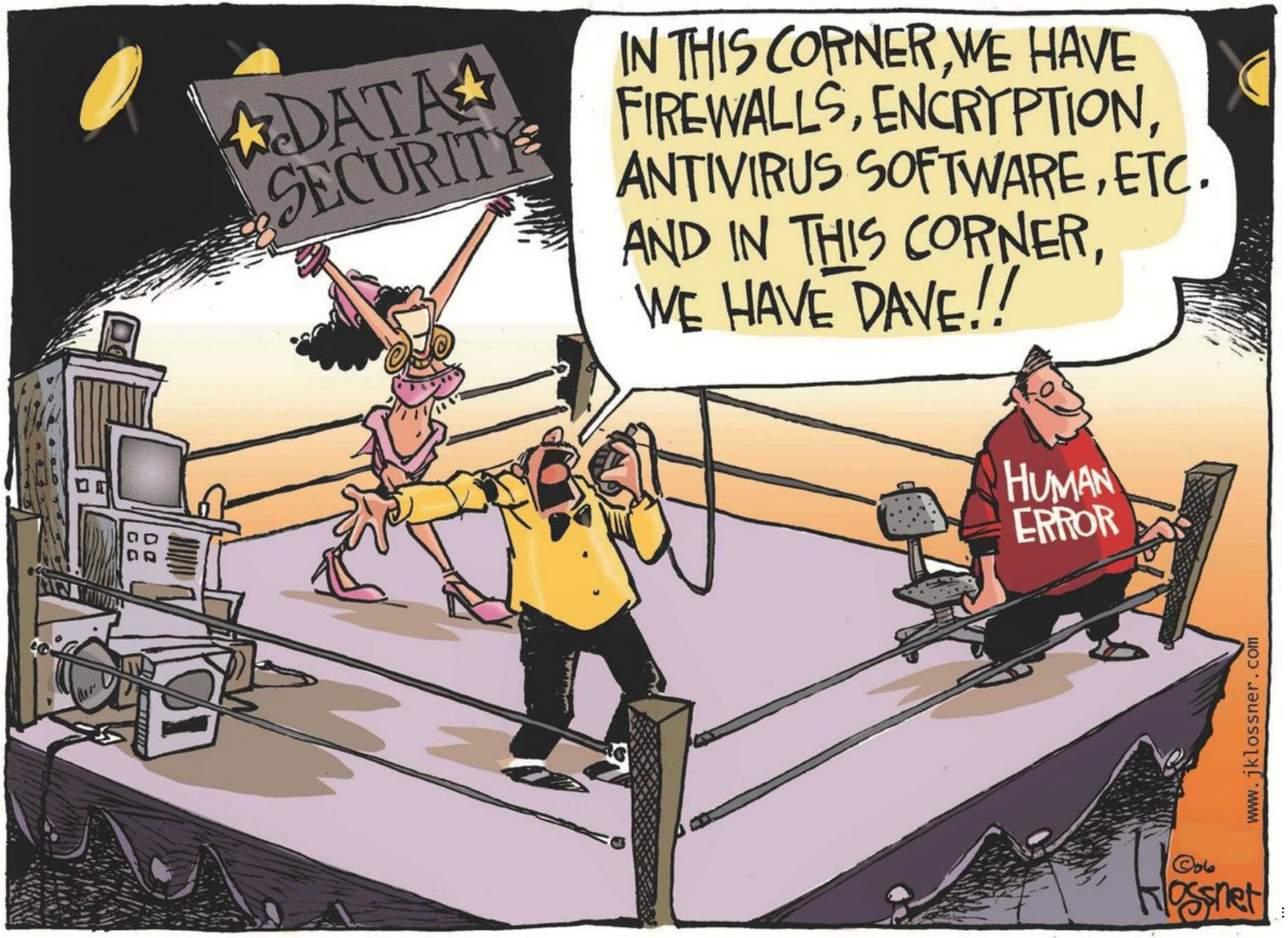
Cybersikkerhed i klinikken.
Modstand og medvind

