Velkommen

Sikkert digitalt samarbejde i byggeriet

22. Januar 2026

CON
TECH
LAB_

Tak til projektpartnerne

IMPLEMENT
CONSULTING GROUP_

DI Byggeri

CON
TECH
LAB_

COWI

buildingSMART
Danmark

MOLT WENGEL

MOLIO
viden, du bygger på

CON
TECH
LAB_

Program

15:00 **Velkommen**
v/ Christina Hvid, CEO i Molio og ConTech Lab

15:10 **Ledelse i en foranderlig verden**
v/Mette Kaagaard, CEO i Microsoft Danmark

15:30 **Hvad siger NIS2 om ledelsens ansvar**
v. Nicolaus Falk-Scheibel, Advokat, Molt Wengel

15:45 **Paneldebat: Når virkeligheden rammer - hvem tager ansvaret?**
v/Malene Stidsen, Programchef for Industriens Fonds cyberindsats | Charlotte Miolane, CISO hos COWI | Ulrik Branner, CEO i Sitehub | Lillian Rasch Madsen, Vicedirektør, Center for Ejendomme, Region H

16:10 **Fra sikkerhedsbrist til konkurrencefordel**
v/ Anders Balslev, Partner i Implement Consulting Group

16:30 **Fra bestyrelse til beredskab - ledelse, ansvar og kontrol i cybersikkerhed**
v/v. Kirsten Hede, Udviklingsdirektør Bestyrelsesforeningens Center for Cyberkompetencer

17:00 **Netværk og snacks**

Mette Kaagaard

CEO, Microsoft Danmark

Ledelse i en foranderlig verden

CON
TECH
LAB_

Microsoft

Ledelse i en foranderlig verden

Mette Louise Kaagaard
CEO Microsoft Denmark & Iceland
Mette Louise Kaagaard | LinkedIn
22. Januar 2026

Resiliens er en forudsætning for moderne ledelse

- ‘Kriser’ opstår hele tiden
- Organisationen skal kunne absorbere dem uden at miste orientering
- Fokus fra ydre brandslukning til indre kapacitetsopbygning – fra reaktion til resiliens
- Løsningerne er: Fleksibilitet, agilitet og digital prepping – at kunne stå fast i det man ikke kan styre
- Kapacitet og effektivitet skal balancere

Microsofts forpligtelser til Europa

Beskytte privatliv og data under europæisk lovgivning

Soverign løsninger med lokale data

Opretholde Europas digitale robusthed – også under geopolitisk uro

Styrke cybersikkerheden i Europa

Fremme Europas økonomiske konkurrenceevne (AI og cloud økosystem)

Microsoft blokerer 600 mio. cyberangreb om dagen

Cyber er Verdens 3. største økonomi

Angreb fra statsaktører voksede 25% sidste år

AI er afgørende for at være godt beskyttet

Cloud teknologi er stærkest mod cyber

Husk også at investere i medarbejderne

Er I klar på hvad I skal gøre hvis lyset går ud?

AI sker NU og driver konkurrencekraft og innovation

Overgangen er strukturel og uundgåelig: Ikke et hype-fænomen

Produktivitet pr. medarbejder stiger markant: +40 % på konkrete opgaver

IT-entry jobs falder i USA: 13% færre jobs for unge i AI-eksponerede roller

Arbejde ændrer karakter, ikke bare volumen: Timer automatiseres, ikke jobs

Redesign og proces innovation vinder: Produktivitet er ikke nok

I skal tænke AI helt i jeres DNA: Frontier Firm modellen (OECD)

I har en strategisk og organisatorisk opgave foran jer

Enrich employee experiences

By equipping the workforce from the shop floor to the top floor with AI agents

Reinvent customer engagement

With AI agents supporting sales and marketing operations and field service teams

Reshape business processes

By solving persistent factory and supply chain challenges with AI

Bend the curve on innovation

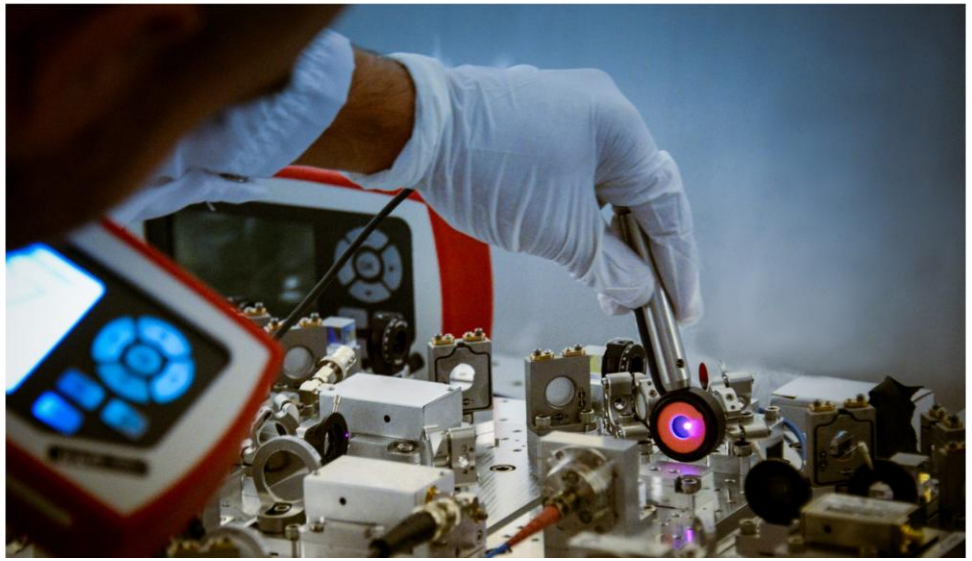
Through AI-accelerated R&D, engineering, and product design

I skal tænke langt og fokusere på skala og kort ROI

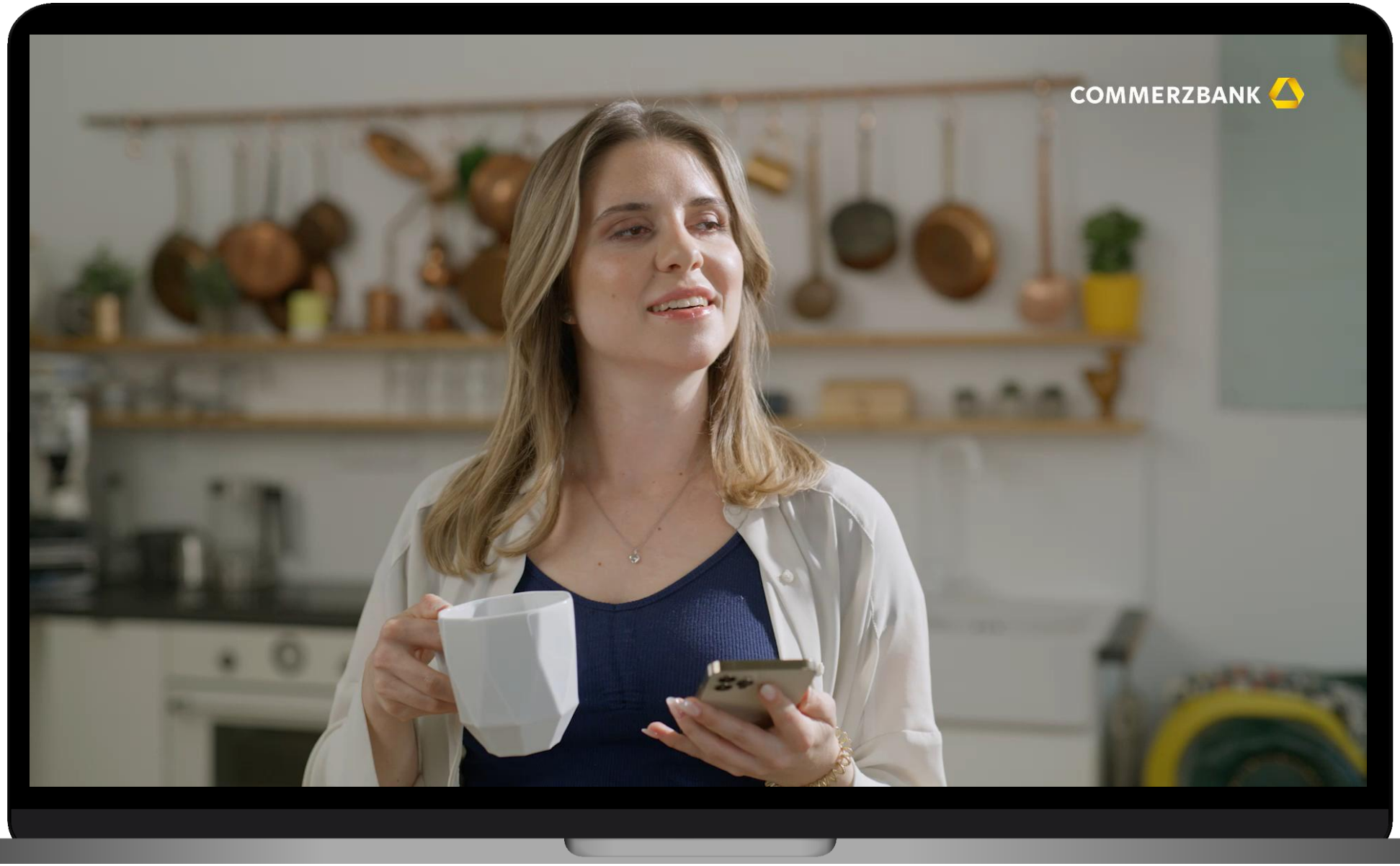
Ny AI-model er "et kæmpe hop fremad", mener Dansk Industri

Torsdag aften dansk tid har techfirmaet OpenAI lanceret selskabets nye sprogmodel, GPT-5.

Ny kvantecomputer med stort potentiale til at styrke nordisk forskning og innovation



Introduction of our new colleague Ava



Ledelsens fokus i at drive AI forandringen

- ✓ Strategisk forankring og governance: Følg med, stil krav og brug det selv!
- ✓ Kompetencer og kultur: Skab en stærk vision – WHY?
- ✓ Datafundament og sikkerhed
- ✓ Målbare use cases og skalering er key
- ✓ Operer med kort ROI og brug standard

Kriser er blevet grundrytmen i moderne virksomhedsledelse ..

Resiliens skal indbygges I kulturen

Nicolaus Falk-Scheibel

Advokat, Molt Wengel

Hvad siger NIS2 om ledelsens ansvar?

CON
TECH
LAB_

Cyber security og NIS2

Ledelsens ansvar

Nicolaus Falk-Scheibel
Advokat og ph.d.
22. januar 2026

CON
TECH
LAB

MOLT | WENGEL

NIS 2

NIS2 og byggebranchen

MOLT | WENGEL

Anvendelsesområdet

NIS2 gælder både direkte og indirekte

Byggebranchen er ikke generelt omfattet af NIS2.

Bygherrer, kan være omfattet af NIS2.

Entreprenører, rådgivere og leverandører kan ***indirekte*** være underlagt NIS2's krav, idet enhederne direkte omfattet af NIS2 skal sikre ***forsyningskædesikkerheden***.

Videreførelsen af NIS2-lovens krav er aftalebaseret.

NIS 2

Formål og anvendelsesområde

MOLT | WENGEL

Formål og anvendelsesområde

MOLT | WENGEL

Formålet

Styrkelse af cybersikkerhed og risikostyring.

Udvidelse af dækningsområdet.

Forbedre samarbejde og rapporteringspligt.

Anvendelsesområdet

	Sektor		
	Transport		Digital infrastruktur
	Energi		Forvaltning af IKT-tjenester
	Drikke- og spildevand		Statslig og regional forvaltning
	Sundhed		Rummet
	Bankvirksomhed og finansielle markedsinfrastruktur		
	Post- og kurertjenester		Affaldshåndtering
	Kemikalier		Fødevarevirksomheder
	Digitale serviceudbydere		Forskning
	Produktionsvirksomheder af særlig vigtigt udstyr		

NIS 2

Ledelsens rolle

MOLT | WENGEL

Definition

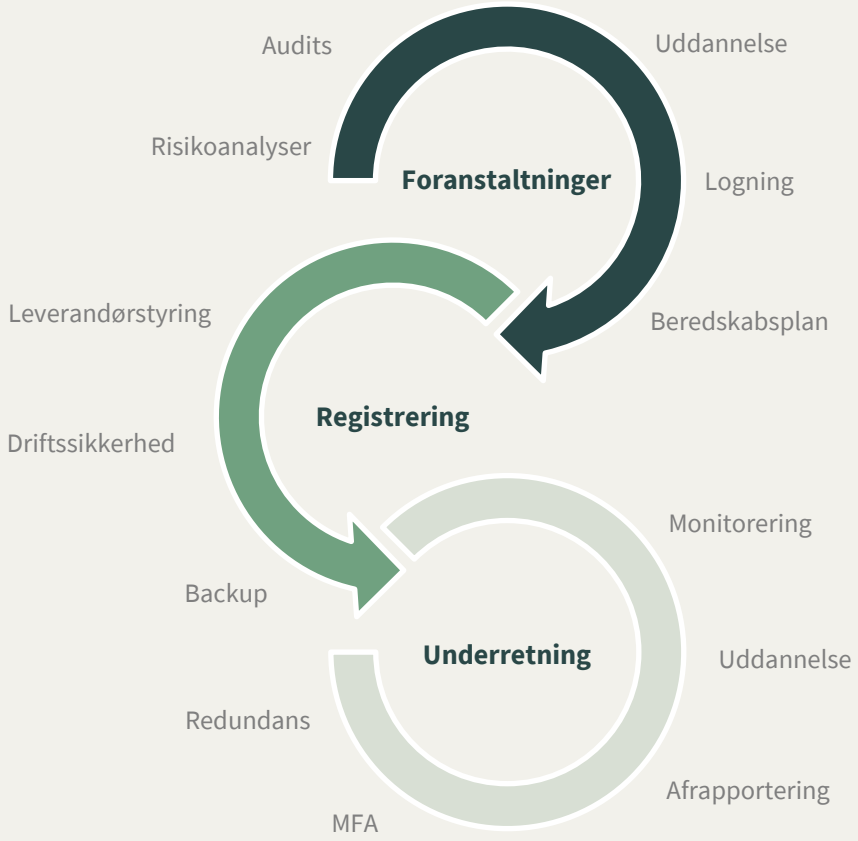
Ledelsesorganet, jf. NIS2-lovens § 3, nr. 20:

- Bestyrelsen eller direktionen (*selskaber omfattet af selskabsloven*).
- Det organ/person der har de beføjelser, der ellers tilkommer bestyrelsen/direktionen (virksomheder omfattet af LEV-loven).
- Den øverste administrative ledelse (offentlige myndigheder).

Krav og opgaver

MOLT | WENGEL

NIS2 foranstaltninger og pligter



Krav og opgaver til ledelsesorganet, jf. NIS2-lovens § 7, stk. 1 og 2:

Ledelsesorganet skal godkende foranstaltninger i medfør af NIS2-lovens § 6.

Ledelsesorganet skal føre tilsyn med disses gennemførelse.

Ledelsesorganet skal tilegne sig de fornødne kompetencer vedrørende styringen af cybersikkerhed og tilskynde, at de øvrige ansatte også tilegner sig sådanne kompetencer.

NIS 2

Ledelsens ansvar

MOLT | WENGEL

Ansvar

Hvad er ledelsesorganet ansvarlig for ?

Ledelsesorganet har ansvaret for, at foranstaltninger i medfør af NIS2-lovens § 6, gennemføres og at den lever op til kravene i NIS2-lovens § 7.

Konstateres der svigt i gennemførelsen af sådanne foranstaltninger, kan ledelsesorganet pålægges håndhævelsesforanstaltninger i medfør af NIS2-lovens § 22.

Efterkommer ledelsesorganet ikke sådanne håndhævelsesforanstaltninger kan dette sanktioneres, jf. NIS2-lovens § 23.

Sanktioner

Forbud og bøder

Midlertidigt forbud mod at udøve ledelsesfunktioner, jf. NIS2-lovens § 23, stk. 1, nr. 2. (gælder kun væsentlige enheder og ikke offentlige myndigheder).

