CYBERSIKKERHED FOR BESTYRELSER
Styrkelse af Cyberkompetencer

Konference i samarbejde med

Dansk Standard, **Dansk Erhverv, DI Digital og IT-Branchen**

7. Juni 2021

Kirsten Hede

Bestyrelsesforeningens Center for Cyberkompetencer

Bestyrelsesforeningens
Center for Cyberkompetencer

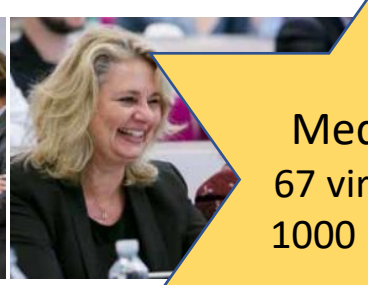
INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

BESTYRELSESFORENINGEN – DEN KORTE VERSION

...







Medlemmer:
67 virksomheder
1000 individuelle

Velliv · Forsikring & Pension · BØRSEN. · SimCorp · netcompany · DFDS · Realdania · MÆRSK
novozymes · MORGENAVISEN Jyllands-Posten · Chr. Augustinus Fabrikker · Carlsberg · Nykredit · Nasdaq
Danfoss · BITTEN & MADS CLAUSENS FOND · KPMG · GRUNDFOS · PFA Mere til dig · Danske Bank
Nordea · ROCKWOOL · ERHVERVSSTYRELSEN · Toms · ASNETBoard · pka · CBS EXECUTIVE · SpencerStuart · Carnegie
GN · HALDOR TOPSOE · pwc · DSV
AXCEL · DANSKE REVISORER FSR · Deloitte. · TDC Group · FINANS DANMARK · PANDORA · KRAKS FOND
VKR · DSB · skanderborg forsyning a/s · FREDERIKSBERG BOLIGFOND · LD Fonde
MAJ INVEST · DANSKE REGIONER · Coloplast · jeudan · coop · atp= · RAMBØLL FONDEN
JYSKE BANK · ODGERS BERNDTSON · KL · EgonZehnder · COWI · Ørsted
KROMANN REUMERT · PensionDanmark · EY · DANSK ERHVERV · CBS COPENHAGEN BUSINESS SCHOOL · >E AKTIVE EJERE

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

BESTYRELSESFORENINGEN EST. 2013

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

Projekt Styrkelse af Strategiske Cyberkompetencer - 2019-23

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

- ✓ Beskytte **virksomhedens forretning**
- ✓ Skabe **vækst i en digital tid og** udnytte **den digitale transformation**
- ✓ Leve op **til sit bestyrelsesansvar**

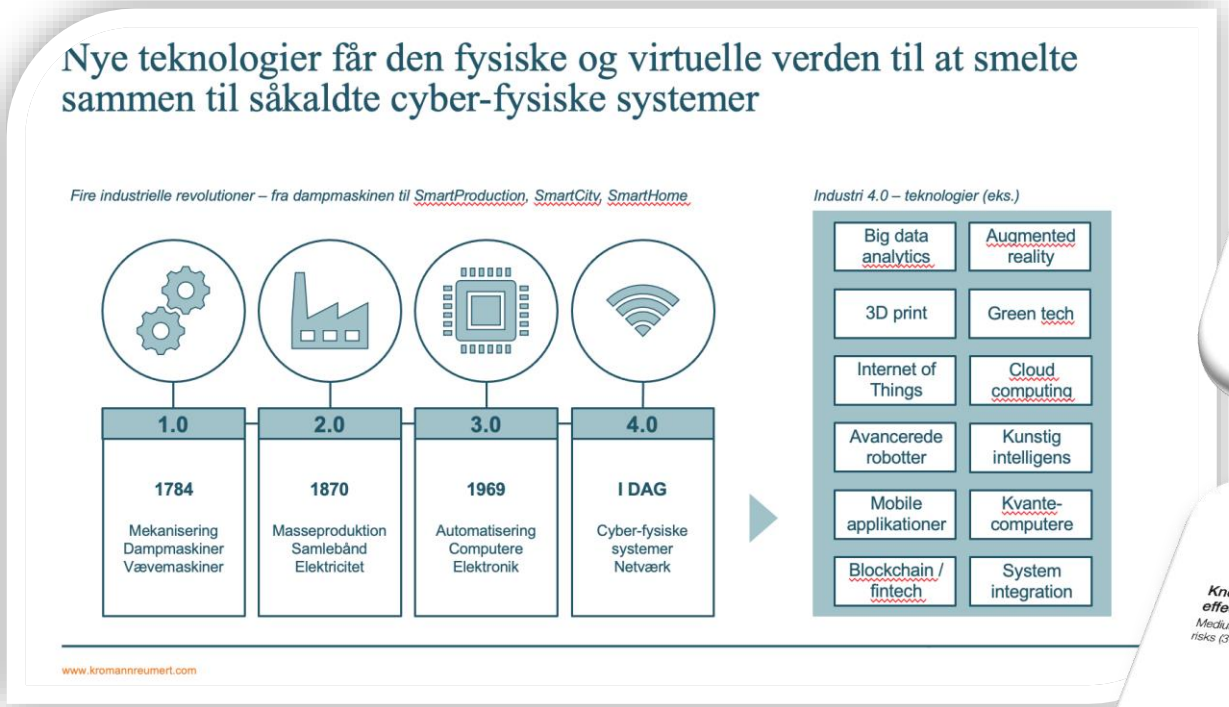
Bestyrelsesforeningens
Center for Cyberkompetencer

