

DINH UY TRAN



INFORMASJONS- SIKKERHETS- LEDELSE

EN HOLISTISK TILNÆRMING

Dinh Uy Tran

Informasjonssikker- hetsledelse

En holistisk tilnærming

ÇAPPELEN DAMM AKADEMISK

Innhold

Forord	13
Introduksjon	16
Målgruppen	16
Datainnsamling	16
Personlige egenskaper	17
Relevante fagfelt som ikke er direkte relatert til informasjonssikkerhet	18
Informasjonssikkerhetsfaget	18
Faglitteratur	18
Oppsummering	21
Struktur	21
Del 1	
PERSONLIG UTVIKLING	23
Kapittel 1	
Selvinnsikt	25
1.1 Stimuli	26
1.2 Tankesett	27
Kjerneverdier	27
Lærende og låst tankesett	31
Effektiv læring	31
Realistisk og idealistisk tankesett	33
1.3 Oppsummering	37
Kapittel 2	
Selvbeherskelse	38
2.1 Motivasjon	39
2.2 Hindringer	42
2.3 Oppsummering	43

Kapittel 3

Personlig effektivitet	44
3.1 Speedreading	46
3.2 Memo	47
3.3 Oppsummering	49

Del 2

LEDELSE	51
----------------------	----

Kapittel 4

Mellommenneskelig ledelse	55
4.1 Motivering	56
4.2 Veileding/coaching	57
Lytting	58
Sokratisk metode	60
Coachingstil	61
4.3 Kommunikasjon	64
Konflikthåndtering	65
Presentasjonsteknikker	67
4.4 Oppsummering	68

Kapittel 5

Administrativ ledelse	69
5.1 Omsetting av strategisk mål til praktisk mål	70
5.2 Organisering	72
5.3 Organisasjonsstruktur og prosess	73
Prosessmodenhet	78
5.4 Organisasjonskultur	79
Hvordan påvirke kulturen?	80
Hvordan bevare ønsket kultur?	81
5.5 Jobbutforming	82
5.6 Oppsummering	83

Kapittel 6

Strategisk ledelse	84
6.1 Organisering av styret	86
6.2 Organisering av styringsmodell	87
6.3 Beslutningstagning	93