Bødeansvar for virksomheden:

- op til 10 millioner euro eller 2 % af den globale omsætning (*væsentlige enheder*).
- op til 7 millioner euro eller 1,4 % af omsætningen (*vigtige enheder*).

Erstatningsansvar efter de almindelige erstatningsregler, herunder selskabslovens § 361, stk. 1, jf. § 115.

Entreprenører, rådgivere og leverandører

Sanktioner

Disse aktører er ikke omfattet af NIS2-loven. Lovens sanktioner gælder derfor ikke direkte for disse og deres ledelsesorganer.

Ansvar kan dog pålægges virksomheden i medfør af parternes aftale og de almindelige erstatningsregler, herunder selskabslovens § 361, stk. 1, jf. § 115.

NIS 2

Værdi for virksomheden

MOLT | WENGEL

Mere end blot compliance

Værdien i NIS2

NIS2 klæder virksomheder på til en ny virkelighed.

NIS2 er med til at gøre virksomheder mere robust.

NIS2 er med til at gøre virksomheder konkurrencedygtige.

MOLT
WENGEL

Nicolaus Falk-Scheibel

Advokat, ph.d.

Mobil: +45 25 10 05 90
E-mail: nif@mowe.dk

MOLT | WENGEL

En mærkbar forskel i byggeriet

www.mowe.dk

Paneldebat: Når virkeligheden rammer - hvem tager ansvaret?

Malene Stidsen

Programchef

Industriens Fond

Ulrik Branner

CEO

SiteHub

Charlotte Miolane

Chief Information Security Officer

COWI

Lillian Rasch Madsen

Vicedirektør, Center for Ejendomme

Region H

CON
TECH
LAB_

Anders Balslev

Partner, Implement Consulting Group

Fra sikkerhedsbrist til konkurrencefordel

CON
TECH
LAB_

IMPLEMENT

CONSULTING GROUP_

.the tech collective

powered by Implement

Fra sikkerhedsbrist

Konkurrencefordel

January 22nd 2026

Hvem er jeg?

Anders Balslev

Equity Partner ved Implement Consulting Group,

Rådgive og vejlede virksomheder før, under og efter en cyber-hændelse altid imod et højere niveau af modenhed,

Implement, Partner – Cyber Tech Services

June 2025 –

PwC, Director - Incident Response

2021 – 2025

Deloitte, Director - Cyber Operation

2017 - 2021

Outpost24, Director – Nordic & Baltic

2012 - 2017

Hvem er vi? – How does the toolbox looks like…

A unified and strong **collaborative offering between The Tech Collective and Implement Consulting Group**

We are a collective of technologists, developers, testers and engineers with a passion for using technology and digital solutions to drive meaningful outcomes for people.

We are techies.

We have organized ourselves in companies of specific subject matter expertise. The Company serving you is the "Cyber Tech Service A/S", a part of The Tech Collective. The company have become a market and community leader in its specialized domain focusing on implementation and operating services.

.the tech collective
powered by Implement

IMPLEMENT
CONSULTING GROUP_

Together, we are a **one-stop shop** that offers expertise spanning all the needs of the suite of work packages – from technical implementation to legal advisory and management consulting.

We are a collective of subject matter experts with strong analytical competencies. And we care just as much about the soft skills as we do about the hard skills.

We are nerds.

We have a deep commitment to bringing our expertise into play in a way that engages other people through best-practice but also creative ways. We call it change with impact. Every project introduces a change into an organisation, therefore everything we do is grounded in change management practices. And we tailor the team size and engagement methods to your exact needs for maximum flexibility.

Our stats

- 0 clients has left us
- Cost effective
- No salespeople
- Known to be unknown
- High quality deliverables

50+

Cyber technicians with deep, operational Microsoft capabilities across Entra, Sentinel, M365 and Defender

65+

Cyber advisors with demonstrated domain knowledge within compliance, privacy and information security

10+

Security leaders with CISO and top-leadership experience from large cooperations

15+

ICS/OT security professionals across both technical and advisory domains

15+

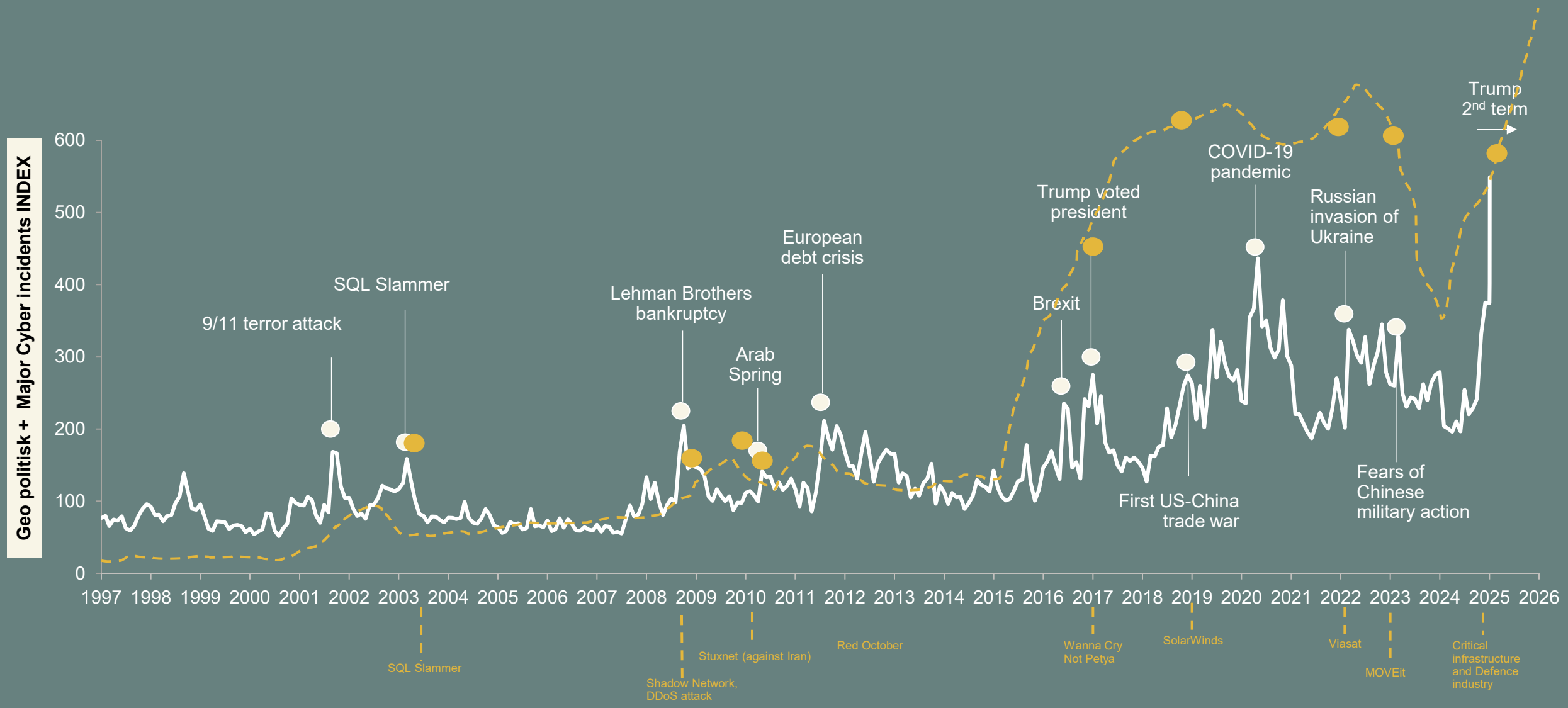
Offensive technicians, incident responders and forensic experts

Our SOC and IR credentials by sector

- Pharmaceuticals
- Mining & minerals
- Utility & water
- Financial Services
- Logistics

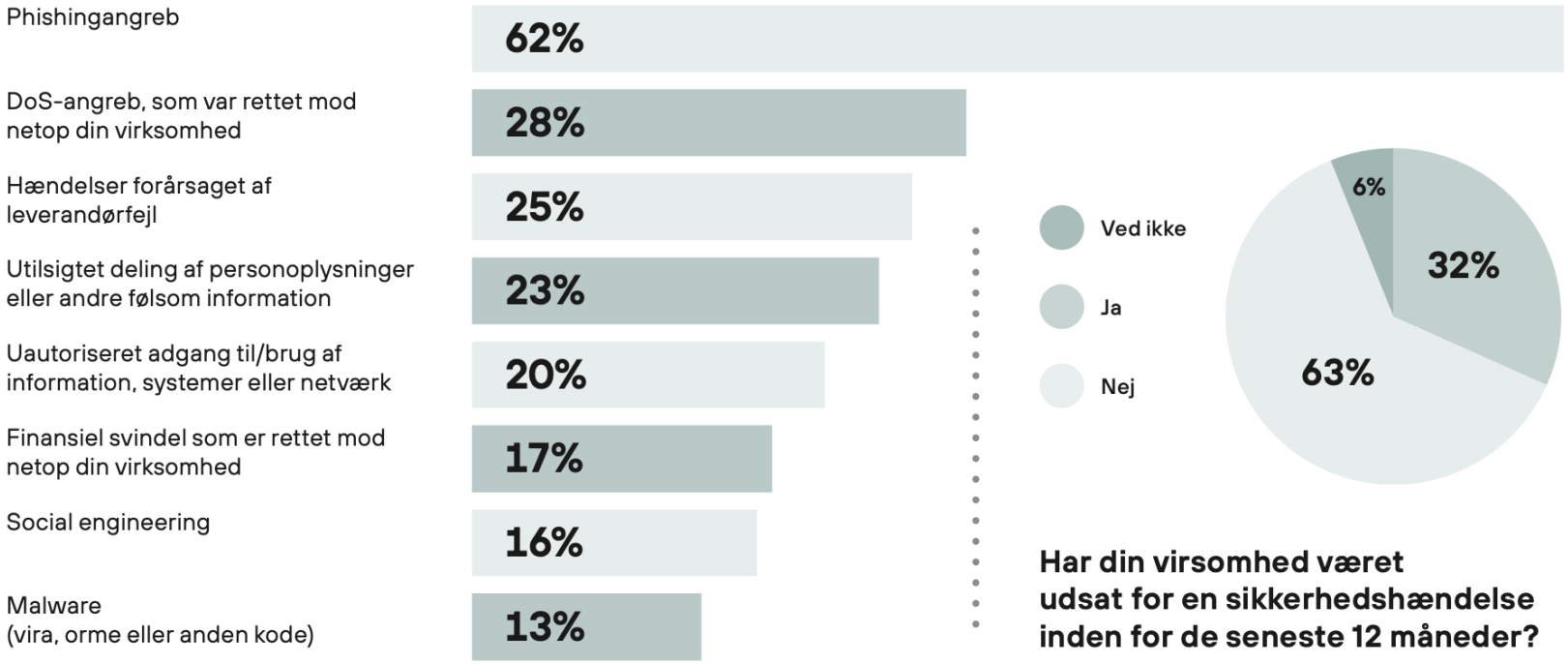
Hvad er det vi ser derude…

Stigende global usikkerhed og geopolitiske spændinger er ved at omforme sikkerhedsindustrien…



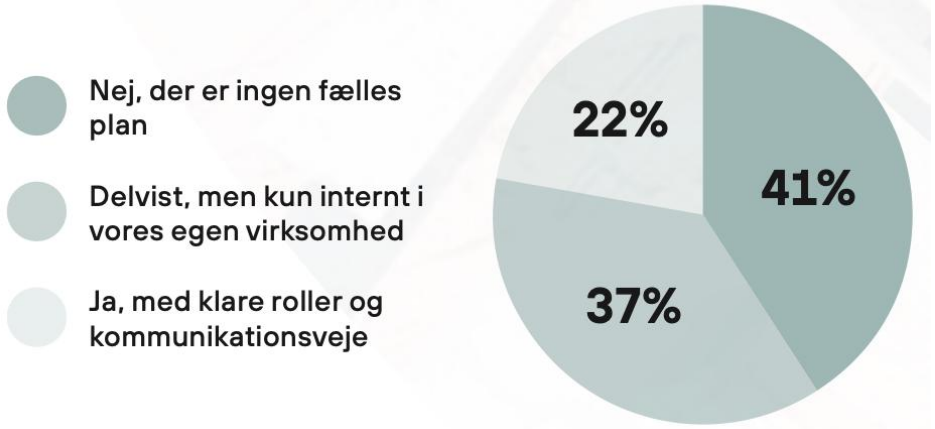
Source: Implement based on The GEPU Index (Global Economic Policy Uncertainty Index) measures the level of uncertainty in global economic policy based on the frequency of related terms in leading international newspapers.

Hvilken type sikkerhedshændelse(r) er der tale om?



Har din virsomhed været udsat for en sikkerhedshændelse inden for de seneste 12 måneder?

Findes der en fælles procedure for håndtering af cyberhændelser eller databrud i projekter eller på byggeladsen?



Tallene viser, at byggebranchen er hårdt ramt af cyberhændelser, samtidig med at mange virksomheder mangler fælles procedurer og koordinering på tværs af projekter. Resultatet er en sektor, hvor ***risikoen er høj, men beredskabet lavt*** *og hvor selv simple angreb kan få store konsekvenser for drift og tidsplaner.*

I byggebranchen

Byggebranchen er særligt udsat, fordi den har mange underentreprenører med lav modenhed, store datamængder i bevægelse og en ekstrem afhængighed af digitale systemer, der ikke må fejle. Angribere ved, at forsinkelser er ekstremt dyre og ***derfor betaler mange byggevirksomheder hurtigt.*** *Det gør branchen til en attraktiv målskive.*

IT-sikkerhedsforanstaltninger i små virksomheder fordelt på brancher i 2024

Figuren viser resultaterne fra Danmarks Statestiks spørgeskema	Alle	Industri	Bygge og anlæg	Handel og transport	Information og Kommunikation	Erhvervs service
	Pct. af alle små virksomheder					
Mindst én type foranstaltning	92	97	91 ↓	90	98 ↑	94
Stærke adgangskoder	55	51	45 ↓	55	75 ↑	59
Systematisk opdatering af software	82	84	79 ↓	79	88 ↑	86
Biometriske metoder til brugerid.	23	18	24	19 ↓	41 ↑	28
Mindst to godkendelsesmekanismer	47	48	38 ↓	41	80 ↑	54
Kryptering af data, filer eller e-mails	39	36	27 ↓	33	68 ↑	54
Backup til en alternativ placering	80	86	76	75 ↓	93 ↑	86
Adgangskontrol til netværk	69	73	59 ↓	67	85 ↑	75
VPN (virtuelt privat netværk)	41	38	31 ↓	38	56 ↑	53
It-sikkerhedsovervågningssystem	51	48	40 ↓	50	74 ↑	60
Lagring af logfiler	48	44	28 ↓	48	73 ↑	62
Risikoanalyse	36	30	22 ↓	35	66 ↑	48
Tests af it-sikkerhed	34	28	23 ↓	33	57 ↑	42
Dokumentation om it-sikkerhed	45	41	29 ↓	41	75 ↑	59
Mindst én type info om it-sikkerhed	59	57	46 ↓	56	88 ↑	71
Frivillig uddannelse og træning	43	36	24 ↓	42	73 ↑	57
Obligatorisk uddannelse og træning	29	24	16 ↓	27	58 ↑	40
Via skriftlig kontrakt	34	31	26 ↓	29	64 ↑	44

