KROMANN REUMERT

Har bestyrelsen et skærpet ansvar for styring af cyberrisici?

9. november 2021

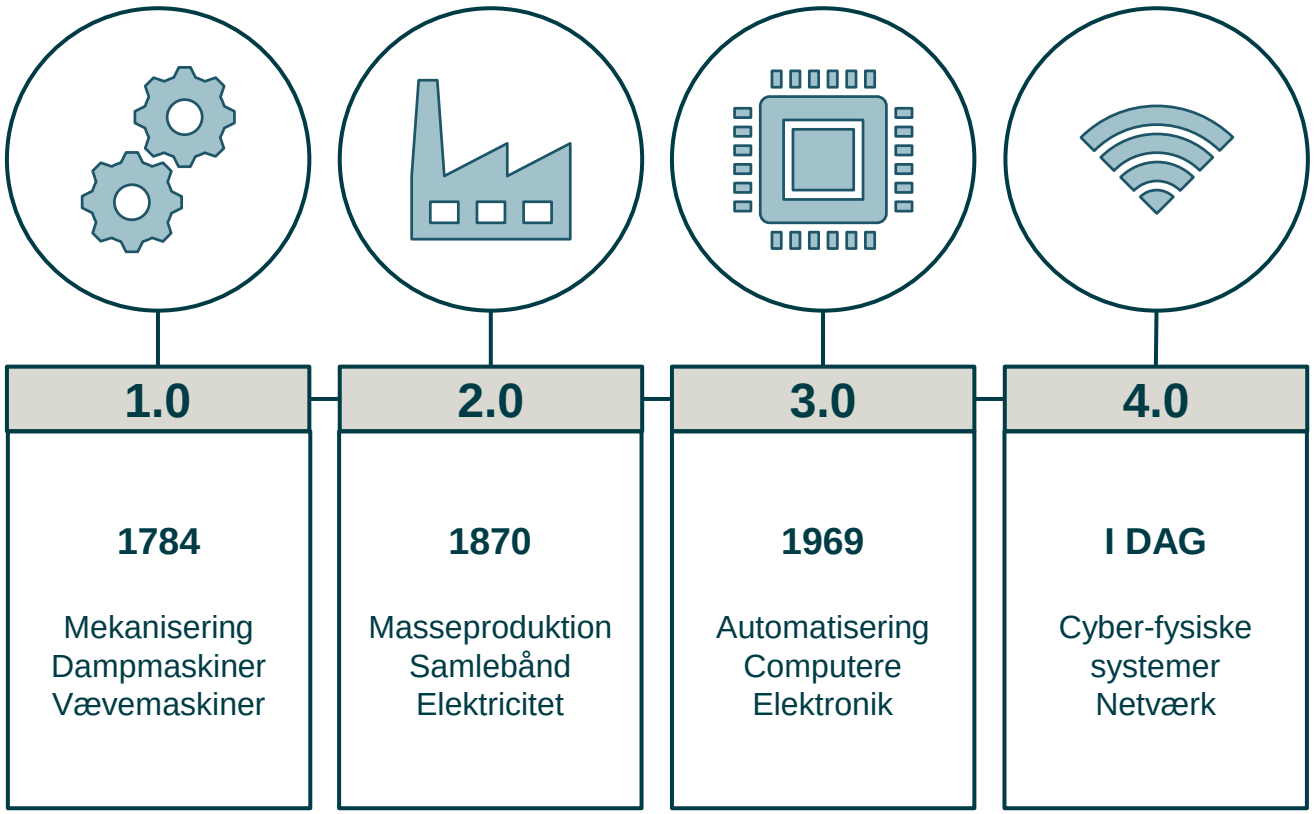
1. Den væsentlige anvendelse af cyberfølsom teknologi ***skærper*** ansvarsnormen

2. Styrken af den cyber-relaterede trussel ***skærper*** ansvarsnormen

3. Reguleringen er sparsom i dag, men der tegner sig et billede af, hvad der er ***god praksis*** og den ***juridiske ansvarsnorm***

Nye teknologier får den fysiske og virtuelle verden til at smelte sammen til såkaldte cyber-fysiske systemer