6.4	Oppsummering	96
-----	--------------------	----

Kapittel 7

	Faglig ledelse og sektor-/bransjekunnskap	97
--	--	-----------

7.1	Ledelsesspråk	98
-----	---------------------	----

7.2	Oppsummering	102
-----	--------------------	-----

Del 3

	INFORMASJONSSIKKERHET	103
--	------------------------------------	------------

Kapittel 8

	Grunnlaget for informasjonssikkerhetsarbeid	105
--	--	------------

8.1	De 4 P-ene	106
-----	------------------	-----

8.2	Sikkerhetstiltak	108
-----	------------------------	-----

8.3	Sammenhengen mellom sikkerhetstiltak og de 4 P-ene	110
-----	--	-----

Kapittel 9

	Informasjonssikkerhetsfag	112
--	--	------------

Kapittel 10

	Grunnleggende nivå	115
--	---------------------------------	------------

10.1	Juridiske aspekter	117
------	--------------------------	-----

10.2	Håndtering av informasjonsverdi	117
------	---------------------------------------	-----

10.3	Operativsystem, virtualisering og systemarkitektur	119
------	--	-----

10.4	Kryptografi	119
------	-------------------	-----

10.5	Kommunikasjonssikkerhet	124
------	-------------------------------	-----

10.6	Identitet og tilgangsstyring (IAM)	127
------	--	-----

10.7	Etterforskning, logging og overvåkning	130
------	--	-----

10.8	Fysisk sikkerhet og personellsikkerhet	132
------	--	-----

10.9	Konfigurasjons- og endringshåndtering	134
------	---	-----

10.10	Sikker utvikling	135
-------	------------------------	-----

10.11	Skadevarer	135
-------	------------------	-----

Kapittel 11

	Fordypningsnivå	138
--	------------------------------	------------

11.1	Trusseletterretning	139
------	---------------------------	-----

	Trusseletterretningsprosessen	140
--	-------------------------------------	-----

	Trusselvurderinger	142
--	--------------------------	-----

11.2	Sosial påvirkning.....	144
	Hva er sosial påvirkning?	145
	Rammeverket for sosial påvirkning	146
11.3	Styring av etterlevelse.....	152
11.4	Virksomhets-, IKT- og applikasjonsarkitektur	154
11.5	Sikkerhetsvurdering og testing	155
	Hva er en penetrasjonstest, og hvilke andre tester finnes det?	155
	Hva er fasene innenfor penetrasjonstesting?	157
11.6	Hendelsehåndtering.....	158
	Hva er en hendelse?	159
	Hva er forskjellen mellom en hendelse og en trussel?	162
11.7	Livssyklus håndtering for programvareutvikling.....	164
	Fasene innenfor livssyklus håndtering for programvareutvikling ...	164
	Utviklingsmodeller.....	166

Kapittel 12

Spesialistnivå	167	
12.1	Informasjonssikkerhetsstyring.....	168
	Hva er informasjonssikkerhetsstyring?	169
	Hva består informasjonssikkerhetsstyring av?.....	169
	Hva er et dokumentasjonshierarki?	172
	Hvordan måle informasjonssikkerhet?.....	174
12.2	Risikostyring	176
	Hva er risikostyring?.....	177
	Finnes det ulike nivåer av risikostyring?.....	178
	Hva er en risiko?	178
	Hva er de ulike risiko- og konsekvenstypene?.....	181
	Hva er forskjellen mellom risiko og en hendelse?.....	184
	Hva er uvisshetsdimensjonen?.....	185
	Hva er tidsdimensjonen?.....	186
	Hva er forskjellen mellom positiv og negativ risiko?.....	187
	Hva er de ulike fasene innenfor risikostyring?	187
	Hva er forskjellen mellom risikovurdering og risikostyring?.....	194
12.3	Beredskap	195
	Hva er beredskap, og hva består det av?	196
	Hva er forskjellen mellom business continuity og disaster recovery plan?	196
	Hvordan utvikler man en beredskapsplan?.....	197

12.4	Livssyklusen for håndtering av informasjonsverdier.....	202
	Hva er de ulike fasene innenfor livssyklusen for håndtering av informasjonsverdier?.....	203
12.5	Oppsummering	204

Del 4

AVSLUTNING	207
-------------------------	-----

Kapittel 13

Sammenkobling av ferdighetene	209
Har man behov for alle disse ferdighetene?.....	210
Hvordan skal man huske ferdighetene og praktisere dem?.....	210
Hva er det universale konseptet?	215
Den ideelle CISO-en	224
Konklusjon.....	225

Forkortelser	226
---------------------------	-----

Litteratur	229
-------------------------	-----

Stikkordregister	234
-------------------------------	-----

Figurer og tabeller

Figur 0.0.1 – Struktur for informasjonssikkerhetsledelse.....	21
Figur 1.1.1 – Respekt i praksis.....	29
Figur 1.1.2 – To tenkemoduser.....	32
Figur 1.1.3 – Kjennetegn på «idealistisk» tankesett.....	34
Figur 1.1.4 – Kjennetegn på «realistisk» tankesett.....	35
Figur 1.1.5 – Bias	36
Figur 1.2.1 – IKIGAI	40
Figur 1.2.2 – Maslows behovspyramide	41
Figur 1.3.1 – Struktur for memo	48
Figur 1.3.2 – Nedbryting av nøkkelord.....	48
Figur 2.0.1 – Ledelsesfagområder innen informasjonssikkerhetsledelse...	53
Figur 2.1.1 – Coaching	57
Figur 2.1.2 – Lytting	58
Figur 2.1.3 – Aktiv lytting.....	58
Figur 2.1.4 – Anti-lytting	59
Figur 2.1.5 – Lytter du?.....	60
Figur 2.1.6 – Coachingstil.....	61
Figur 2.1.7 – Kommunikasjon	65
Figur 2.1.8 – Nivåer før konflikt	65
Figur 2.1.9 – Konflikthåndtering	66
Figur 2.1.10 – Prosess for presentasjon	67
Figur 2.2.1 – Nedbryting av mål.....	71
Figur 2.2.2 – Prosess	74
Figur 2.2.3 – Helhetlig prosess	76
Figur 2.2.4 – Synergi mellom prosesselementene	78
Figur 2.2.5 – Prosessmodenhet: CMM.....	79
Figur 2.2.6 – Betingelsene for å endre kultur.....	80
Figur 2.2.7 – Eksempel på jobbutforming.....	82
Tabell 2.3.1 – Beslutningskart.....	89
Figur 2.3.2 – Styringsmekanismer.....	90
Figur 2.3.3 – Skjema for styringsmekanismer	91