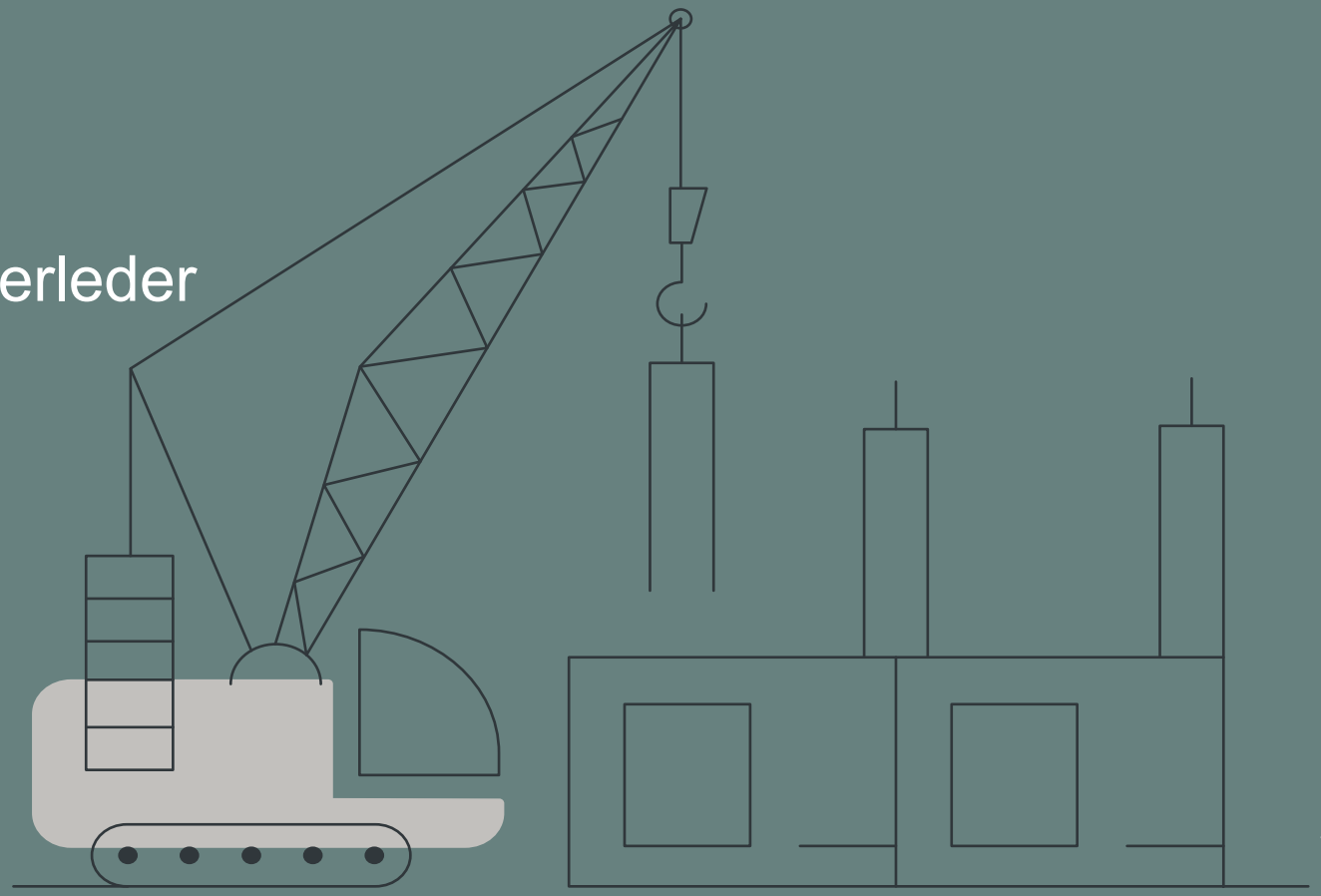
Succesfuld inddæmning af omfattende ransomware-angreb

En fiktiv fortælling meget meget tæt på sandheden..

Scenesætning

Fiktiv virksomhed: VOGNPARK

Branche: Bygge & Anlæg
Hovedsæde: Nordjylland
Antal medarbejdere: Ca. 170 - Ejerleder
Omsætning: 355 mio. DKK
Etableret: 1995
Marked: Europa
Produktionslinje: 3-holds skift



Scenesætning

Hændelsen

En **fredag morgen kl. 06:15** rapporterer produktionslederen, at:

1. De ikke kan logge ind i deres produktionsmaskiner
2. Mobile enheder time-out'er
3. Nogle projektmapper er forsvundet på deres egne maskiner
4. Der popper en besked op:
   "Your files have been encrypted. Contact us at secure-recover@proton.me"

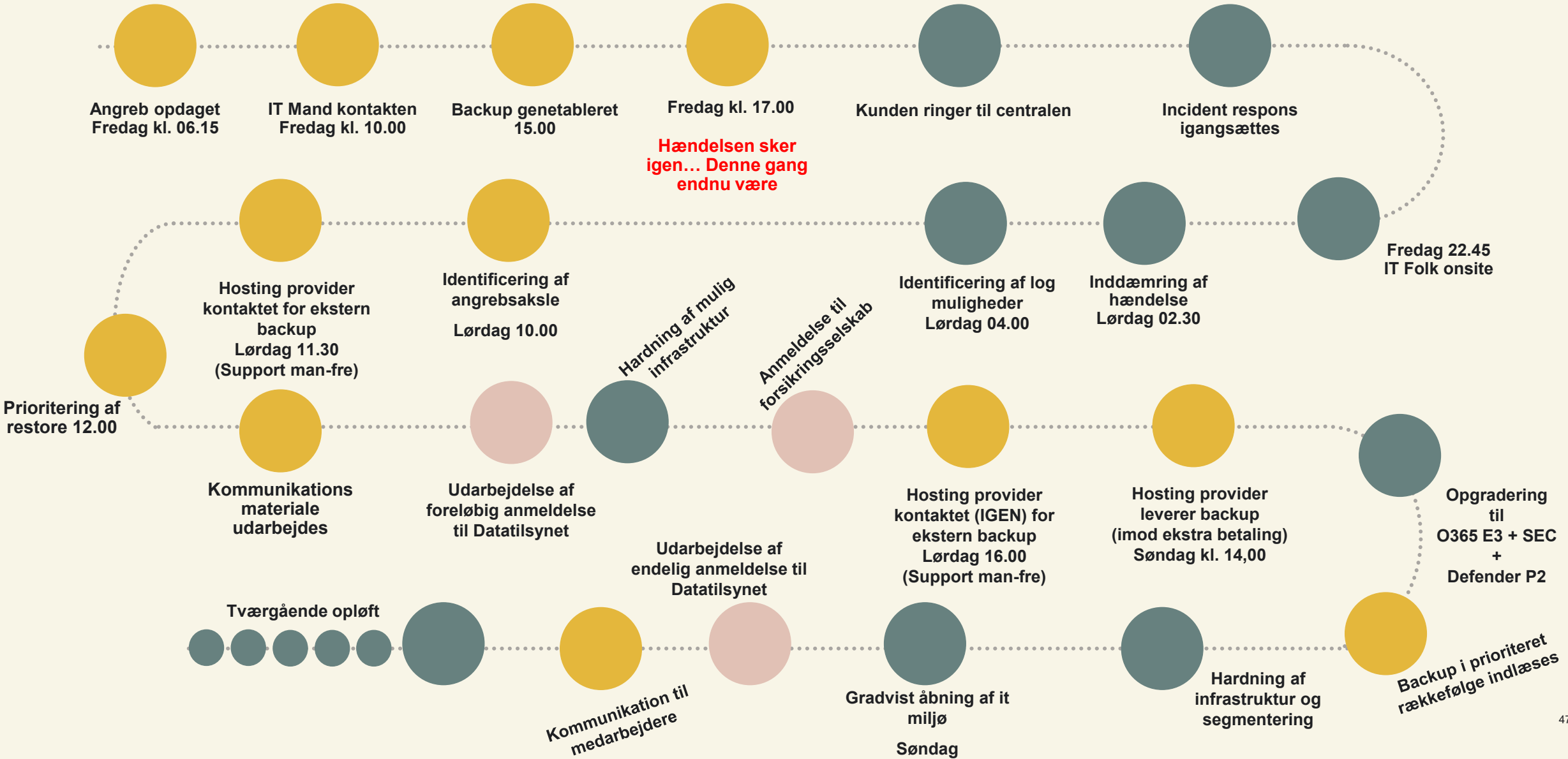
Virksomheden igangsætter deres standard reaktion, som de er blevet enige om på Sikkerhedsudvalgsmødet de har én gang om året…

IT kompetencen til rådighed er deres ”eksterne IT mand” som har været med siden 1995, og som er til rådighed mandag – fredag fra 10-14. Der var bare lige det, at IT mandens kone, desværre var rigtig syg, hvorfor han ikke havde tid, men han ville da gerne forsøge at hjælpe. IT manden udføre derfor den ønskede standard reaktion, men må altså melde pas på at hjælpe yderligere.

Standardreaktionen indbefattede:

Genetablering til seneste backup… … … … … … … … …

Tidslinjen

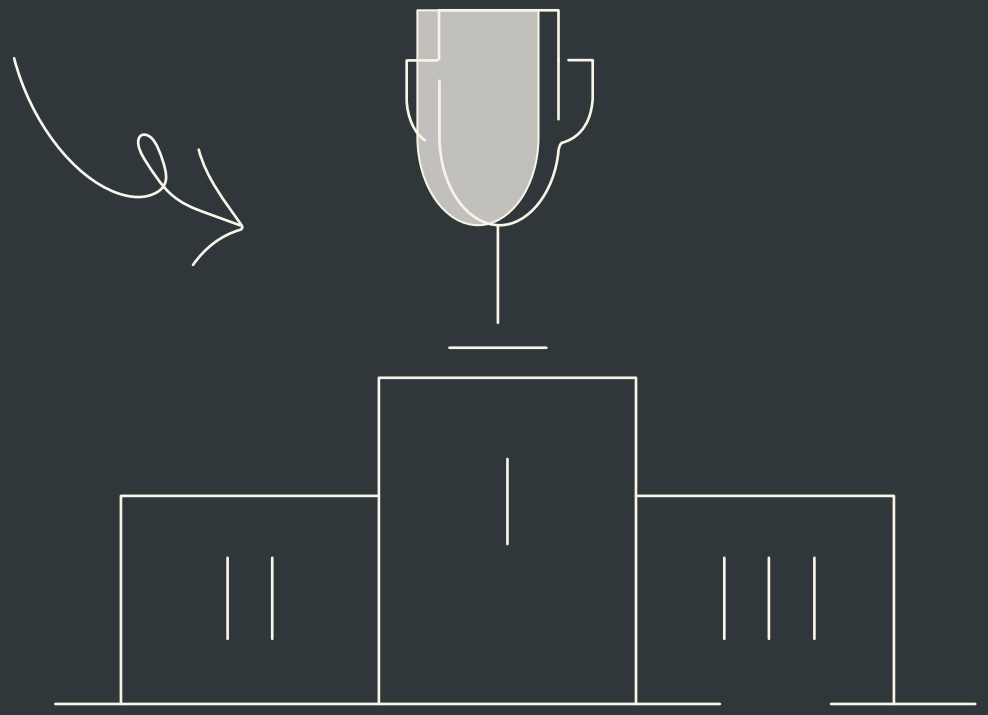

Angreb opdaget
Fredag kl. 06.15
IT Mand kontakten
Fredag kl. 10.00
Backup genetableret
15.00
Fredag kl. 17.00
Hændelsen sker igen… Denne gang endnu være
Kunden ringer til centralen
Incident respons igangsættes
Fredag 22.45
IT Folk onsite
Inddæmring af hændelse
Lørdag 02.30
Identificering af log muligheder
Lørdag 04.00
Identificering af angrebsaksle
Lørdag 10.00
Hosting provider kontaktet for ekstern backup
Lørdag 11.30
(Support man-fre)
Prioritering af restore 12.00
Kommunikations materiale udarbejdes
Udarbejdelse af foreløbig anmeldelse til Datatilsynet
Hardning af mulig infrastruktur
Anmeldelse til forsikringsselskab
Hosting provider kontaktet (IGEN) for ekstern backup
Lørdag 16.00
(Support man-fre)
Hosting provider leverer backup
(imod ekstra betaling)
Søndag kl. 14,00
Opgradering til
O365 E3 + SEC
+
Defender P2
Backup i prioriteret rækkefølge indlæses
Hardning af infrastruktur og segmentering
Gradvist åbning af it miljø
Søndag
Udarbejdelse af endelig anmeldelse til Datatilsynet
Kommunikation til medarbejdere
Tværgående opløft

Konsekvenser for VOGNPARK

- Tab af produktionstid
- Tab / Respons – og genopretningsomkostninger
- Tab af data og forretningskritisk information
- Omdømmetab og tab af kundetillid
- Leverandør – og supply chain-konsekvenser
- Interne personaleomkostninger & tabt arbejdstid

- (Juridiske krav, bøder og compliance tab)

Hvordan blev det så en konkurrencefordel?



49

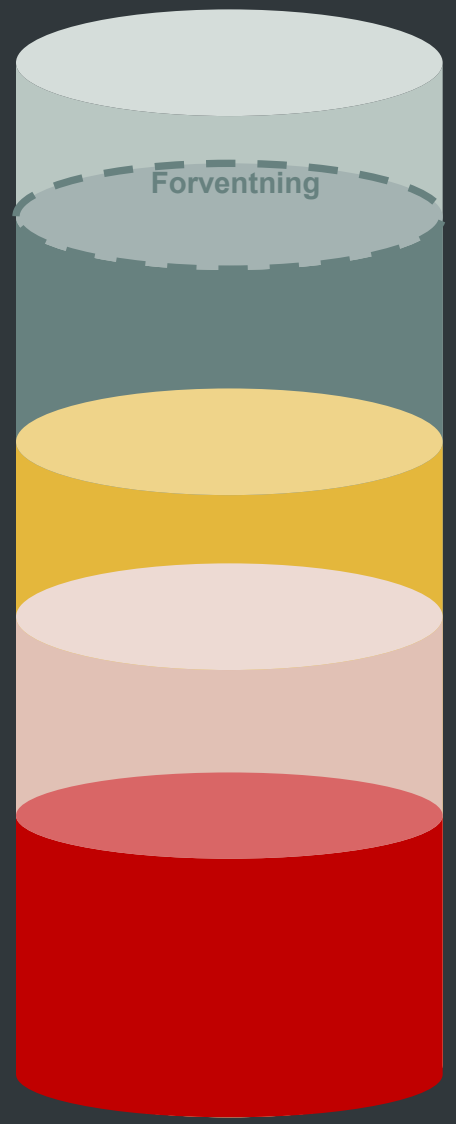
Modenheds barometeret

”Det er jo gået gået fint i 30 år!?”

Genskab til seneste backup

Hændelsen sker igen…

Ringer efter hjælp



Compliance- og myndighedsopgaver
Leverandørstyring og supply-chain opjustering

Forbedringer på bruger- og organisationsniveau

Strategiske sikkerhedsløft

Governance, roller og procesforbedringer

Opbygning af logning, overvågning og detektion
Backup- og restore-opjustering

Infrastruktur- og systemopjustering
Identificering og lukning af sårbarheder

En cyberhændelse er en konkurrencefordel, hvis den udnyttes rigtigt

Den bliver en fordel når virksomheden:

- Lærer hurtigt og investerer strategisk
- Bygger resiliens og kommunikerer åbent
- Håndterer krisen professionelt og gennemsigtigt
- Demonstrerer modenhed overfor markedet
- Bruger hændelsen til at forbedre teknologi, governance og kultur

Det er ikke hændelsen i sig selv, der giver fordelen – det er **reaktionen**, **forberedelsen** og **kommunikationen**.

Hvis jeg var jer i 2026

Skab overblik med risikorapport

Udarbejd en ledelsesvenlig risikorapport, der fokuserer på top 5 risici og deres konsekvenser for jeres virksomhed.

Prioritér strategiske bevægelser

Fokuser på 2–3 nøglestrategier som Zero Trust, identitetsmodernisering og beredskab for bedre sikkerhed.

Træn beredskabet med øvelser

Gennemfør realistiske topleder-øvelser og scenarier for at sikre organisationens reaktionsparathed ved hændelser.

Følg op med KPI'er og governance

Implementer governance og regelmæssig rapportering til bestyrelsen for løbende performanceopfølgning.

IMPLEMENT
CONSULTING GROUP_

Spørgsmål?