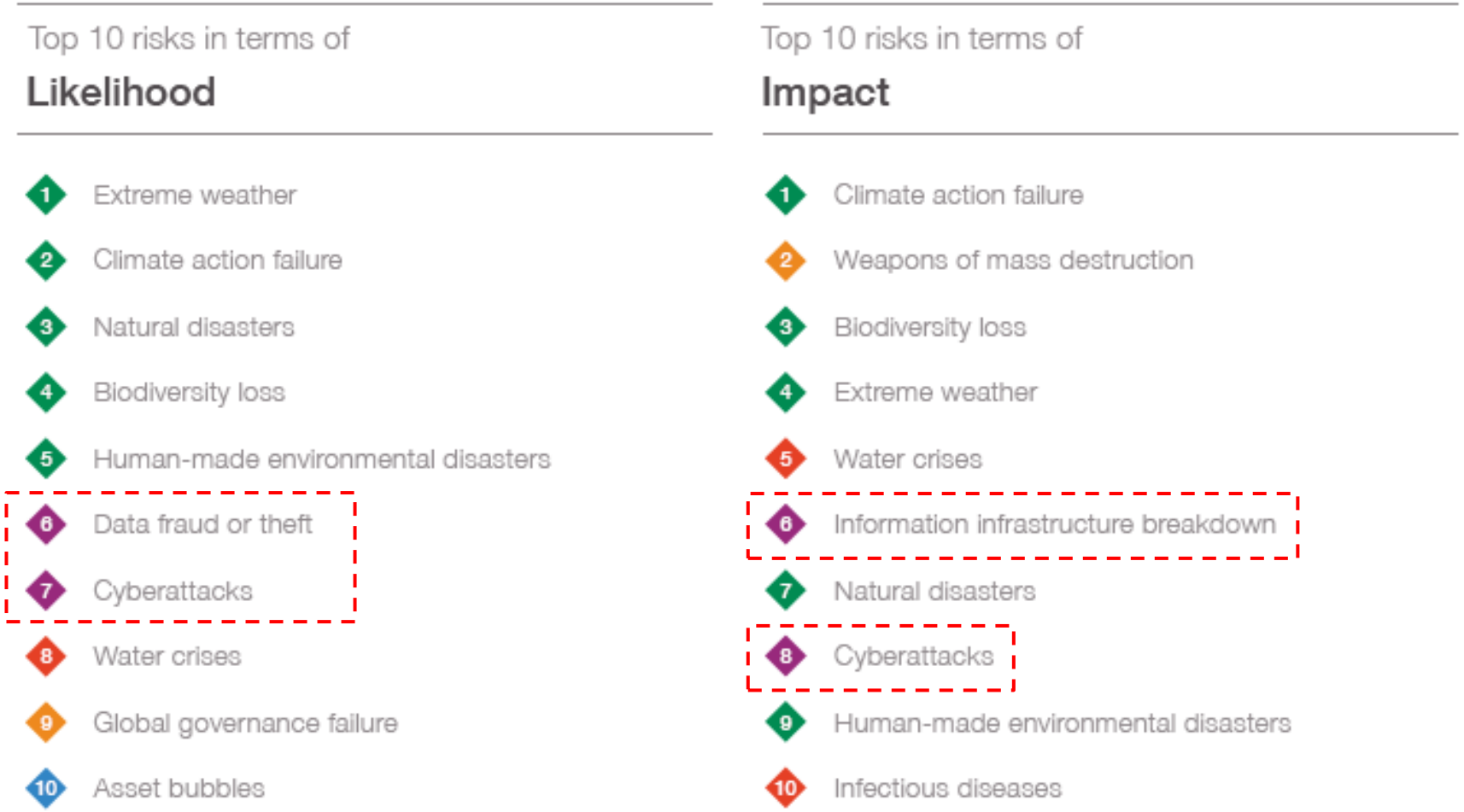
Fire industrielle revolutioner – fra dampmaskinen til SmartProduction, SmartCity, SmartHome



Industri 4.0 – teknologier (eks.)