E-Sundhedsobservatoriet 2019

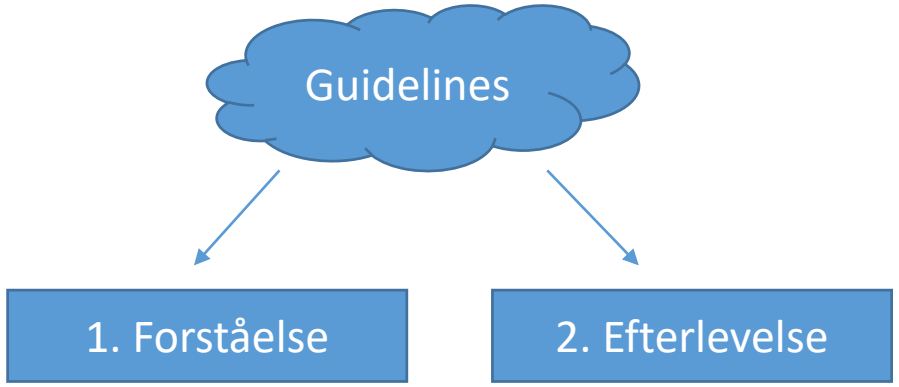
Thomas Schmidt

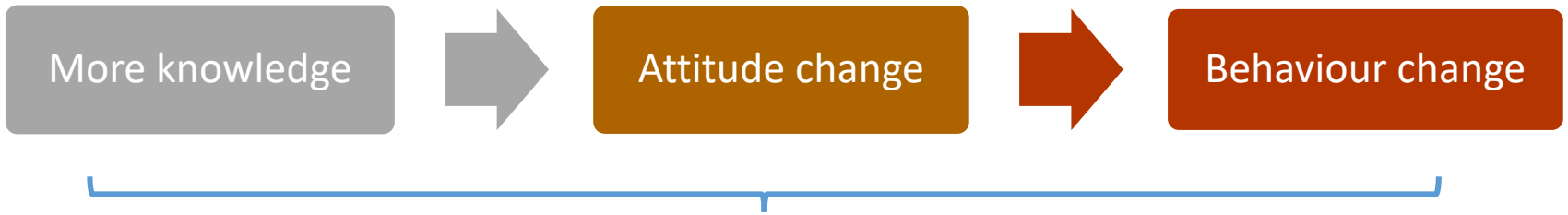
schmidt@mmmi.sdu.dk


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06
Klossner

Information Security Awareness (ISA)

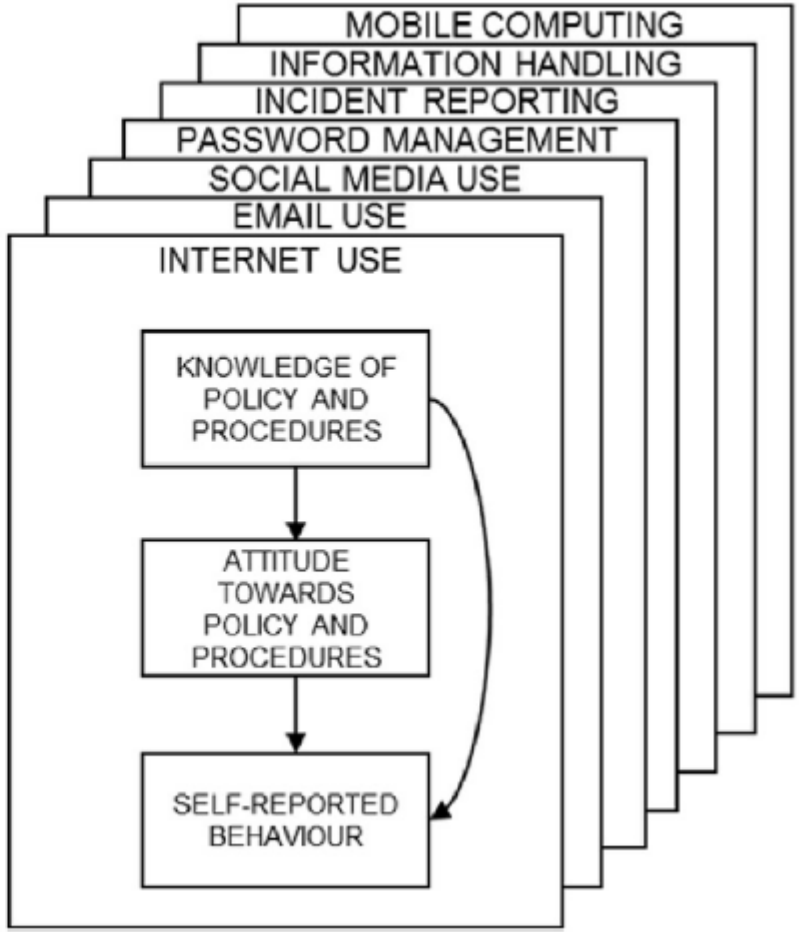
- Menneskelige fejl spiller ind i 95% af sikkerhedshændelser
- Medarbejdernes kendskab til informationssikkerhed er fundamentalt vigtigt for at reducere risikoen for hændelser
- Definitioner af informationssikkerhedskendskab (…) fokuserer typisk på to aspekter
  1. Forståelse for god og sikker opførsel
  - Efterlevelse af guidelines, best practices mm.