Anders Balslev

E-mail: anev@thetechcollective.eu

Kirsten Hede

Udviklingsdirektør, Bestyrelsesforeningens Center for Cyberkompetencer

Fra bestyrelse til beredskab - ledelse, ansvar og kontrol i cybersikkerhed

CON
TECH
LAB_

FRA BESTYRELSE TIL BEREDSKAB - Ledelse, ansvar og kontrol i cybersikkerhed

22. januar 2026

Kirsten Hede, Udviklingsdirektør
Bestyrelsesforeningens Center for Cyberkompetencer

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

BESTYRELSESFORENINGEN – DEN KORTE VERSION

Foreningens formål er på **non-profit** basis at arbejde for en stadig **opkvalificering** af bestyrelsesarbejdet i **danske selskaber, virksomheder, organisationer og institutioner**

Bestyrelsesforeningen blev stiftet den 7. maj 2013 som et tværnationalt projekt af 8 virksomheder, 24 bestyrelsesformænd og 10 professorer.
I dag har foreningen 1000 medlemmer heraf ca. 70 medlemsvirksomheder

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

CBS Bestyrelsesuddannelserne – DEN KORTE VERSION

CBS Executive Bestyrelsesuddannelsen Februar 2026

Board Leadership · Åben

16 dage · 5.2.2026 · 9:00 - 17:00 DKK 120.000

Bestyrelsesud
bestyrelsens c

Se kursus D

Bestyrelsesarbejde i Erhvervsfonde 2026

Board Leadership · Åben

2 dage · 2.2.2026 · 09:00 - 18:00 DKK 26.800

Få den nødvendige viden og værktøjer til at navige
udfordringer, som bestyrelsesmedlemmer i fonde

Se kursus Download kursusinformation

Børsens Bestyrelsesuddannelse Marts 2026

Board Leadership · Åben

8 dage · 3.3.2026 · 09:00 - 17:00 DKK 69.999

CBS Bestyrelsesuddannelserne udbyder i samarbejde med Børsen
Uddannelse en fælles bestyrelsesuddannelse....

Bestyrelsesarbejde i Startups & Scaleups 2026

Board Leadership · Åben

3 dage · 23.3.2026 · 9:00 - 17:30 DKK 26.000

CBS Bestyrelsesuddannelserne går i samarbejde
Business Angels (DanBan). Uddannelsen henver

Se kursus Download kursusinformation

Grundlæggende bestyrelsesuddannelse August 2026

Board Leadership · Åben

3 dage · 24.8.2026 · 09:00 - 18:00 DKK 26.800

Formålet med denne uddannelse er at give dig et gr
fundament for effektivt bestyrelsesarbejde, uanset

Se kursus Download kursusinformation

Bestyrelsesarbejde i Pension & Forsikring 2026

Board Leadership · Åben

5 dage · 23.9.2026 · 9:00 - 17:00 DKK 41.600

Bestyrelsesarbejde i finansielle virksomheder introducer
såvel som erfarne bestyrelsesmedlemmer til opdateret vi

Se kursus Download kursusinformation

Bestyrelsesuddannelse i ESG 2025

Board Leadership · Åben

3 dage · 10.11.2025 · 9:00 - 17:00 DKK 29.000

et giver overblik og større strategisk forståelse for

Blue Board Leadership 2026

Board Leadership · Åben

8 days · 7.9.2026 · 9.00 - 18.00 DKK 78.225

The purpose of The Blue Board Leadership Program is to improve the competencies of future and present 'blue' board members in...

Se kursus Download kursusinformation

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

Styrkelse af Strategiske Cyberkompetencer projekter/2019-26

- ✓ Styrke **danske virksomheders konkurrenceevne**
- ✓ Skabe **vækst i en digital tid og** udnytte **den digitale transformation**
- ✓ Beskytte **virksomhedens værdier**
- ✓ Leve op til **bestyrelsesansvar**

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

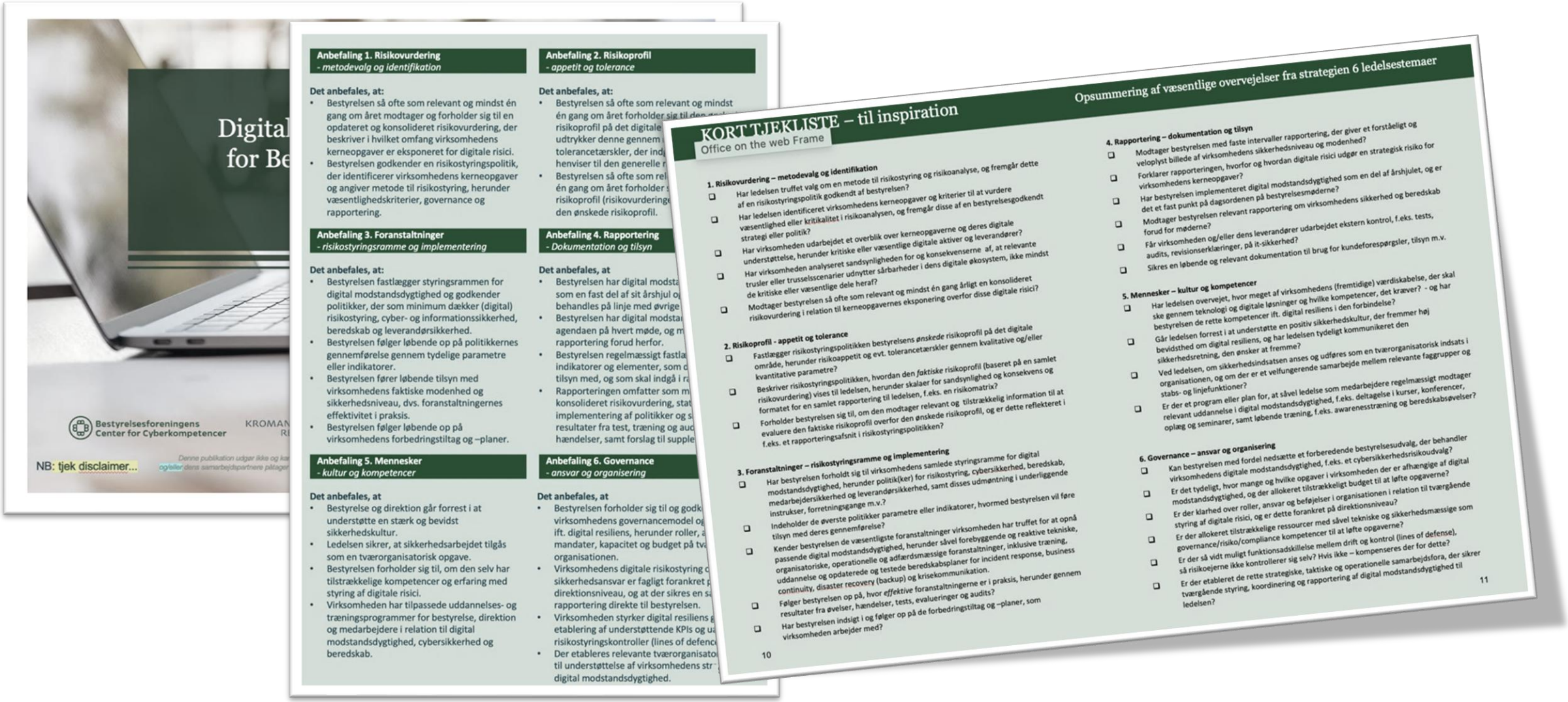
INDUSTRIENS FOND

BESTYRELSENS ROLLE OG ANSVAR ift CYBERSIKKERHED

- ✓ Styrke **danske virksomheders konkurrenceevne**
- ✓ Skabe **vækst i en digital tid og** udnytte **den digitale transformation**
- ✓ Beskytte **virksomhedens værdier**
- ✓ Leve op til **bestyrelsesansvar**

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

ANBEFALINGER TIL BESTYRELSE og DIREKTION – ny version 5.0 NB foreløbig



Digital
for Be

Bestyrelsesforeningens Center for Cyberkompetencer

NB: tjek disclaimer...

Anbefaling 1. Risikovurdering
- metodevalg og identifikation

Det anbefales, at:
- Bestyrelsen så ofte som relevant og mindst én gang om året modtager og forholder sig til en opdateret og konsolideret risikovurdering, der beskriver i hvilket omfang virksomhedens kerneopgaver er eksponeret for digitale risici.
- Bestyrelsen godkender en risikostyringspolitik, der identificerer virksomhedens kerneopgaver og angiver metode til risikostyring, herunder væsentlighedskriterier, governance og rapportering.

Anbefaling 2. Risikoprofil
- appetit og tolerance

Det anbefales, at:
- Bestyrelsen så ofte som relevant og mindst én gang om året forholder sig til den
risikoprofil på det digitale
udtrykker denne gennem
tolerancetærskler, der ind
henviser til den generelle
- Bestyrelsen så ofte som rel
én gang om året forholder
risikoprofil (risikovurdering
den ønskede risikoprofil.

Anbefaling 3. Foranstaltninger
- risikostyringsramme og implementering

Det anbefales, at:
- Bestyrelsen fastlægger styringsrammen for digital modstandsdygtighed og godkender politikker, der som minimum dækker (digital) risikostyring, cyber- og informationssikkerhed, beredskab og leverandørsikkerhed.
- Bestyrelsen følger løbende op på politikkernes gennemførelse gennem tydelige parametre eller indikatorer.
- Bestyrelsen fører løbende tilsyn med virksomhedens faktiske modenhed og sikkerhedsniveau, dvs. foranstaltningernes effektivitet i praksis.
- Bestyrelsen følger løbende op på virksomhedens forbedringstiltag og –planer.

Anbefaling 4. Rapportering
- Dokumentation og tilsyn

Det anbefales, at
- Bestyrelsen har digital modsta
som en fast del af sit årshjul o
behandles på linje med øvrige
- Bestyrelsen har digital modsta
agendaen på hvert møde, og m
rapportering forud herfor.
- Bestyrelsen regelmæssigt fastla
indikatorer og elementer, som d
tilsyn med, og som skal indgå i r
- Rapporteringen omfatter som m
konsolideret risikovurdering, stat
implementering af politikker og s
resultater fra test, træning og aud
hændelser, samt forslag til supple

Anbefaling 5. Mennesker
- kultur og kompetencer

Det anbefales, at
- Bestyrelse og direktion går forrest i at understøtte en stærk og bevidst sikkerhedskultur.
- Ledelsen sikrer, at sikkerhedsarbejdet tilgås som en tværorganisatorisk opgave.
- Bestyrelsen forholder sig til, om den selv har tilstrækkelige kompetencer og erfaring med styring af digitale risici.
- Virksomheden har tilpassede uddannelses- og træningsprogrammer for bestyrelse, direktion og medarbejdere i relation til digital modstandsdygtighed, cybersikkerhed og beredskab.

Anbefaling 6. Governance
- ansvar og organisering

Det anbefales, at
- Bestyrelsen forholder sig til og godk
virksomhedens governancemodel o
ift. digital resiliens, herunder roller,
mandater, kapacitet og budget på tv
organisationen.
- Virksomhedens digitale risikostyring
sikkerhedsansvar er fagligt forankret
direktionsniveau, og at der sikres en s
rapportering direkte til bestyrelsen.
- Virksomheden styrker digital resiliens
etablering af understøttende KPIs og u
risikostyringskontroller (lines of defenc
- Der etableres relevante tværorganisato
til understøttelse af virksomhedens str
digital modstandsdygtighed.

KORT TJEKLISTE – til inspiration
Office on the web Frame

Opsummering af væsentlige overvejelser fra strategien 6 ledelsestemaer

1. Risikovurdering – metodevalg og identifikation
- ❑ Har ledelsen truffet valg om en metode til risikostyring og risikoanalyse, og fremgår dette af en risikostyringspolitik godkendt af bestyrelsen?
- ❑ Har ledelsen identificeret virksomhedens kerneopgaver og kriterier til at vurdere væsentlighed eller kritikalitet i risikoanalysen, og fremgår disse af en bestyrelsesgodkendt strategi eller politik?
- ❑ Har virksomheden udarbejdet et overblik over kerneopgaverne og deres digitale understøttelse, herunder kritiske eller væsentlige digitale aktiver og leverandører?
- ❑ Har virksomheden analyseret sandsynligheden for og konsekvenserne af, at relevante trusler eller trusselsscenarier udnytter sårbarheder i dens digitale økosystem, ikke mindst de kritiske eller væsentlige dele heraf?
- ❑ Modtager bestyrelsen så ofte som relevant og mindst én gang årligt en konsolideret risikovurdering i relation til kerneopgavernes eksponering overfor disse digitale risici?

2. Risikoprofil - appetit og tolerance
- ❑ Fastlægger risikostyringspolitikken bestyrelsens *ønskede* risikoprofil på det digitale område, herunder risikoappetit og evt. tolerancetærsker gennem kvalitative og/eller kvantitative parametre?
- ❑ Beskriver risikostyringspolitikken, hvordan den *faktiske* risikoprofil (baseret på en samlet risikovurdering) vises til ledelsen, herunder skalaer for sandsynlighed og konsekvens og formatet for en samlet rapportering til ledelsen, f.eks. en risikomatrix?
- ❑ Forholder bestyrelsen sig til, om den modtager relevant og tilstrækkelig information til at evaluere den faktiske risikoprofil overfor den ønskede risikoprofil, og er dette reflekteret i f.eks. et rapporteringsafsnit i risikostyringspolitikken?

3. Foranstaltninger – risikostyringsramme og implementering
- ❑ Har bestyrelsen forholdt sig til virksomhedens samlede styringsramme for digital modstandsdygtighed, herunder politik(ker) for risikostyring, cybersikkerhed, beredskab, medarbejdersikkerhed og leverandørsikkerhed, samt disses udmøntning i underliggende instrukser, forretningsgange m.v.?
- ❑ Indeholder de øverste politikker parametre eller indikatorer, hvormed bestyrelsen vil føre tilsyn med deres gennemførelse?
- ❑ Kender bestyrelsen de væsentligste foranstaltninger virksomheden har truffet for at opnå passende digital modstandsdygtighed, herunder såvel forebyggende og reaktive tekniske, organisatoriske, operationelle og adfærdsmæssige foranstaltninger, inklusive træning, uddannelse og opdaterede og testede beredskabsplaner for incident response, business continuity, disaster recovery (backup) og krisekommunikation.
- ❑ Følger bestyrelsen op på, hvor *effektive* foranstaltningerne er i praksis, herunder gennem resultater fra øvelser, hændelser, tests, evalueringer og audits?
- ❑ Har bestyrelsen indsigt i og følger op på de forbedringstiltag og –planer, som virksomheden arbejder med?

10

4. Rapportering – dokumentation og tilsyn
- ❑ Modtager bestyrelsen med faste intervaller rapportering, der giver et forståeligt og velopbygt billede af virksomhedens sikkerhedsniveau og modenhed?
- ❑ Forklarer rapporteringen, hvorfor og hvordan digitale risici udgør en strategisk risiko for virksomhedens kerneopgaver?
- ❑ Har bestyrelsen implementeret digital modstandsdygtighed som en del af årshjulet, og er det et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ Modtager bestyrelsen relevant rapportering om virksomhedens sikkerhed og beredskab forud for møderne?
- ❑ Får virksomheden og/eller dens leverandører udarbejdet ekstern kontrol, f.eks. tests, audits, revisionserklæringer, på it-sikkerhed?
- ❑ Sikres en løbende og relevant dokumentation til brug for kundeforespørgsler, tilsyn m.v.

5. Mennesker – kultur og kompetencer
- ❑ Har ledelsen overvejet, hvor meget af virksomhedens (fremtidige) værdiskabelse, der skal ske gennem teknologi og digitale løsninger og hvilke kompetencer, det kræver? - og har bestyrelsen de rette kompetencer ift. digital resiliens i den forbindelse?
- ❑ Går ledelsen forrest i at understøtte en positiv sikkerhedskultur, der fremmer høj bevidsthed om digital resiliens, og har ledelsen tydeligt kommunikeret den sikkerhedsretning, den ønsker at fremme?
- ❑ Ved ledelsen, om sikkerhedsindsatsen anses og udføres som en tværorganisatorisk indsats i organisationen, og om der er et velfungerende samarbejde mellem relevante faggrupper og stabs- og linjefunktioner?
- ❑ Er der et program eller plan for, at såvel ledelse som medarbejdere regelmæssigt modtager relevant uddannelse i digital modstandsdygtighed, f.eks. deltagelse i kurser, konferencer, oplæg og seminarer, samt løbende træning, f.eks. awarenesstræning og beredskabsøvelser?