Figur 2.3.4 – PROACT-URL – beslutningsprosess	94
Figur 2.5.1 – Metode for ledessspråk	99
Figur 2.5.2 – Business case	100
Figur 3.0.1 – Struktur for del 3 – Informasjonssikkerhet	104
Figur 3.2.1 – De 4 P-ene	107
Figur 3.2.2 – Forståelse for people	107
Figur 3.2.3 – Sikkerhetstiltak	109
Tabell 3.2.4 – Eksempler på sikkerhetstiltak	110
Figur 3.3.1 – Informasjonssikkerhetsfagene	114
Figur 3.4.1 – Livssyklus for kryptografiske systemer	120
Figur 3.4.2 – Nøkkelforvaltning	123
Figur 3.4.3 – OSI-modellen	124
Figur 3.4.4 – OSI-modellen i praksis	125
Figur 3.4.5 – IAMs livssyklus	129
Figur 3.4.6 – Prosess for etterforskning	131
Figur 3.4.7 – Innhold i skadevare	136
Figur 3.4.8 – Typer skadevare	136
Figur 3.5.1 – Trusseletterrettningsprosess	140
Figur 3.5.2 – Trusselvurdering	142
Figur 3.5.3 – Trusselmodellering	143
Figur 3.5.4 – Sosial påvirkning	146
Figur 3.5.5 – Rammeverket for sosial påvirkning	147
Figur 3.5.6 – OSINT	147
Figur 3.5.7 – OSINT-Observasjon	148
Figur 3.5.8 – Teknisk OSINT	149
Tabell 3.5.9 – Tekniske OSINT-teknikker	149
Figur 3.5.10 – Taktikker	150
Figur 3.5.11 – Angrepsvektor	151
Figur 3.5.12 – Prosess for styring av etterlevelse	153
Figur 3.5.13 – Helhetlig penetrasjonstest	156
Figur 3.5.14 – Faser ved penetrasjonstesting	157
Figur 3.5.15 – Attributter for en hendelse	160
Figur 3.5.16 – Gjensidig påvirkning mellom økonomiske og ikke-økonomiske aspekter	161
Figur 3.5.17 – Trussel	163
Figur 3.5.18 – Livssyklus håndtering for programvareutvikling	165
Figur 3.6.1 – Elementene i informasjonssikkerhetsstyring	170
Figur 3.6.2 – Dokumentasjonshierarki	172