Knowledge, Attitude, Behaviour Model (McGuire, 1969)

Human Aspects of Information Security Questionaire



(McCormac et al, Individual differences and Information Security Awareness, 2017, Computers In Human Behavior,69)

Human Aspects of Information Security Questionaire

Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/cose
ELSEVIER
Computers & Security

The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies

Kathryn Parsons [a,*], *Dragana Calic* [a], *Malcolm Pattinson* [b], *Marcus Butavicius* [a], *Agata McCormac* [a], *Tara Zwaans* [c]

[a] Defence Science and Technology Group, PO Box 1500, Edinburgh, SA 5111, Australia
[b] Business School, The University of Adelaide, Adelaide, SA 5005, Australia
[c] School of Psychology, The University of Adelaide, Adelaide, SA 5005, Australia

63 items fordelt ud over de 7 kategorier

HAIS-Q focus areas
Password management
Email use
Internet use
Social media use
Mobile devices
Information handling
Incident reporting

	Knowledge	Attitude	Behaviour
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job. ^	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done. ^
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to. ^
Entering information online	I am allowed to enter any information on any website if it helps me do my job. ^	If it helps me to do my job, it doesn't matter what information I put on a website. ^	I assess the safety of websites before entering information.

Tre spørgsmål

- [**Viden**] – I mit daglige arbejde er jeg også opmærksom på udefrakommende trusler mod vores data og computere.
- [**Attitude**] – I mit daglige arbejde er IT-afdelingens tiltag for at sikre informationssikkerhed mere til besvær end gavn.
- [**Adfærd**] – I mit daglige arbejde tænker jeg over hvordan jeg håndterer computerne for at undgå at blive hacket

Fremgangsmåde

- Udarbejdelse af de tre simple spørgsmål
- Landsdækkende spørgeskema (Monitorering af klinikernes brug og holdninger til sundheds it 2018) udsendt til diverse klinisk faglige organisationer.
- Tekstanalyse og struktureret kodning af Nordiske sikkerhedsstrategier

De beskrevne værktøjer er ikke stærke nok til at vi kan cementere bestemte sammenhænge!

Koblet med

- **#Passwords i daglig brug**
- **#IT systemer i daglig brug**
- [**Tilfredshed**] – Er du overordnet tilfreds med dit EPJ system? {Meget tilfreds, tilfreds, hverken/eller, utilfreds, meget utilfreds}
- [**Kompetence**] - Hvis en kollega, der kender dig godt, skal beskrive dine kompetencer inden for brug af de arbejdsrelaterede it-systemer, du anvender i hverdagen, vil vedkommende så betegne dig som {Almindelig bruger, avanceret bruger, ekspert, ved ikke}
- [**Arbejdsregion**] – Region {Nord, Midt, Syd, Sjælland, Hovedstaden}
- [**Profession**] – {Læge, Sygeplejerske, Sekretær, Radiograf}

Resultater

Spørgeskema udsendt til 9148 modtagere. 1621 besvarelser, og udvalgte de 1432 med tilhørsforhold til de 5 danske regioner

	Læge n=231 (16%)	Sygeplejerske n=593 (41%)	Sekretær n=467 (33%)	Radiograf n=141 (10%)
Region of employment				
Region Hovedstaden(32%)				
Region Sjælland (15%)				
Region Syd (23%)				
Region Midt (20%)				
Region Nord (10%)				
Expert user (10%)				
Advanced user (40%)				
Regular user (48%)				
Not sure (2%)				
# passwords [mean (SD)]				

Svarede ikke på nogle af spørgsmålene (n=296)

Læge n=29 (10%)	Sygeplejerske n=129 (43%)	Sekretær n=88 (30%)	Radiograf N=50 (17%)	
0	1	2	4	