6. Governance – ansvar og organisering
- ❑ Kan bestyrelsen med fordel nedsætte et forberedende bestyrelsesudvalg, der behandler virksomhedens digitale modstandsdygtighed, f.eks. et cybersikkerhedsrisikoudvalg?
- ❑ Er det tydeligt, hvor mange og hvilke opgaver i virksomheden der er afhængige af digital modstandsdygtighed, og der allokeret tilstrækkeligt budget til at løfte opgaverne?
- ❑ Er der klarhed over roller, ansvar og beføjelser i organisationen i relation til tværgående styring af digitale risici, og er dette forankret på direktionsniveau?
- ❑ Er der allokeret tilstrækkelige ressourcer med såvel tekniske og sikkerhedsmæssige som governance/risiko/compliance kompetencer til at løfte opgaverne?
- ❑ Er der så vidt muligt funktionsadskillelse mellem drift og kontrol (lines of defense), så risikoejerne ikke kontrollerer sig selv? Hvis ikke – kompenseres der for dette?
- ❑ Er der etableret de rette strategiske, taktiske og operationelle samarbejdsfora, der sikrer tværgående styring, koordinering og rapportering af digital modstandsdygtighed til ledelsen?

11

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

BESTYRELSENS OPGAVER og ANSVAR

Jobbeskrivelsen for Bestyrelsen (…og LEDELSEN)

- Bestyrelsen er **som et kollektiv** ansvarlig for selskabet – og med **personligt ansvar**…
- Bestyrelsen skal **varetage selskabets interesser** (…ejernes – men også medarbejdere, pengeinstitut, kunder osv osv…)

Der er således to overordnede **opgaver for bestyrelsen (og ledelsen)** :

- At passe på **selskabets aktiver**, som er bestyrelsen betroet af ejerne (og andre stakeholders…)
- At **skabe værdi** på selskabets aktiver (finansielt afkast på investeret kapital) - afstemt med ejerne og deres risikoprofil og prioriteter inkl. afvejninger omkring bæredygtighedsdagsorden mm.

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

BESTYRELSENS OPGAVER og ANSVAR … og REALITET

Jobbeskrivelsen for Bestyrelsen (…og LEDELSEN)

360 grader om bestyrelsens opgaver, problemstillinger & relationer

Strategisk og operationelt niveau i helt tæt samarbejde

Orden i penalhuset: Generalforsamling og bestyrelsesmødeplanlægning, mødereferater, mødeevalueringer, årshjul, orden i penalhuset mv.

Slides fra CBS-Executive Bestyrelsesuddannelserne

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

BESTYRELSENS OPGAVER og ANSVAR … og REALITET

Jobbeskrivelsen for Bestyrelsen (…og LEDELSEN)

BØRSEN. LEDELSE

torsdag 29. oktober 2020

ESTYRELSESANSVAR
lestyrelsernes juridiske nsvar gælder også data-tik og sikkerhed

LEDELSESDILEMMA
Hvordan håndterer du som leder et brud på datasikkerheden?

DIGITAL SIKKERHED
"Som leder skal du kunne give slip"
Thomas Lund-Sørensen, chef for Center for Cybersikkerhed under Forsvarets Efterretningstjeneste

Side 8-9

Side 7

Topchef: Vi er et andet selskab efter hackerangreb

Søren Nielsen, topchef for Demant, lærte at tage cybertrusler seriøst, da virksomheden blev ramt af et hackerangreb, der kostede over en halv milliard. Eksperter er enige: Med en stigende trussel er der øget behov for, at dansk erhvervsliv sætter fokus på sikkerheden i de øverste lag af organisationen.

Stort tema om datasikkerhed.

Det er den største realtrussel nu om dage for et samlet kollaps af en global virksomhed

Søren Nielsen, topchef i Demant

"Now a days, it is the largest real threat for a total collapse of a global corporation"

…i GOD tro
… på OPLYST grundlag
… forretningsmæssigt FORSVARLIGT
… og altid i SELSKABETS interesse

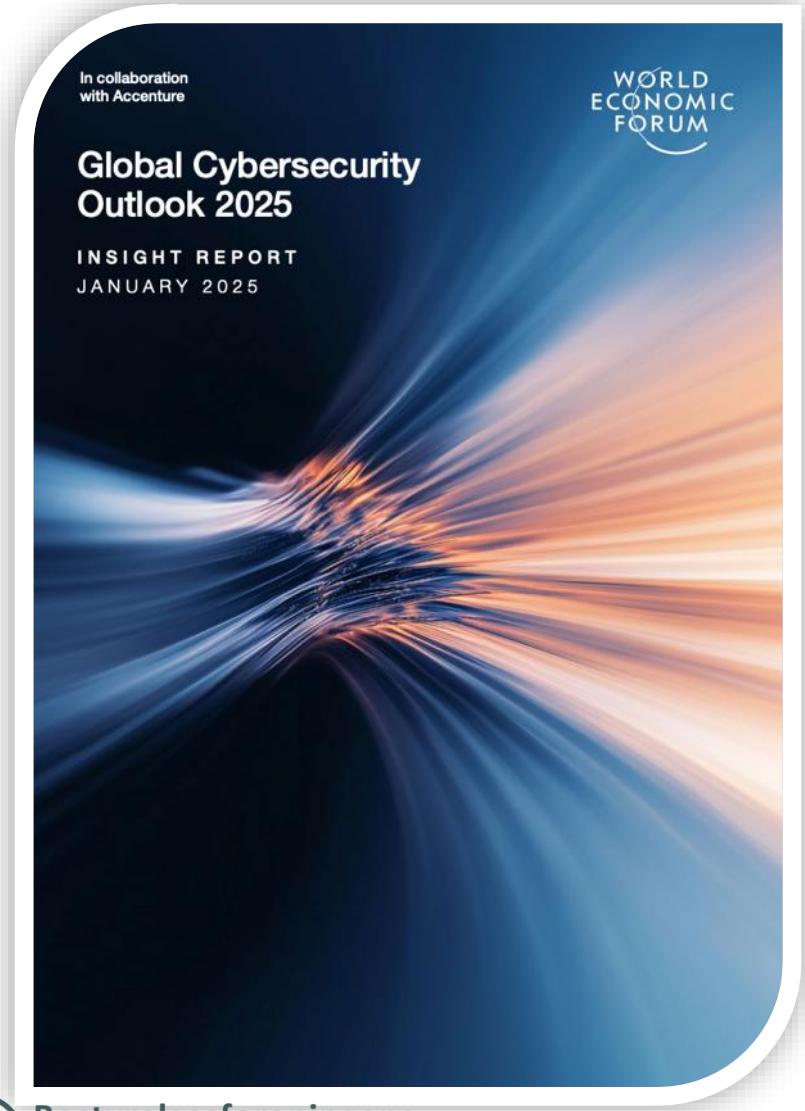
Ejerstrategi, vedtægter, formål mm.

Bestyrelsesforeningens Center for Cyberkompetencer

INDUSTRIENS FOND

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

ANALYSER FRA WORLD ECONOMIC FORUM mm.



WORLD ECONOMIC FORUM

Join us | Sign in

Key insights

In a complex cyberspace characterized by geopolitical uncertainties, widening cyber inequity and sophisticated cyberthreats, leaders must adopt a security-first mindset.

While the 2024 edition of the Global Cybersecurity Outlook highlighted the growing inequity in cyberspace, this year's report shines a light on the increasing complexity of the cyber landscape, which has profound and far-reaching implications for organizations and nations.

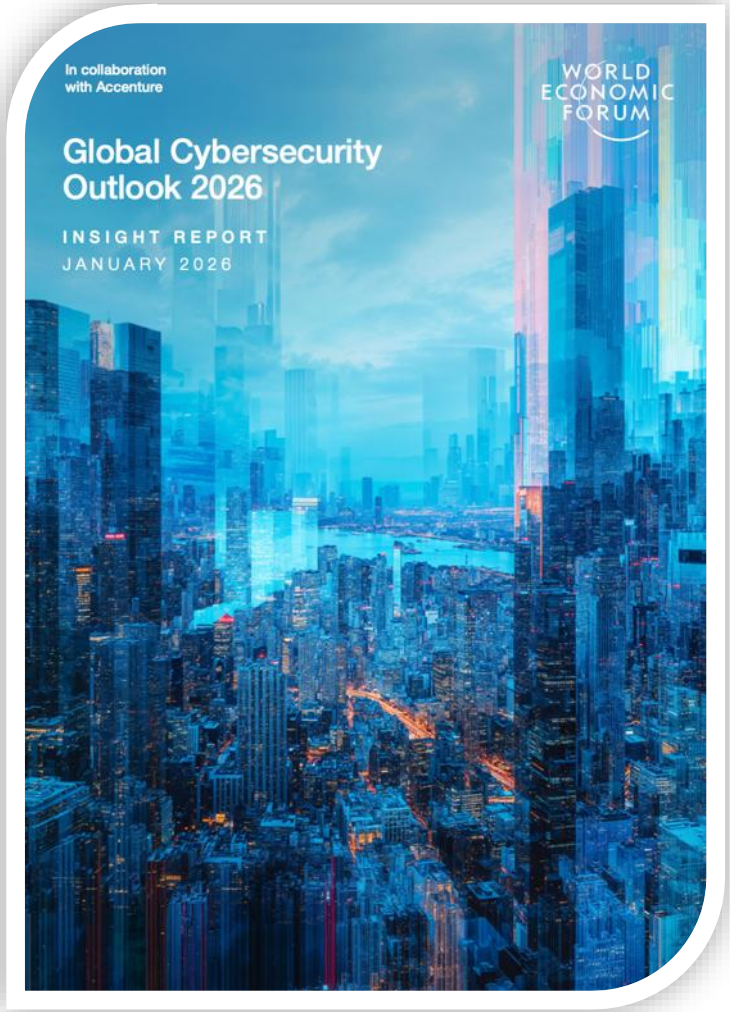
This complexity is driven by a series of compounding factors:

- Escalating geopolitical tensions are contributing to a more uncertain environment.
- Increased integration of and dependence on more complex supply chains is leading to a more opaque and unpredictable risk landscape.
- The rapid adoption of emerging technologies is contributing to new vulnerabilities as cybercriminals harness them effectively to achieve greater sophistication and scale.
- Simultaneously, the proliferation of regulatory requirements around the world is adding a significant compliance burden for organizations.

All of these challenges are exacerbated by a widening skills gap, making it extremely challenging to manage cyber risks effectively.

Materials developed for Board Leadership Society – Center for Cybercompetences.
All rights reserved.

ANALYSER FRA WORLD ECONOMIC FORUM mm.



Bestyrelsesforeningens Center for Cyberkompetencer

Materials developed for Board Leadership Society – Center for Cybercompetences.
All rights reserved.

INDUSTRIENS FOND

ANALYSER FRA WORLD ECONOMIC FORUM mm.

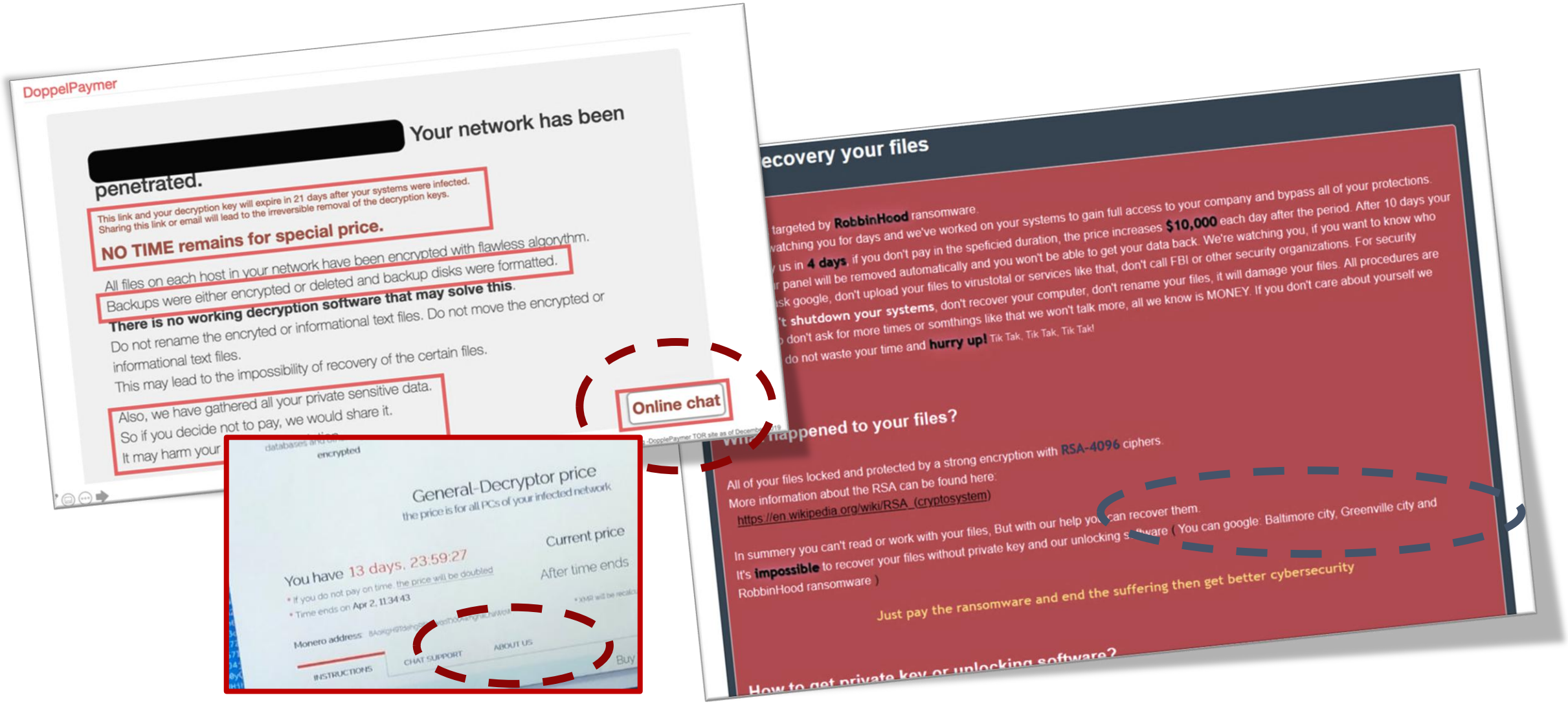
- Cyberkriminalitet koster verden mere end **40.000 mia. kr**., hvilket er mere end USA's statsbudget i indeværende finansår *(og det er tal fra 2021-22)*
- **88% of respondenterne** indikerer, at de er bekymrede for cybersikkerheden i de mindre og mellemstore **virksomheder i deres værdikæder.**
- Cyber ledere anfører, at det vil være godt med **klare og implementerbare reguleringer**, som kan tillade og opfordre til **vidensdeling og samarbejde.**
- Ganske tankevækkende svarer **92 pct.** af de koncernchefer, der er blevet spurgt i forbindelse med tilblivelsen af Global Cyber Security Outlook 2022, at de anser modstandsdygtighed over for cyberangreb for at være **en integreret del af virksomhedens risikostyringsstrategi,** hvorimod kun **55 pct**. af de it-ansvarlige mener, at det er tilfældet.

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

VÆRDISKABELSE og TRUSSELSBILLEDET



Bestyrelsesforeningens
Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2 og DORA mm.)

EU's Cybersecurity Strategy fra 2020

- Cybersikkerhedsstrategien blev fremlagt i december 2020 af EU-Kommissionen og EU-Udenrigstjenesten
- Skitserer rammen for EU's indsats for at beskytte sine borgere og virksomheder mod cybertrusler, fremme sikre informationssystemer og beskytte et globalt, åbent, frit og sikkert cyberspace.
- Målet er at styrke Europas modstandsdygtighed over for cybertrusler og sikre, at alle borgere og virksomheder fuldt ud kan drage fordel af pålidelige tjenester og digitale værktøjer.

NIS2 Directive

DORA Digital Operational Resilience Act

CER

The Artificial Intelligence Act

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2 og DORA)

sikker digital DK

HOTLINE OM SIKKERDIGITAL.DK KONTAKT Indtast søgeord

Borger Virksomhed Myndighed

Sikkerdigital.dk › NIS2 › Forbered dig på NIS2 – læs om de nye krav til cybersikkerhed

Krav til styring af cybersikkerhedsrisici

Hvis din virksomhed eller myndighed er omfattet af NIS2, skal I have en række planer for styring af cybersikkerhedsrisici og cybersikkerhedstiltag på plads, for at beskytte jeres systemer mod cybertrusler.