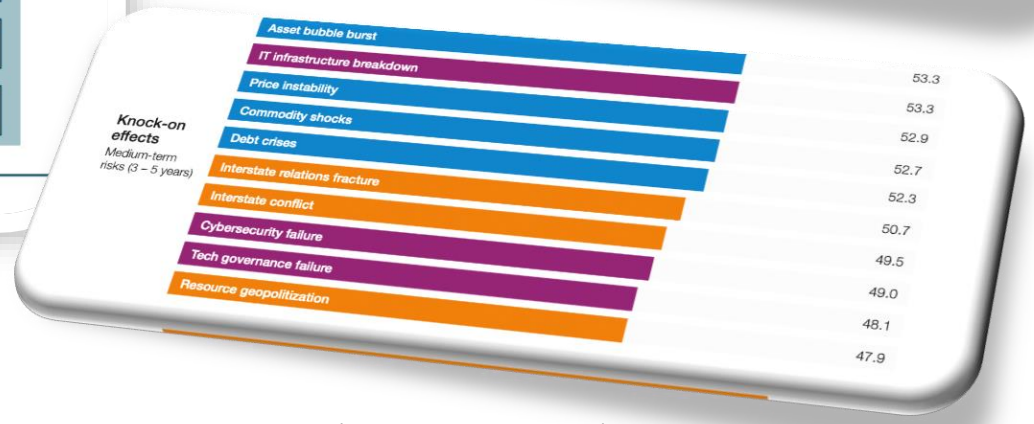
Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

CYBERSIKKERHED og VIRKSOMHEDERS VÆRDISKABELSE

…





World Economic Forum (Global Risk Report 2021)