SISA = Viden + Attitude^-1+Adfærd [Score fra 3-15]

CIMT

THE MAERSK MC-KINNEY MOLLER INSTITUTE SDU

Opmærksomhed

Attitude

Adfærd

Sygeplejersker

Sekretærer

Læger

Radiografer

Opmærksomhed på regionsniveau

RSjælland har proportionsmæssig overvægt i stor uenighed →

Relativt stor gruppe RSyd besvarelser er uenige at have daglig opmærsomhed →

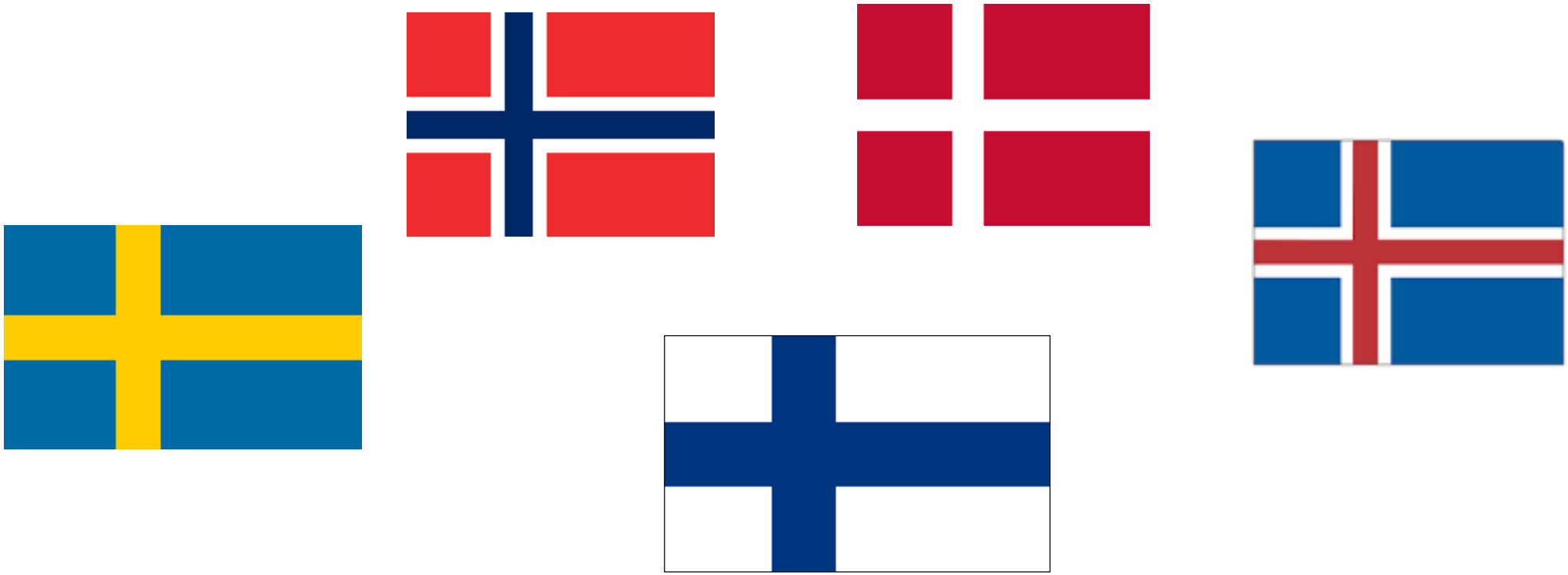
‘Umodne’ resultater

OLS Regression på alle der har leveret komplette svar i sikkerhedsspørgsmål (n=945):

`SISA ~ (Profession+Region+Kompetence+Tilfredshed+Erfaring+#PW+#Systemer)`

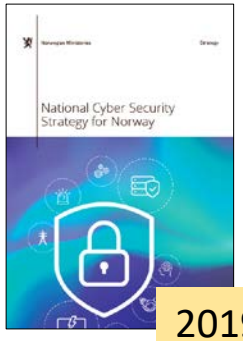
Koblet med nordiske sikkerhedsstrategier

Hvad sker der på nationalt niveau i de nordiske lande?