Virksomheder og myndigheder skal som minimum indføre følgende cybersikkerhedstiltag:

1. politikker for risikoanalyse og informationssystemsikkerhed
2. håndtering af hændelser
3. driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring
4. forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte virksomhed eller myndighed og dens direkte leverandører eller tjenesteudbydere
5. sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder
6. politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici
7. grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse
8. politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering
9. personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver
10. brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.

Når NIS2 bliver implementeret i de nationale bekendtgørelser, bliver det forklaret yderligere, hvordan man i den enkelte sektorer lever op til kravene i NIS2. Det er også muligt, at der inden for den enkelte sektor er behov for yderligere krav til at beskytte enhederne mod cybertrusler.

Krav om registrering og indberetning

Virksomheder og myndigheder, der er omfattet af NIS2, skal registrere sig i et offentligt register og indberette væsentlige hændelser.

Registrering

Du skal registrere din virksomhed eller myndighed via et register, der vil være åbent, når loven træder i kraft 1. juli 2025.

Der er forskel på, hvilke oplysninger du skal indgive og hvornår de skal indgives, det afhænger af typen af virksomhed eller myndighed.

Væsentlige og vigtige enheder samt enheder, der leverer domænenavnsregistreringstjenester, skal oplyse:

1. Enhedens navn
2. Adresse og ajourførte kontaktoplysninger, herunder e-mailadresser, IP-intervaller og telefonnumre
3. Den relevante sektor og delsektor som enheden er omfattet af.
4. Hvis relevant, en liste over de øvrige medlemsstater i Den Europæiske Union, hvor enhed[illegible] anvendelsesområdet i NIS 2-direktivet.

Krav til ledelsen

Lovforslaget stiller krav til, at ledelsen kender til de obligatoriske cybersikkerhedskrav og slår fast, at det er ledelsens ansvar at sikre, at virksomheden eller myndigheden lever op til kravene.

NIS2-lovforslaget stiller følgende cybersikkerhedskrav til ledelsen:

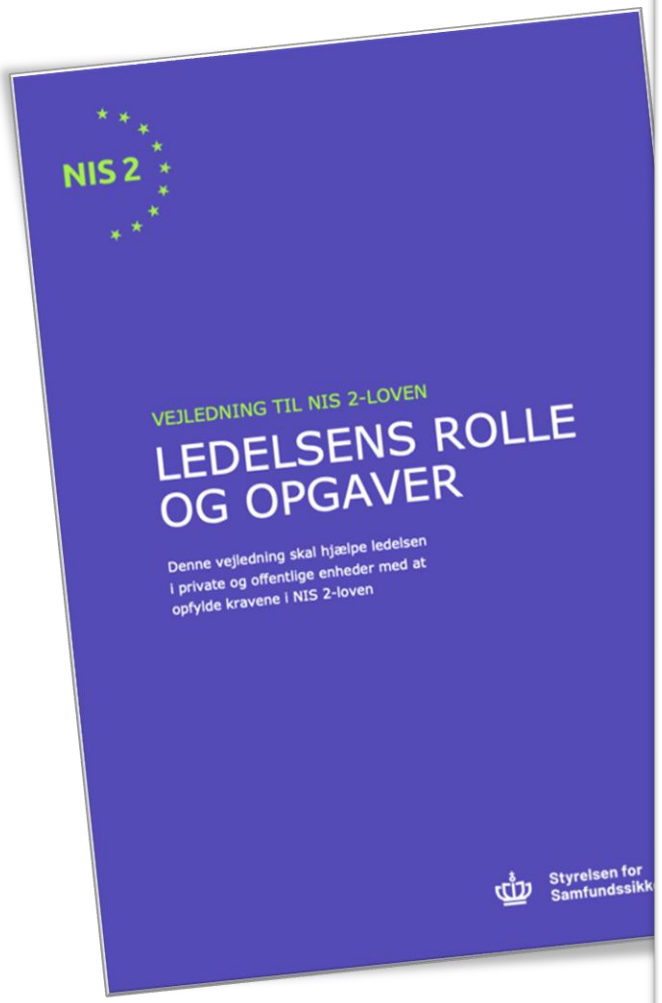
- Ledelsen skal godkende de krav til styring af cybersikkerhedsrisici, som implementeres og skal føre tilsyn med at det gennemføres.
- Ledelsen er forpligtet til at deltage i relevante kurser om styring af cybersikkerhedsrisici, og overveje at tilbyde tilsvarende kurser til sine medarbejdere.

Lovforslaget giver desuden mulighed for, at ledelsen af væsentlige enheder i særligt alvorlige tilfælde kan hjemsendes.

Kilde: sikkerdigital.dk

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2 og DORA)



1. HVORDAN ER LEDELSESBEGREBET DEFINERET

Det siger NIS 2-loven:

§ 3, nr. 20 *Ledelsesorganet:*
a) *For virksomheder omfattet af selskabslover*
i) bestyrelsen i selskaber, der har en direktion
ii) direktionen i selskaber, der alene har en dir
iii) direktionen i selskaber, der både har en dir
tilsynsråd.

b) *For virksomheder omfattet af lov om visse*
virksomheder er ledelsesorganet
i) bestyrelsen i selskaber, der har en direktion
ii) direktionen i selskaber, der alene har en dir
iii) for de selskaber, der hverken har en besty
direktion, det ledelsesorgan, der har en kompe
den almindelige opfattelse af den kompetence,
bestyrelse eller en direktion.

c) *For offentlige myndigheder er ledelsesorgan*
administrative ledelse i myndigheden.

NIS 2-loven stiller krav til "ledelsesorganet" i væsentlige og vigtige enheder. Hvem der udgør ledelsesorganet afhænger af, om der er tale om en privat virksomhed/organisation eller en offentlig myndighed.

I PRIVATE VIRKSOMHEDER/ORGANISATIONER
I private virksomheder/organisationer er ledelsesorganet i NIS 2-loven defineret i overensstemmelse med definitionerne af henholdsvis det "centrale ledelsesorgan" i § 5, nr. 4 i *Lov om aktie- og anpartsselskaber, jf. lovbekendtgørelse nr. 1168 af 1. september 2023* (selskabsloven) og "ledelsen" i § 4 a, nr. 2 i *Lov om visse erhvervsdrivende virksomheder, jf. lovbekendtgørelse nr. 249 af 1. februar 2021* (LEV-loven).

For virksomheder omfattet af selskabsloven er ledelsesorganet:

1. Bestyrelsen i selskaber, der har en direktion og en bestyrelse
2. Direktionen i selskaber, der alene har en direktion
3. Direktionen i selskaber, der både har en direktion og et tilsynsråd

NIS 2-VEJLEDNING

4. HVORDAN SKAL LEDELSEN FØRE TILSYN MED CYBERSIKKERHEDEN?

Ledelsesorganet i enheden skal føre tilsyn med, at de godkendte cybersikkerheds-foranstaltninger gennemføres og sikre, at foranstaltningerne har den fornødne effekt ift. de identificerede risici. Ledelsen skal derfor følge op på og føre kontrol med, at de sikkerhedstiltag, ledelsen har iværksat, realiseres og har den ønskede virkning.

Tilsynet kan ske på forskellige måder, eksempelvis gennem periodiske ledelsesrapporter, hvor ledelsesorganet får status på de strategiske målsætninger, handleplaner samt udvalgte nøgletal og kontrolmål for enhedens arbejde med cyber- og informationssikkerhed. Ledelses-organet kan også føre tilsyn ved at etablere processer for intern revision, som rapporterer til ledelsen eller ved gennemførelse af ekstern revision af NIS 2-kravene, som rapporterer deres resultater til ledelsen.

NIS 2-VEJLEDNING

ANDRE RELEVANTE MATERIALER

Nedenfor fremgår en række vejlednings- og kommunikationsmaterialer, som kan være relevante i forhold til ledelsens rolle og opgaver. Materialet er til inspiration og er ikke udviklet med henblik på at opfylde specifikke lovkrav.

Sikkerdigital.dk
På sikkerdigital.dk kan virksomheder og myndigheder finde viden, vejledning og konkrete værktøjer til deres arbejde med cyber- og informationssikkerhed.

Bestyrelsesforeningen
Bestyrelsesforeningens Center for Cyberkompetencer har udarbejdet vejledning, anbefalinger og uddannelsestilbud målrettet bestyrelser og direktioners strategiske arbejde med cybersikkerhed.

Kilde: cfcs.dk

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2, CER, DORA mm)

Ledelsens opgaver og ansvar *(– den meget kondenserede og ikke juridiske udgave…)*

Et tværsnit over forskellige lovgivninger mm. fastlægger og udtrykker, at det er ledelsens – dvs. bestyrelsen og direktionens opgave at:

- Være endeligt ansvarlig for risikostyring og herunder at fastlægge og godkende en **strategi for digital modstandsdygtighed** og ligeledes fastlægge virksomhedens **risikoprofil/appetit**
- Tildele og regelmæssigt gennemgå at der findes et **passende budget** for den digitale modstandsdygtighed
- Løbende følge **kurser** indenfor cybersikkerhed
- Sikre en god governancestruktur med **klare roller og ansvar** – og ligeledes sikre høje standarder for virksomhedens håndtering af data
- Forholde sig til, godkende og føre tilsyn med at der er forsvarlige **business continuity planer**
- Sikre og løbende føre tilsyn med relevante politikker for bl.a. **outsourcing/tredjepartsprodukter**
- Sikre at der er et overblik over risikoeksponeringer – samt **sikre løbende dokumentation.**

Kilde: efter inspiration fra Kromannreumert.dk

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

BESTYRELSENS OPGAVER og ANSVAR … og REALITET

Det vi godt ved…

Værdiskabelse … på alle planer og i forhold til alle bundlinjer - rimer i dag på digitalisering. Jo mere digitale virksomheders produkter og infrastruktur er, jo mere **sårbare er vi over for cyberangreb.**

I kernen af enhver forretningsmæssig beslutning er **styring og afvejning af risici.**

Cyberangreb er blandt de største forretningsrisici, virksomheder står overfor, og koster danske virksomheder på **bundlinje, kundeforhold og renommé.**

… og det handler ikke kun om IT – men også om **processer, ledelse, governance og ikke mindst mennesker…**

Det er vigtigt **at stille skarpt** på **digital modstandsdygtighed** også på **ledelsesgangene** og i **bestyrelseslokalet**

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

VÆRDISKABELSE og TRUSSELSBILLEDET

Det tager virkelig lang tid…

Det er utrolig dyrt…

En del af kerneopgaven ift. virksomhedsledelse i 2025+

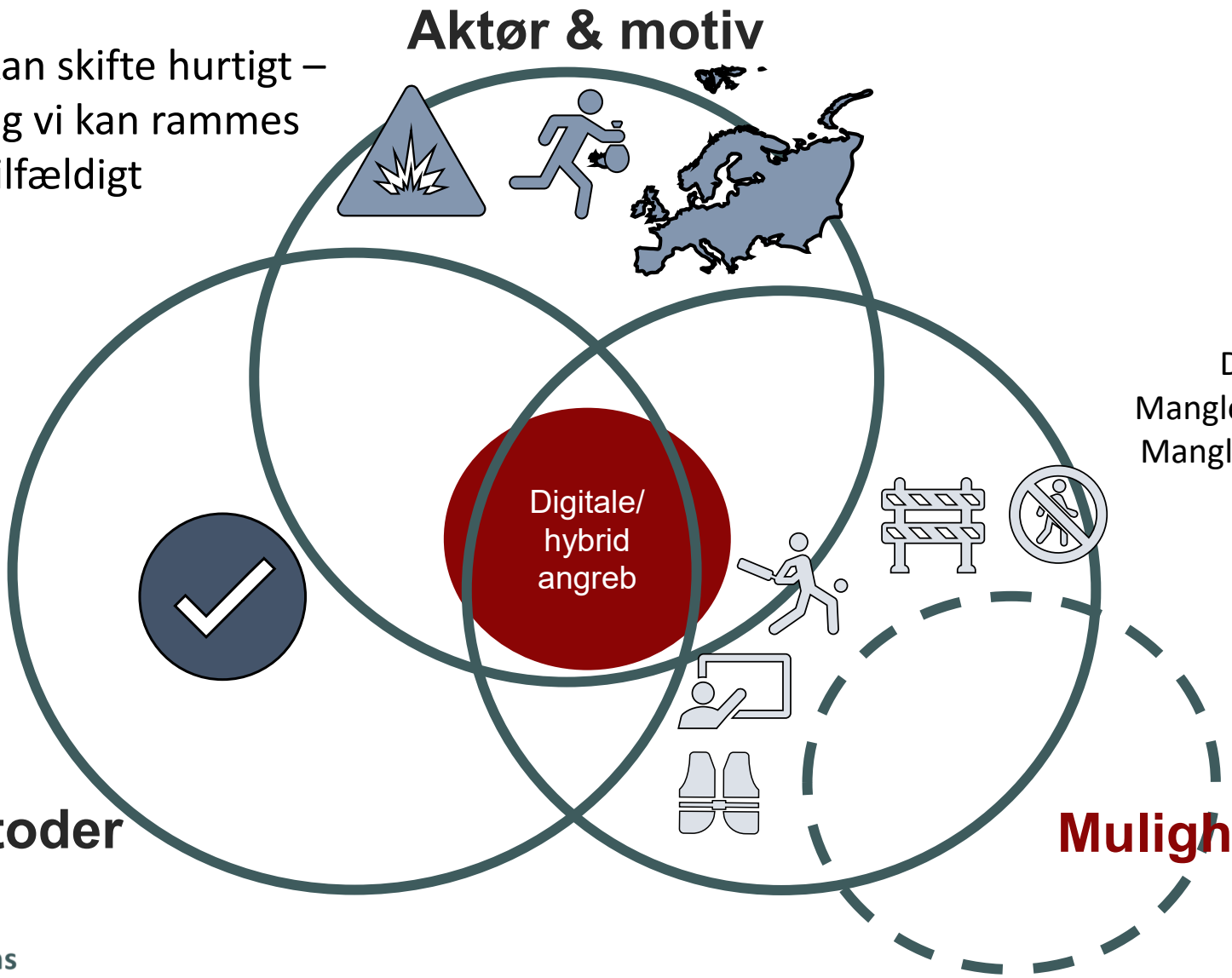
Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

VÆRDISKABELSE og TRUSSELSBILLEDET

Kan skifte hurtigt – og vi kan rammes tilfældigt



Desværre har de rigtig mange evner og metoder…

Dårlig systemssikkerhed
Manglende system adskillelse
Manglende fokus på adgange
Manglende træning
uopmærksomhed
Leverandører
Insidere
Osv osv …

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

LEDELSENS OPGAVER og ANSVAR … og NY LOVGIVNING (NIS2, CER, DORA mm)

DANSKE LOVE

Forside › Selskabsloven › § 115

Selskabsloven § 115

§ 115 I kapitalselskaber, der har en bestyrelse, skal denne ud over at varetage den overordnede og strategiske ledelse og sikre en forsvarlig organisation af kapitalselskabets virksomhed påse, at

1) bogføringen og regnskabsaflæggelsen foregår på en måde, der efter kapitalselskabets forhold er tilfredsstillende,
2) der er etableret de fornødne procedurer for risikostyring og interne kontroller,
3) bestyrelsen løbende modtager den fornødne rapportering om kapitalselskabets finansielle forhold,
4) direktionen udøver sit hverv på en behørig måde og efter bestyrelsens retningslinjer og
5) kapitalselskabets kapitalberedskab til enhver tid er forsvarligt, herunder at der er tilstrækkelig [illegible] kapitalselskabets nuværende og fremtidige forpligtelser, efterhånden som de [illegible] til at vurdere den økonomiske situation og

NIS2 Directive

Ledelsens opgaver og ansvar (– den meget kondenserede og ikke juridiske udgave…)

Et tværsnit over forskellige lovgivninger mm. fastlægger og udtrykker, at det er ledelsens – dvs. bestyrelsen og direktionens opgave at:

- Være endeligt ansvarlig for risikostyring og herunder at fastlægge og godkende en **strategi for digital modstandsdygtighed** og ligeledes fastlægge virksomhedens **risikoprofil/appetit**
- Tildele og regelmæssigt gennemgå at der findes et passende budget for den digitale modstandsdygtighed
- Løbende følge **kurser** indenfor cybersikkerhed
- Sikre en god governancestruktur med **klare roller og ansvar** – og ligeledes sikre høje standarder for virksomhedens håndtering af data
- Forholde sig til, godkende og føre tilsyn med at der er forsvarlige **business continuity planer**
- Sikre og løbende føre tilsyn med relevante politikker for bl.a. **outsourcing/tredjepartsprodukter**
- Sikre at der er et overblik over risikoeksponeringer – samt **sikre løbende dokumentation**

Kilde: efter inspiration fra Kromannreumert.dk

Bestyrelsesforeningens

1. Risikovurdering
- værdier og trusler

Det anbefales, at
- bestyrelsen mindst to gange om året modtager og forholder sig til en opdateret risikovurdering på cyberområdet baseret på virksomhedens vigtigste værdier, it-infrastruktur, forretningsmodel, primære sårbarheder, indsynlige trusler, mulige tab ved angreb samt mulige konkurrencemæssige vurderinger.