Figur 3.6.3 – Fra måling til visjon.....	175
Figur 3.6.4 – Risiko- og konsekvenstyper	183
Figur 3.6.5 – Forskjellen mellom hendelse og risiko	185
Figur 3.6.6 – Eksempel på tids- og uvisshetsdimensjonen (skjermdump fra yr.no).....	187
Figur 3.6.7 – Faser innen risikostyring.....	188
Figur 3.6.8 – Eksempler på bruk av risikoformel.....	190
Figur 3.6.9 – Eksempel på uvisshet, toleranse og akseptkriterier.....	193
Figur 3.6.10 – Kost/nytte	194
Figur 3.6.11 – Risikovurdering.....	195
Figur 3.6.12 – Formål med beredskap.....	196
Figur 3.6.13 – Utvikling av beredskapsplan.....	197
Figur 3.6.14 – Utvikle BCP og DRP	200
Figur 3.6.15 – Livssyklus for håndtering av informasjonsverdier	203
Figur 4.2.2 – Hyllesystem	211
Figur 4.2.1 – Tips for å huske og praktisere	211
Figur 4.2.3 – Koblinger	212
Figur 4.2.4 – Sterke koblinger	213
Figur 4.2.5 – Tankeprosess for problemløsning.....	214
Figur 4.3.1 – PDCA.....	215
Figur 4.3.2 – PDCA og likheter med andre fagområder	217
Tabell 4.3.3 – Likheter.....	218
Figur 4.3.4 – Prosesstankegang.....	219
Figur 4.3.5 – Oppgave.....	220
Figur 4.3.6 – Plan.....	221
Figur 4.3.7 – Do	223
Figur 4.3.8 – Check	223
Figur 4.3.9 – Act.....	224

Forord

Det er spesielle utfordringer forbundet med å være CISO (Chief Information Security Officer) eller leder av informasjonssikkerhet i en virksomhet.

For det første er informasjonssikkerhet et enormt bredt fagområde som utvikles og fornyes i raskt tempo. For ledere i dette fagfeltet er det derfor vanskelig å følge med på alle de enkelte elementene og aspektene ved informasjonssikkerhet og forstå betydningen av dem i det store bildet. For det andre er informasjonssikkerhetsrisiko temmelig forskjellig fra finansrisiko, som virksomhetsledere typisk forholder seg til, slik at når en CISO presenterer informasjonssikkerhetsrisiko for toppledelsen, kan tolkningen bli feil. For det tredje anses informasjonssikkerhet ofte som en salderingspost for virksomhetene, uten at man helt innser at nedskjæringer kan utsette virksomheten for uforholdsmessig stor risiko.

Denne boken er CISO-ens verktøykasse for å mestre disse utfordringene. Den beskriver spesifikke personlige egenskaper en CISO bør ha, ledelsesmetoder som egner seg for å kunne innpasse styring av informasjonssikkerhet i den helhetlige virksomhetsstyringen, og den gir en konsis beskrivelse av sentrale deler av faget som en CISO bør forstå og se betydningen av.

Mye av innholdet i boken er basert på forskningslitteratur og har gode referanser. Boken er praktisk rettet, og vil være svært inspirerende også for andre enn bare CISO-er og ledere av informasjonssikkerhet. Den er f.eks. svært nyttig for studenter og ansatte som studerer eller jobber med ledelse og som er interessert i informasjonssikkerhet, og vice versa. I tillegg til å gi en konsis oversikt over fagfeltet informasjonssikkerhet, demonstrerer den hvilke personlige egenskaper som er gunstige når man vil fungere i en virksomhet, og den gir en innføring i gode ledelsesmetoder generelt.

Boken anbefales til alle som ønsker å forstå og praktisere ledelse av informasjonssikkerhet.

Oslo, februar 2023

Audun Jøsang

Professor i informasjonssikkerhet, UiO

Forfatterens forord

Dette er boken jeg ønsket at jeg hadde, da jeg under studiene ville forberede meg enda bedre til arbeidslivet og ønsket meg en bedre forståelse av informasjonssikkerhetsledelse med en holistisk tilnærming. Jeg håper denne boken kan være nyttig for dem som synes faget informasjonssikkerhetsledelse høres spennende ut, for fremtidige informasjonssikkerhetsledere og for dagens fagspesialister.