Overblik over strategier

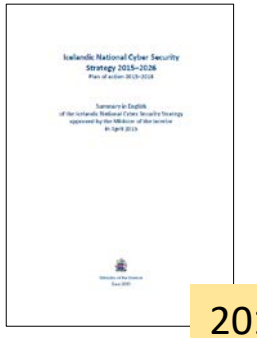
Nationale strategier



2019

2018

2016



2015

2013

Sektorspecifickke

Trussels vurderinger

CIMT

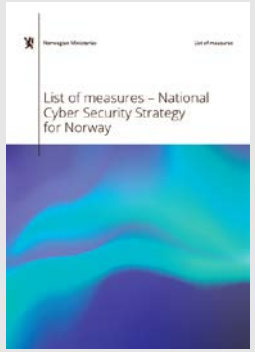
Andre dokumenter

Sverige

Finland

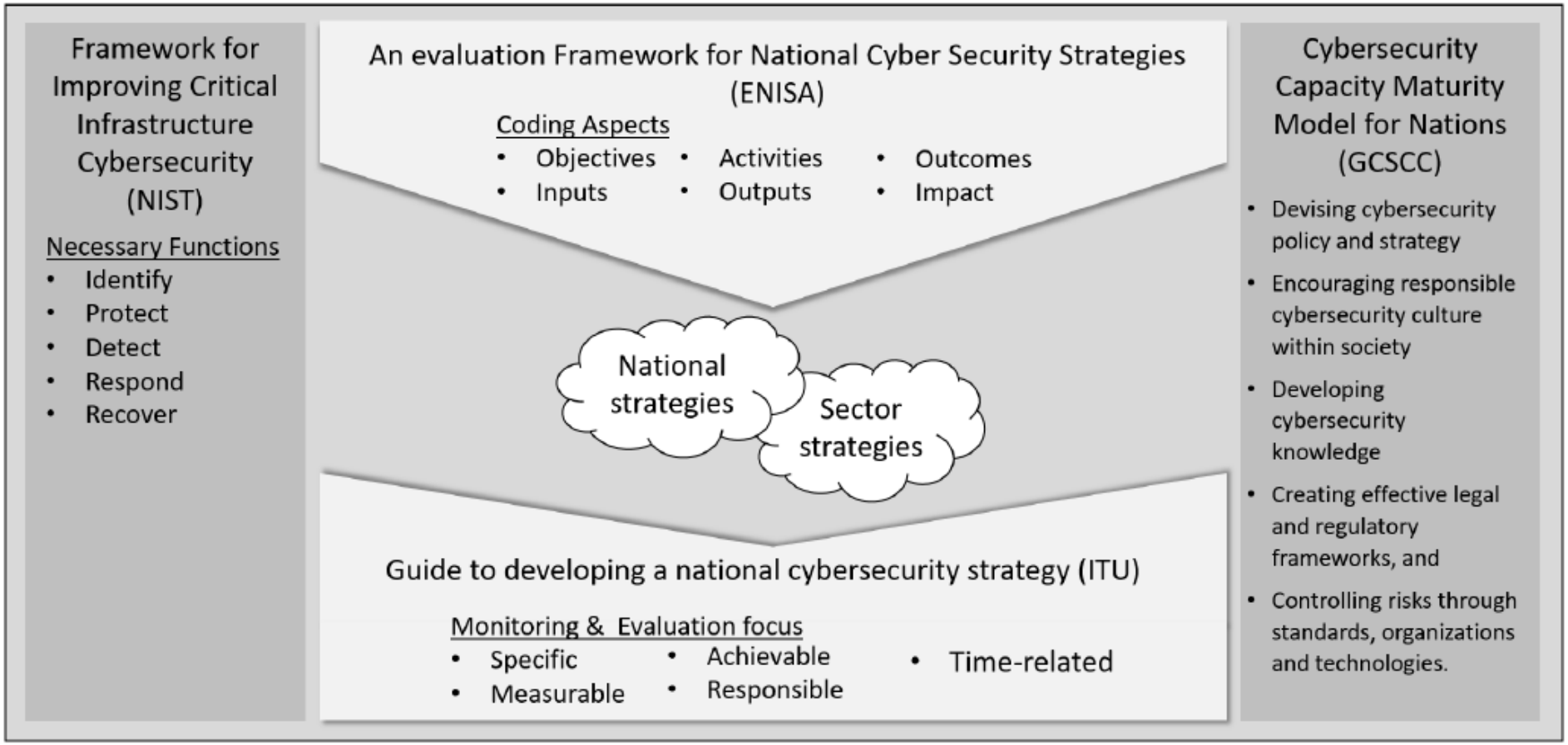
Island

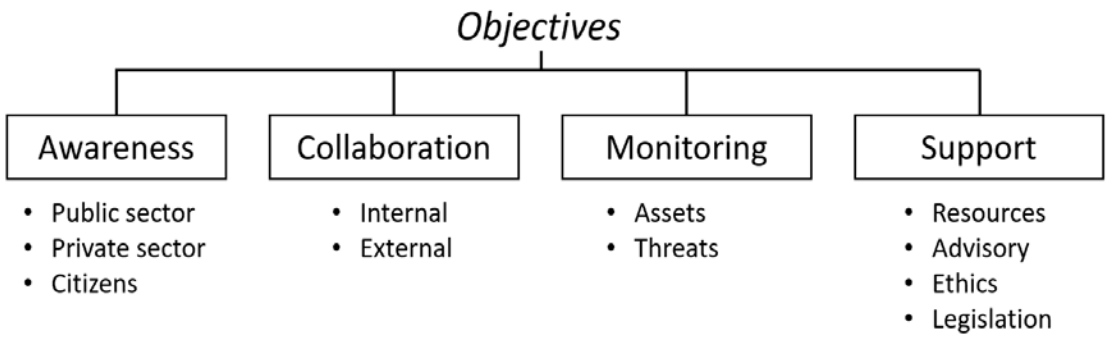
Norge



Danmark

EU


Framework for Improving Critical Infrastructure Cybersecurity (NIST)
Necessary Functions
Identify
Protect
Detect
Respond
Recover
An evaluation Framework for National Cyber Security Strategies (ENISA)
Coding Aspects
Objectives
Activities
Outcomes
Inputs
Outputs
Impact
National strategies
Sector strategies
Guide to developing a national cybersecurity strategy (ITU)
Monitoring & Evaluation focus
Specific
Achievable
Time-related
Measurable
Responsible
Cybersecurity Capacity Maturity Model for Nations (GCSCC)
Devising cybersecurity policy and strategy
Encouraging responsible cybersecurity culture within society
Developing cybersecurity knowledge
Creating effective legal and regulatory frameworks, and
Controlling risks through standards, organizations and technologies.


Objectives
Awareness
Public sector
Private sector
Citizens
Collaboration
Internal
External
Monitoring
Assets
Threats
Support
Resources
Advisory
Ethics
Legislation

Eksempler fra

Awareness

omgå dem i en travl hverdag. Derfor skal bedre og mere kompetenceudvikling for sundhedssektorens mange forskellige medarbejdergrupper højne deres opmærksomhed på – og viden om – cyber- og informationssikkerhed og sikre en passende sikkerhedsadfærd.

