trygge» teknologiske rammer.

Å drive med informasjonssikkerhet ble beskrevet som en generalistoppgave som oversteg de teknologiske rammene for datasikkerheten og som følgelig omdefinerte hva arbeidet i bunn og grunn handlet om. En slik omdefinering innebar, ifølge de som hevdet dette synspunktet, økt prioritering av ikke-tekniske oppgaver, blant annet holdningsskapende arbeid, informasjonsspredning, etablering av en «sikkerhetskultur» blant ansatte og studenter eller sterkere fokus på juridiske utfordringer (for eksempel inngåelse av avtaler eller kontrakter med eksterne leverandører av IT-løsninger). Dette var oppgaver som de enten mente

at de manglet kompetanse til å løse eller som lå langt fra deres faglige interessefelt (eller begge deler).

Et skifte av fokus fra det ene (IT- eller datasikkerhet) til det andre (informasjonssikkerhet) var noe disse intervjuobjektene i begrenset grad kunne tenke seg. For enkelte av dem virket et slikt fokusskifte å bli betraktet som en form for fremmedgjøring, det vil si at arbeidet ble lite faglig interessant og mindre personlig motiverende.

Nyvinninger og ansvarsplassering

Det var altså en relativt sterk sammenheng mellom den organisatoriske forankring av informasjonssikkerhetsarbeidet (i IT-avdelingene/seksjonene) og forståelsen av kjerneinnholdet i det praktiske arbeidet (fokuset på IT- eller datasikkerhet). Flere av de som ble intervjuet var likevel kritiske til at informasjonssikkerhet i så sterk grad ble assosiert med IT og teknologi. Denne kritikken ble også fremført av enkelte av de som primært ønsket å jobbe med IT-sikkerhet.

Hovedargumentet til kritikerne var todelt. Dels at den organisatoriske forankringen av arbeidet (i IT-avdelingene/seksjonene) førte til at institusjonenes øvrige ledere og ansatte feilaktig oppfattet informasjonssikkerhet som en rent IT-teknisk oppgave. Dels at øvrige lederne og ansatte fritok seg selv for ansvar og ekstraarbeid ved å definere informasjonssikkerhet som en rent IT-teknisk oppgave. Det ble for eksempel rapportert at det ikke var uvanlig at sikkerhetsrelaterte oppgaver ble «dyttet» over på IT-avdelingene/seksjonene, og at de i praksis ble stående som eneansvarlige for informasjonssikkerheten.[57] Blant de som uttrykte denne typen kritiske oppfatninger, virket holdningen å være at IT-avdelingene/seksjonene hadde for stort ansvar for informasjonssikkerheten og at deres rolle og ansvar ideelt sett burde begrenses. Samtidig ble det hevdet at ansvaret og rollene til øvrige ledere og ansatte burde tydeliggjøres og følges tettere opp av toppledelsen. Resultatet av slike spenninger mellom IT-avdelingene/seksjonene og andre ledere/ansatte virket å være at det oppstod en skjevhet i arbeidet med informasjonssikkerhet: IT-sikkerhet ble ivaretatt av IT-avdelingene/seksjonene mens de ikke-tekniske delene av arbeidet ble «hengende i luften» fordi det manglet en tilsvarende organisatorisk og profesjonsspesifikk forankring.

57 Eneansvaret ble oppfattet som særlig problematisk dersom noe «riktig galt» skulle inntreffe, for eksempel at viktige IT-systemer var nede – utilgjengelige – over lengre tid. En vanlig oppfatning var at dersom dette skjedde ville IT-avdelingen/seksjonen bli gjort ansvarlig for problemet, mens det virkelige ansvaret lå hos toppledere som ikke hadde tatt informasjonssikkerheten tilstrekkelig på alvor.

I enkelte institusjoner var spenningene mellom IT-avdelingene/seksjonene og øvrige ledere/ansatte forsøkt løst gjennom ulike typer organisatoriske nyvinninger. Den vanligste nyvinningen var at rollen som ansvarlig for det daglige arbeidet med informasjonssikkerhet (rollen som CISO/CSO eller informasjonssikkerhetsrådgiver) ble løftet ut av IT-avdelingene/seksjonene og plassert noe nærmere den administrative og faglige toppledelsen.[58] Tanken med dette var dels å signalisere at informasjonssikkerhet ikke kun handlet om IT- eller datasikkerhet og dels en oppfatning om at hele bredden i arbeidet best ble ivaretatt ved å plassere det daglige ansvaret utenfor IT-avdelingene/seksjonene. En annen sentral motivasjon virket å være et ønske om å oppgradere viktigheten av oppgaven – å gi arbeidet med informasjonssikkerhet et strategisk løft.

I flere av institusjonene førte slike organisatoriske endringer til at det daglige ansvaret ble ivaretatt av personer med en ikke-teknologisk kompetanseprofil, for eksempel eiendoms-, personal-, organisasjons- eller økonomiledere. På denne måten ble betydningen av overordnet ledelse og styring understreket samtidig som IT-avdelingene/seksjonene fikk konsentrere seg om tekniske sikkerhetsoppgaver. Enkelte uttrykte imidlertid tvil om de nye ansvarlige ville være i stand til å ivareta sine oppgaver på en hensiktsmessig måte: ville de ha tid og motivasjon til dette arbeidet når det kom i tillegg til mange andre og krevende oppgaver som stillingene deres innebar? Dersom dette ikke var tilfelle, ville slike endringer i ansvarsplasseringen virkelig innebære en ny giv i – og sterkere ledelse og styring av – institusjonenes arbeid med informasjonssikkerhet?

Om endringer i ansvarsplasseringen betydde realitetsendringer i arbeidets innhold, det vil si en vridning fra IT-systemer og datateknisk sikkerhet til generell informasjonssikkerhet, virket også å være noe usikkert. Sikkerhetsdokumentasjonen til institusjoner som hadde valgt å løfte det daglige ansvaret ut av IT-avdelingene/seksjonene antydet at fokuset på IT-systemer, teknisk infrastruktur og datasikkerhet var like fremtredende som i de øvrige institusjonene i undersøkelsen. Noen institusjoner virket likevel å ha funnet en større grad av balanse mellom IT-sikkerhet og informasjonssikkerhet enn hva som ellers virket å være vanlig. Men dette syntes ikke primært å skyldes organisatoriske nyvinninger og endringer i ansvarsplasseringen. Det handlet snarere om institusjoner som hadde avsatt flere dedikerte personalressurser til informasjonssikkerhetsarbeidet enn hva som ellers var vanlig: de hadde flere folk som kunne jobbe med informasjonssikkerhet på en bredere front enn hva tilfellet var for flertallet av de

58 I enkelte andre institusjoner ble behovet for nærhet til den administrative og faglige toppledelsen løst uten at det daglige ansvaret ble løftet ut av IT-avdelingene/seksjonene. Dette ble gjort ved at IT-lederen ivaretok rollen som CISO.

kartlagte institusjonene. Dermed kunne de fokusere på andre sider av informasjonssikkerheten enn de rent IT-tekniske.

Dette innebærer at dersom vi ser de 20 institusjonene under ett, virker det korrekt å si at IT-avdelingene/seksjonene fortsatte å være den operative «krumtappen» (og, i de fleste institusjonene, langt på vei den eneste «krumtappen») i arbeidet med informasjonssikkerhet.

Del III: Innføring og drift

Selv om 13 av 20 undersøkte universiteter og høyskoler i noen grad kunne sies å ha skriftliggjorte styringssystemer for informasjonssikkerhet, betyr ikke det at systemene hadde forlatt papiret de var skrevet på, det vil si at de var innført og satt i drift. Ovenfor har vi for eksempel nevnt at enkelte institusjoner som hadde opprettet informasjonssikkerhetsforum rapporterte at forumene enten ikke fungerte slik som beskrevet eller var «sovende» organer. I denne delen av rapporten drøftes derfor følgende problemstillinger: I hvilken grad var de styringssystemene som eksisterte på papiret også en organisatorisk realitet? Var styringssystemene etablert i institusjonene og fungerte de slik som beskrevet? Eller var det vesentlige forskjeller mellom det institusjonene hadde skrevet at de skulle gjøre og det de faktisk gjorde?

Det korte og generelle svaret på problemstillingene er at flertallet av institusjonenes styringssystemer for informasjonssikkerhet først og fremst eksisterte på papiret: dokumentinnholdet var i begrenset grad innført og systemene var i liten utstrekning satt i drift. Isteden kunne det virke som at utarbeidelsen av «informasjonssikkerhetspolicy» og «prinsipper for informasjonssikkerhet» – og å sikre at dokumentene hadde «riktig» form og innhold – var et mål i seg selv snarere enn et første steg på veien mot faktisk fungerende styringssystemer. Det som var festet til papiret og det som ble gjort i praksis var derfor vanligvis to litt forskjellige ting.

Fra ord til praksis

At styringssystemene i begrenset grad hadde forlatt papiret de var skrevet på, var et forhold som flertallet av de som ble intervjuet var innforstått med – de rapporterte at det var til dels betydelige forskjeller mellom dokumentinnhold og institusjonspraksis. Tykkelsen på dokumentbunkene var følgelig en relativt svak indikasjon på (a) om toppledelsen (rektor eller universitets-/høyskoledirektør) faktisk stilte krav til og fulgte opp arbeidet med informasjonssikkerhet og (b) om øvrige ledere og ansatte ivaretok sine oppgaver og sitt ansvar slik som beskrevet i systemdokumentasjonen.

Generelt sett var det altså ikke slik at institusjoner med fyldig og systematisk systemdokumentasjon alltid hadde bedre styring med, et høyere aktivitetsnivå

og iverksatte flere eller mer målrettede sikringstiltak enn institusjoner med fragmentert eller svært lite systemdokumentasjon. Fremfor at systemdokumentasjonen beskrev virkeligheten slik den var, virker det – med visse unntak (se nedenfor) – riktigere å si at dokumentinnholdet var noe de fleste institusjonene hadde forhåpning eller visjoner om å realisere en gang i fremtiden. Samtidig ble det rapportert at langt fra alle ledere og ansatte visste om eller forstod de forhåpningene og visjonene som dokumentene uttrykte.

Sikkerhetsorganiseringen – dokumenter og realiteter

Misforholdet mellom systemdokumentasjon og institusjonspraksis kom spesielt (men ikke bare) til uttrykk gjennom institusjonenes vurderinger av sin egen sikkerhetsorganisering. Gjennomgangsmelodien var at skriftliggjorte sikkerhetsorganisasjoner verken var etablert, aktivisert eller hadde fått tildelt nødvendige ressurser for å ivareta sine oppgaver. Det som i flertallet av institusjonene hadde skjedd var at sikkerhetsorganiseringen var vedtatt, ofte av universitets- eller høyskolestyret. Deretter var den i stor grad blitt glemt eller ignorert av toppledelsen og overlatt til seg selv. I enkelte institusjoner ble det derfor rapportert at nøkkelpersonell i sikkerhetsorganisasjonen, for eksempel systemeiere, ikke var klar over den rollen de hadde i informasjonssikkerhetsarbeidet og hva rollen deres i praksis innebar. Daglig ansvarlige for informasjonssikkerheten i flere av disse institusjoner erkjente også at det ikke fantes en sentral oversikt over hvem som inngikk i sikkerhetsorganisasjonen. Det fantes derfor ingen lister med navn og kontaktinformasjon til de som var pålagt sikkerhetsrelaterte oppgaver og ansvar. Det fantes heller ingen oversikt over hvem som eventuelt hadde utført hvilke oppgaver og når dette eventuelt var gjort. Dermed hadde de fleste institusjonene liten eller ingen samlet status på hvilke aktiviteter som var utført (eller ikke), ut over enkelte konkrete tiltak som IT-avdelingene/seksjonene hadde gjennomført.

Videre mente representanter for flere andre institusjoner det var problematisk å bruke begrepet «sikkerhetsorganisasjon» i det hele tatt. Organisasjonen var, ifølge disse røstene, en ren abstraksjon. Den besto av noen roller (og aktiviteter/oppgaver) som kun eksisterte på et stykke papir, men rollene var ikke fylt med «kjøtt og blod». Organisasjonen bestod altså ikke av ledere og ansatte som kommuniserte med hverandre og koordinerte viktige initiativ; planla og gjennomførte aktiviteter; delte erfaringer og utvekslet kunnskaper.

Dernest var det de som enten mente at sikkerhetsorganiseringen var feil eller uhensiktsmessig oppbygd, for eksempel at det daglige hovedansvaret var tildelt

en leder som verken hadde tid eller kompetanse til å følge opp sitt ansvar (se også diskusjon ovenfor). Andre igjen mente at organisasjonen i noen grad fungerte – enkelte aktiviteter ble utført – men at ulike fakulteter eller institutter gjorde ting på sin spesielle måte. Her ble det blant annet rapportert om fakulteter som forsøkte å gjøre en seriøs innsats for å følge opp sine oppgaver og ansvar, mens institutter under de samme fakultetene ikke gjorde noe som helst. I disse institusjonene ble det derfor hevdet at arbeidet manglet helhet og systematikk – ressursbruk og arbeidsmetodikk var forskjellig fra enhet til enhet og rutiner ble praktisert i varierende grad (eller ikke i det hele tatt). Arbeidet fremstod følgelig som fragmentert – det foregikk stykkevis og delt – og det var problematisk å snakke om en sikkerhetsorganisering med felles mål/strategi, arbeidsmetodikk, forståelse/bevissthet og en styringskraftig ledelse på toppen.

Til sist ble det rapportert om betydelig grad av personavhengighet i et par av de fire institusjonene hvor sikkerhetsorganisasjonen helt eller i noen grad ble hevdet å fungere etter hensikten. Dette var vanligvis mindre institusjoner hvor det ble rapportert at én eller to drivende personer (vanligvis CSO/CISO eller informasjonssikkerhetsrådgiver) hadde hatt betydelig innflytelse på innføring og drift av styringssystemene. Inntrykket her var at det var disse enkeltpersonene – og ikke toppledelsen – som i praksis representerte styrings- og ledelseselementet i sikkerhetsorganiseringen: det var de som forankring arbeidet på ledelsesnivået og det var de som bestemte «tonen på toppen» (formulerte, formidlet, iverksatte og fulgte opp lokale krav til informasjonssikkerhetsarbeidet nedfelt i mål- og strategidokumenter). Det ble imidlertid uttrykt bekymring for at arbeidet kunne falle sammen igjen dersom disse personene (eller den ene personen) skiftet stilling eller sluttet i jobben. Også denne typen forhold – avhengighet av én eller to enkeltpersoner – indikerte at sikkerhetsorganiseringen ikke hadde «bitt seg permanent fast» hos institusjonene.

Et annet illustrerende eksempel på de utfordringene som innføring og drift av styringssystemer stod overfor, var praktiseringen av «indrefileten» i et systematisk og planlagt informasjonssikkerhetsarbeid: risikovurderinger.

Risikovurderinger – begivenhet eller rutine?

Ovenfor er det nevnt at systemdokumentasjonen (til de 13 institusjonene som hadde dette) understreket at sikringstiltak skulle basere seg på risikovurderinger (men at enkelte konkrete tiltak trolig hadde status som «grunnsikring», det vil si at de skulle gjennomføres uten forutgående risikovurderinger). Risikovurderinger var derfor ment å være det viktigste redskapet i disse institusjonenes

informasjonssikkerhetsarbeidet. Det fremgikk dessuten av systemdokumentasjonen at risikovurderinger (spesielt av IT-systemer og teknisk infrastruktur) skulle gjennomføres rutinemessig, for eksempel hvert annet år. Samtidig kunne det være noe uklart hvem som hadde ansvaret for å foreta vurderingene, men i intervjuene ble det rapportert at oppgaven enten var delegert til systemeierne eller linjelederne. CSO/CISO eller informasjonssikkerhetsrådgivere kunne ha som oppgave å bistå systemeiere og linjeledere i den praktiske gjennomføringen av risikovurderinger, eventuelt ta initiativ til at vurderingene ble utført.

Av intervjuene fremgikk det imidlertid at majoriteten av de 13 institusjonene med skriftliggjorte styringssystemer manglet en plan for informasjonssikkerhetsarbeidet, for eksempel årshjul eller årsplan, med konkrete målsettinger og arbeidsoppgaver for perioden. Det vanligste var derfor at det ikke eksisterte planverk for gjennomføringer av risikovurderinger, det vil si klare føringer for hvilke informasjonssystemer eller områder som skulle risikovurderes, hvilke organisatoriske enheter som skulle utføre risikovurderingene og når det var forventet at vurderingene ble gjort. En av konsekvensene av dette var at risikovurderinger i liten grad ble utført på rutinemessig basis. En annen konsekvens var at flertallet av institusjonene rapporterte at de ikke hadde oversikt over hvem som hadde risikovurdert hva og hvilke sikringstiltak som eventuelt var nødvendige. Slik informasjon ble ikke etterspurte av toppledelsen. Toppledelsen manglet derfor viktig informasjon som de, ifølge beskrivelsene av styringssystemet, skulle holdes oppdatert på (via ledelsens gjennomgang) og basere sin styring av arbeidet på.

Med unntak av i fire institusjoner, innebar dette at risikovurderinger best kan beskrives som enkeltstående begivenheter snarere enn plan- eller rutinemessig aktiviteter. Det vanligste virket å være at risikovurderinger ble gjennomført i «skippertakets ånd», ofte initiert av eller utført med assistanse fra ansatte i UNINETT. Når det ble spurt om hvilke eller hvor mange risikovurderinger som var gjennomført ved de ulike institusjonene, svarte flertallet at enkelte vurderinger var utført for noen år siden, og at vurderingene ofte hadde resultert i ulike typer sikringstiltak og nødvendige forbedringer. Dette gjaldt også i noen av de sju institusjonene som ikke hadde skriftliggjorte styringssystemer. Etter at «skippertaket» var gjennomført var det normalt at arbeidet ble stilt i bero.

I flere av institusjonene hvor det ble rapportert at UNINETT hadde bistått med «overordnede risikovurderinger» for en tid tilbake, ble denne assistansen fremhevet som hovedårsaken til at institusjonene hadde fått på plass skriftliggjorte styringssystemer for informasjonssikkerhet. Her ble det samtidig uttrykt et ønske om å følge opp de «overordnede risikovurderingene» med mer detaljerte

vurderinger på utvalgte områder. Det typiske var at dette ønsket ikke var realisert og det var uklart når slike risikovurderinger ville bli utført. Fra enkelte andre institusjoner ble det rapportert om noe mer håndfaste og konkrete planer for fremtidige risikovurderinger, men også her fremstod det som uklart når planene ville bli iverksatt. Til slutt var det noen få institusjoner som mente at risikovurderinger ofte – eller av og til – ble utført ved oppstart av medisinske eller helsefaglige forskningsprosjekter. Det ble rapportert at tilsvarende vurderinger trolig ikke ble gjort i andre typer forskningsprosjekter og i liten grad i de administrative delene av virksomheten.

Mot denne bakgrunn kan bruken av risikovurderinger i de 20 kartlagte institusjonene oppsummeres på følgende måte:

1. Risikovurderinger ble i hovedsak gjennomført i de 13 institusjonene med skriftliggjorte styringssystemer for informasjonssikkerhet. Slike vurderinger ble i mindre grad gjennomført i de sju institusjonene som manglet dette.
2. Likevel – og med unntak av fire institusjoner – var arbeidet med risikovurderinger i disse 13 institusjonene sporadisk og ad hoc. Det var snakk om enkeltstående begivenheter som ofte hadde blitt utført flere år tilbake i tid.
3. Risikovurderinger ble vanligvis ikke initiert eller utført på «egen kjøl». Flertallet av institusjonene hadde fått og var avhengige av ekstern assistanse (primært fra UNINETT).