2. Risikoappetit
- risikoafvejning og risikovillighed

Det anbefales, at
- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter virksomhedens cybersikkerhedsstrategi, herunder risikoappetit, baseret på en afvejning af virksomhedens generelle forretningsstrategi, forretningsmål, it-infrastruktur, generelle risikoappetit, sikkerhedsbudget og investeringsvilje m.v.

3. Politikker, processer og beredskab
- delegering og operationalisering

Det anbefales, at
- bestyrelsen fører kontrol med, at cybersikkerhedsstrategien er operationaliseret i politikker, processer og forretningsgange.
- bestyrelsen fører kontrol med, at virksomheden har implementeret passende cyberhygiejne, herunder en relevant backup, der løbende er testet,
- bestyrelsen fører kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner i tilfælde af alt fra hackerangreb til strømnedbrud.

4. Rapportering
- kontrol og tilsyn

Det anbefales, at
- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul og, på linje med øvrige væsentlige risici,
- bestyrelsen har cybersikkerhed på agendaen på hvert møde, og modtager relevant rapportering forud for mødet med bl.a. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest, awareness aktiviteter og revisionsgennemgange, samt evt. forslag til supplerende tiltag.

5. Kultur
- mennesker og træning

Det anbefales, at
- medlemmer af bestyrelse og direktion regelmæssigt følger specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift,
- virksomheden regelmæssigt har tilpassede uddannelses- og træningsprogrammer for bestyrelse, direktion og medarbejdere i relation til cybersikkerhed,
- bestyrelsen og daglig ledelse går forrest i at understøtte en stærk og bevidst cybersikkerhedskultur.

6. Governance
- kompetencer og organisering

Det anbefales, at
- bestyrelsen forholder sig til, om den har tilstrækkelige kompetencer og erfaring med risikostyring af it- og cyberrisici,
- virksomhedens sikkerhedsorganisation fagligt er direkte forankret på direktionsniveau, og rapporterer direkte til bestyrelsen,
- styrke virksomhedens cybersikkerhed gennem etablering af uafhængige risikostyringskontroller (lines of defence).

31

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS ARBEJDE MED CYBERSIKKERHED

- Det har vi outsourcet…
- Vi er ikke IT-specialister…
- Det har IT-Morten styr på…
- Vi har en forsikring…
- Det har vi i cloudløsninger

… Så hvad er de bedste råd, jeg kan give til andre bestyrelser

Jacob Dahl / Best.medl. Danske Bank

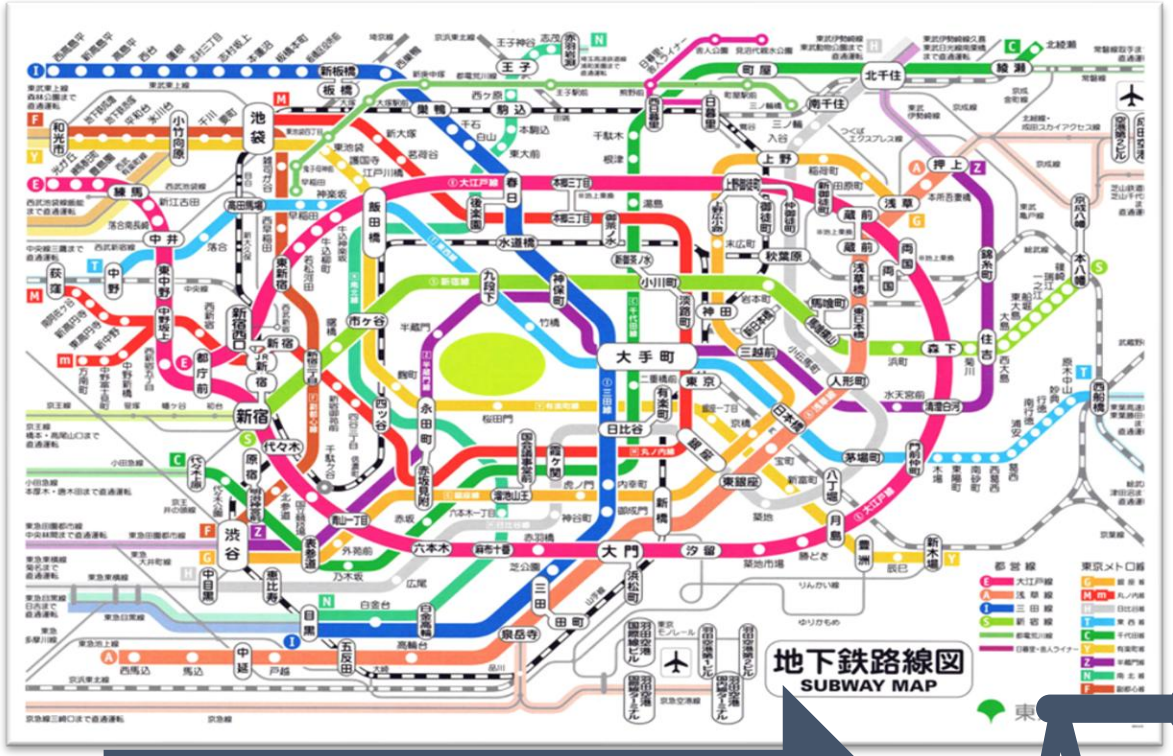
1. Få nogle gode tech/IT profiler ind i bestyrelsen
2. …Men gør der til bestyrelsens **fælles** ansvar og integreret med overordnet strategi
3. Invester meget i uddannelse/opdatering af bestyrelsen – vær åben for mange eksterne perspektiver
4. Vi er på ukendt territorie – tillad direktionen at eksperimentere og fejle
5. Få dyb indsigt i tech/IT organisationen, mød niveau 1, 2 og 3 samt vigtigste outsourcing partnere
6. Sikre tæt samspil mellem forretningen, tech/IT og HR
7. Få fornemmelse for hvilke tekniske features er vigtigst for kunden (inviter dem ind) – og på hvilke måder vi kan differentiere os (vælg få!)
8. Tech mulighederne åbner op for en masse nye risici – forstå dem og integrer dem i risiko komiteens arbejde

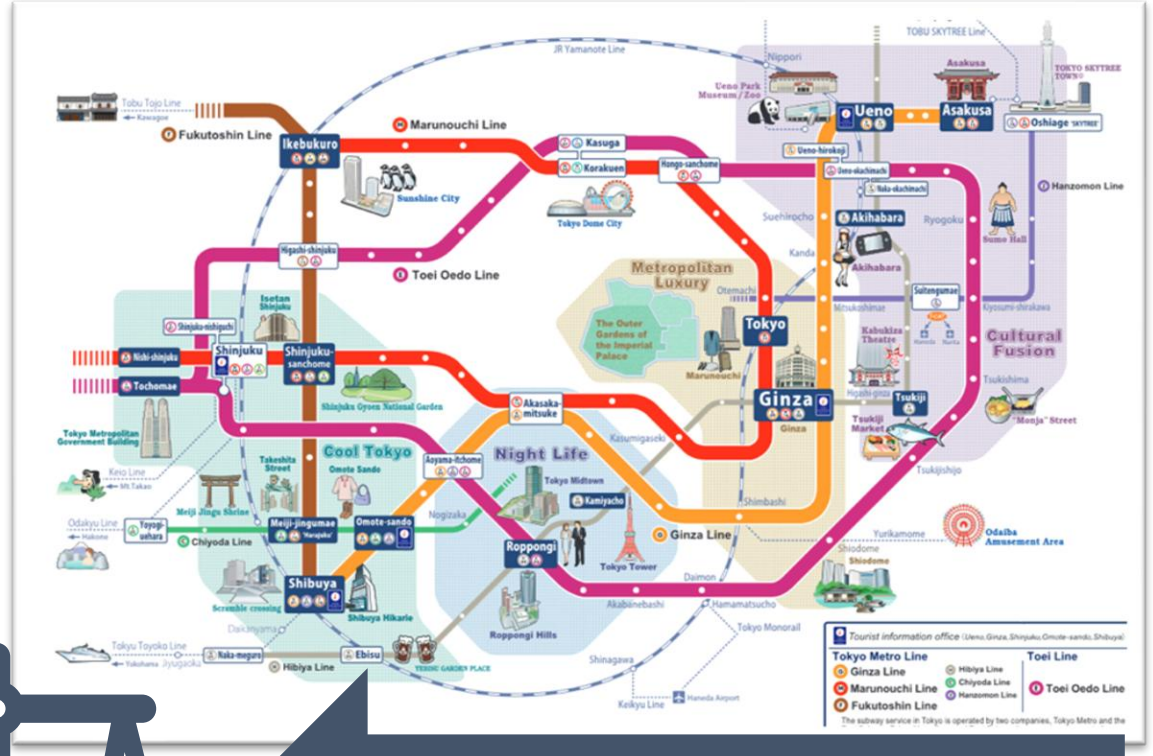
Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS ARBEJDE MED CYBERSIKKERHED





Tal det rigtige sprog…

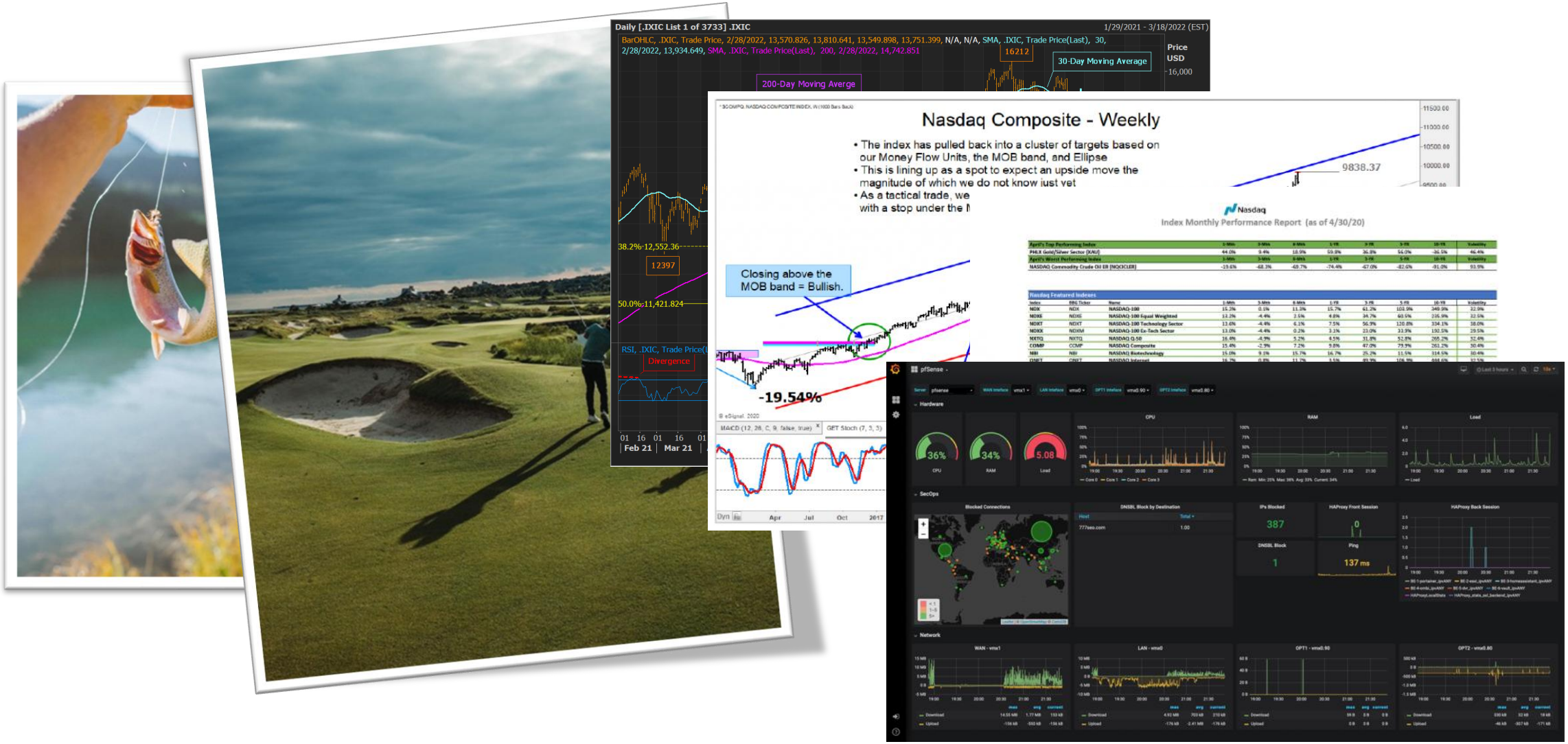
…læn jer ind i begreberne

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS ARBEJDE MED CYBERSIKKERHED



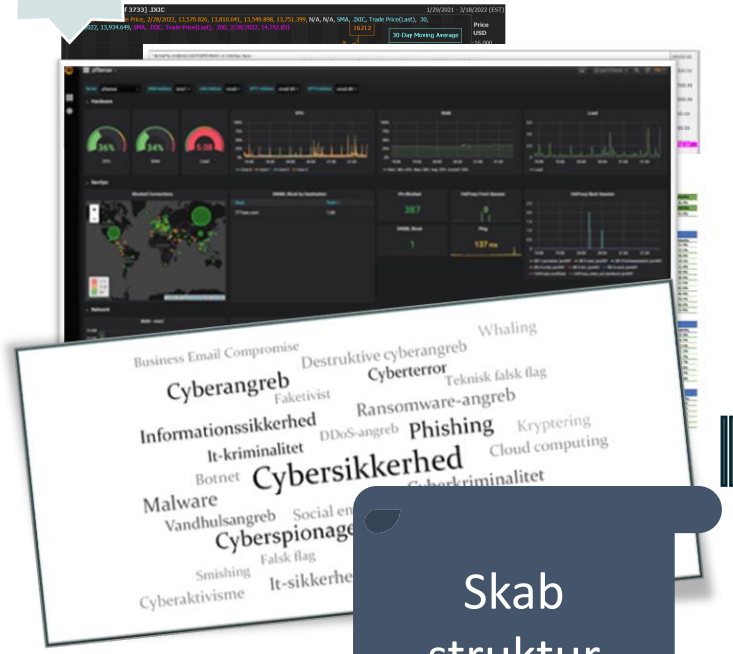
Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS ARBEJDE MED CYBERSIKKERHED

1

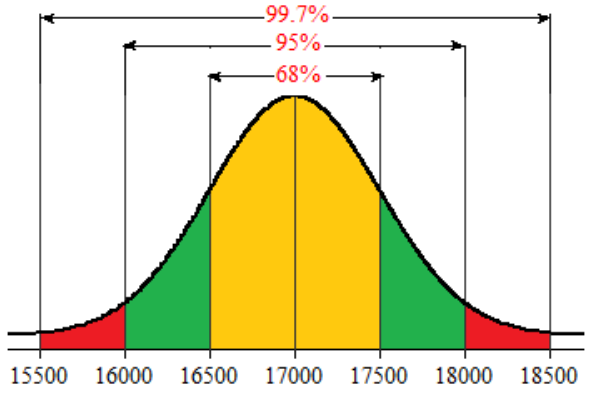


Skab struktur - og vær konkret!