Big data analytics	Augmented reality
3D print	Green tech
Internet of Things	Cloud computing
Avancerede robotter	Kunstig intelligens
Mobile applikationer	Kvante-computere
Blockchain / fintech	System integration

Cyber-relaterede risici regnes blandt de største globale risici for virksomheder og organisationer



Kilde: World Economic Forum Global Risks Report 2020

Den regulatoriske ramme udgøres primært af NIS-lovgivningen
(og databeskyttelseslovgivningen)

NIS1 – direktivet
(2016/1148)

- Operatører af væsentlige tjenester
- Udbydere af digitale tjenester
- Overordnede sikkerhedskrav
- Underretning om væsentlige hændelser

Nyt NIS2 – direktiv på vej
(forventes vedtaget 2022)

- Udvidet anvendelsesområde
- Skærpede krav til risikostyring
- Udvidet underretningspligt
- Ledelsesansvar og bødeforlæg

NIS-lovgivningen i DK
(sektorbaseret implementering)

- Energi
- Finans
- Sundhed
- Søfart
- Tele
- Transport
- Vand
- Digital infrastruktur

”Passende og forholdsmæssige tekniske og organisatoriske foranstaltninger” – og hvad så?

NIS-direktivets artikel 14, stk. 1
”passende og forholdsmæssige tekniske og organisatoriske foranstaltninger”

Persondataforordningens artikel 32, stk. 1
”passende tekniske og organisatoriske foranstaltninger”

Lov om finansiel virksomhed, § 71, nr. 4 og 6 (finans)
”betryggende kontrol- og sikringsforanstaltninger på it-området”

Outsourcingbekendtgørelsen, § 20, stk. 1 og 2, nr. 5 (finans)
”passende tekniske og organisatoriske foranstaltninger”

Bekendtgørelse 2016-06-01 nr. 567, § 2, stk. 3 (teleudbydere)
”passende foranstaltninger”

Lov 2018-05-08 nr. 441, § 4, stk. 1 (transport)
”passende og forholdsmæssige tekniske og organisatoriske foranstaltninger”

Lov 2018-05-08 nr. 436, § 4, stk. 1 (digital infrastruktur): *”passende og forholdsmæssige tekniske og organisatoriske foranstaltninger”*

Lov 2018-05-08 nr. 440, § 4, stk. 1 (sundhed):
”passende og forholdsmæssige tekniske og organisatoriske foranstaltninger”

ISO og NIST er udbredte standarder for styring af cyberrisici

December 2020

CYBERSIKKERHED FOR BESTYRELSER

Anbefalinger til Styrkelse af Cyberkompetencer

www.bestyrelsesforeningen.dk/vejledninger-og-anbefalinger/

BESTYRELSESFORENINGEN
Fokus på værdiskabelse, ledelse og governance
Bestyrelsesforeningens Center for Cyberkompetencer

KROMANN REUMERT

FE CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

Ledelsen kan ifalde ansvar for utilstrækkelig risikostyring og sikkerhedsbrud

Ansvarsnorm: Culpa

Ansvarsgrundlag: Business judgment rule

- Tilstrækkeligt beslutningsgrundlag: Nødvendige oplysninger skal tilvejebringes
- Forsvarlig beslutning (HR: tilbageholdende), bl.a. baseret på:
  - "*Passende og forholdsmæssige tekniske og organisatoriske foranstaltninger*"
  - Selskabslovens §115: Etableret "*fornødne procedurer til risikostyring*"
  - Bestyrelsesforeningens vejledning

Problem: Ikke nok at blive frifundet

- I dag skal man undgå at blive stævnet, og det kræver omhyggelighed, så man er ude af tvivlszonen

Eksempler

- Uberørt i bestyrelsesprotokol
- Ingen dialog med eksperter
- Ingen instruks eller undervisning
- Intet klart organisatorisk ansvar
- Intet systemmæssigt overblik
- Ikke regelmæssig back-up
- Ikke regelmæssig password-skifte
- Ikke regelmæssig opdatering af antivirus-programmel
- Manglende multi factor authentication
- CFO fraud - 3. gang
- Stor infrastrukturoutsourcing - slet ikke tænker cyber ind

Spørgsmål, afrunding og tak for i dag