Det siste punktet – avhengighet av ekstern assistanse – virket dels å være et utslag av manglende egenkompetanse på hva risikovurderinger er og hvordan de kan gjennomføres i praksis. Men samtidig kunne det ligge taktisk vurdering bak ønsker for ekstern assistanse. Flere av de som ble intervjuet mente for eksempel at et viktig hensyn var å sikre at eventuelle forslag til sikringstiltak fikk større legitimitet og gjennomslagskraft i institusjonene (spesielt overfor toppledelsen) enn hva forslagene ville hatt uten dersom de ikke ble utført i samarbeid med eksterne spesialister. Tanken virket altså å være at involveringen av ekstern spisskompetanse ga vurderingene og tiltaksforslagene ekstra tyngde og autoritet i den interne konkurransen om knappe ressurser.

Risikovurderinger fremstod altså som en ad hoc-aktivitet – en prosjektsatsning – som flere institusjoner mente de manglet ressurser, kompetanse eller intern støtte til å gjennomføre på egen hånd. Samtidig virket det som avhengigheten av ekstern spisskompetanse (primært UNINETT) kunne føre til at det ble vanskelig å få kontinuitet i arbeidet med beskyttelse av viktige informasjonsverdier og det miljøet (tekniske, organisatoriske og fysiske) som informasjonsverdiene be-

fant seg i. Generelt sett synes det riktig å si at avhengigheten av eksterne spesialister skapet en viss grad av intern passivitet. Med dette menes at den eksterne assistansen ofte ikke førte til særlig grad av kompetanseoverføring og fungerte i begrenset utstrekning som «hjelp til selvhjelp». Isteden kan det virke som ekstern avhengighet bekreftet eller forsterket en allerede eksisterende oppfatning om at risikovurderinger var noe som mange av institusjonene selv vanskelig kunne få til. På denne måten kunne assistansen – og ideen om ekstern avhengighet og egen utilstrekkelighet – bremse for økt selvstendighet og egne initiativ.

I enkelte institusjoner virket dette å gi seg utslag i relativt store fluktrasjoner i aktivitetsnivået: arbeidet kunne variere mellom «høy topper» (korte perioder med intens aktivitet når ekstern assistanse var tilgjengelig) og «dype daler» (lengre perioder med liten eller ingen aktivitet når ekstern assistanse ikke var tilgjengelig). Likevel var det flere av intervjuobjektene som mente at ekstern assistanse innebar et ikke ubetydelig element av kompetanseoverføring (fra UNINETT til institusjonene), men at institusjonene manglet et «mottaksapparat» til å foredle og nyttiggjøre seg denne kompetansen på en hensiktsmessig måte. I institusjoner som hadde mottatt lite eller ingen ekstern assistanse, ble det vanligvis rapportert at aktivitetsnivået var «stabilt lavt».

Som allerede antydet, virket risikovurderinger å være en integrert del av organisasjonshverdagen i fire institusjoner (i alle fall når det gjaldt deler av institusjonslandskapet). Også enkelte av disse institusjonene hadde fått (og fikk til dels fortsatt) assistanse fra eksterne spesialister (særlig UNINETT). Forskjellen fra de øvrige institusjonene var at den eksterne spisskompetansen i mindre grad fremstod som en nødvendig forutsetning for at risikovurderinger ble planlagt og gjennomført. De virket derfor å ha et «mottaksapparat» som gjorde det mulig for dem å nyttiggjøre seg kompetanseoverføringen og dermed bli forholdsvis selvhjulpne. Eksterne spesialister kunne for eksempel bidra ved de første rundene med risikovurderinger, mens senere runder ble initiert, planlagt og gjennomført av institusjonene selv.

Likevel kunne også noen av disse institusjonene be om ekstern assistanse i spesielle tilfeller, for eksempel dersom det var snakk om risikovurderinger av store og komplekse IT-systemer hvor det var behov for (eller en fordel med) en annen type ekspertise enn hva de hadde tilgjengelig internt. Dette innebar at det bare var én av fire institusjoner som rapporterte at risikovurderinger ble gjennomført

uten noen form for ekstern assistanse, verken fra UNINETT eller private konsulentfirmaer.[59]

Risikovurderinger og sikringstiltak

Selv om risikovurderinger gjennomføres, er det ikke sikkert at det fører til endringer eller forbedringer i informasjonssikkerheten. Det avhenger av om vurderingene følges opp med sikringstiltak på områder hvor dette viser seg nødvendig. Spørsmålet er derfor om institusjonene iverksatte sikringstiltak i kjølvannet av risikovurderingene eller om behovet for slike tiltak ble ignorert?

Sammenhengen mellom risikovurderinger og sikringstiltak var en problematikk som ble nevnt av flere av intervjuobjektene. Dette gjaldt også i én av de fire institusjonene som helt eller delvis rapporterte at de hadde fungerende styringssystemer og hvor risikovurderinger derfor ble gjennomført relativt rutinemessig (i alle fall i deler av institusjonene). I denne institusjonen ble det blant annet stilt spørsmålstegn ved poenget med å gjennomføre risikovurderinger når de, ifølge denne respondenten, ble lagt til siden så fort vurderingene var sluttført. Oppfatningen var at risikovurderinger ble gjennomført som en slags formalistisk øvelse, det vil si noe som ble gjort fordi lovverket krevde det (personopplysningsloven med forskrift) eller fordi dokumentasjon på risikovurderinger ble etterspurt av Kunnskapsdepartementet. Det ble videre hevdet at uønskede hendelser med så høy risikofaktor at det var behov for sikringstiltak (eller der hvor sikringstiltak burde vurderes), ble notert og kommentert, men ut over dette skjedde lite eller ingenting. I en annen av institusjonene med helt eller delvis fungerende styringssystemer, ble det rapportert at det nettopp var gjennomført en omfattende prosess med risikovurderinger. Samtidig var det usikkerhet knyttet til om nødvendige sikringstiltak ville bli iverksatt, spesielt tiltak som hadde en ikke neglisjerbar økonomisk utgiftsside. Også andre institusjoner mente at oppfølgingen av resultater fra risikovurderinger var problematisk: veien fra vurderinger til etablering av tiltak ble beskrevet som lang og til dels lite farbar.

Bildet var likevel ikke entydig. I noen av institusjoner ble det rapportert at resultatene ble tatt på alvor og at selv relativt kostbare sikringstiltak var innført i etterkant av vurderingene, for eksempel bygningsmessige endringer for å beskytte data- og serverrom eller investeringer i nye kjøleanlegg. Ovenfor har vi sett at

59 I denne institusjonen ble det hevdet at det kunne være behov for en viss assistanse utenifra, men at toppledelsen mente at man skulle være helt selvhjulpen på informasjonssikkerhetsområdet.

dette var tilfelle i institusjoner hvor risikovurderinger var «en begivenhet» og ble utført med assistanse fra eksterne eksperter.

Disse funnene indikerer at det ikke nødvendigvis er slik at institusjoner som hyppigst utfører risikovurderinger også iverksatte flere eller mer målrettede og effektive sikringstiltak enn de øvrige institusjonene. Dersom dette ikke er tilfelle (noe resultatene kan indikere), kan det skyldes flere forhold. Det kan for eksempel tenkes at sikringstiltak ikke etableres simpelthen fordi risikovurderingene viser at det ikke er behov for nye tiltak – informasjonssikkerheten er uansett tilfredsstillende. Men dersom intervjuobjektenes oppfatninger legges til grunn, er det mer sannsynlig at manglende sammenheng mellom vurderinger og tiltak skyldes tre andre forhold:

- For det første, og som nevnt ovenfor, at det var en tendens til at risikovurderinger ble oppfattet som en formell øvelse. Vurderingene ble dermed et mål i seg selv, og når vurderingene var utført var også hensikten med aktiviteten oppnådd. Derfor ble ikke vurderingene alltid fulgt opp med sikringstiltak.
- For det andre at enkelte institusjoner iverksatte sikringstiltak selv om de ikke baserer tiltaksetableringen på risikovurderinger. Dette kunne være tilfelle i en del institusjoner som så på tiltakene i prinsippdokumentene som en form for «grunnsikring». Det samme var tilfelle i institusjoner som manglet skriftliggjorte styringssystemer for informasjonssikkerhet. Her var det ofte iverksatt en rekke tekniske sikringstiltak som ble oppfattet som «standard» eller «helt vanlige», for eksempel beskyttelse av tilganger til ulike IT-systemer (brukernavn og passord).[60]
- For det tredje at flertallet at institusjonene som rapporterte at risikovurderinger var utført manglet et systematisk informasjonssikkerhetsarbeid. Mangelen på planmessighet og systematikk kunne føre til at sammenhenger mellom sentrale aktiviteter, blant annet risikovurderinger og tiltaksgjennomføring, ikke var etablert eller ikke ble tatt på alvor.

Forebygging og gjenoppretting

Antallet risikovurderinger var altså ikke alltid en god indikasjon på om sikringstiltak ble etablert, om styringssystemer for informasjonssikkerhet faktisk fungerte slik som tenkt og om grunntankene i risikostyrt informasjonssikker-

60 Her kunne det virke som iverksetting av tekniske sikringstiltak – og vurderinger av behovet for disse – var en integrert del av den daglige IT-driften, det vil si at tiltakene ble etablert uten formaliserte og dokumenterte risikovurderinger.

het var forstått. Drøftelsene så langt virker isteden å indikere at risikovurderinger var relativt isolerte aktiviteter som i begrenset utstrekning var en integrert del av et større og mer helhetlig styringssystem. Samtidig førte dette til at arbeidet med informasjonssikkerhet ikke alltid kunne defineres som forebyggende. Med forebyggende arbeid menes at institusjonene anvendte risikovurderinger for (så godt det lot seg gjøre) å foregripe og være i forkant av uønskede hendelser istedenfor å iverksette gjenopprettende tiltak etter at «uhellet var ute.»

Flere av de som ble intervjuet mente at arbeidet med informasjonssikkerhet fortsatt bestod i å avhjelpe problemer etter hvert som de oppstod snarere enn å minske sannsynligheten for eller konsekvensene av uønskede hendelser før de oppstod. Disse røstene hevdet at selv om risikovurderinger ble gjennomført og enkelte sikringstiltak iverksatt, løp de fortsatt fra det ene «overraskende branntilløpet» til det neste. Til sammen indikerer dette at grunntanken i risikostyrt informasjonssikkerhetsarbeid i begrenset grad (og med enkelte unntak) hadde slått rot på institusjonsnivå: selv om risikovurderinger ble foretatt garanterte ikke det at arbeidet ble preget av samme planmessighet og forutsigbarhet som den skriftliggjorte systemdokumentasjonen beskrev.

Datatilsynets kontrollrapporter

Datatilsynets kontrollrapporter fra stedlige tilsyn ved universiteter og høyskoler (i perioden 2001-2013) synes å bekrefte inntrykket av at styringssystemer som eksisterte på papiret hadde begrenset betydning for den daglige håndteringen av informasjonsverdier (personopplysninger). I enkelte kontrollrapporter kunne institusjonene få anerkjennelse for å ha etablert et styringssystem (eller internkontrollsystem) – og at styrende, gjennomførende og kontrollerende elementer kunne finnes igjen i dokumentasjonen. Institusjonene fikk like fullt kritikk for mangelfull implementering av systemene på fakultets- og instituttnivå. I én av kontrollrapportene skriver Datatilsynet følgende:

> Det presiseres at plikten ikke bare gjelder etablering av et styringssystem, men også å håndheve det i organisasjonen (…) Videre tilråder tilsynet at det skapes klarere rammer rundt ansvar og myndighet i relasjon til internkontroll. Det sentrale er å stadfeste hvem det er som håndhever pliktene nedover i organisasjonen.[61]

Sitatet indikerer at innføring og håndheving er større utfordringer enn selve etableringen av styringssystemer for informasjonssikkerhet. Det er disse utfordringene som er tematikken i neste del av rapporten.

61 Endelig kontrollrapport fra NTNU/NSEP, 20.04.2010, s. 14.

Del IV: Utfordringer

Drøftelsene ovenfor indikerte at flertallet av de 13 institusjonene som hadde skriftliggjort sine styringssystemer for informasjonssikkerhet, virket å ha til dels betydelige utfordringer med å overføre styringssystemene fra papiret de var skrevet på til den organisatoriske virkeligheten de var ment å fungere i. Det reiser spørsmålet om hva som kan forklare den mangelfulle sammenhengen mellom ord og praksis. Problemstillingene som drøftes i denne delen av rapporten er derfor følgende: Hva kan være årsakene til at styringssystemer for informasjonssikkerhet var utfordrende å innføre og drifte? Hvilke forhold pekte institusjonene selv på som særlig problematiske ved innføring og drift av styringssystemene?

På bakgrunn av intervjuene med representanter for universiteter og høyskoler, var det fire forhold som utkrystalliserte seg som særlig viktige for å forklare sammenhengen mellom ord og praksis. Disse forholdene var:

1. Ressurser som institusjonene brukte på innføring og drift av styringssystemer for informasjonssikkerhet.
2. Virkemidler som de daglig ansvarlige for arbeidet med informasjonssikkerhet (CSO, CISO eller informasjonssikkerhetsrådgiver) hadde til rådighet.
3. Kjennetegn ved selve styringssystemene.
4. Kjennetegn ved institusjonene.

Nedenfor drøftes først hvordan ressurser og prioriteringer kunne påvirke arbeidet med innføring og drift av styringssystemene. Deretter diskuteres hvordan institusjonenes virkemiddelbruk og hvilke kjennetegn ved styringssystemene som kunne skape utfordringer i overgangen fra ord til praksis. Til slutt drøftes hvordan ulike organisatoriske og kulturelle kjennetegn ved institusjonene kunne påvirke betingelsene for innføring og drift av systemene.

Ressurser

Flertallet av intervjuobjektene mente at en viktig forklaring på institusjonenes utfordringer med innføring og drift av styringssystemer for informasjonssikkerhet – og dermed til misforholdet mellom dokumentinnholdet og institu-

sjonspraksis – ikke bare (eller først og fremst) handlet om holdninger og oppmerksomhet blant ledere og ansatte. Holdninger og oppmerksomhet var isteden forklaringer som selv trengte forklaring: hvorfor var det ofte slik at ledere og ansatte var lite opptatt av, kjent med og oppmerksom på arbeidet med informasjonssikkerhet?

Forklaringene på holdninger og oppmerksomhet ble i første rekke knyttet til forskjellige typer ressursbegrensninger. Mange intervjuobjekter hevdet at ressursinnsatsen var for svak sammenliknet med behovet, men at toppledelsen vanligvis ikke var villig til å prioritere arbeidet ut over dagens nivå. Samtidig var det enkelte med ansvar for det daglige informasjonssikkerhetsarbeidet (CISO/CSO eller informasjonssikkerhetsrådgivere) som mente at de selv hadde vært for beskjedne når det gjaldt å påpeke ressursbehovene, og at dette kunne være en medvirkende årsak til at arbeidet ble utilstrekkelig prioritert. Hva innebar så denne ressursmangelen – hvilke ressurser var det flertallet av intervjuobjektene mente at institusjonene manglet?

Utgangspunktet her er at det finnes flere ulike måter å måle ressursinnsatsen på. Én målemetode kan for eksempel være å si at alle som inngår i sikkerhetsorganisasjonen jobber (eller er ment å jobbe) med informasjonssikkerhet. Hvem og hvor mange som formelt sett har sikkerhetsrelaterte oppgaver kan dermed brukes som et mål på ressursinnsatsen. Men drøftelsene ovenfor – og intervjuene på institusjonsnivå – indikerer at denne målemetoden i beste fall gir et misvisende bilde av den faktiske situasjonen: «alle» som «i teorien» inngår i sikkerhetsorganisasjonen jobber ikke med informasjonssikkerhet. En mer realistisk målemetode er derfor å anvende en kombinasjon av ulike ressursindikatorer. De viktigste som ble nevnt av intervjuobjektene var disse:

1. Stillinger: antallet stillinger som hver institusjon hadde dedikert – helt eller delvis – til arbeidet med informasjonssikkerhet.
2. Kompetanse: den kunnskapen (eller mangelen på sådan) som institusjonene forvaltet når det gjaldt praktisk informasjonssikkerhetsarbeid.
3. Tid: hvor mye tid ledere og ansatte med viktige roller i sikkerhetsorganisasjonen hadde anledning til å bruke på sikkerhetsrelaterte oppgaver (i konkurranse med deres «ordinære» arbeidsoppgaver).

Dedikerte stillinger

Det var i første rekke mangelen på dedikerte stillinger som flertallet av intervjuobjektene selv siktet til når det ble spurt om ressurser og prioriteringer. Institusjoner med og uten skriftliggjorte styringssystemer rapporterte at antallet dedikerte stillinger varierte fra omkring seks/sju til godt i underkant av én. De-

dikerte stillinger inkluderte både (a) lederen for det daglige informasjonssikkerhetsarbeidet (CSO/CISO eller informasjonssikkerhetsrådgivere) og (b) andre ansatte, spesielt i IT-avdelingene/seksjonene, som på ulike måter jobbet (helt eller delvis) med teknisk sikkerhet (datasikkerhet). Ikke overraskende var det de største institusjonene som brukte flest personalressurser på informasjonssikkerhet, men det var også i disse institusjonene at arbeidet var mest omfattende og komplekst, spesielt på grunn av det store mangfoldet av fakulteter og grunnenheter (se også diskusjon nedenfor).

I tillegg til de dedikerte stillingene kom deltakelsen til andre ledere og ansatte i gjennomføringen av ulike typer sikkerhetsaktiviteter, for eksempel risikovurderinger eller ved etablering av sikringstiltak. Til tross for visse variasjoner på tvers av institusjonene, fremstod bidraget fra ledere og ansatte utenfor IT-avdelingene/seksjonene generelt sett som relativt beskjedent. Likevel ble det rapportert at også andre avdelinger jobbet med informasjonssikkerhet, for eksempel eiendomsavdelinger eller arkivansatte, men det var uklart hvor stor denne innsatsen eventuelt var.

Det er likevel verdt å legge merke til at de fleste institusjonene hadde utpekt egne daglige ledere for informasjonssikkerhets- eller IT-sikkerhetsarbeidet. Noen institusjoner hadde også etablert rådgivende stillinger for det generelle sikkerhets- og beredskapsarbeidet. Hos flere av institusjonene var dette en ny utvikling, og innebar en viktig styrking av ressursinnsatsen sammenliknet med hva situasjonen hadde vært for bare noen få år tilbake. Prioriteringene når det gjaldt dedikerte stillinger var derfor ikke på «nullpunktet», og ressursinnsatsen virket å ha blitt styrket i løpet av de siste årene.

Til tross styrket innsats, ble det rapportert at prioriteringen av dedikerte stillinger ikke holdt tritt med det reelle behovet, og at dette blant annet hang sammen med et ønske om å holde antallet administrativt ansatte på dagens nivå. Samtidig mente flertallet av intervjuobjektene at misforholdet mellom ressurser og behov hadde økt i den senere tiden. Bakgrunnen for dette synspunktet var at selv om antallet dedikerte stillinger hadde økt noe, hadde kravene til styring av arbeidet med informasjonssikkerhet økt i enda sterkere grad (først og fremst fra aktører som Riksrevisjonen og Kunnskapsdepartementet). Dessuten var utfordringene langt større enn tidligere, noe som i særlig grad ble forklart med økt bruk av bærbare dataenheter og nettbaserte tjenester (spesielt skytjenester). Dermed hadde ikke ressursinnsatsen på stillingssiden holdt tritt med de forventningene og utfordringene som institusjonene i økende utstrekning opplevde å bli stilt overfor.