2

- Landeeksponeringer
- Industri / Sektor
- Selskabsstørrelser
- Aktuel risikostatus
- Myndighedskrav
- Interne hændelser
- Eksterne hændelser
- Projekt status
- System status
- Træning og beredskab

3



Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

LEDELSENS ARBEJDE MED CYBERSIKKERHED

Bestyrelsens (LEDELSENS) opgaver:

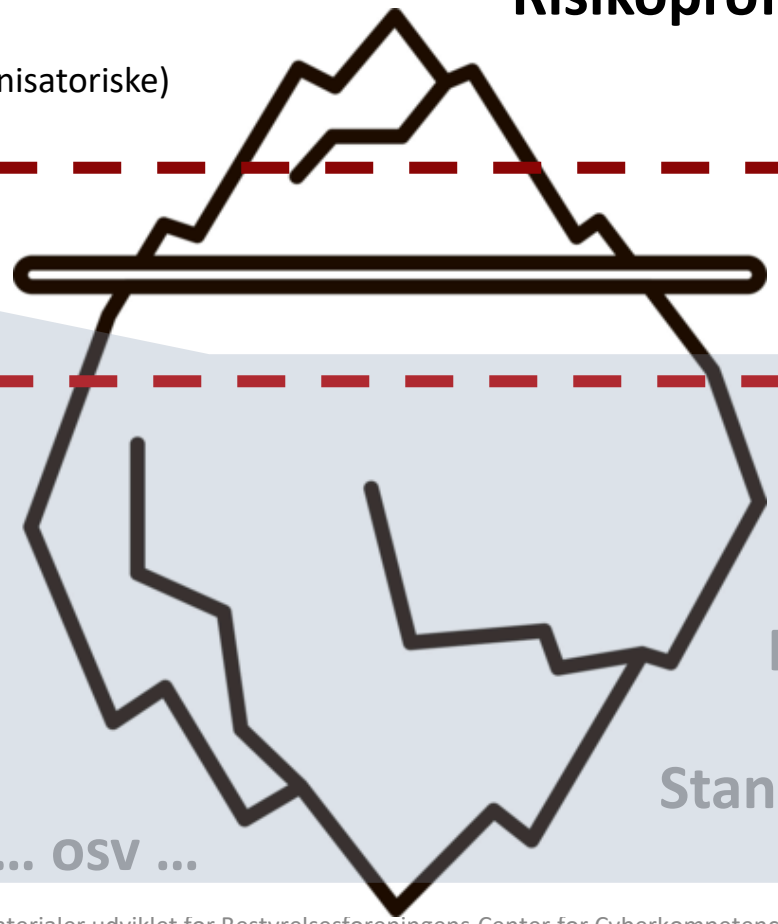
Digital- / cybersikkerhed Strategi

Risikovurdering

Risikoprofil / - tolerance /-appetit

Foranstaltninger
(operationelle/tekniske/organisatoriske)

Rapportering



Bestyrelses-involvering fastlægges individuelt i virksomhederne

Implementering

Leverandører

Træning

Outsourcing

osv... osv ...

Drift

Tests

Forretningsgange

Back-ups

Standarder mm.

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

Anbefaling 1. Risikovurdering
- metodevalg og identifikation

Det anbefales, at:

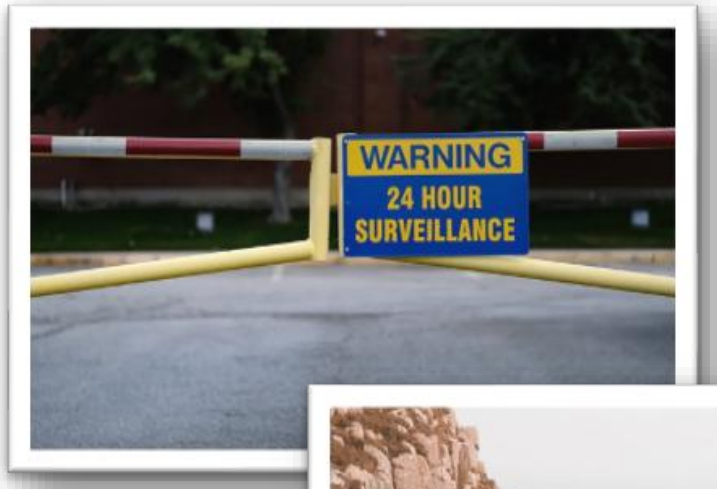
- Bestyrelsen så ofte som relevant og mindst én gang om året **modtager og forholder sig til en opdateret og konsolideret risikovurdering**, der beskriver i hvilket omfang virksomhedens kerneopgaver er eksponeret for digitale risici.
- Bestyrelsen **godkender en risikostyringspolitik**, der identificerer virksomhedens **kerneopgaver** og angiver metode til risikostyring, herunder væsentlighedskriterier, governance og rapportering.

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

Anbefaling 2. Risikoprofil
- appetit og tolerance

Det anbefales, at:

- Bestyrelsen så ofte som relevant og mindst én gang om året forholder sig til den **ønskede risikoprofil** på det digitale område, og udtrykker denne gennem **risikoappetit og evt. tolerancetærskler**, der indgår som del af eller henviser til den generelle risikostyringspolitik.
- Bestyrelsen så ofte som relevant og mindst én gang om året forholder sig til **den faktiske risikoprofil** (risikovurderingen) i forhold til den ønskede risikoprofil.



Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

Anbefaling 3. Foranstaltninger
- risikostyringsramme og implementering

Det anbefales, at:

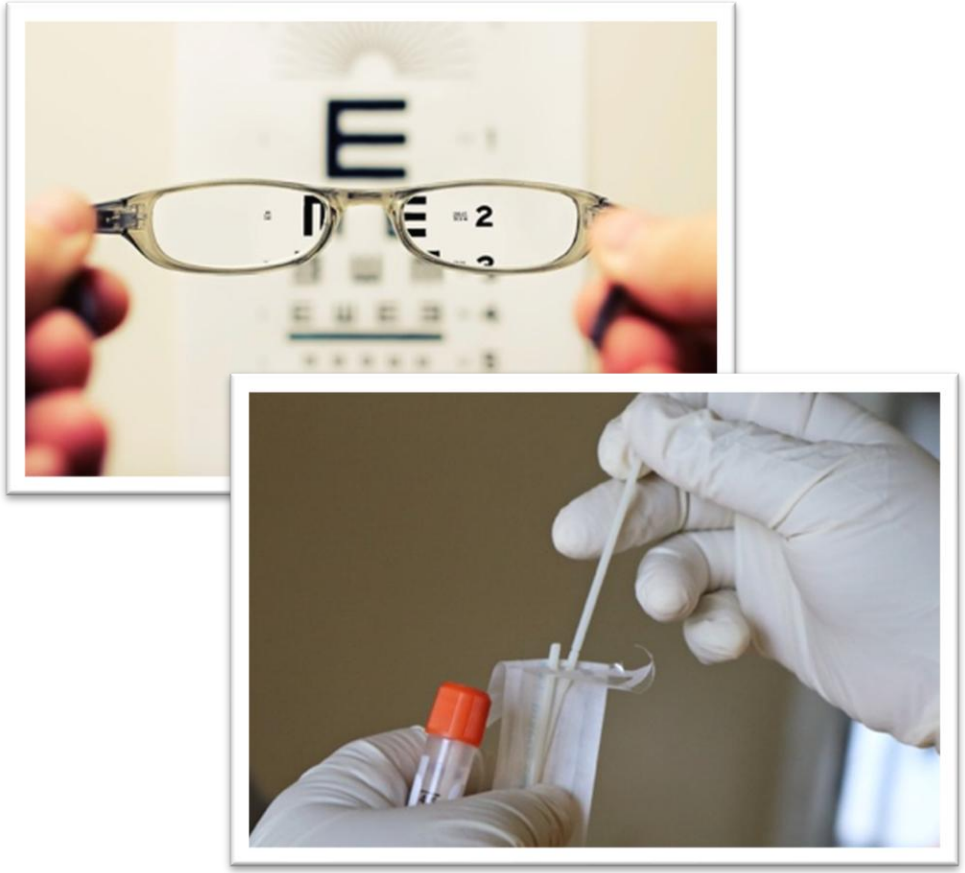
- Bestyrelsen fastlægger **styringsrammen** for digital modstandsdygtighed og godkender politikker, der som minimum dækker (digital) risikostyring, cyber- og informationssikkerhed, beredskab og leverandørsikkerhed.
- Bestyrelsen følger løbende op på **politikkernes** gennemførelse gennem tydelige parametre eller indikatorer.
- Bestyrelsen fører **løbende tilsyn med virksomhedens faktiske modenhed** og sikkerhedsniveau, dvs. foranstaltningernes effektivitet i praksis.
- Bestyrelsen følger løbende op på virksomhedens **forbedringstiltag og -planer**.

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

Anbefaling 4. Rapportering
- Dokumentation og tilsyn

Det anbefales, at

- Bestyrelsen har digital modstandsdygtighed som en **fast del af sit årshjul** og at digitale risici behandles på linje med øvrige **væsentlige risici.**
- Bestyrelsen har digital modstandsdygtighed på agendaen på hvert møde, og **modtager relevant rapportering** forud herfor.
- Bestyrelsen regelmæssigt fastlægger **de indikatorer og elementer**, som den skal/vil føre tilsyn med, og som skal indgå i rapporteringen.
- Rapporteringen omfatter som minimum en konsolideret **risikovurdering**, status på implementering af politikker og sikkerhedstiltag, resultater fra **test, træning og audits,** eventuelle hændelser, samt forslag til supplerende tiltag.



Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

LEDELSENS ARBEJDE MED CYBERSIKKERHED

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

Anbefaling 5. Mennesker
- kultur og kompetencer

Det anbefales, at

- **Bestyrelse og direktion går forrest** i at understøtte en stærk og bevidst sikkerhedskultur.
- Ledelsen sikrer, at sikkerhedsarbejdet tilgås som en **tværorganisatorisk opgave**.
- Bestyrelsen forholder sig til, om den selv har **tilstrækkelige kompetencer** og erfaring med styring af digitale risici.
- Virksomheden har **tilpassede uddannelses- og træningsprogrammer** for bestyrelse, direktion og medarbejdere i relation til digital modstandsdygtighed, cybersikkerhed og beredskab.

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

Anbefaling 6. Governance
- ansvar og organisering

Det anbefales, at

- Bestyrelsen forholder sig til og godkender virksomhedens **governancemodel** og organisering ift. digital resiliens, herunder **roller, ansvar, mandater, kapacitet og budget** på tværs af organisationen.
- Virksomhedens digitale risikostyring og sikkerhedsansvar er fagligt forankret på direktionsniveau, og at der sikres en samlet rapportering direkte til bestyrelsen.
- Virksomheden styrker digital resiliens gennem etablering af understøttende KPIs og **uafhængige risikostyringskontroller** (lines of defence).
- Der etableres relevante **tværorganisatoriske fora** til understøttelse af virksomhedens strategi for digital modstandsdygtighed.

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

CYBERSIKKERHED FOR BESTYRELSER – VEJLEDNING sep. 2023 (ny kommer jan. 2026)

…i GOD tro
… på OPLYST grundlag
… forretningsmæssigt FORSVARLIGT
… og altid i SELSKABETS interesse

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

UDDANNELSESDAGE TIL BESTYRELSE og DIREKTION – se mere på bcfc.dk

Hvad får I?

- Skræddersyet indhold til jeres branche og virksomhedens behov
- Cyberrisikosimuleringer og praktiske øvelser, hvor I træner beredskab og beslutningstagning
- Indsigt i branchens trusler, sårbarheder og regulatoriske krav
- Konkrete værktøjer til at styrke virksomhedens cybermodstandsdygtighed
- Mulighed for erfaringsudveksling og netværk med andre ledere i samme sektor

Hvem er det for?

- Bestyrelsesmedlemmer og direktører, der ønsker praktisk og strategisk indsigt i cybersikkerhed
- Virksomheder, der skal leve op til krav fra fx NIS2 eller anden relevant lovgivning
- Organisationer, som vil styrke deres beredskab og governance i forhold til cybertrusler

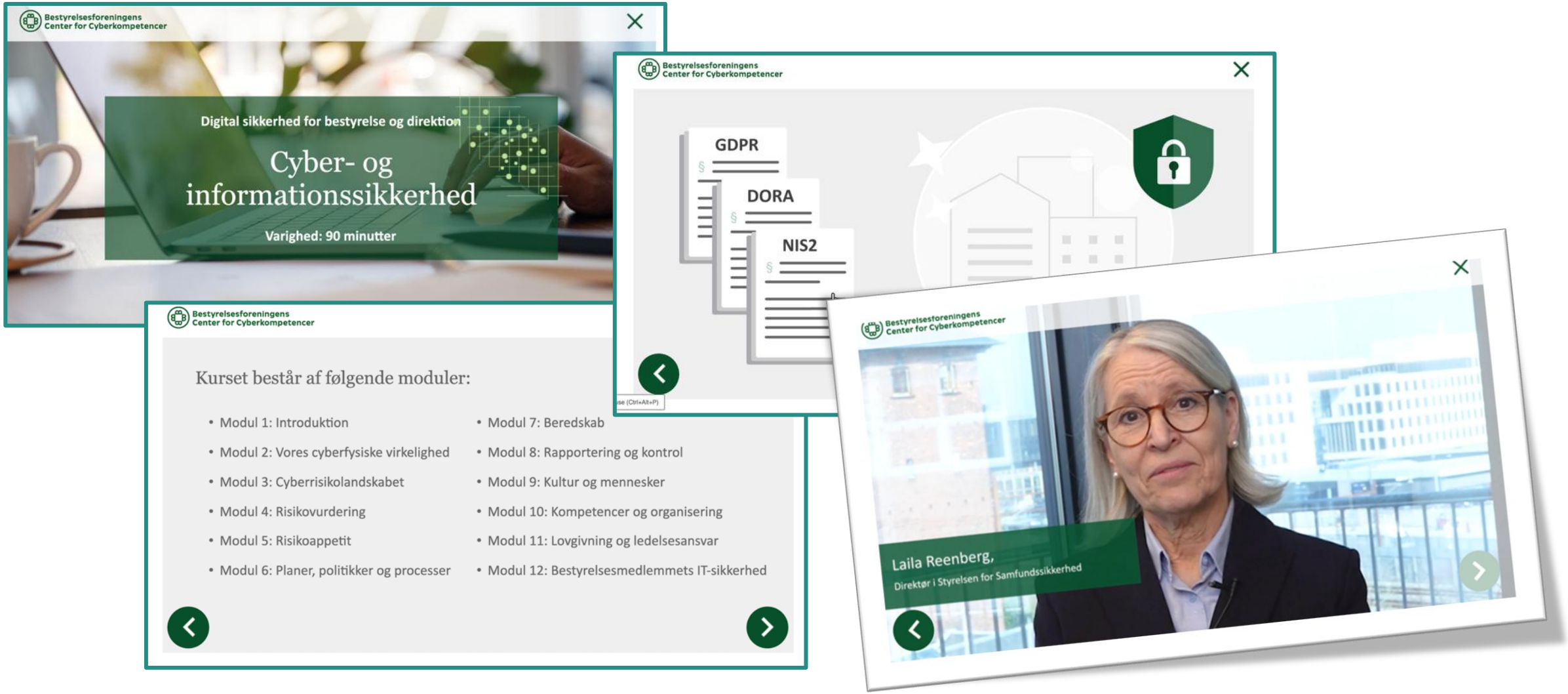
Hvis en branchespecifik uddannelsesmodel lyder som en attraktiv løsning for jer, er I velkomne til at kontakte os på cybersikkerhed@bcfc.dk.

Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

E-LEARNING TIL BESTYRELSE og DIREKTION



Bestyrelsesforeningens Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

… og LEDELSENS KOMPAS – er som altid :

Bestyrelsesforeningens
Center for Cyberkompetencer

Materialer udviklet for Bestyrelsesforeningens Center for Cyberkompetencer.
Alle rettigheder forbeholdes.

INDUSTRIENS FOND

TAK FOR I DAG

Evaluér dagens arrangement her, så vi løbende kan blive bedre.

CON
TECH
LAB_