Samarbejde

Dernæst er det vigtigt, at sundhedssektorens overvågningsfunktioner er tænkt sammen med kommunikationslinjer, beredskab og handlingsplaner inden for sektoren. Det gælder også på tværs af de samfundskritiske sektorer og på tværs af sundhedssektorerne i de lande, vi minder om og arbejder sammen med på cyber- og informationssikkerhedsområdet. Hvis uheldet er ude, skal en hændelse hur-

Med et fælles h
sektoren styr
modstandsdygtig
og sikkerhed

Support

Et væsentlig element heri er gennemtestede kommunikationslinjer, så sektorens aktører ved, hvor og til hvem de skal henvende sig, og hvad der kan gøres lokalt i tilfælde af en hændelse. Som led heri skal sektorens aktører såvel som deres medarbejdere have en fælles forståelse af opgave- og ansvarsfordeling samt konkrete og veletablerede aftaler for håndtering af cyber- og informationssikkerhedshændelser.

Monitoring

For at understøtte opdagelse af angreb og sikkerhedshændelser er der behov for, at sektorens aktører proaktivt overvåger aktivitet på såvel fælles som lokal infrastruktur og systemer. Det kræver, at de rette overvågningsfunktioner er på plads på de rette steder i sektoren, og at sektoren også på dette område er velkoordineret med henblik på at styrke kapaciteten til at opdage brud på cyber- og informationssikkerheden på tværs af sektorens aktører. Med et fælles højt niveau