Enkelte med CSO/CISO-oppgaver ga uttrykk for at dette misforholdet satte dem i en vanskelig posisjon: De var i det daglige ansvarlige for informasjonssikkerheten, men mente samtidig at de ikke fikk rammebetingelser som stod i et rimelig forhold til omfanget av det ansvaret de skulle ivareta. Spørsmålet disse intervjuobjektene stilte var hva som ville skje dersom en alvorlig sikkerhetshendelse inntraff. Ville ledelsen fraskrive seg ansvaret og legge skyld og ansvar på CSO/CISO: «vi har gjort vårt – vi har opprettet en egen stilling for dette – men har vår sikkerhetsansvarlig gjort jobben sin?» Eller ville ledelsen erkjenne manglene og forbedre rammebetingelsene (øke ressursinnsatsen)?

Kompetanseheving og opplæring

Den andre utfordringen som ble nevnt som viktig, gjaldt prioriteringer av ressurser til kompetanseheving og opplæring av ledere og ansatte. Her ble det hevdet å være et stort misforhold mellom behovet for kompetanse og den kompetansen som institusjonene faktisk forvaltet, spesielt sett i lys av de senere årenes økte krav og forventninger til arbeidet med styring av informasjonssikkerhet.

Det ble hevdet at institusjonene generelt sett gjorde lite for å minske dette misforholdet, det vil si å tilføre nødvendig kompetanse til ledere og ansatte med ansvar for viktige sikkerhetsoppgaver. I enkelte institusjoner ble det riktignok rapportert om at det forekom noe opplæring av administrativt ansatte i sentraladministrasjonen og på fakultets- eller grunnenhetsnivå. Men den opplæringen det her var snakk om handlet ikke først og fremst om informasjonssikkerhet eller hvilke rettslige krav som gjaldt for institusjonene (for eksempel sikker håndtering av informasjonsverdier, kursing i risikostyringsmetodikk eller innføring i regelverk for informasjonssikkerhet/personvern). Det dreide seg isteden om tradisjonell brukeropplæring, altså kursing i praktisk anvendelse av administrative IT-systemer eller elektroniske arbeidsverktøy. Noen av intervjuobjektene mente likevel at det var mulig at kursingen også omfattet visse sikkerhetsrelaterte aspekter, for eksempel håndtering av brukernavn og passord, men at de var usikre på dette. Også vitenskapelige ansatte kunne bli tilbudt kurs i bruk av IT-systemer eller elektroniske arbeidsverktøy, men heller ikke her ble det rapportert at informasjonssikkerhet (eller personvern) inngikk i kursopplegget.

I enkelte andre institusjoner ble det hevdet at opplæring, både når det gjaldt brukeropplæring generelt og informasjonssikkerhet/personvern spesielt, ikke ble prioritert i det hele tatt (verken når det gjaldt administrativt eller vitenskapelige ansatte). Manglende tilbud om kompetanseheving og opplæring inkluderte også ledere eller ansatte med det daglige ansvaret for informasjonssikkerheten. I noen få institusjoner ble det meldt om at slike ledere eller ansatte nylig hadde

deltatt på eksterne kurs, hvor de blant annet hadde fått grunnleggende innføring i internasjonale standarder for styringssystemer for informasjonssikkerhet (ISO/IEC 27001: 2013). Dette var enten gratis kurs arrangert i regi av Direktoratet for forvaltning og IKT, eller konferanser og seminarer som UNINETT organiserte. I tillegg rapporterte noen få institusjoner om at enkelte ansatte som hadde deltatt på kurs i regi av Datatilsynet.[62] Inntrykket av den samlede kurs- og opplæringsvirksomheten var likevel at den enten var ikke-eksisterende eller omfattet et lite mindretall av de som hadde behov for kompetanseheving i informasjonssikkerhet.

Etter som kompetanseheving og opplæring i informasjonssikkerhet/personvern – der hvor slike tilbud ble gitt – rettet seg mot noen relativt få ledere og ansatte, primært de med daglig ansvar for informasjonssikkerheten, var ikke resultatet bare at det oppstod et misforhold mellom behovet for kunnskap og den kunnskapen som institusjonene faktisk forvaltet. Resultatet syntes i tillegg å være at den kunnskapen som eksisterte var skjevfordelt internt: den var sentralisert i noen få hoder istedenfor å være distribuert til alle de som, ifølge sikkerhetsorganiseringen, skulle utføre viktige oppgaver. Svært mange av de som ble intervjuet mente derfor at mangelfullt distribuert kompetanse førte til at ledere og ansatte som inngikk i sikkerhetsorganisasjonen var lite selvstendige – de var avhengige av sentrale ressurser for å ivareta sine oppgaver. Men fordi de sentrale ressursene også var begrenset (se drøftelsen av dedikerte stillinger ovenfor), ble den manglende selvstendigheten i resten av institusjonslandskapet en flaskehals i arbeidet med informasjonssikkerhet. De sentrale ressursene hadde simpelthen ikke kapasitet til å bistå alle de som hadde behov for eller som etterspurte bistand (og alle de som ikke etterspurte bistand, men likevel hadde behov for det). Oppfatningen var derfor at utfordringen ikke bare handlet om å tilføre institusjonene mer kompetanse, men at det også handlet om at kompetansen måtte fordeles internt på en annen måte enn hva som var tilfelle nå. Dersom dette ikke skjedde, det vil si at den kompetansen som fantes fortsatte å være sentralisert, ble det dels uttrykt frykt for at viktige oppgaver aldri ville bli utført og dels at arbeidet ville bli for personavhengig.

Tid

Den tredje ressursen som det ble rapportert om knapphet på, var tid. Ovenfor har vi sett at tid ble oppfattet som en kritisk faktor i enkelte institusjoner hvor rollen som CSO eller CISO eller var tildelt avdelingsledere i sentraladministra-

62 Her dreide det seg om opplæring av personvernombud, det vil si en uavhengig ressursperson som skal se til at institusjonenes behandling av personopplysninger skjer i henhold til reglene i personopplysningsloven med forskrift. Personvernombudsordningen er frivillig, men ombudenes oppgaver reguleres i personopplysningsforskriften (§ 7-12). Bestemmelsene om informasjonssikkerhet er en del av denne opplæringen.

sjonen: ville arbeidet med styring av informasjonssikkerheten tape i kampen om ledernes tid og oppmerksomhet når informasjonssikkerhet trolig ikke ble oppfattet som en av deres kjerneoppgaver? Tilsvarende synspunkter ble uttrykt når det gjaldt fakultets- og instituttledelsen og ledere i forskningsprosjekter (spesielt med hensyn til ikke-medisinsk forskning). I hvilken grad ville disse aktørene oppfatte arbeidet med informasjonssikkerhet som en unødvendig distraksjon – noe som stjal tid fra deres kjerneoppgaver (forskning, undervisning, administrasjon, osv.)?

Noen av intervjuobjektene mente imidlertid at tid nok kunne være en begrensende faktor på ledelsesnivået, men at det samme ikke i like stor grad var tilfelle blant administrativt eller vitenskapelige ansatte. Det ble derfor hevdet at majoriteten av administrativt og vitenskapelige ansatte både kunne finne tid og anledning til å utføre sikkerhetsoppgaver dersom institusjonene stilt strengere krav om det. Disse røstene mente samtidig at det kunne være en sammenheng mellom kunnskapen om informasjonssikkerhet og oppfatningen om at arbeidet var for tidkrevende. Her ble det hevdet at jo mindre kompetanse og egen erfaring ledere/ansatte hadde med det praktiske arbeidet, desto større var sannsynligheten for at det ble sett på som en distraksjon eller «tidstyv». De hevdet derfor at mer kompetanse og opplæring ikke bare var ønskelig for å få «ting gjort». Kompetanse og opplæring kunne også påvirke oppfatningen om informasjonssikkerhet som en aktivitet fjernt fra kjerneoppgavene og som stjal tid fra «ordinære oppgaver».

Til tross for at tid ble ansett som en viktig knapphetsressurs, var det svært få institusjoner som rapporterte at de hadde oversikt over den samlede innsats og tidsbruk på informasjonssikkerhetsområdet. Den innsatsen og tidsbruken som ble rapportert knyttet seg hovedsakelig til IT-avdelingene/seksjonene og CSO/CISO (eventuelt informasjonssikkerhetsrådgiveren). Når det gjaldt øvrige avdelinger/seksjoner, ledere og ansatte, var anslagene mer usikre og bar til dels preg av ren gjetning. Majoriteten av institusjonene mente likevel at innsatsen og tidsbruken var minimal eller ikke-eksisterende. Noen institusjoner mente at tidsbruken var nokså begrenset (og størst innenfor deler av sentraladministrasjonen og i medisinsk/helsefaglig forskning), mens svært få institusjoner mente at tidsbruken var tilfredsstillende (uten at dette ble nærmere spesifisert).

Tekniske tiltak

Selv om dedikerte stillinger, kompetanse og tid ble oppfattet som begrensninger i arbeidet med innføring og drift av styringssystemer for informasjonssikkerhet, ble det pekt på ett område hvor viljen til prioritering og ressursbruk generelt sett var vesentlig større. Dette handlet om ledelsens vilje til å avsette penger til iverk-

setting av konkrete tekniske sikringstiltak: her satt ressursene (penger) løsere enn dersom det ble spurt om flere stillinger eller nye opplæringstiltak. Det kunne derfor virke som institusjonsledelsen hadde større forståelse for investeringer i ulike typer maskin- og programvare – brannmurer, virusprogrammer, spamfiltre, osv. – enn i stillinger, kompetanseheving og opplæring. Dette var likevel ikke ressurser som gikk til innføring eller drift av styringssystemer. Isteden handlet det primært om ressurser til konkrete tiltak som IT-avdelingene/seksjonene fikk tildelt over sine ordinære budsjetter. Ressurser til slike tekniske tiltak virket følgelig å være en del av den ordinære IT-driften snarere enn et utslag av et planmessig informasjonssikkerhetsarbeid innenfor rammen av et styringssystem.

Virkemidler

Flere av virkemidlene som institusjonene hadde til rådighet i arbeidet med informasjonssikkerhet generelt, og innføring og drift av styringssystemer for informasjonssikkerhet spesielt, er allerede drøftet. Dette gjelder tiltak som kompetanseheving og opplæring (pedagogiske virkemidler), fordeling av ansvar og oppgaver i tilknytning til sikkerhetsarbeidet (organisatoriske virkemidler) og prioritering av penger til konkrete tekniske sikringstiltak (økonomiske og tekniske virkemidler). Drøftelsene nedenfor handler om de virkemidlene som daglig ansvarlige for informasjonssikkerheten rapporterte at de hadde til rådighet i sitt arbeid med innføring og drift av styringssystemer for informasjonssikkerhet.

Ingen av de daglig ansvarlige for informasjonssikkerheten som ble intervjuet rapporterte at de forvaltet «harde» virkemidler. Dette innebar at de i praksis hadde begrenset myndighet til å instruere avdelinger i sentraladministrasjonen, fakulteter, grunnenheter eller andre enheter om å ivareta sitt ansvar og sine oppgaver. I institusjoner med skriftliggjorte styringssystemer kunne det riktignok være slik at toppledelsens myndighet og ansvar var delegert til den daglig ansvarlige for arbeidet. Delegasjonen omfattet normalt en viss instruksjonsmyndighet, men inntrykket var at myndigheten var «sovende» og eksisterte i hovedsak på papiret. Derfor ble den i praksis sjelden eller aldri brukt.

Problemet med delegert instruksjonsmyndigheten virket dels å være at delegasjonen var lite kjent utover i institusjonslandskapet. Derfor manglet den aksept og legitimitet blant mange av de som i teorien kunne instrueres. Dels at enkelte daglig ansvarlige virket å være lite bevisst på den instruksjonsmyndigheten de selv (ifølge sikkerhetsorganiseringen og delegasjon) forvaltet. Dels at

det ble oppfattet som lite hensiktsmessig å instruere ledere og ansatte når de manglet forutsetninger (spesielt kompetanse) til å utføre det de ble instruert om. Og dels at det virket å eksistere en viss motvilje mot å bruke den instruksjonsmyndigheten som de daglig ansvarlige (eventuelt) forvaltet.

Likevel var det enkelte daglige ansvarlige som rapporterte at de anvendte «instruksjonsliknende» metoder, og som derfor var mer bevisste på bruken av denne typen virkemidler enn hva som fremstod som vanlig blant de 20 undersøkte institusjonene. Her kunne det for eksempel dreie seg om at avdelingsledere ble bedt om å rapportere hvilke tiltak de hadde iverksatt for å forbedre informasjonssikkerhet, eller om å gjøre rede for om avtalte aktiviteter var utført. Det var imidlertid relativt få av de daglig ansvarlige som rapporterte at de jobbet på denne måten. Og de som rapporterte om det mente at det var vanskelig å basere arbeidet på instruksjon eller instruksjonsliknende virkemidler – man risikerte å skape større misnøye og motstand mot snarere enn økt forståelse for arbeidet med informasjonssikkerhet.

Dette innebar at de virkemidlene som typisk ble brukt, må kunne defineres som «myke» og pedagogiske: det handlet i hovedsak om informering, rådgiving og bistand. Mange institusjoner hadde for eksempel egne sider på internett som informerte om styringssystemet, trusler mot informasjonssikkerheten eller de rutiner og prosedyrer som fantes for sikker håndtering av informasjonsverdier. Informasjonen på internett kunne samtidig omfatte en rekke andre og tilstøtende tema, for eksempel hvilke regler som gjaldt for bruk av rettighetsbeskyttet materiale (videoer, tekster, bilder, osv.) eller generelle krav som ble stilt til håndtering av personopplysninger. Det var også vanlig at brukerne (ansatte og studenter) ble informert via e-post dersom det ble avdekket akutte trusler mot informasjonssikkerheten, for eksempel advarsler mot å åpne vedlegg i e-poster som inneholdt datavirus eller som forsøkte å lure brukerne til å oppgi kredittkortnumre eller andre personlige opplysninger. Til slutt var det enkelte institusjoner som deltok på årlige sikkerhetskampanjer i regi av nasjonale myndighetsorganer (se drøftelse nedenfor).

Det ble rapportert at det var vanskelig å se eventuelle effekter av denne virkemiddelbruken. Om informasjonstiltak og kampanjer hadde noen virkning (eller ikke) stod derfor igjen som et ubesvart spørsmål. Det syntes likevel lite trolig at de hadde særlige effekter på innføring og drift av styringssystemer for informasjonssikkerhet. I så fall var det å forvente at innføringen og driften av systemene hadde vært noe mindre utfordrende enn hva som virket å være tilfelle i flertallet av institusjonene. Heller ikke de daglig ansvarlige for informasjonssikkerheten trodde at informasjon og kampanjer hadde hatt effekt på styringssystemene. Det

ble isteden festet lit til at virkemiddelbruken kunne ha andre effekter, for eksempel å øke brukernes generelle bevissthet om informasjonssikkerhet (og tilstøtende tema som opphavsrett og personvern).

Det virkemidlet som ble rapportert å ha størst effekt når det gjaldt styringssystemet for informasjonssikkerhet, var rådgiving og bistand (tilrettelegging) ved gjennomføring av konkret arbeidsoppgaver, for eksempel risikovurderinger, utarbeidelse av beredskapsplaner eller iverksetting av sikringstiltak. Det ble hevdet at denne virkemiddelbruken ikke bare førte til at oppgaver faktisk ble utført. Den bidro også til intern kompetanseoppbygging, og til å «avmystifisere» og å skape større aksept for arbeidet med informasjonssikkerhet (se også diskusjon i neste del av rapporten). Det var imidlertid relativt store variasjoner mellom institusjonene når det gjaldt rådgivings- og bistandsaktiviteten. I enkelte institusjoner foregikk ikke dette i det hele tatt. Her var informasjonssikkerhet en «intern affære» for IT-avdelingene/seksjonene, det vil si at fokuset begrenset seg til IT- eller datasikkerhet. I andre institusjoner ble det drevet en viss intern rådgiving og bistand.

Selv om flere institusjoner rapportert om positive erfaringer med denne virkemiddelbruken, hadde den sine begrensninger. For det første var det enkelte som ga uttrykk for at råd og bistand tok mye av den daglig ansvarliges tid. Dette var særlig en utfordring i litt større institusjoner (mange som kunne trenge råd og bistand) og i institusjoner hvor den daglig ansvarlige også var forventet å utføre andre oppgaver (begrenset hvor mye råd og veiledning som kunne gis). For det andre rapportert en del institusjoner om relativt få tilfeller hvor ledere eller ansatte aktivt ønsket rådgiving og bistand. I disse institusjonene virket det isteden å være at den daglig ansvarlige som selv initierte aktiviteter hvor han/hun bistod med råd og assistanse. Samtidig ble det hevdet at langt fra alle avdelinger, fakulteter eller grunnenheter ønsket råd og bistand fra sentralt institusjonshold når de fikk tilbud om det.

Få henvendelser om råd og bistand ble vanligvis ikke tolket som uttrykk for aktiv motstand mot arbeidet med informasjonssikkerhet: det var bare et par institusjoner som meldte om åpen kritikk fra eller uttalt misnøye blant ledere og ansatte (nedenfor skal vi flere steder se at skepsisen til styringssystemene trolig var noe mer utbredt enn hva disse synspunktene gir inntrykk av).[63] Ifølge flertallet av intervjuobjektene, handlet det primært om det som kan karakteriseres

63 Dette er et noe overraskende funn. Tilsvarende undersøkelser i kommunal forvaltning avdekket en ikke ubetydelig grad av åpen kritikk og uttalt misnøye, se Tommy Tranvik (2012): «Kommunal regeletterlevelse: Realiteter og illusjoner på personvernområdet». *Tidsskrift for samfunnsforskning*, nr. 2, s. 131-156, og Tommy Tranvik (2009): *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor.* Oslo: Unipub.

som passiv motstand, det vil si at tilbud om råd og bistand (spesielt til fakulteter eller grunnenheter) ble ignorert i det stille eller raskt glemt. Bare det å skaffe seg tilgang til interne arenaer eller møteplasser hvor slike tilbud kunne presenteres, ble beskrevet som en ikke ubetydelig utfordring som kunne kreve både tid og tålmodighet. Slike vanskeligheter ble tolket som utslag av at ledere og ansatte hadde såpass liten kompetanse på området at de ikke visste (eller ikke var nok bevisst på) at informasjonssikkerhet var en oppgave som også omfattet dem selv. Oppfatningen var ofte at «sikkerhet har vi egne folk til å ta seg av, så det har ikke noe med meg/oss å gjøre». Rådgiving og bistand til konkrete oppgaver var derfor ikke et «universalmiddel», men fremstod isteden som det beste alternativet blant flere mindre effektive virkemiddelvalg.

Det virker sannsynlig at virkemiddelbruken både ble påvirket av kjennetegn ved styringssystemene – og måten de ble «markedsført» internt på – og egenskaper ved institusjonene selv (organisering og kultur). I de to neste hovedavsnittene drøftes hvordan disse faktorene – egenskaper ved styringssystemene og institusjonene selv – påvirket innføring og drift av styringssystemer for informasjonssikkerhet.