Det er mange jeg vil takke i forbindelse med denne utgivelsen! Takk til mine kollegaer fra Sykehuspartner for de gode faglige diskusjonene, for samarbeidet og for tilliten jeg fikk til å gjennomføre spennende arbeidsoppgaver og komplekse prosjekter. Det er Sykehuspartners samfunnsoppdrag og fagmiljø som har motivert meg til videreutvikling innen informasjonssikkerhetsledelsesfaget. Jeg vil også takke Sykehuspartner for å ha gitt meg muligheten til å ta en doktorgrad og for å ha finansiert utdanningen. Jeg vil rette en spesiell takk til min mentor og informasjonssikkerhetsleder ved Sykehuspartner, Christian Jacobsen, for de gode faglige diskusjoner spesielt om sikkerhets- og risikostyring, og gode råd om praktisk tilnærming til informasjonssikkerhet. Det er disse diskusjonene som motiverte meg til å skrive denne boka.

Til mine kollegaer ved Institutt for Informatikk ved Universitetet i Oslo (UiO) vil jeg rette en takk for godt samarbeid, gode faglige diskusjoner og bistand under doktorgradsforløpet. Jeg vil også takke mine kollegaer som er informasjonssikkerhetsledere i Helse Sør-Øst RHF (HSØ-RHF), Akershus universitetssykehus (AHUS), Oslo universitetssykehus (OUS), Sunnaas Sykehus (SunHF), Sykehuset i Vestfold (SiV), Sykehuset Innlandet (SIHF), Sykehuset Telemark (STHF), Sykehuset Østfold (SØHF), Sykehuspartner (SP), Sørlandet sykehus (SØHF) og Vestre Viken (VVHF) for at dere har satt av tid til å gi meg råd, latt dere bli intervjuet, og for å ha delt deres store kompetanse og erfaring med meg.

Jeg vil også takke mine kollegaer ved Martina Hansen Hospital (MHH) for tilliten dere har gitt meg. Den erfaringen jeg har fått fra MHH har vært meget verdifull, og mye av metodene og tankegangen beskrevet i boka har jeg kunne videreutvikle på grunn av dere.

Videre vil jeg takke den eksterne fageksperten innen ledelse for meget konstruktive kommentarer til del 1 og 2 av boka. Innspillene har bidratt til å heve kvaliteten på boka, noe jeg setter stor pris på.

Jeg vil også rette en stor takk til professor Audun Jøsang, som har vært både ekstern konsulent for dette bokprosjektet og min faglige veileder på UiO. Tusen takk for at du har gjennomgått hele boka med fokus på informasjonssikkerhetsdelen. Jeg setter stor pris på at du har vært meget støttende og satt av tid til å gjennomføre kvalitetssjekk av boka med detaljerte og gjennomtenkte innspill. Ikke nok med det, men du har frivillig stilt deg til disposisjon for å gjennomgå boka i flere omganger.

Jeg ønsker å rette en stor takk til redaktør Elisabeth Holmberg, som med sin utrolige ekspertise hjalp meg til å gjøre boka mer leservennlig, uten at det gikk utover det faglige innholdet. Takk også til både deg og Cappelen Damm Akademisk for tilliten og at dere hadde tro på bokprosjektet.

Til slutt vil jeg rette en stor takk til min familie som har støttet meg gjennom hele denne perioden, og har motivert meg til å stå på. Jeg vil takke min kone for å være støttende gjennom hele prosessen og hjulpet til med korrekturlesning og gitt gode råd om boka. Uten din forståelse og støtte hadde jeg ikke kunne fullført denne boka. Jeg vil også takke mine døtre som har stilt gode spørsmål, vært nysgjerrige om boka og hjulpet til å velge omslag. Dere har vist meg at barn er naturlige forskere, og jeg håper dere beholder denne viktige egenskapen gjennom hele livet. Nysgjerrigheten og engasjementet deres har hjulpet meg til å finne min indre motivasjon for å skrive denne boken. Og ikke å forglemme de gangene dere har våknet opp tidlig sammen med meg for å skrive eller tegne deres egne bøker og tegneserier, mens jeg har jobbet med boka.

Og til deg som sitter med boken i hendene: Lykke til med lesingen!

Oslo, februar 2023

Dinh Uy Tran