CIMT

Trends fra strategianalyse

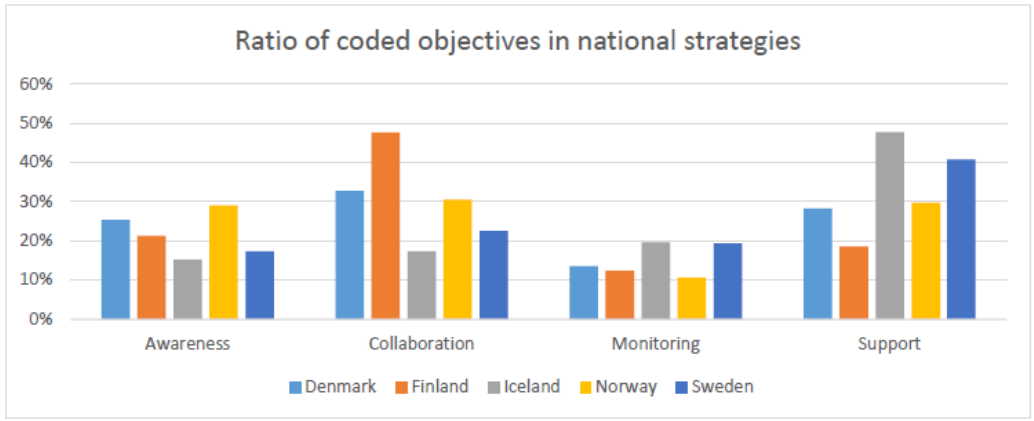


Figure 3. Ratio of coded objectives in national strategies

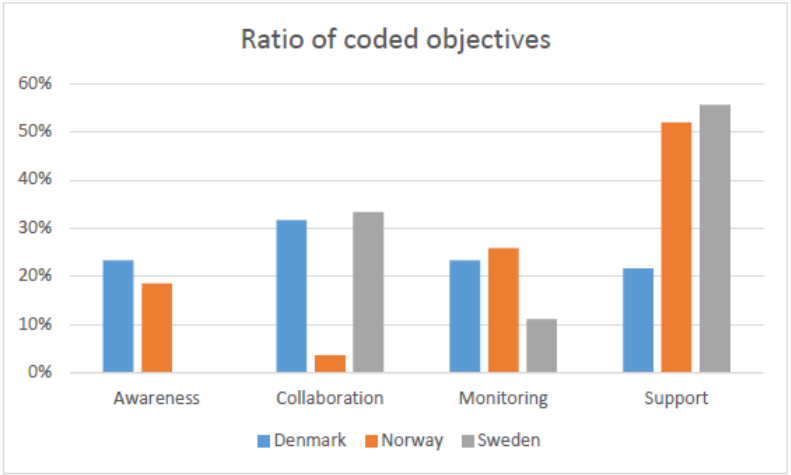


Figure 4. Ratio of coded objectives

Strategierne bliver

- mere konkrete og håndgribelige
- Rettet mod en bredere målgruppe
- Markante sektor forskelle mellem Norge, Sverige og Danmark

Svar

- Er der en sammenhæng mellem profession og ISA?
- Er der en sammenhæng mellem tilfredshed og ISA?
- Er der en sammenhæng mellem systemlandskab og ISA?
- …. Ikke klokkeklart
  - - I hvert fald ikke med et så simpelt værktøj som vi har anvendt!

Fremad herfra

- Tilpasning & validering af simple ISA spørgsmål

Spørgsmål – til jer og til mig

- Hvad tænker I er gode (læs: simple) måder at måle medarbejdernes forståelse for informationssikkerhed?

- Det gik f.eks. lidt galt her i Nyborg i vinters

Stor historie i DR- men Nyborg Kommunes kontrol-metode af it-sikkerhed er helt almindelig praksis: "Det her er side to i håndbogen for etiske hackere"

Det er helt almindelig praksis, at it-sikkerhedsfirmaer udgiver sig for at være en anden for at få adgang til virksomheder eller kommuners data. Sådan lyder reaktionen fra flere etiske hackere efter DR tirsdag viste, at Nyborg Kommune havde bestilt en penetratonstest på en af skolerne i kommunen.

6. februar 2019 kl. 13.05

JAKOB SCHJOLDAGER
Journalist

https://www.computerworld.dk/art/246328/stor-historie-i-dr-men-nyborg-kommunes-kontrol-metode-af-it-sikkerhed-er-helt-almindelig-praksis-det-her-er-side-to-i-haandbogen-for-etiske-hackere