Egenskaper ved styringssystemene

Vi har tidligere sett at sikkerhetsdokumentasjonen varierte en del i omfang mellom de 20 institusjonene som ble undersøkt. Enkelte institusjoner hadde for eksempel svært omfattende dokumentasjon (fordelt på mange dokumenter), andre nøyde seg med noe mindre (fordelt på et par dokumenter) og noen hadde lite eller ingenting. Det som var felles for mye av dokumentasjonen var at den var nokså spesialisert, det vil si at den både var preget av «IT-terminologi» og sikkerhetsfaglig begrepsbruk. Dette var ikke bare tilfelle i institusjoner som rapporterte at de primært eller bare jobbet med IT- og datasikkerhet, men var også vanlig i institusjoner som meldte at de hadde en bredere innfallsvinkel til arbeidet med informasjonssikkerhet.

Om primærfokuset var IT- og datasikkerhet spesielt eller informasjonssikkerhet generelt syntes altså å ha relativt liten betydning for innholdet i de viktigste delene av sikkerhetsdokumentasjonen: policyer og prinsipper for informasjonssikkerhet. Dette hang sammen med at uansett hvor primærfokuset lå, var utgangspunktet for arbeidet sikring av IT-systemer og teknisk infrastruktur (hos alle institusjonene unntatt én), det vil si det tekniske miljøet som informasjonsverdiene befant seg i. Følgelig var det heller ikke unaturlig at sikkerhetsdoku-

mentasjonen bar preg av å være utarbeidet av og for IT-personell med en viss forhåndskjennskap til datasikkerhet.

Kommunikasjon og spredning

Intervjuene ga grunnlag for å reise spørsmål om hvor hensiktsmessig utformingen av innholdet i sikkerhetsdokumentasjonen var. Problemstillingen var særlig relevant når det gjaldt mange av faggruppene uten IT-kompetanse som, ifølge institusjonenes sikkerhetsorganisering, var pålagt å utføre viktige arbeidsoppgaver. I hvilken utstrekning var disse faggruppene – administrativt og vitenskapelige ansatte – i stand til å tilegne seg innholdet i sikkerhetsdokumentasjonen, spesielt sett i lys av den mangelfulle opplæringen i informasjonssikkerhet som preget institusjonene? Hadde rektorer og dekaner, universitets- og høyskoledirektører, fakultetsdirektører og instituttledere, forskningsledere og prosjektansatte, økonomi- og regnskapsmedarbeidere, HR-ledere og eiendomssjefer forutsetninger for å sette seg inn i det som sikkerhetsdokumentene forsøkte å kommunisere? I hvilken grad evnet dokumentene å formidle informasjon om oppgaver, ansvar og arbeidsmetodikk til en mangfoldig og sammensatt «brukergruppe»?

Intervjuer med nøkkelpersonell på institusjonsnivå indikerte at samtlige institusjoner stod overfor viktige utfordringer med hensyn til intern kommunikasjon og spredning av innholdet i sikkerhetsdokumentasjonen. Det ble for eksempel rapportert at dokumentasjonen i liten grad var bekjentgjort etter at den var vedtatt. Det ble videre hevdet at de som hadde lest hele eller deler av dokumentasjonen, men som ikke hadde vært med å lage den, virket å ha problemer med å forstå hva som ble forsøkt formidlet. Disse utfordringer syntes å være av grunnleggende karakter. Ledere eller ansatte som inngikk i sikkerhetsorganisasjonene kunne for eksempel ha vansker med å forstå hva informasjonssikkerhet handlet om, hvorfor arbeidet med informasjonssikkerhet var viktig, hvorfor akkurat de ble bedt om å bidra i arbeidet og hva deres bidrag skulle være: «hva er det meningen at jeg skal gjøre og hvordan?»

I tillegg ble det i enkelte institusjoner rapportert om at konkrete arbeidsredskap, for eksempel metodikk og maler for gjennomføring av risikovurderinger, i noen grad ble anvendt, men at kvaliteten på utført arbeid ble vurdert som mangelfull. Denne kompetansebristen ble i hovedsak forklart med lav prioritering av intern opplæring, men det ble også spekulert i om det kunne skyldes at sikkerhetsdokumentasjonen ikke kommuniserte godt nok mot faggrupper som hadde liten eller ingen forhåndskjennskap til risikostyrt informasjonssikkerhet.

Det bildet som avtegnet seg var at kompetansen på risikostyrt informasjonssikkerhet (og tilhørende arbeidsredskaper) var sentralisert – den fordelte seg på

noen få hoder i institusjonene, typisk CSO/CISO eller informasjonssikkerhetsrådgivere (se også diskusjon ovenfor). Samtidig virket kompetansen å være relativt lite mobil: den flyttet seg ikke lett fra sentrale aktører til nøkkelpersonell ved avdelinger, fakulteter, institutter og andre enheter. Det er også verdt å merke seg at kvaliteten på den sentraliserte kompetansen fremstod som relativt varierende. I enkelte institusjoner ble det blant sentrale aktører (CSO/CISO eller informasjonssikkerhetsrådgivere) rapportert om usikkerhet knyttet til bruken av viktige arbeidsredskaper: hva skulle dokumenteres og rapporteres i forbindelse med ledelsens gjennomgang, hvordan burde sikkerhetsrevisjoner foregå eller hvordan skulle kriterier for akseptabel risiko anvendes ved gjennomføring av risikovurderinger?

Denne usikkerheten førte til at mange av de som ble intervjuet etterlyste mer praktisk rettet informasjon og veiledningsmateriale fra nasjonale aktører, spesielt UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren. Tanken var at dette kunne danne basis for at institusjonene egen sikkerhetsdokumentasjon fikk et mer praktisk og lettere tilgjengelig innhold enn hva som var tilfelle nå.

I enkelte institusjoner ble det rapportert at sentrale begreper som ble benyttet i sikkerhetsdokumentasjonen, for eksempel «systemeiere», kommuniserte godt med de mest aktuelle målgruppene. «Systemeier» var derfor et begrep som ble forstått og tatt på alvor av flertallet av de som utøvde systemeierskapet (overfor har vi imidlertid sett at i andre institusjoner var dette i mindre grad tilfelle). I disse institusjonene ble det for eksempel hevdet at systemeierne faktisk var opptatt av å beskytte sine IT-systemer mot uønskede hendelser og avvik. Deler av innholdet i sikkerhetsdokumentasjonen virket følgelig å ha spredt seg til enkelte «nisjer» disse institusjonene. Spredning og kommunikasjon av andre deler av dokumentinnholdet syntes likevel å være en like stor utfordring her som i de øvrige institusjonene. Det var for eksempel lite som tydet på at systematikken i risikostyrt informasjonssikkerhetsarbeid – og at det var snakk om et styringssystem – var sterkere forankret blant ledere og ansatte enn i andre institusjoner. Enkelte hevdet derfor at fokuset på systemeierskap og på egne IT-systemer kunne føre til at styringen av informasjonssikkerheten ble fragmentert, det vil si at styringen primært foregikk på systemnivå og blant enkelte systemeiere istedenfor at institusjonen som sådan hadde styring med arbeidet.

Kommunikasjon og spredning – om dokumentinnholdet «traff» målgruppene eller ikke – virket samtidig å ha betydning for hvordan de ansatte oppfattet arbeidet med informasjonssikkerhet. Her nevnte flere av de som ble intervjuet at vanskelig tilgjengelige dokumenter kunne bremse innføringen og driften av styrings-

systemene. I et par institusjoner ble det for eksempel nevnt at dokumentutformingen kunne bidra til økt skepsis til og motstand mot informasjonssikkerhetsarbeidet. Det ble blant annet hevdet at utformingen kunne bidra til at arbeidet fremstod som mer byråkratisk, upraktisk og kjedelig enn hva det var grunnlag for. Argumentet var derfor at omfanget av og innholdet i dokumentasjonen kunne føre til at informasjonssikkerhet fremstod som en tidstyv, det vil si en administrativ tilleggsoppgave som tok oppmerksomheten bort fra de interessante oppgavene.

Enkelte institusjoner rapportert at begrunnelser for og den praktiske nytten av informasjonssikkerhet ble bedre forstått når ansatte (inkludert vitenskapelige ansatte) ble involvert i konkrete aktiviteter (her var det i første rekke snakk om risikovurderinger). Synspunktet i disse institusjonene var at deltakelse i konkrete og spesifikke aktiviteter var en mer effektiv kommunikator enn dokumenter og planverk.

Kommunikasjon av ansvar og oppgaver

Til sist er det verdt å nevne utfordringer knyttet til beskrivelser av sikkerhetsorganisasjonene. Tidligere har vi vist at oppbyggingen av sikkerhetsorganisasjonene (i hovedsak) var basert på to prinsipper: (1) fordeling av oppgaver og ansvar i linjen og (2) fordeling av oppgaver og ansvar mellom systemeiere og systemansvarlige. Vi har også nevnt at i enkelte institusjoner var det noe usikkerhet knyttet til hvordan denne organiseringen skulle fungere i praksis. Men det var også usikkerhet rundt måten sikkerhetsorganiseringen – formidling av informasjon om oppgaver og ansvar til ledere og ansatte – ble beskrevet og formidlet på. Denne problematikken virket i særlig grad å bero på to forhold.

For det første, og som drøftet ovenfor, at beskrivelsene av sikkerhetsorganisasjonen ikke alltid var samlet på ett sted. I mange av de 13 institusjonene som helt eller delvis hadde et skriftliggjort styringssystem var riktignok «skjelettet» i sikkerhetsorganiseringen beskrevet på ett sted, vanligvis som en del av policydokumentet. Men i enkelte andre institusjoner var beskrivelsen av sikkerhetsorganiseringen delt i to: noen deler ble presentert i policydokumentet, mens andre deler ble presentert i prinsippdokumentet. Dette førte til at det kunne være vanskelig for ledere og ansatte å se konturene av den helheten og sammenhengen som deres oppgaver og ansvar inngikk i.

For det andre, virket noe av det samme å være tilfelle når det gjaldt beskrivelsene av innholdet i de ulike rollene som inngikk i sikkerhetsorganisasjonen. Noen arbeidsoppgaver – og hvem som skulle utføre dem – var for eksempel spesifisert i policydokumentet. Andre arbeidsoppgaver eller konkrete tiltak – og hvem som skulle utføre dem – kunne være beskrevet i prinsippdokumentet, for eksempel

at CSO/CISO (eventuelt informasjonssikkerhetsrådgiveren) var ansvarlig for at IT-utstyr ble sikret mot virus og annen skadelig kode. Som nevnt tidligere, kunne uklare rollebeskrivelser og manglende spesifisering av relasjonene mellom de ulike rollene føre til at ledere og ansatte fikk problemer med å vite hva som var forventet av dem. Dette virket også å gjelde enkelte CSO/CISO (eventuelt informasjonssikkerhetsrådgivere). Det fremstod for eksempel som uklart hvor bevisste de var på at det var de selv – ikke IT-avdelingen, enhetsledere eller ledere av forskningsprosjekter – som hadde ansvaret for å beskytte IT-utstyr mot virusangrep. Samtidig var det uklart om IT-avdelingene, enhetsledere eller ledere av forskningsprosjekter var klar over at denne oppgaven var tillagt CSO/CISO (eventuelt informasjonssikkerhetsrådgiver).

I institusjoner som rapporterte at de (i noen grad) hadde fungerende sikkerhetsorganisasjoner, var inntrykket at den praktiske organiseringen av arbeidet var vesentlig forenklet sammenliknet med slik den ble beskrevet i sikkerhetsdokumentasjonen. Det som syntes å ha skjedd var at noen sentrale funksjoner og oppgaver var blitt prioritert, spesielt risikovurderinger, oppfølgende sikringstiltak og rutiner for egenkontroll. I én av disse institusjonene ble det for eksempel rapportert at hovedårsaken til at aktiviteter ble gjennomført og sikringstiltak iverksatt stod å lese på noen få linjer mot slutten av et dokument på 23 sider: det var her kjernen i sikkerhetsorganiseringen – og fordelingen av hovedoppgavene mellom utvalgte ledere og ansatte – stod beskrevet. Uten disse få linjene, og uten at de ble fulgt opp i praksis, ville ikke sikkerhetsarbeidet fungert. Nøkkelen til suksess i denne institusjonen syntes derfor å være at man hadde unngått å innføre alt som var skriftliggjort. Isteden hadde man forsøkt å redusere komplekse dokumenter til relativt enkle og tydelig fordelte arbeidsoppgaver.

Egenskaper ved institusjonene

Kommunikasjon og spredning av dokumentinnhold til aktuelle målgrupper var ikke den eneste og heller ikke den viktigste utfordringen de 20 kartlagte institusjonene rapporterte at de stod overfor. De viktigste utfordringene – eller barrierene – ved innføring og drift av styringssystemer for informasjonssikkerhet, knyttet seg til lokale institusjonsforhold. Spørsmålet som drøftes nedenfor er derfor hvilke vanskeligheter som oppbyggingen av og kulturen i akademiske institusjoner skapte ved innføring og drift av et helhetlig og topplederforankret styringssystem?

Senere rapporter vil gi en bredere og grundigere fremstilling av disse forholdene og hvordan de påvirket arbeidet med informasjonssikkerhet. Det som følger

nedenfor er en relativt kort og skissemessig drøfting av de viktigste momentene, slik de ble beskrevet i intervjuene med nøkkelpersonell på institusjonsnivå.

Ledelsesforankring

Tidligere har vi sett at i litteraturen om risikostyrt informasjonssikkerhet er det stort fokus på ledelsesforankring, det vil si at toppledelsen (rektor/direktør) forstår betydningen av, engasjerer seg i, bevilger ressurser til og utøver innflytelse på det praktiske arbeidet. Ledelsesforankring fremstilles derfor som en helt avgjørende forutsetning for vellykket innføring og drift av styringssystemer, og som en avgjørende indikator på om virksomhetene har lykkes med etablering av styringssystemer. Kort sagt: uten ledelsesforankring, ingen vellykket innføring og drift. Ledelsesforankring er også en faktor som i betydelig grad vektlegges i informasjons- og veiledningsmaterialet til ulike myndighetsorganer, for eksempel DIFI,[64] Nasjonal Sikkerhetsmyndighet[65] og Datatilsynet.[66] Samtidig fremstilles ledelsesforankring ofte som et problem og en utfordring: hvordan skal man få ledelsen til å ta sitt ansvar for styring av informasjonssikkerheten på alvor?

I de 20 institusjonene som deltok i studien, var det ulike beskrivelser av graden av ledelsesforankring. I enkelte institusjoner ble dette oppfattet som et viktig problem og som en barriere mot etablering av styringssystemer for informasjonssikkerhet. Selv i institusjoner hvor policyer og prinsippdokumenter var styrebehandlet (og vedtatt) – og til tross for at toppledelsen (vanligvis universitets- eller høyskoledirektører) formelt sett hadde påtatt seg det overordnede ansvaret for informasjonssikkerheten – var oppfatningen hos CSO/CISO (eventuelt informasjonssikkerhetsrådgivere) at ledelsen tok for lett på sin egen styringsrolle. Det ble for eksempel rapportert at årlige ledelsesgjennomganger, hvor de viktigste punktene på agendaen er status for informasjonssikkerheten i institusjonene og utarbeidelse av nye mål/planer for det videre arbeidet, sjelden eller aldri forekom. Toppledelsens forståelse for og praktisering av egen styringsrolle ble derfor (og med noen unntak) beskrevet som relativt svak eller helt fraværende.

Det ble videre rapportert at ledelsens manglende ivaretakelse av egen styringsrolle trolig ikke bare kunne forklares med liten interesse for og begrenset kompetanse på området. Det kunne også skyldes organisatoriske kjennetegn, det vil si måten institusjonene var oppbygd og fungerte på. Et eksempel som ble nevnt i noen institusjoner var at de daglig ansvarlige for informasjonssikkerheten ikke rapporterte direkte til toppledelsen (rektor/direktør). De hadde derfor ikke en direkte kanal inn til de viktigste beslutningstakerne. Det ble hevdet at dette

64 http://www.difi.no/digital-forvaltning/informasjonssikkerhet.

65 https://www.nsm.stat.no/.

66 https://www.datatilsynet.no/Sikkerhet-internkontroll/internkontroll_informasjonssikkerhet/.

kunne føre til at (a) informasjonssikkerhet ikke ble synliggjort i tilstrekkelig utstrekning overfor de som (i teorien) skulle styre og lede arbeidet og (b) at toppledelsen dermed heller ikke fikk den assistansen (eller påtrykket) de kunne trenge til å ivareta sin styringsrolle.

Det ble også rapportert at manglende kanaler inn til toppledelsen kunne bidra til å forsterke eksisterende kunnskapsmessige eller pedagogiske utfordringer. Her ble det spesielt siktet til at direktekanaler var en viktig betingelse for «å skolere» ledelsen i hva risikostyrt informasjonssikkerhet handlet om og hvorfor dette er viktig i en universitets- eller høyskolesammenheng. Til slutt kunne manglende ivaretakelse av styringsrollen bero på at toppledelsen satte tradisjonelle UH-verdier som åpenhet og transparent i høysete, eller at universiteter og høyskoler hadde liten kultur for toppstyring, spesielt av den akademiske virksomheten. I dette verdilandskapet kunne informasjonssikkerhet bli oppfattet som en «fremmed fugl» – noe som i liten grad tiltrakk seg ledelsens interesse, oppmerksomhet og engasjement (se også diskusjon nedenfor).

I andre institusjoner var tonen en annen. Her ble det rapportert om at ledere, både på topp- og mellomnivå (for eksempel avdelingsledere i sentraladministrasjonen eller enkelte fakultetsdirektører), hadde en viss innsikt i og i noen grad var villige til å prioritere arbeidet med informasjonssikkerhet. Det ble samtidig rapportert at uten støtte fra disse lederne ville arbeidet høyst sannsynlig blitt liggende brakk. Likevel mente de som hevdet dette synspunktet at ledelsesforankringen, og dermed også prioriteringen av arbeidet, var sårbart. De var for eksempel usikre på hva som ville skje dersom navngitte ledere sluttet i institusjonen eller gikk over i andre stillinger: ville nye ledere opprettholde dagens fokus på og prioritering av informasjonssikkerhet? Disse røstene mente at selv om styringssystemet fungerte tilfredsstillende i dag, så var det ikke sterkt nok institusjonalisert – blitt en naturlig og integrert del av den daglige virksomheten – til at det ville overleve relativt små personellendringer.

Institusjonslandskapet

Forankringen av styringssystemene på ledelsesnivå reiser viktige spørsmål om institusjonslandskapet. Med institusjonslandskapet menes hvordan organisatoriske forhold påvirket arbeidet med styringssystemer for informasjonssikkerhet, for eksempel graden av ledelsesforankring. Følgende kjennetegn ved institusjonslandskapet pekte seg ut som særlig betydningsfulle:

- Størrelse, det vil si antallet ansatte og studenter.
- Kompleksitet, det vil si antallet fakulteter og grunnenheter med ulik faglig orientering og betydelig autonomi/selvstendighet.

- Ledelsesstrukturer, det vil si hvordan den faglige og administrative ledelsen sentralt eller på fakultets- og grunnenhetsnivået var organisert.
- Organisatorisk avstand (graden av formalitet), det vil si om relasjonene mellom ledere og ansatte ble beskrevet som formell eller uformell.
- Geografisk avstand, det vil si om institusjonenes virksomhet var samlokalisert eller spredt på to eller flere ulike steder.

Intervjuene gir (ikke overraskende) grunnlag for å konkludere med at institusjonslandskapet påvirket arbeidet med innføring og drift av styringssystemer for informasjonssikkerhet. Det kom blant annet til uttrykk i intervjuobjektenes vurderinger av tematikken i forrige avsnitt: ledelsesforankring. Her er det verdt å legge merke til at institusjoner som rapporterte om at ledelsesforankring ikke var en vesentlig utfordring (i alle fall ikke per dags dato) nesten uten unntak var relativt små og lite komplekse. Avstanden – både fysisk og organisatorisk – mellom daglig og overordnet ansvarlig for informasjonssikkerheten var derfor kort, og relasjonene dem imellom ble beskrevet som uformelle. CSO/CISO (eventuelt informasjonssikkerhetsrådgiver) kunne for eksempel «stikke innom» direktørens kontor dersom det var noe – «det er rett nede i gangen her og han/hun har en 'åpen-dør-policy'».

I tillegg kunne ledelsesstrukturen på mellomnivå – fakultets- eller fagavdelingsnivå – være noe enklere enn i de største institusjonene, for eksempel ved at dekan både var faglig og administrativ leder. I større institusjoner ble det rapportert at ledelsesstrukturen var mindre sentralisert og mer utfordrende å jobbe med: det fantes både en faglig og en administrativ ledelse å forholde seg til (se drøftelse nedenfor). Det kunne derfor virke som at enklere ledelsesstrukturer i mindre institusjoner bidro til å forenkle arbeidet med å involvere ledere på alle virksomhetsnivåer.

Begrenset størrelse, kompleksitet, korte organisatoriske avstander (uformelle relasjoner) og enklere ledelsesstrukturer fremstod følgelig som faktorer som bidro til å styrke ledelsesforankringen.[67] Institusjoner som beskrev ledelsesforankringen som mer problematisk, var gjennomgående større (flere ansatte og

67 Dette funnet er noe overraskende. I den internasjonale forskningslitteraturen på innføring og drift av tilsvarende styringssystemer som benyttes på informasjonssikkerhetsområdet (som ofte er lovpålagte), hevdes det vanligvis at systemene er enklere å innføre og drifte i større enn i mindre virksomheter, blant annet på grunn av at systemdriften er ressurskrevende og kompetanseintensiv (for diskusjoner, se for eksempel Lauren B. Edelman og Mark C. Suchman (red.) (2007): *The Legal Lives of Private Organizations*. Burlington: Ashgate; Bridgit Hutter og Michael Power (red.) (2005): *Organizational Encounters With Risk*. Cambridge: Cambridge University Press; Sim B. Sitkin og Robert J. Bies (red.) (1994): *The Legalistic Organization*. Thousand Oaks: Sage Publications; Christopher D. Stone (1975): *Where the Law Ends. The Social Control of Corporate Behaviour*. New York: Harper & Row).

studenter), hadde ofte doble ledelsesstrukturer på mellomnivået (dekan og fakultetsdirektør) og var mer komplekse (mangfold av fakulteter og grunnenheter) enn der hvor forankring ble fremstilt som mindre problematisk. Bildet var likevel ikke entydig: også flere mindre institusjoner rapporterte om betydelige utfordringer knyttet til ledelsesforankring. Samtidig er antallet institusjoner som er undersøkt så langt for begrenset til at vi kan trekke sikre konklusjoner med hensyn til hvilken betydning disse faktorene – størrelse, kompleksitet, avstander/formalisering og ledelsesstrukturer – har for ledelsesforankringen spesielt.

Det som likevel synes relativt sikkert er at institusjonslandskapet påvirket det generelle arbeidet med styringssystemer for informasjonssikkerhet. Spesielt i de største institusjonene ble det rapportert at landskapet var såpass mangfoldig og sammensatt at dette i seg selv representerte en vesentlig utfordring. Utfordringene bestod i at det ble vanskeligere å koordinere det praktiske arbeidet, holde oversikt over aktiviteten og nå ut med informasjon til alle som inngikk i sikkerhetsorganisasjonen. I de største institusjonene var virksomheten som regel mer geografisk spredt og organiseringen mer kompleks enn i de mindre institusjonene – flere enheter med doble ledelsesstrukturer (faglig og administrativ ledelse) og egne styrende organer (fakultetsstyrer, instituttråd, osv.) som ikke var samlokaliserte.

Intern oppsplitting og kompleksitet kunne dessuten føre til store variasjoner i holdninger til informasjonssikkerhet og sikkerhetskultur, ikke bare mellom fakulteter, men også mellom institutter (og andre enheter) ved det samme fakultetet. Dermed kunne det være vanskelig å skreddersy informasjon og veiledning til mangfoldet av ulike mottakergrupper. Samtidig virket det som trenden med sammenslåing av mindre institusjoner til større læresteder bidro til å forsterke de utfordringene som geografisk spredt virksomhet, organisatorisk kompleksitet og interne variasjoner representerte, spesielt (men ikke bare) i overgangen fra gammel til ny organisering.

Arbeidet med å orientere seg i et stort, sammensatt og mangfoldig institusjonslandskap ble altså beskrevet som utfordrende av CSO/CISO eller informasjonssikkerhetsrådgivere. Det var da også de største institusjonene som anvendte mest ressurser (i form av dedikerte stillinger) på arbeidet med informasjonssikkerhet. Men ressurser er en relativ størrelse, det vil si at institusjoner med høyest ressursbruk også stod overfor de største organiserings- og styringsutfordringene. Her var det mer (i form av ansatte, studenter og organisatoriske enheter) som trengte organisering og styring. Det virket derfor tvilsomt om omfanget av ressursbruken tilsvarte størrelsen på de organisatoriske og styringsmessige utford-

ringene som disse institusjonene stod ovenfor. Enkelte mente for eksempel at det kunne være vanskelig nok å påvirke toppledelsens prioriteringer (rektor eller universitets-/høyskoledirektør), men her dreide det seg tross alt om noen relativt få personer. Det ble hevdet å være noe helt annet – og langt mer problematisk – å komme i inngrep med ledere (og ansatte) på fakultets- og instituttnivå, spesielt faglige ledere (dekaner, prodekaner eller instituttledere). Til forskjell fra toppledelsen, var det mange flere av dem, de kunne være spredt geografisk, ledelsesstrukturen var splittet (faglig og administrativ) og «byråkratiske påfunn» fra sentraladministrasjonens side ble ikke alltid sett på med velvillige øyne, spesielt ikke dersom de ble oppfattet som «tidstyver».

I flere av de større institusjonene ble fakultetsnivået fremhevet som særlig problematisk: det var her de viktigste barrierene mot innføring og drift av styringssystemene ble rapportert å befinne seg. Ovenfor har vi sett at dette i første rekke handlet om at det var vanskelig å få tilgang til de viktigste møteplassene og beslutningsarenaene for å informere, drøfte eller initiere arbeidet med informasjonssikkerhet. Dernest handlet det om at ledere og ansatte på fakultetsnivået i stor grad manglet innsikt i betydningen av informasjonssikkerhet og hadde begrenset kunnskap om metodikken som ble benyttet i arbeidet. Til slutt dreide det seg om en viss skepsis mot å bruke krefter på arbeid som ble oppfattet å ligge fjernt fra kjernevirksomheten (forskning og utdanning).

Både i store og mindre institusjoner ble det rapportert at forskningsprosjekter kunne utgjøre en spesiell utfordring. Utfordringen dreide seg primært om at forskningsprosjekter ofte var nokså autonome, selvdrevne og derfor relativt lukket for ekstern påvirkning. Vitenskapelige ansatte som jobbet på prosjekter hadde for eksempel sine egne økonomiske midler som de disponerte forholdsvis fritt, for eksempel når det gjaldt innkjøp av nytt IT-utstyr. I teorien var det vanligvis slik at innkjøpene skulle forhåndsgodkjennes av IT-avdelingene/seksjonene, blant annet for å sikre utstyret mot brudd på informasjonssikkerheten. Men det ble rapportert at slike rutiner ikke alltid fungerte i praksis: prosjektene kunne ofte kjøpte inn utstyr helt på egen hånd, det vil si uten noen form for forhåndsgodkjenning. IT-avdelingene/seksjonene og de operativt ansvarlige for informasjonssikkerheten miste dermed oversikten over utstyret, hvilken informasjon som ble lagret på det og hvordan informasjonen eventuelt var sikret mot tap, skade eller uautorisert innsyn.

Enkelte av de som ble intervjuet antok at lokalt IT-ansatte hadde en viss oversikt over hvilket IT-utstyr som ble innkjøpt og brukt i forskningsprosjekter på de forskjellige fakultetene og instituttene – og at de hjalp til med sikring av utstyret og informasjonen. I flere av institusjonene virket det likevel usikkert om den

lokale kontrollen med og sikringen av IT-utstyr og informasjonsverdier var like stor som enkelte sentralt ansatte antok. I mange av institusjonene virket det isteden som IT-utstyr innkjøpt på prosjektmidler lå utenfor rekkevidden til arbeidet med informasjonssikkerhet.

Til tross for at informasjonssikkerhetsarbeidet fremstod som særlig utfordrende i de største institusjonene, ble det rapportert om visse forbedringer. I én av de største institusjonene ble det blant annet vist til informasjons- og bevisstgjøringskampanjer (i forbindelse med nasjonal sikkerhetsmåned[68]) som nylig var gjennomført, og det ble rapportert at disse kampanjene hadde vært populære både blant ansatte og studenter. Men om kampanjene hadde noen langsiktig effekt på kunnskapen om og holdningene til informasjonssikkerhet, fremstod som usikkert. I en annen stor institusjon ble det rapportert om økt kunnskap om informasjonssikkerhet og personvern blant de administrativt ansatte på fakultets- og instituttnivå. Her ble endringer i kunnskapen målt ved hjelp av et spørreskjema som ble sendt ut til de forskjellige enhetene hvert år i forbindelse med revisjonen av personvern- og informasjonssikkerhetsarbeidet.[69] I flere andre institusjoner (både store og små) ble det nevnt at systemeiere i sentraladministrasjonen viste en viss interesse og forståelse for behovet for sikring av «sine» administrative IT-systemer.

Hovedinntrykket var likevel at arbeidet med innføring og drift av styringssystemer for informasjonssikkerhet var i støpeskjeen. Dette kom blant annet til uttrykk gjennom rapporter om til dels betydelige institusjonsinterne variasjoner: fakulteter, institutter og avdelinger kunne prioritere arbeidet svært forskjellig. Spesielt forskningsdata fremstod som mangelfullt sikret. Det var for eksempel bare én institusjon som rapporterte at den hadde risikovurdert sine forskningsprosesser, det vil si hvordan informasjon produsert i forskningsprosjekter ble håndtert fra planleggings- og innsamlingsstadiet og helt frem til prosjektslutt. I andre institusjoner ble det meldt om at en del medisinske eller helsefaglige forskningsprosjekter ble risikovurdert. Som nevnt ovenfor, virket det likevel ikke som disse institusjonene hadde risikovurdert ikke-medisinske forskningsprosjekter som også behandlet personopplysninger eller andre typer sensitive forskningsdata.

68 Se https://sikkert.no/.

69 Den ansvarlige for revisjonen mente imidlertid at det kunne stilles spørsmålstegn ved hvor reelle resultatene fra spørreundersøkelsene i virkeligheten var. Vedkommende hadde mistanke om at de som svarte på undersøkelsene trolig hadde en tendens overrapporterte sin kunnskap om personvern og informasjonssikkerhet, det vil si at de hevdet å vite mer enn hva de faktisk gjorde. Dette ble begrunnet med at stedlige kontroller hos de samme enhetene som svarte på spørreundersøkelsene avdekket at det reelle kunnskapsnivået var lavere – og hadde endret seg mindre – enn hva spørreundersøkelsene indikerte.

Institusjonskulturen

I intervjuene ble det spurt om «den akademiske kulturen» påvirket arbeidet med styringssystemer og informasjonssikkerhet. Det var særlig to kjennetegn ved «den akademiske kulturen som mange av intervjuobjektene mente kunne påvirke dette arbeidet. Begge kjennetegnene ble i større grad assosiert med den vitenskapelige enn med den administrative delen av virksomheten. Samtidig kunne det virke som organisering og kultur speilte hverandre, for eksempel ved at desentralisert organisering hang sammen med en kultur for autonomi og selvstendighet, både på enhets- og individnivå. Deler av drøftelsene nedenfor kunne derfor like gjerne vært plassert i avsnittet ovenfor («Institusjonslandskapet») som i dette avsnittet.

De to kjennetegnene som flertallet av intervjuobjektene virket å assosiere med «den akademiske kulturen» var:

1. **Åpenhet**, det vil si en kultur – og en institusjonell praksis – preget av fri kunnskapsformidling, menings- og idéutveksling og faglig kritikk (eksemplifisert med åpne forelesninger, seminarer og muntlige eksaminasjoner eller fritt tilgjengelig pensumlitteratur og annen type faglitteratur).
2. **Forskerfrihet**, det vil si at en kultur – og en institusjonell praksis – preget av relativt liten grad av sentral styring og kontroll av forsknings- og undervisningsvirksomheten: forskernes frihet til å bestemme hva det er verdt å forske på og når/hvordan resultatene skal publiseres eller på annen måte formidles.[70]

Med bakgrunn i disse kjennetegnene er det lett å tenke at «den akademiske kulturen» og informasjonssikkerhet er to uforenelige størrelser. For det første fordi åpenheten i universiteter og høyskoler kan føre til at det blir vanskelig å få gehør for arbeidet med informasjonssikkerhet, spesielt hensynet til sikring av konfidensialiteten til informasjon (primært forskningsdata). Informasjonen skal istedenfor være åpen slik at kvaliteten på den (og måten den er innhentet og bearbeidet på) kan etterprøves og diskuteres. For det andre fordi forskerfriheten kan føre til at institusjonene blir mer avhengig av forskerne enn hva forskerne er av institusjonene. Den vitenskapelige virksomheten kan for eksempel være drevet av individuelle forskere eller forskningsgrupper med høy faglig anseelse, nasjonalt

70 Forskerfriheten er dermed ment å være en barriere mot sterke politiske eller økonomiske aktørgruppers interesse i å styre hva det forskes på, hvilke resultater som produseres (og hvilke resultater som ikke produseres), hvordan resultatene offentliggjøres for et større publikum og hva institusjonene gir undervisning eller opplæring i. Se for eksempel Robert Merton (1973): *The Sociology of Science: Theoretical and Empirical Investigations*. Chicago: University of Chicago Press, eller Max Weber (2010): *Makt og byråkrati. Essays om politikk og klasse, samfunnsforskning og verdier*. Oslo: Gyldendal akademiske.

og internasjonalt. Institusjonenes omdømme, status og økonomi kan derfor bli svært avhengig av kvaliteten på den vitenskapelige virksomheten, og dette kan ha stor betydning for rekrutteringen av studenter og evnen til å skaffe ekstern finansiering for nye prosjekter. Til sammen kan dette føre til at institusjonene er varsomme med å innføre styringssystemer som de mener kan undergrave den åpenheten, autonomien og selvstendigheten som ligger til grunn for forsknings- og undervisningsarbeidet.[71]

Selv om åpenheten og forskerfriheten kan representerer barrierer mot etablering av nye styringssystemer, uttrykte intervjuobjektene ulike og til dels motstridende oppfatninger om og i hvilken grad dette faktisk var tilfelle. Det var derfor ikke konsensus om betydningen av «den akademiske kulturen» og hvordan den skulle vurderes.

Flere av de som ble intervjuet mente riktignok at det kunne være en viss motsetning mellom (a) ledelsesstyrt informasjonssikkerhet og (b) åpenheten og forskerfriheten som preger akademiske institusjoner. Synspunktet til disse intervjuobjektene var altså at det forelå en generell motsetning mellom «den akademiske kulturen» og informasjonssikkerhet, og at motsetningen preget arbeidet med styringssystemer uavhengig av fagområder.

Synspunktet virket å være særlig vanlig blant daglig ansvarlige for informasjonssikkerheten (CSO/CISO eller informasjonssikkerhetsrådgivere) som tidligere hadde jobbet med informasjonssikkerhet i andre deler av offentlig sektor eller som hadde bakgrunn fra det private næringslivet. Oppfatningen om at det forelå en generell motsetning ble begrunnet med flere forhold som allerede er nevnt, for eksempel at vitenskapelig ansatte kunne være skeptiske til rutiner og prosedyrer de mente begrenset forskerfriheten eller som stjal tid fra deres kjerneoppgaver (forskning og utdanning). Enkelte mente derfor at kulturen i universiteter og høyskoler innebar at informasjonssikkerhet ikke lå i «ryggraden» til institusjonene (i alle fall ikke på samme måte som de var vant med fra andre sektorer eller bransjer).

Konkrete eksempler som ble nevnt på at «den akademiske kulturen» skapte utfordringer for styring av informasjonssikkerheten, var bruken av mobile dataenheter, skytjenester og e-post til kommunikasjon av konfidensielle forskningsdata. Argumentet var at forskerfriheten, det vil si den selvstendigheten og autonomien som akademisk arbeid ofte innebærer, kunne bidra til ukontrollert bruk av denne typen IT-løsninger, for eksempel fordi IT-utstyr ble innkjøpt uten

71 Både forskerfriheten (faglig frihet) og åpenhet knyttet til forskningen er regulert i universitets- og høyskoleloven, se spesielt § 1-5.

noen form for forhåndsgodkjenning eller fordi forskergrupper på eget initiativ tok i bruk skyløsninger (nettbaserte tjenester) for deling av forskningsdata og annet skriftlig materiale. I tillegg til at dette gjorde det vanskelig å skaffe seg oversikt over behandlingen av viktige informasjonsverdier, kunne det undergrave den informasjonssikkerheten som institusjonene selv hadde vedtatt: informasjonsverdier ble ikke tilfredsstillende sikret på bærbart utstyr eller i skyen, samtidig som rettslige plikter, spesielt på personvernområdet, ikke ble ivaretatt.[72] Det ble derfor etterspurt fellesløsninger for sektoren som kunne avhjelpe disse utfordringene, særlig sikre skytjenester for lagring av konfidensielle forskningsdata (primært, men ikke bare, sensitive personopplysninger). Dette ble beskrevet som et nødvendig alternativ til den frie bruken av skytjenester som de daglig ansvarlige for informasjonssikkerheten visste/mistenkte foregikk, men som de hadde liten eller ingen kontroll med.

Et annet eksempel på motsetningen mellom styring av informasjonssikkerhet og «den akademiske kulturen» fremgikk av Datatilsynets rapporter fra tilsyn med behandlingen og sikringen av sensitive personopplysninger (helseopplysninger) i medisinske forskningsprosjekter. I flertallet av kontrollrapportene ble det hevdet at toppledelsen ved de institusjonene som hadde hatt tilsyn i løpet av de siste 12 årene, manglet styring og kontroll med informasjonsforvaltningen. Datatilsynet mente for eksempel at de verken hadde oversikt over hvilke forskningsprosjekter som ble gjennomført, hvordan forskningsdeltakernes personvernrettigheter ble ivaretatt eller hvordan personopplysningene ble sikret.[73]

Toppledelsen (ved forskningsadministrasjonen) forsvarte seg med at det ikke var vanlig med sentralstyring av og sentralisert kontroll med forskningsvirksomheten – det fantes ikke kultur (eller administrative strukturer) for dette i de aktuelle institusjonene. Toppledelsen løsning på utfordringen var derfor desentralisering og selvstendig ansvar i samsvar med «den akademiske kulturens»

72 Dette gjaldt spesielt ved bruk av eksterne tjenesteleverandører, primært skytjenester. Her krever personopplysningsloven at institusjonene inngår databehandleravtaler med alle tjenesteleverandørene når de behandler personopplysninger på vegne av institusjonene. Avtalene skal i særlig grad inneholde bestemmelser om informasjonssikkerhet (se personopplysningsloven §§ 13 og 15). Men dersom bruken av eksterne tjenesteleverandører «privatiseres», det vil si at de tas i bruk på individuelt grunnlag eller av selvstyrte forskningsgrupper, er det fare for at institusjonene ikke vet om dette. Dermed har institusjonene små muligheter til å ivareta de rettslige forpliktelsene som følger med bruken av eksterne tjenesteleverandører.

73 I enkelte kontrollrapporter ble det kommentert at toppledelsen mente at det var det nasjonale personvernombudet for forskning – Norsk samfunnsvitenskapelig datatjeneste (NSD) – som var ansvarlig for at disse forholdene ble ivaretatt. Synspunktet til toppledelsen var, ifølge disse rapportene, at så lenge forskningen var meldt til NSD, eller var godkjent av regionale komiteer for medisinsk og helsefaglig forskningsetikk, hadde institusjonene gjort det som var krevd av dem.

ånd. Det innebar blant annet at prosjektlederne selv (forskerne eller forskergruppene) måtte sørge for at lover og regler, inkludert bestemmelsene om informasjonssikkerhet i personopplysningsloven med forskrift, ble ivaretatt (eventuelt at fakulteter eller institutter – der hvor forskningen hadde sitt organisatoriske «hjem» – hadde ansvaret for hvordan «deres» forskere etterlevde regelverket). Det var jo tross alt forskerne og de ulike fakultetene/grunnenhetene som var ansvarlige for sin egen forskningsvirksomhet: her fantes det forskningsstrategier, godkjenningsordninger og forskningsadministrativ ekspertise. Toppledelsen mente følgelig at den ikke kunne blande seg for mye inn i hvordan forskningsarbeidet foregikk lokalt – dette var jo beskyttet av forskerfriheten.

Kontrollrapportene fra Datatilsynet indikerte to interessante forhold. For det første at ansvars- og arbeidsfordelingen mellom ulike organisatoriske nivåer – sentralapparatet og lokale enheter – kunne være uklar, og føre til at nivåene skyldte på hverandre når regelbrudd ble avdekket. For det andre at innføring og drift av toppstyrte styringssystemer kunne ha vanskelige vilkår når verdier som forskerfrihet og desentralisert, faglig ansvar ble prioritert høyt. Dette ble også bemerket av Datatilsynet selv. I én av kontrollrapportene heter det for eksempel:

> «(…) universitetsmiljøer, herunder de ulike instituttene, er generelt sett preget av stor grad av autonomi. Datatilsynet oppfatter det slik at det kan være en ekstra utfordring å implementere styringssystemer i slike organisasjoner.» [74]

Men det var også andre sider ved kulturen i akademiske institusjoner som ble problematisert av flere av de som ble intervjuet. Daglig ansvarlige for informasjonssikkerhet med bakgrunn fra det private næringslivet, beskrev for eksempel en kultur hvor beslutninger aldri var helt endelige – hvor det var rom for omkamper og stadig nye debatter om vedtak som allerede var fattet. Iverksetting av sikringstiltak, spesielt dersom det berørte de ansatte direkte (for eksempel begrensninger i bruk av bærbare dateenheter), kunne derfor, ifølge disse respondentene, være en relativt frustrerende opplevelse med gjentagende diskusjoner frem og tilbake om hva som var bestemt, hvem som skulle omfattes av tiltakene og hvordan de skulle gjennomføres.

Andre intervjuobjekter nyanserte dette bildet noe. De mente at holdningen til informasjonssikkerhet ikke var ensartet internt, men varierte en god del mellom fagområder. Tidligere har vi for eksempel sett at enkelte institusjoner rapporterte at arbeidet med informasjonssikkerhet hadde fått sterkere fotfeste innenfor helsefag og medisinsk forskning enn hva som typisk var tilfelle innenfor andre fagområder. Dette ble forklart med at informasjonssikkerhet og personvern tra-

74 *Endelig rapport fra tilsyn – Universitetet i Oslo*, side 5. Saksnummer 2007/00572.

disjonelt var særlig viktig på helseområdet, både når det gjaldt forskere og praktikere, og det ble vist til den sterke «taushetspliktkulturen» innenfor helse- og medisinområdet. Samtidig ble det rapportert at innenfor andre fagområder, blant annet enkelte informatikkfag, stod arbeidet med informasjonssikkerhet overfor betydelig større utfordringer. Visse informatikkfag var for eksempel preget av en «hackerkultur» hvor eksponering snarere enn sikring av informasjonsverdier stod i høysete.

Disse intervjuobjektene var derfor uenige i at «den akademiske kulturen» som sådan skapte utfordringer for arbeidet med informasjonssikkerhet. Deres oppfatning var isteden at kulturen i akademiske institusjoner ikke var uniform på tvers av fagområder, men var splittet opp i forskjellige «fagspesifikke tradisjoner». Hvordan de «fagspesifikke tradisjonene» påvirket arbeidet med informasjonssikkerhet kunne være noe ulikt, og man måtte vurdere hvert enkelt fagområde for seg for å finne ut om (eller i hvilken grad) de støtte opp om eller vanskeliggjøre innføring og drift av styringssystemer.

En tredje gruppe intervjuobjekter forfektet et annet syn på arbeidet med informasjonssikkerhet enn de som er drøftet ovenfor. Også disse intervjuobjektene mente det var misvisende å snakke om en generell motsetning mellom «den akademiske kulturen» og styringssystemer for informasjonssikkerhet. Samtidig var de skeptiske til om det forelå systematiske variasjoner mellom ulike «fagspesifikke tradisjoner» når det gjaldt holdninger til og praktiseringen av informasjonssikkerhet. Her ble det isteden hevdet at det var snakk om et utpreget tvisyn, spesielt når det gjaldt holdningene til konfidensialitet, og at tvisynet var sterkt påvirket av egeninteresser snarere enn av «kultur» og «tradisjon». De mente for eksempel at konfidensialitet (eller «hemmelighold») ble verdsatt av vitenskapelige ansatte i visse faser av en forskningsprosess, typisk mens datainnsamling og analyser av data pågikk. I disse fasene kunne det være viktig for forskerne å skjerme datamaterialet (eller annet forskningsmateriale) mot uautorisert innsyn, spesielt fra konkurrerende forskere eller forskningsmiljøer. Egeninteressen i konfidensialitet kunne handle om flere forhold. For det første å sikre at konkurrerende miljøer ikke «stjal» resultater og ideer før man selv hadde publisert dem. For det andre at status («ære og berømmelse») i fagmiljøene var knyttet til hvem som var først ute med viktige forskningsfunn. For det tredje at mulighetene for fremtidig finansiering kunne være avhengig av at forskningsdata ble håndtert på en konfidensiell måte.

Når det gjaldt det siste punktet ble det blant annet hevdet at eksternfinansiert forskning, spesielt med midler fra store næringslivsaktører, førte til at forskerne (og institusjonene) hadde betydelig økonomisk egeninteresse knyttet til at kon-

fidensialiteten ble ivaretatt. Alvorlige sikkerhetsbrudd kunne for eksempel føre til at private samarbeidsparter trakk seg ut, at finansiering av nye prosjekter ble vanskeliggjort og at institusjonenes omdømme ble skadelidende.

Det ble videre hevdet at når forskningsdataene var ferdig analysert og klare for publisering, ble konfidensialitet et mindre sentralt hensyn for de vitenskapelige ansatte. Da var det spredning og kvalitet, det vil si at forskningsresultatene ble gjort kjent og at resultatene ikke ble «tuklet med», som hadde førsteprioriteten. Synspunktet var derfor at arbeidet med informasjonssikkerhet måtte ta hensyn til denne dynamikken i forskningsaktivitetens sikkerhetsbehov.

Til slutt var det enkelte intervjuobjekter som verken så motsetninger eller tvisyn. Disse intervjuobjektene mente at de fleste vitenskapelig ansatte var genuint opptatt av at forskningsdata (eller annet forskningsmateriale) ble sikret på forsvarlig måte, både med hensyn til konfidensialitet, integritet og tilgjengelighet. Oppfatningen var at dette ikke primært handlet om «snevre egeninteresser», men at informasjonssikkerhet var en (mer eller mindre) integrert del av «den akademiske kulturen». Det ble for eksempel argumentert med at forskerne mente at de hadde en forpliktelse til å sikre forskningsdata som det hadde tatt lang tid å innhente og bearbeide – og hvor arbeidet var finansiert av offentlige midler. Det ble også hevdet at informasjonssikkerhet var viktig fordi enkeltpersoners personvern ble tillagt betydelig egenverdi (oppfattet som viktig og riktig i seg selv), både blant vitenskapelig og administrativt ansatte (selv om Datatilsynets kontrollrapporter indikerte at personvernreglene i begrenset grad ble overholdt). Dessuten ble det gitt uttrykk for at forskere ønsket informasjonssikkerhet velkommen når det gjaldt spesielt sensitiv forskning, for eksempel på områder som var av betydning for rikets sikkerhet.[75] Den store bristen som disse intervjuobjektene pekte på var derfor ikke kulturen i akademiske institusjoner. Det handlet isteden om mangel på kompetanse og organisatoriske utfordringer.

Av intervjuene fremgikk det at administrativt ansatte ikke i samme utstrekning som vitenskapelig ansatte ble forstått som en del av «den akademiske kulturen». Intervjuobjektenes syn på universitets- eller høyskoleadministrasjonen tok isteden utgangspunkt i det som mer kan beskrives som en «forvaltningskultur», det vil si en kultur som kjennetegnes av at systemer for intern styring, rapportering og kontroll i større grad er en integrert og akseptert del av arbeidshverdagen.

75 Oppslag i massemedia indikerer likevel at enkelte institusjoner ikke er like fornøyd med myndighetenes behandling av utenlandske teknologistudenters søknader om midlertidig opphold. Her vises det til flere eksempler på iranske studenter som har fått avslag på sine søknader lenge etter at de startet sine pH. D-prosjekter. Se for eksempel http://www.nrk.no/trondelag/iranske-stipendiater-kastes-ut-1.11756019 eller http://www.vg.no/nyheter/meninger/vg-mener-ntnu-og-iran/a/23222529/.

Tidligere har vi sett at innføring og drift av styringssystemer for informasjonssikkerhet også kunne støte mot utfordringer og barrierer i ulike deler av administrasjonsapparatet. Likevel ga mange intervjuobjekter uttrykk for at arbeidet med informasjonssikkerhet hadde *lettere* for å finne aksept i administrasjonsapparatet enn hva som typisk var tilfelle i viktige deler av forsknings- og undervisningsvirksomheten.

I tillegg til at administrasjonens «forvaltningskultur» impliserte fortrolighet med bruken av ulike typer styringssystemer, ble det rapportert at større aksept også kunne henge sammen med at tyngdepunktet i arbeidet lå på administrasjonssiden, det vil si at mesteparten av innsatsen var rettet mot sikring av administrative IT-systemer og teknisk infrastruktur. Samtidig opplevde nok de daglig ansvarlige for informasjonssikkerheten et nærmere slektskap til de administrativt enn til de vitenskapelige ansatte. De daglig ansvarlige var jo selv en del av administrasjonen, mens de vitenskapelige ansatte «spilte på en annen banehalvdel». Her var det litt andre regler som gjaldt enn i administrasjonsapparatet, og oppfatningen virket å være at forskere og undervisere tilhørte en noe fjern og lukket sfære som «vi andre» hadde begrenset innsyn i og forstand på.

Dette innebar at når det ble stilt generelle spørsmål om arbeidet med informasjonssikkerhet i institusjonene, var det nesten alltid innsatsen mot administrasjonsapparatet som intervjuobjektene først snakket om. De hadde vanligvis mindre å si, og måtte som oftest spørres særskilt om, hva som ble gjort i relasjon til forsknings- og undervisningsvirksomheten.

Del V: Mulige løsninger

Drøftelsene i del IV har pekt på at de 20 undersøkte institusjonene stod overfor en rekke utfordringer i arbeidet med innføring og drift av styringssystemer for informasjonssikkerhet. Denne delen av rapporten vil diskutere hvilke løsninger på utfordringene som institusjonene selv mente var realistiske eller mulige. Hovedspørsmålene som drøftes nedenfor er derfor hvilke mulige løsninger institusjonene selv pekte på når det gjaldt innføring og drift av styringssystemene? Hva kunne bidra til at utfordringene ble løst eller føre til at de ble enklere å håndtere?

Enkelte av utfordringene som ble diskutert i del IV, er vanskelige å gjøre noe med. Spesielt institusjonslandskapet og den akademiske kulturen er forhold som de daglig ansvarlige for informasjonssikkerheten (eller andre ledere/ansatte med viktige sikkerhetsoppgaver) ikke kan (og kanskje heller ikke bør) påvirke i særlig utstrekning, i alle fall ikke når det gjelder de grunnleggende kjennetegnene. Samtidig er det slik at flere av utfordringene også representerer mulige løsninger. Dette gjelder for eksempel ressurssituasjonen – flere dedikerte stillinger og økte vekt på skolering og kompetanseheving – og endringer i måten styringssystemene presenteres og kommuniseres på. Disse utfordringene kan de daglig ansvarlige (med støtte fra andre ledere) faktisk kunne påvirke. Det som drøftes nedenfor er derfor hva som, ifølge intervjuobjektene, kunne endre de forholdene eller utfordringene som institusjonene kunne gjøre noe med, for eksempel hva som måtte til for å utløse flere ressurser til stillinger eller til skolering/kompetanseheving.

Fokuset i drøftelsene rettes mot tre momenter/forhold som intervjuobjektene mente kunne bevege arbeidet med styring av informasjonssikkerhet i en mer offensiv retning. Det første er effekten av sikkerhetshendelser, det vil si brudd på informasjonsverdienes konfidensialitet, integritet eller tilgjengelighet: hvilken innvirkning (om noen) hadde denne typen uønskede hendelser på innføring og drift av styringssystemer for informasjonssikkerhet? Det andre er måten arbeidet med lokaltilpasning av styringssystemene foregikk på: hvilken betydning (om noen) hadde graden av lokaltilpasning for driften av styringssystemene og i hvilken grad ble dette gjort? Det tredje er hvordan press fra eksterne aktører, for eksempel Kunnskapsdepartementet, Riksrevisjonen eller Datatilsynet, har påvirket arbeidet med informasjonssikkerhet: hvilken virkning (om noen) hadde krav eller forventninger fra denne typen aktører på institusjonenes innsats og ressursbruk?

Sikkerhetshendelser

Tidligere undersøkelser av arbeidet med styringssystemer for informasjonssikkerhet i kommunesektoren har indikert at uønskede hendelser (sikkerhetshendelser), for eksempel uautorisert eksponering av personopplysninger på internettet eller avbrudd i tilgangen til viktige IT-systemer, satte fart i innsatsen på området (i alle fall for en avgrenset tidsperiode).[76] Det betyr at brudd på informasjonsverdienes konfidensialitet, integritet eller tilgjengelighet kan bidra til å øke oppmerksomheten omkring informasjonssikkerhet og forsterke innsatsen rettet mot innføring og drift av styringssystemer.

Tidligere undersøkelser indikerte dessuten at dette gjaldt spesielt dersom de uønskede hendelsene førte til negativ medieomtale. Negativt oppslag i media skapte (spesielt hos toppledelsen) en viss frykt for at omtalen skadet kommunenes omdømme, det vil si at innbyggerne og samarbeidsparter i det lokale organisasjons- eller næringslivet ikke i samme grad som tidligere så på kommunen som et kompetent og profesjonelt forvaltningsorgan. Spørsmålet er derfor om institusjonene i denne undersøkelsen hadde opplevd tilsvarende uønskede hendelser – og negativ medieomtale? Hvordan hadde dette i så fall påvirket måten spørsmål om styring av informasjonssikkerheten ble håndtert på internt?

Flertallet av de som ble intervjuet på institusjonsnivå ga uttrykk for at alvorlige sikkerhetshendelser nok kunne føre til at informasjonssikkerhet ble prioritert sterkere, spesielt (men ikke bare) av toppledelsen. Det var imidlertid relativt få som rapporterte at de hadde opplevd alvorlige sikkerhetshendelser i løpet av de siste 4-5 årene. De vanligste uønskede hendelsene (sikkerhetshendelsene) som ble nevnt ble beskrevet som mindre alvorlige og påkalte derfor liten eller begrenset oppmerksomhet internt. De førte heller ikke til negative medieoppslag eller offentlig oppmerksomhet.

Det var likevel enkelte unntak. Ved én av institusjonene ble det nevnt to episoder med utilsiktet publisering av personopplysninger (fødselsnumre) på internettet for noen år tilbake. Disse hendelsene fikk en viss medial oppmerksomhet, og førte til at Datatilsynet opprettet tilsynssak mot institusjonen.[77] I tillegg ble det nevnt flere tilsvarende eksempler på utilsiktet publisering av personopplys-

76 Se spesielt Tommy Tranvik (2012): «Kommunal regeletterlevelse: Realiteter og illusjoner på personvernområdet». *Tidsskrift for samfunnsforskning*, nr. 2, s. 131-156, og Tommy Tranvik (2009): *Personvern og informasjonssikkerhet. En studie av rettsreglers etterlevelse i kommunal sektor*. Oslo: Unipub.

77 I kontrollrapporten fra Datatilsynet fremgikk det at institusjonen manglet et styringssystem for informasjonssikkerhet. Håndteringen av opplysningene hadde derfor ikke blitt risikovurdert og tilfredsstillende sikret.

ninger på internett som skyldes feilaktig bruk av publiseringsverktøy (rutinesvikt). Disse sakene ble meldt til Datatilsynet av institusjonene selv, og førte til krav fra tilsynet om gjennomføring av risikovurderinger og iverksetting av nye sikringstiltak. Det ble også vist til medieoppslag om håndtering av elektroniske adgangskort – og logging av kortbruken – ved enkelte institusjoner. Her handlet det om hvorvidt logging av kortbruken var å forstå som ulovlig overvåking av studenter og ansatte, det vil si om institusjonene hadde registrert og lagret disse opplysningene uten lovlig grunn og uten å informere brukerne.[78] I et annet medieoppslag (som ikke ble nevnt av intervjuobjektene) ble det avdekket at det hadde foregått ulovlig kameraovervåkning av pauserom ved ett av instituttene ved den aktuelle institusjonen.[79]

Selv om disse sakene helt eller delvis berører problemstillinger om informasjonssikkerhet, handlet de i første rekke om andre typer brudd på personvernlovgivningen. Det virket likevel som medieoppmerksomheten hadde bidratt til at informasjonssikkerhet kom noe høyere på de involverte institusjonenes agenda. I enkelte av institusjonene ble det rapportert at medieoppmerksomhet som hadde innflytelse på arbeidet med informasjonssikkerhet ikke bare dreide seg om oppslag i regionale media eller riksmedia. Det kunne også handle om oppslag i studentaviser – og at disse oppslagene deretter kunne finne veien til regionale media eller riksmedia. Flere av intervjuobjektene uttrykte derfor at studentaviser fungerte som lokale «vaktbikkjer», og at oppslag i denne typen media kunne føre til ikke ubetydelig merarbeid for å rette opp i kritikkverdige forhold.

De uønskede informasjonshendelsene som oftest ble nevnt av institusjonene selv var at enkelte IT-systemer hadde vært utilgjengelige for kortere perioder, for eksempel som følge av strømbrudd eller svikt i kjøleanlegg i serverrom. Det ble også nevnt episoder med tap av håndholdte dataenheter, for eksempel minnepinner eller bærbar pc, problemer med back-up (lang gjenopprettingstid) og enkelte hackerangrep (DDOS, Botnet). I tillegg ble det rapportert om enkelte tilfeller med ulovlig publisering av personopplysninger på internettet (søknadspapirer)[80] og utfordringer med håndtering av borgere fra særskilte land (spesielt Iran) som søkte stillinger innenfor sensitive forskningsområder.[81]

78 Se for eksempel http://www.vg.no/nyheter/innenriks/universitet-innroemmer-ulovlig-overvaaking/a/10128880/ eller http://www.studenttorget.no/index.php?show=5195&expand=3797,5195&artikkelid=13434.

79 http://universitas.no/nyhet/59120/uio-far-personvernrefs.

80 I dette tilfelle rapporterte institusjonen selv sikkerhetsbruddet til Datatilsynet.

81 Denne problematikken ble (i noen grad) håndtert i samarbeid mellom de aktuelle institusjonene og Politiets Sikkerhetstjeneste.

De uønskede hendelsene som til daglig skapte størst bekymring, dreide seg mer om opphavsretts- og personvernrelaterte spørsmål enn om informasjonssikkerhet som sådan. Her handlet det om studenter som ulovlig nedlastet rettighetsbeskyttet materiale (primært norske eller utenlandske filmer eller tv-serier) ved bruk av institusjonenes datamaskiner eller tekniske infrastruktur (datanettverk). Svært mange av institusjonene rapporterte at de månedlig mottok en rekke henvendelser fra rettighetseiere – eller aktører som handlet på vegne av rettighetseierne – med krav om utlevering av identiteten til studenter eller ansatte som ulovlig nedlastet denne typen materiale. De fleste institusjonene hadde et IT-reglement som forbød nedlasting, men samtidig var de usikre på hvordan henvendelsene skulle håndteres: hadde institusjonene plikt til å undersøke saken (granske sine datalogger) og informere rettighetseierne om studentenes identitet, eller ville dette være brudd på de aktuelle individenes personvernrettigheter? Enkelte institusjoner hadde kontaktet Datatilsynet for å avklare spørsmålet, og resultatet ble at disse institusjonene ikke uten videre utleverte opplysninger om identitet (henvendelsene ble isteden håndtert på andre måter, for eksempel ved at de aktuelle individene fikk advarsler eller at tilgangen til datanettverket ble suspendert for en viss periode ved gjentatte hendelser).[82] Dette virket også å være vanlig praksis i flertallet av de øvrige institusjonene.

Selv om omfanget av denne typen hendelser ble rapportert å være betydelig, virket hendelsesomfanget å ha liten eller ingen betydning for arbeidet med styring av informasjonssikkerheten. Hendelsene ble vanligvis håndtert som en del av IT-avdelingene/seksjonene ordinære «oppgaveportefølje», og det ble ikke rapportert at de førte til medieomtale som kunne anspore til økt trykk rundt innføringen eller driften av styringssystemer for informasjonssikkerhet.

Samtidig med at de vanligste uønskede hendelsene ikke fremstod som en viktig motivasjonsfaktor i arbeidet med styring av informasjonssikkerheten, virket det tvilsomt om institusjonene hadde full oversikt over hendelsesomfanget. Dette hang sammen med at de fleste institusjonene rapporterte at de manglet velfungerende systemer for melding av brudd på sikkerheten eller avvik fra lokale rutiner for håndtering av informasjonsverdier (avviksmeldingssystemer). Det er derfor sannsynlig at en del hendelser ikke ble rapportert og dermed heller ikke ble synliggjort for personer med det daglige eller det overordnede ansvaret for informasjonssikkerheten.

82 I en av institusjonene ble det rapportert at den ikke lengre driftet IT-nettverket til studenthyblene på grunn av problematikken med ulovlig nedlasting. Ekstern drift av IT-nettverket var en strategi som ble valgt for å unngå vanskelige personvernrettslige spørsmål som krav om innsyn i studentenes nettaktivitet reiste.

I tillegg kan det virke som kort fartstid i stillingene førte til at enkelte intervjuobjekter ikke kjente til episoder med alvorlige sikkerhetsbrudd som hadde skjedd ved deres institusjoner før de ble ansatt. Slike episoder ble imidlertid nevnt i Datatilsynets kontrollrapporter fra stedlige tilsyn ved enkelte av institusjonene. Her ble det vist til flere eksempler på alvorlige og relativt ferske sikkerhetsbrudd, for eksempel at det hadde forekommet fysisk transport av ukrypterte lagringsmedium som inneholdt sensitive personopplysninger (elektroniske pasientjournaler). Kontrollrapportene vist også til eksempler på at forskere hadde oppbevart ukrypterte lagringsmedium med sensitive personopplysninger (som ble brukt til forskningsformål) i sine privatboliger. Kontrollrapportene viste også andre alvorlige sikkerhetsbrudd/avvik, for eksempel at forskere hadde inngått databehandleravtaler (med eksterne leverandører av datatjenester[83]) på vegne av egen institusjon uten å være autorisert til å inngå slike avtaler.

Til tross for få egenrapporterte sikkerhetshendelser og avvik, mente de fleste intervjuobjektene at deres institusjoner trolig levde med et risikonivå som var uakseptabelt høyt, noe Datatilsynets kontrollrapporter synes å bekrefte. Bekymringen rettet seg særlig mot de vitenskapelige ansatte og måten de håndterte informasjonsverdier i forskningen på. Dette gjaldt for eksempel bruken av e-post til forsendelse av konfidensielle forskningsdata til samarbeidspartnere ved andre institusjoner i Norge eller i utlandet. Vi har tidligere sett at det også ble uttrykt bekymring for informasjonssikkerheten ved lokal lagring av konfidensielle forskningsdata. Det ble videre hevdet at håndholdte dataenheter (og «Bring Your Own Device») stilte institusjonene overfor nye sikkerhetsutfordringer som var vanskelige å håndtere. Disse utfordringene ble, ifølge flertallet av de som ble intervjuet, forsterket ved at bevisstheten om trusler mot informasjonssikkerheten blant vitenskapelig (og administrativt) ansatte ble ansett som mangelfull.

Selv om truslene mot informasjonssikkerheten ble vurdert som økende og sammensatte, ble det i liten grad rapportert om at dette førte til økt satsing på informasjonssikkerhet (eller at økte satsninger var utilstrekkelige). Ved noen få institusjoner hadde enkelte uønskede hendelsene blitt brukt til intern «markedsføring» av informasjonssikkerhet, spesielt overfor ledelsen sentralt eller på fakultetsnivå. Men den gjennomgående vurderingen var at uønskede hendelser (og mer kompliserte sikkerhetsutfordringer) ikke i vesentlig utstrekning påvirket arbeidet med styring av informasjonssikkerheten. Mange tilkjennega derfor en viss bekymring for at toppledere eller fakultetsledelsen i praksis enten aksepterte

83 Databehandleravtaler er lovpålagt når personopplysninger behandles av en ekstern tjenesteleverandør, se personopplysningsloven § 15, jf. § 13. Datatilsynet har utarbeidet en veileder og mal for databehandleravtaler som er tilgjengelig på http://www.datatilsynet.no/Sikkerhet-internkontroll/Databehandleravtale/.

eller var «lykkelig uvitende» om potensielle og alvorlige trusler mot institusjonenes informasjonsverdier. Frem til nå var det, ifølge disse intervjuobjektene, flaks eller tilfeldigheter som hadde forskånet institusjonene for alvorlige sikkerhetsbrudd.

Tilpasning av styringssystemene

Standarder for informasjonssikkerhet, for eksempel ISO/IEC 27001: 2013, og viktige deler av lovgivningen på området (spesielt bestemmelsene om informasjonssikkerhet i personopplysningsloven med forskrift), forutsetter at styringssystemenes omfang og utforming tilpasses lokale organisasjonsforhold. I universiteter og høyskoler vil det typisk dreie seg om forhold som institusjonsstørrelse (antallet ansatte og studenter), organisatorisk kompleksitet (ulike typer fakultet, grunnenheter, museum, bibliotek, osv.), faglige satsningsområder (tradisjonelle universitetsfag, yrkesutdanning eller spesialiserte universiteter/høyskoler) eller geografisk avstand (samlokalisert eller spredt virksomhet).[84] Lokaltilpasning er derfor en viktig del av standarder for og rettslige regler om informasjonssikkerhet, og oppfattes som avgjørende for at hver enkelt organisasjon eller institusjon skal utvikle et styringssystem som harmonerer best mulig med deres spesifikke behov og utfordringer.[85] Det innebærer at lokaltilpasning (i teorien) blir sett på som en viktig betingelse for vellykket innføring og drift av styringssystemene.

Drøftelsene i del II av denne rapporten indikerte at i de 13 institusjonene som helt eller delvis hadde skriftliggjort sine styringssystemer for informasjonssikkerhet, var systemene i begrenset grad forsøkt lokaltilpasset. Som vi så i denne delen, hadde helt ulike institusjoner tilnærmet identiske styringssystemer på papiret. I del III så vi i tillegg at bare noen få av disse institusjonene rapporterte at de helt eller delvis hadde lyktes med å implementere styringssystemene. Utfordringen som dette virket å skape i majoriteten av de 13 institusjonene, var at systemene i mange tilfeller fremstod (på papiret) som overdimensjonerte – de virket å være omfattende, ambisiøse og ressurskrevende sammenliknet med de forskjellige institusjonenes mer nøkterne behov.

---

84 Behovet for og forventninger om lokaltilpasning av styringssystemene kommer også klart til uttrykk i Kunnskapsdepartementets tildelingsbrev til institusjonene (2013).

85 Se for eksempel Steve G. Watkins (2013): *An Introduction to Information Security and ISO 27001: 2013*. Ely: IT Governance Pub., eller Dag W. Schartum (2005): «Krav til sikring av personopplysninger». I Arild Jansen og Dag W. Schartum (red.): *Informasjonssikkerhet. Rettslige krav til sikker bruk av IKT*. Bergen: Fagbokforlaget. Se også Datatilsynet (2000): *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*. Tilgjengelig på https://www.datatilsynet.no/Global/05_regelverk/sikkerhetsbest_personopplforskriften_kom.pdf.

Mange av de som ble intervjuet ga da også uttrykk for at arbeidet med styringssystemer var preget av mye «papirarbeid» og at dokumentasjonen hadde kommet på plass som følge av et «skippertak» for noen tid tilbake. I denne prosessen hadde behovet for lokaltilpasning ikke blitt tillagt like stor vekt som hensynet til å få et dokumentert styringssystem på plass. Deretter var det meningen av styringssystemene skulle innføres i institusjonene slik de ble beskrevet i dokumentene. Vi har imidlertid sett at bare noen få institusjoner mente de hadde lykkes med dette. Isteden kunne det i flertallet av institusjonene virke som dokumentasjonsomfanget og kompleksiteten stod litt i veien for lokaltilpasningen og det praktiske arbeidet.

Dette hang dels sammen med at policyer og prinsipper for informasjonssikkerhet var vedtatt uten at det samtidig ble tilført tilstrekkelige ressurser til arbeidet med innføring og drift av styringssystemene. Dermed ble enkelte institusjoner sittende med overdimensjonerte og underfinansierte styringssystemer. Dels hang det sammen med at enkelte institusjoner manglet kompetanse på hvordan styringssystemene kunne tilpasses lokale institusjonsbehov på en måte som førte til at systemene verken ble overdimensjonerte eller underfinansierte. I noen institusjoner ga man for eksempel uttrykk for at man ikke helt så for seg hvordan man skulle greie å komme seg fra «skrivebordet» til «arbeidsbenken» – fra teori til praksis – med de styringssystemene som var vedtatt (det ville i så fall kreve endringer i måten systemene i teorien var tenkt å fungere på).

I flere andre institusjoner virket det som behovet for lokal tilpasning var en problemstilling som i liten grad ble vurdert eller tatt på alvor. Hovedårsaken til dette syntes å være en bekymring for at prosesser med lokal tilpasning kunne føre til at styringssystemene enten avvek for mye fra anbefalte standarder for slike systemer eller at de ikke lengre harmonerte med rettslige krav som ble stilt til hvordan systemene skulle oppbygges og fungere. Det var derfor tryggere «å følge den smale sti» – ikke foreta for mange egne valg og lokale tilpasninger – og heller legge seg tett opp til nasjonale eller internasjonale normer for denne typen styringssystemer. Da var man på den sikre siden og unngikk å gjøre for mye galt.

Selv i de få institusjonene hvor det ble rapportert at styringssystemene i noen grad fungerte, det vil si at viktige aktiviteter (spesielt gjennomføring av risikovurderinger og innføring av sikringstiltak) ble planlagt og gjennomført, ble det erkjent at lokal tilpasning av styringssystemene var utfordrende. Istedenfor at dokumentinnholdet var tilpasset lokale institusjonsforhold og behov, virket det som praksisen – selve arbeidet og hvordan det ble organisert og utført – hadde gjennomgått en slik tilpasningsprosess, ofte drevet av én eller et par personer med særlig ansvar for informasjonssikkerheten. Dermed oppstod det et misfor-

hold mellom praksis, som til en viss grad var lokaltilpasset, og sikkerhetsdokumentasjonen, som ikke var det. Det viktigste for disse institusjonene var likevel ikke at dokumentasjonen i alle detaljer var i henhold til nasjonale eller internasjonale normer for styringssystemer, men at aktiviteter ble planlagt og iverksatt selv måten dette ble gjort på ikke alltid samsvaret med innholdet i den lokale sikkerhetsdokumentasjonen.

Det som preget disse institusjonene var følgelig at de hadde (bevisst eller ubevisst) sett bort i fra deler av sin egen dokumentasjon – og problemene den representerte når det gjaldt innføring og drift. Isteden hadde de prøvd seg frem og «latt veien bli til mens de gikk». Det innebar at fremfor å innføre «standard skrivebordsprodukter» hadde de bygd opp et sitt eget styringssystem på siden av det offisielle og dokumenterte, vanligvis ved hjelp av relativt enkle midler (for eksempel skjema for risikovurderinger og sjekklister for egenkontroll). På denne måten hadde styringssystemene i praksis (men ikke i like stor grad på papiret) fått en lokal valør som ga dem en overlevelseskraft de trolig ellers ikke ville hatt.

Eksterne aktørers betydning

I del I av rapporten så vi at eksterne aktørers fokus på informasjonssikkerhet i universiteter og høyskoler har økt i løpet av de siste årene. I tildelingsbrevene fra Kunnskapsdepartementet til institusjonene stilles det for eksempel eksplisitte krav til arbeidet med informasjonssikkerhet og etablering av styringssystemer. For å styrke innsatsen på området har Kunnskapsdepartementet opprettet «Sekretariatet for informasjonssikkerhet i UH-sektoren». Samtidig har Riksrevisjonen fokusert på informasjonssikkerhet og styringssystemer ved revisjoner hos universiteter og høyskoler. Til slutt har Datatilsynet gjennomført en rekke stedlige tilsyn hos universiteter og høyskoler for å kontrollere etterlevelsen av bestemmelsene i personopplysningsloven med forskrift. I dette kontrollarbeidet har tilsyn med praktisering av reglene om informasjonssikkerhet stått sentralt.

Til sammen innebærer dette at krav og forventninger fra eksterne aktører (myndighetsorganer) har økt, og at institusjonene er under noe større press enn hva de har vært tidligere. Spørsmålet er hvordan krav og forventninger fra de nevnte eksterne aktørene har påvirket institusjonenes arbeid med informasjonssikkerhet og styringssystemer? Har det økte presset utenfra hatt betydning for institusjonenes egne prioriteringer?

Oppfatningen blant intervjuobjektene var relativt entydig: økte krav og forventninger fra eksterne aktører hadde hatt en viss betydning for institusjonenes prioritering av arbeidet med styring av informasjonssikkerheten. Spesielt tildelingsbrevene fra Kunnskapsdepartementet og revisjoner fra Riksrevisjonen ble vektlagt. Begge deler ble fremstilt som «vekkere»: det hadde bidratt til at den generelle innsatsen på informasjonssikkerhetsområdet var noe styrket og at mellomledere og toppledelsen tok arbeidet med informasjonssikkerhet mer på alvor. I institusjoner som hadde hatt tilsyn fra Datatilsynet, ble tilsvarende effekter av kontrollbesøkene nevnt. Som eksempler på styrket innsats ble det pekt på flere forhold. Enkelte institusjoner hadde for eksempel utnevnt en daglig ansvarlig for informasjonssikkerhet eller hadde overført dette ansvaret til ledere utenfor IT-avdelingen/seksjonen. Andre institusjoner rapporterte at de hadde gjennomført noen flere aktiviteter enn tidligere (spesielt risikovurderinger), at enkelte nye sikringstiltak var iverksatt, at sikkerhetsdokumentasjonen hadde blitt revidert og oppdatert eller at det var igangsatt et arbeid for å etablere et dokumentert styringssystem. Drøftelsene i del III indikerer likevel at det økte innsatsen ikke resulterte i at flere institusjoner hadde etablert fungerende styringssystemer for informasjonssikkerhet. Det kan derfor se ut som den økte innsatsen manglet den systematikken og planmessigheten som er ment å kjennetegne slike styringssystemer.

Samtidig er det verdt å legge merke til at innsatsen, ifølge institusjonene selv, primært ble styrket på områder hvor det eksisterte tydelige rettslige krav til informasjonssikkerheten. Som tidligere nevnt, gjaldt dette i særlig grad på personvernområdet, det vil si at innsatsen skjedde med utgangspunkt i personopplysningsloven og (til en viss grad) helseforskningsloven. Selv om det i sikkerhetsdokumentasjonen til flere institusjoner også ble nevnt andre lover og forskrifter som hadde betydning for arbeidet med informasjonssikkerhet, for eksempel forvaltningsloven, offentlighetsloven og arkivloven, var inntrykket at disse lovene og forskriftene hadde relativt begrenset betydning for det praktiske arbeidet.

Noe av grunnen var trolig at disse regelverkene ikke i samme utstrekning som for eksempel personopplysningsloven (med forskrift) inneholder omfattende og tydelige informasjonssikkerhetsplikter (og at regeletterlevelsen ikke er gjenstand for tilsyn). Sett i et rettslig perspektiv, er det derfor ikke unaturlig at personopplysningsloven (og i mindre grad helseforskningsloven) fikk en spesielt opphøyd posisjon sammenliknet med andre relevante regelverk. At innsatsen ble styrket på områder hvor det forelå tydelige rettslige krav, kan indikere at det var kombinasjonen av eksternt press og rettslige plikter, snarere enn det eksterne presset i seg selv, som hadde betydning for institusjonenes arbeid med infor-

masjonssikkerhet. Likevel virker det trolig at uten større eksternt press ville fokuset på overholdelse av spesielt omfattende rettslige forpliktelser vært noe mindre enn hva som ble rapportert å være tilfelle.

Til slutt var det en annen og «mykere» form for eksternt press som hadde påvirket institusjonenes informasjonssikkerhetsinnsats. Her var det snakk om den påvirkningen som arbeidet til UNINETT representerte. I del II har vi sett at de 13 institusjonene med skriftliggjorte styringssystem i stor grad hadde lagt UNINETTs informasjons- og veiledningsmateriale til grunn for sin egen dokumentasjon. Ut over dette, rapporterte flere institusjoner at de hadde hatt besøk fra ansatte i UNINETT hvor informasjonssikkerhet stod på agendaen. Besøkene hadde enten resultert i at risikovurderinger av informasjonssikkerheten ble gjennomført eller at skriftliggjorte styringssystem ble utarbeidet (eller begge deler). I enkelte institusjoner som hadde mottatt besøk av UNINETT for en tid tilbake (4-6 år), ble det rapportert at nyere krav fra Kunnskapsdepartementet, Riksrevisjonen eller Datatilsynet førte til en videreføring av det arbeidet som da ble gjort, men som deretter ble liggende mer eller mindre brakk. Disse institusjonene erkjente imidlertid at de enda hadde et stort arbeid å gjøre før et fungerende styringssystem var på plass. Likevel kan det virke som kombinasjonen av UNINETTs «myke» press og andre eksterne aktørers «harde» press hadde ført til en viss revitalisering av informasjonssikkerhetsinnsatsen.

Spørsmålet som drøftelsene av mulige løsninger reiser, er hva som skal til for at styringssystemer for informasjonssikkerhet i større grad enn i dag blir innført og satt i drift i universiteter og høyskoler? Den siste delen av denne rapporten vil forsøke å gi en samlet vurdering av dette spørsmålet. Her vil de funnene som er presentert i de tidligere delene bli drøftet (kort) i lys av den internasjonale forskningen på innføring og drift av tilsvarende styringssystemer som arbeidet med informasjonssikkerhet baserer seg på.

Del VI: Resultatene og forskningen

I denne avsluttende delen av rapporten behandles sentrale funn og konklusjoner fra den internasjonale forskningen på innføring og drift av tilsvarende styringssystemer som arbeidet med informasjonssikkerhet bygger på.

Den internasjonale forskningen har ikke sett eksplisitt på informasjonssikkerhet. Isteden handler den i stor grad om innføring og drift av lovpålagte styringssystemer på områder som for eksempel helse-, miljø- og sikkerhet, økonomi- og regnskap, anti-diskriminering, kvalitetssikring eller miljøsertifisering. Forskningen har heller ikke fokusert spesielt på universiteter eller høyskoler, men på andre typer virksomheter i offentlig eller privat sektor. Likevel kan resultatene være av en viss interesse. Dette fordi de styringssystemene som har vært studert bygger på de samme prinsippene, logikken og arbeidsmetodikken som risikostyrt informasjonssikkerhet.

I den internasjonale forskningen fremheves fem forutsetninger (eller forhold) som er avgjørende for at lovpålagte styringssystemer skal fungere etter hensikten. De fem forutsetningene som pekes ut er:

1. Ledelsesforankring.
2. Interne pådrivere.
3. Eksternt press/påvirkning.
4. Lokaltilpasning.
5. Integrering i daglige aktiviteter.[86]

86 Disse forutsetningene oppsummeres og diskuteres i blant annet Robert Baldwin, Martin Cave & Martin Lodge (2012): *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press; Martin Lodge & Kai Wegrich (2012): *Managing Regulation: Regulatory Analysis, Politics and Policy*. Basingtstoke: Palgrave Macmillan; Robert Baldwin, Martin Cave & Martin Lodge (red.) (2010): *The Oxford Handbook of Regulation*. Oxford: Oxford University Press; Bridget Hutter (red.) (2010): *Anticipating Risks and Organising Risk Regulation*. Cambridge, UK: Cambridge University Press; Bronwen Morgan & Karen Yeung (2009): *An Introduction to Law and Regulation*. Cambridge, UK: Cambridge University Press; Bridget Hutter og Michael Power (red.) (2005): *Organizational Encounters with Risk*. Cambridge, UK: Cambridge University Press; Christine Parker (2002): *The Open Corporation. Effective Self-Regulation and Democracy*. Cambridge, UK: Cambridge University Press; Bridget Hutter (2001): *Regulation and Risk. Occupational Health and Safety on the Railways*. Oxford: Oxford University Press. Annen relevant og mer generell litteratur om risikostyring som også ligger til grunn for drøftelsene nedenfor inkluderer: Michael Power (2007): *Organized Uncertainty. Designing a World of Risk Management*. Oxford: Oxford University Press; Christopher Hood, Henry Rothstein og Robert Baldwin (2001): *The Government of Risk. Understanding Risk Regulation Regimes*. Oxford: Oxford University Press; Christopher Hood og David Jones (red.) (2001): *Accident and Design. Contemporary Debates in Risk Management*. London: Routledge.

Det fremheves videre at sjansen for vellykket innføring og drift av interne styringssystemer er størst når alle de fem forutsetningene er til stede. Likevel er enkelte av dem viktigere enn andre, det vil si at noen av forutsetningene har større betydning for vellykket innføring og drift enn andre. Dette vil vi komme tilbake til i drøftelsene nedenfor.

Nedenfor vil innholdet i hver enkelt av de fem forutsetningene bli drøftet og sammenstilt med funnene som er diskutert tidligere i denne rapporten. Spørsmålet som stilles er derfor om (og i hvilken grad) de ulike forutsetningene kan sies å være til stede i de 20 universitetene og høyskolene som er undersøkt? Dersom én eller flere av forutsetningene ikke er til stede (generelt sett), kan det gi indikasjoner på hvor «skoen trykker» og hvilke typer tiltak som kan iverksettes for å styrke arbeidet med informasjonssikkerhet. Drøftelsene kan i tillegg leses som en oppsummering av de mest sentrale funnene fra undersøkelsen.

Ledelsesforankring

I forskningslitteraturen fremheves ledelsesforankring som avgjørende for vellykket etablering og drift av liknende styringssystemer som informasjonssikkerhetsarbeidet i universiteter og høyskoler er ment å basere seg på. Som allerede antydet, handler ledelsesforankring om tre forhold:

1. Synliggjøring av fagområdet internt i virksomhetene (informasjonssikkerhet).
2. Økt prioritering av ressurser og tydelige krav til arbeidet med informasjonssikkerhet.
3. Tettere oppfølging av arbeidet med informasjonssikkerhet.

Vi har sett at noen universiteter og høyskolene rapportert at toppledelsen hadde kjennskap til og var involvert i arbeidet med informasjonssikkerhet. I flertallet av institusjonene var dette imidlertid ikke tilfelle. Også i institusjoner som hadde opprettet sikkerhetsforum var erfaringene varierende med hensyn til om forumet/møteplassen bidro til økt kjennskap og involvering fra toppledelsens side. I noen av institusjonene var svaret «ja», men i flertallet av dem var svaret «nei». Inntrykket var altså at toppledelsen ikke (eller i liten grad) «frontet» arbeidet med informasjonssikkerhet overfor andre ledere og ansatte. Vi kan derfor si at punkt 1 ovenfor – synliggjøring – i noen grad var ivaretatt i noen få institusjoner. I de andre institusjonene var synliggjøringen i beste fall var begrenset til at ledelsen/styret hadde behandlet og vedtatt innføringen av et styringssystem. Deretter involverte toppledelsen seg lite (eller ikke i det hele tatt) i det praktiske

arbeidet, noe som blant annet førte til at styringssystemene (og hva de innebar) i beskjeden grad ble bekjentgjort overfor øvrige ledere og ansatte.

Selv i institusjoner hvor hensynet til synliggjøring (bekjentgjøring) var ivaretatt, ble vanligvis ikke punkt 2 og 3 – prioriteringer og oppfølging – vektlagt. Det var for eksempel relativt sjeldent at ledelsen imøtekom forespørsler om økt ressurser (spesielt dedikerte stillinger og kompetansehevingstiltak) eller holdt seg informert om, stilte krav til og fulgte opp det videre arbeidet med informasjonssikkerhet (via ledelsens gjennomgang). Det synes derfor riktig å si at den første forutsetningen – ledelsesforankring – generelt sett (men med enkelte unntak) ikke var oppfylt i de 20 institusjonene.

Interne pådrivere

I forskningslitteraturen fremheves interne pådrivere som viktig for vellykket innføring og drift av styringssystemer. Med dette menes at arbeidet med innføring og drift ledes av ansatte/ledere (eller grupper av ansatte) som har spesiell interesse for, og som føler et særskilt faglig ansvar for, det aktuelle arbeidsområdet (informasjonssikkerhet). Uten at denne typen medarbeidere finnes internt i organisasjoner eller institusjoner, er mulighetene, ifølge forskningen, små for at styringssystemer blir innført og satt i drift.

I mange av de undersøkte institusjonene fantes medarbeidere som kan beskrives som interne pådrivere. Her handlet det om medarbeidere som enten var utpekt til eller hadde påtatt seg oppgaven som CSO/CISO, informasjonssikkerhetsrådgiver eller personvernombud. Disse medarbeiderne fremstod i mange tilfeller som særlig opptatt av og interesserte i informasjonssikkerhet, men opplevde (ifølge dem selv) ofte at deres personlige innsats ikke alltid gjorde en særlig stor forskjell. Hovedårsaken til dette ble hevdet å være at de interne pådriverne manglet hensiktsmessige rammebetingelser og arbeidsvilkår (med rammebetingelser og arbeidsvilkår siktes det i første rekke til prioriteringer og ressurser). Det typiske var at effektene av engasjementet og innsatsen til interne pådrivere var mindre enn hva som virket å være nødvendig for å få styringssystemene innført og satt i drift. Det kunne også se ut som effektene av engasjementet og innsatsen ble redusert noe av begrenset kjennskap til risikobasert arbeidsmetodikk og bruken av konkrete arbeidsredskaper. Selv om det kan stilles spørsmålstegn ved effekter, rammebetingelser og kompetanse, synes det likevel riktig å konkludere med at eksistensen av interne pådrivere var en forutsetning som var oppfylt i flertallet av de kartlagte universitetene og høyskolene.

Eksternt press eller påvirkning

I forskningslitteraturen fremheves eksternt press eller påvirkning, spesielt fra myndigheter, media eller opinionen, som viktige motivasjonsfaktorer ved innføring og drift av tilsvarende styringssystemer som anvendes i informasjonssikkerhetsarbeidet. Det fremheves også at eksternt press eller påvirkning kan bidra til styrket ledelsesforankring og til å gi faglig eller moralsk støtte til interne pådrivere.

Vi har sett at ulike former for ekstern press eller påvirkning var til stede i universitets- og høyskolesektoren. Presset eller påvirkningene kom for eksempel fra Kunnskapsdepartementet (blant annet gjennom tildelingsbrev til institusjonene), Datatilsynet (gjennom stedlige kontroller) og Riksrevisjonen (gjennom forvaltningsrevisjoner). Vi har også sett at det eksterne presset hadde bidratt til at arbeidet med informasjonssikkerhet generelt sett ble prioritert noe sterkere på institusjonsnivå enn tidligere. Andre eksterne aktører som bidro til dette var UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren. De to siste aktørene spilte en noe annen rolle for det lokale arbeidet enn hva tilfelle var for Kunnskapsdepartementet, Datatilsynet eller Riksrevisjonen – de fungerte i større grad som faglige sparringpartnere og rådgivere. Andre myndighetsorganer, for eksempel Direktoratet for IKT og Forvaltning (DIFI)[87] eller Norsk Senter for Informasjonssikring (NorSIS),[88] var ikke like viktig. Enkelte institusjoner hadde likevel benyttet seg av DIFIs kurstilbud (i ISO/IEC 27001: 2013) eller NorSIS sine informasjonspakker om informasjonssikkerhet.

Med unntak av noen få og store institusjoner, virket det ikke som publisitet og offentlighet, for eksempel oppslag om sikkerhetshendelser i studentaviser, dagspressen eller i etermediene, spilt noen fremtredende rolle som katalysator for arbeid med styringssystemer og informasjonssikkerhet. Likevel synes det riktig å si at de undersøkte institusjonene var utsatt for ikke ubetydelig eksternt press eller påvirkning.

Lokaltilpasning

I forskningslitteraturen legges det vekt på at den typen styringssystemer som arbeidet med informasjonssikkerhet bygger på, må tilpasses lokale forhold og behov. Det er gjennom lokal tilpasningen at styringssystemene får intern for-

87 http://www.difi.no/.
88 https://norsis.no/.

ankring og overlevelseskraft, og det er på denne måten at styringssystemene dimensjoneres «riktig» i relasjon til lokale forhold og behov.

Noen av institusjonene som ble undersøkt hadde forsøkt å gjøre visse lokale tilpasninger i sikkerhetsdokumentasjonen, blant annet for å unngå at styringssystemet ble for omfattende og ressurskrevende. Noen få andre institusjoner hadde i tillegg utviklet en praksis som var mer tilpasset lokale forhold og behov enn hva deres sikkerhetsdokumentasjon antydet. Det virket likevel som de fleste av de 13 institusjonene hadde egne styringssystemer bare i begrenset utstrekning hadde forsøkt å tilpasse dem til lokale organisatoriske eller teknologiske forhold. Formlikheten mellom institusjonenes systemdokumentasjon var derfor relativt stor. Samtidig var det trolig at en del elementer i systemdokumentasjonen kunne gjenbrukes på tvers av institusjoner, for eksempel beskrivelser av sikkerhetsmål eller sikkerhetsstrategier. Hovedinntrykket var likevel at gjenbruk primært handlet om «kopiering» snarere enn lokaltilpasning.

Dessuten virket det som tilfanget og mangfoldet av standarder og «beste praksis» skapte en viss usikkerhet om hva som var «den beste oppskriften her hos oss». Mange institusjoner etterspurte informasjon, veiledninger og konkrete arbeidsverktøy (maler) som var mindre generiske og basert på større grad av skreddersøm (tilpasninger til sektoren eller til egen institusjon). Det ble hevdet at dette ville forenkle arbeidet og redusere kostnadene med innføring og drift av styringssystemene. Generelt sett kan vi derfor si at lokaltilpasning var en forutsetning som bare i begrenset utstrekning var oppfylt i de undersøkte institusjonene.

Integrering i daglige aktiviteter

I forskningslitteraturen understrekes det at det viktigste målet for suksess er om styringssystemene integreres i daglige aktiviteter. Dette handler om i hvilken grad styringssystemene, og de aktivitetene som skal utføres innenfor rammen av styringssystemene, blir en naturlig del av arbeidshverdagen, eller om det dreier seg om ad hoc-tiltak som gjennomføres med stor fanfare fra tid til annen (eller ikke i det hele tatt). Integrering i daglige aktiviteter skal blant annet føre til at styringssystemene blir personelluavhengige: personellendringer – at ledere eller ansatte kommer og går – skal ikke i vesentlig grad påvirke driften av styringssystemene (verken i positiv eller negativ retning).

I de 20 undersøkte institusjonene fremstod integrering av styringssystemer for informasjonssikkerhet i daglige aktiviteter som den største utfordringen. I en-

kelte universiteter og høyskoler hadde IT-teknisk sikkerhet blitt en relativt naturlig og daglig del av virksomheten i IT-avdelingene/seksjonene, for eksempel når det gjaldt systemdrift eller nettverksadministrasjon. Det samme var ikke i like stor grad tilfelle på andre områder eller med hensyn til informasjonssikkerhet generelt, for eksempel innenfor administrasjonsapparatet og store deler av forskningsvirksomheten. Her var det vanlige at verken IT-teknisk sikkerhet spesielt eller informasjonssikkerhet generelt ble oppfattet som naturlige eller dagligdagse arbeidsoppgaver.

I andre institusjoner var informasjonssikkerheten i noen grad en del av IT-relaterte og administrative arbeidsoppgaver, men også her hang forsknings- og undervisningsaktiviteten etter. I en tredje gruppe institusjoner dekket arbeidet med informasjonssikkerhet de fleste relevante virksomhetsområdene, men arbeidet ble beskrevet som sårbart, det vil si avhengig av én eller noen få enkeltpersoner. I en fjerde gruppe institusjoner var arbeidet med informasjonssikkerhet ikke integrert i noen av disse institusjonenes løpende oppgaver (med et visst unntak for IT-drift).

Hovedkonklusjonen er derfor at selv om IT-teknisk sikkerhet til en viss grad hadde fått fotfeste i IT-avdelingene/seksjonene (i alle fall i en del av institusjonene), var integreringen av arbeidet med informasjonssikkerhet i resten av institusjonslandskapet svak eller ikke-eksisterende.

Oppsummering

Drøftelsen i denne avsluttende delen indikerer at to av de fem forutsetningene som forskningslitteraturen identifiserer som viktige ved innføring og drift av risikobaserte styringssystemer, kan sies å være til stede i de 20 universitetene og høyskolene. Dette var (a) interne pådrivere (medarbeidere med interesse og engasjement for IT- eller informasjonssikkerhet) og (b) eksternt press eller påvirkning (spesielt krav og forventninger fra ulike myndighetsorganer).

De tre andre forutsetningene kan ikke – eller kan i svært begrenset utstrekning – sies å være oppfylt. Disse forutsetningene var (a) ledelsesforankring (toppledelsens prioritering av og involvering i arbeidet med informasjonssikkerhet), (b) lokaltilpasning av styringssystemer (styringssystemet «skreddersys» lokale forhold og behov) og (c) integrering i daglige aktiviteter (stabil driftssituasjon med hensyn til styringssystemet). Det kan derfor synes som det er på disse områdene at arbeidet med styringssystemer for informasjonssikkerhet i universiteter og høyskoler har mest å hente.

Samtidig er det verdt å legge merke til at de forutsetningene som i minst utstrekning var oppfylt også er de som forskningslitteraturen fremhever som viktigst (mens de forutsetningene som er mindre avgjørende, i større grad ble oppfylt). Spesielt integrering i daglige aktiviteter og ledelsesforankring fremheves i litteraturen som avgjørende. Når manglene på viktigste områdene kan sies å være relativt store, innebærer det at den vanskeligste delen av jobben gjenstår for majoriteten av de undersøkte institusjonene.

Det er i tillegg viktig å være oppmerksom på at flere av forutsetningene ikke bare er løsninger på et problem. De kan også, paradoksalt nok, være en del av selve problemet. Den internasjonale forskningen sier for eksempel at ledelsesforankring er en viktig suksessfaktor. Men hva skjer dersom ledelsesforankring er problemet, det vil si at ledelsens manglende involvering, engasjement og prioriteringer hindrer innføring og drift? I en slik situasjon må «problemet ledelsesforankring» løses før ledelsesforankring kan bli en suksessfaktor. Men hvem skal gjøre dette og hvordan? Hvilke grep kan gjøres for at ledelsesforankring skal gå fra å være et problem – noe institusjonene ikke får til og ikke helt vet hvordan de skal håndtere – til å bli en ressurs i arbeidet med styringssystemene? Det samme kan sies om en annen avgjørende forutsetning: integrering i daglige aktiviteter. Dersom integrering mangler i institusjon X eller institusjon Y, så er situasjon at «den store løsningen» er «det store problemet». Hvordan kan dette problemet håndteres slik at integreringen bidrar til snarere enn hindrer vellykket innføring og drift?

Å finne praktiske svar på denne typen spørsmål virker å være den største utfordringen som arbeidet med styringssystemer for informasjonssikkerhet i UH-sektoren står overfor.

Prosjektet «Informasjonssikkerhet i universitets- og høyskole-sektoren» finansieres av UNINETT og gjennomføres i samarbeid mellom Sekretariatet for informasjonssikkerhet i UH-sektoren og Senter for rettsinformatikk (SERI), Universitetet i Oslo.

I denne første rapporten fra prosjektet drøftes fire hovedspørsmål:

1. I hvilken grad hadde universiteter og høyskoler etablert skriftliggjorte styringssystemer for informasjonssikkerhet?
2. I hvilken grad hadde universiteter og høyskoler med skriftliggjorte styringssystemer innført systemene og satt dem i drift?
3. Hvilke utfordringer – hindringer eller barrierer – påvirket innføring og drift av styringssystemene?
4. Hvordan forsøkte institusjonene å håndtere utfordringer de stod overfor ved innføring og drift av styringssystemene?

Rapporten gir foreløpige svar på disse spørsmålene. Rapporten bygger på informasjon – skriftlig dokumentasjon og intervjuer med nøkkelpersonell – innhentet fra 20 av drøyt 30 statlige universiteter og høyskoler som er tilknyttet forskningsnettet i Norge og som betjenes av Sekretariatet for informasjonssikkerhet i UH-sektoren.

Tommy Tranvik er ansatt som forsker ved Senter for rettsinformatikk, Universitetet i Oslo.

9 788272 261589

CompLex