BESTYRELSENS VIRKELIGHED … RISIKO og KONKURRENCEFORDEL

…

Det vi godt ved…

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

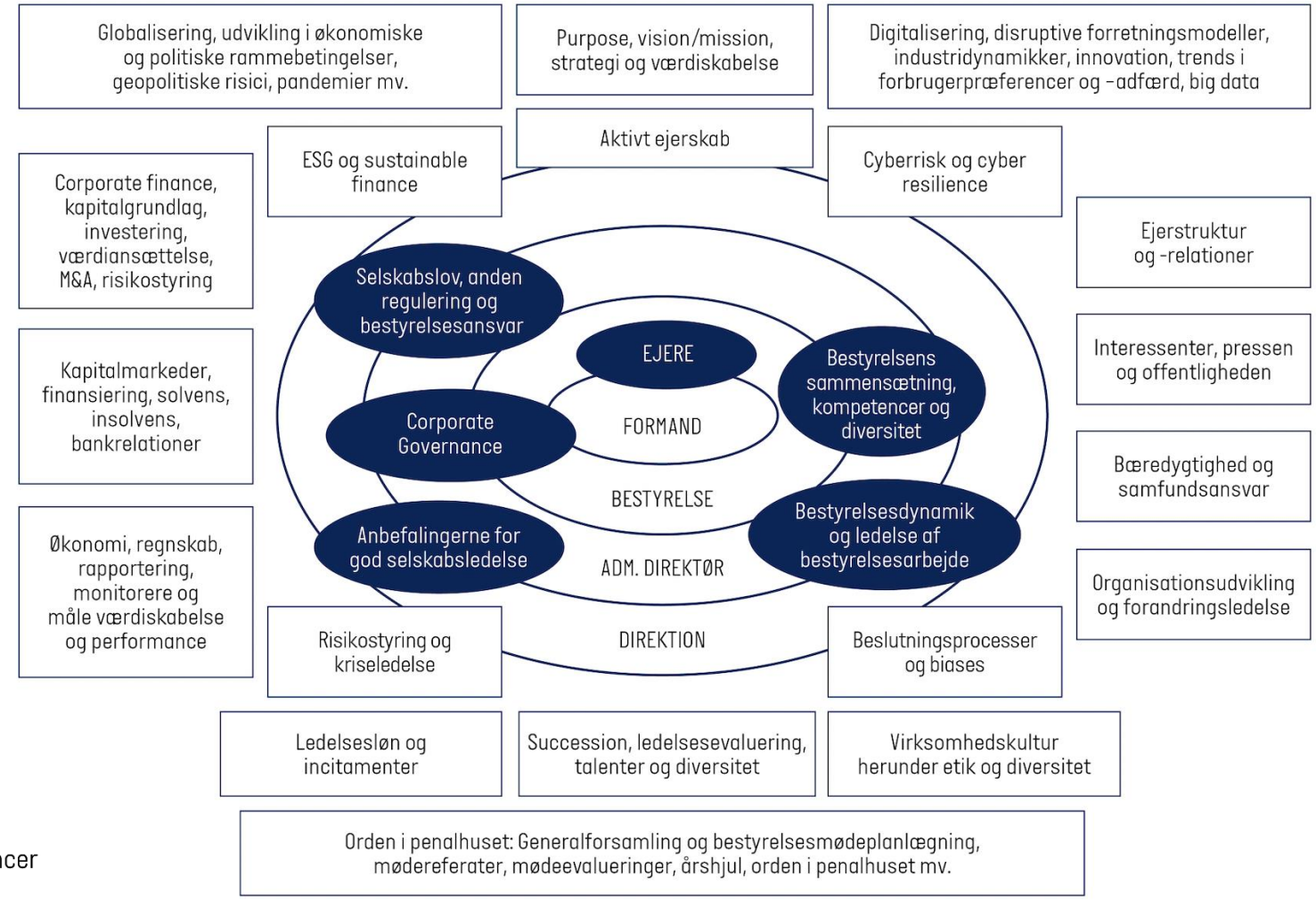
Værdiskabelse rimer i dag på digitalisering – og jo mere digitale virksomheders produkter og infrastruktur er, jo mere **sårbare er de over for cyberangreb.**

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

Det er derfor vigtigt **at stille skarpt** på cyber- og informationssikkerhed **i bestyrelseslokalet**.

BESTYRELSENS OPGAVER og ANSVAR…

360° OM BESTYRELSENS OPGAVER, PROBLEMSTILLINGER & RELATIONER



BESTYRELSENS OPGAVER og ANSVAR… og REALITET

Strategisk niveau + operationelt niveau i tæt samarbejde…

Bestyrelsesforeningens Center for Cyberkompete

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

TEMAER i en CYBERSTRATEGI

Virksomheders arbejde med cyber- og informationssikkerhed **handler om mere end IT.**

Det handler i høj grad også om **governance, ledelse, processer og mennesker.**

Sikkerhed er i sidste ende **bestyrelsens ansvar**, og bør være et vigtigt emne på bestyrelsens dagsorden.

Cybertruslen er reel, og virksomheder er nødt til at have en strategi for at håndtere den.

Bestyrelsens

UDFORDINGER – og løsninger

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND
FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

CYBERSIKKERHED FOR BESTYRELSER - VEJLEDNING

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND
The Danish Industry Foundation

CYBERSTRATEGI i OVERSKRIFTER

Risikovurdering og sårbarheder

Risikoappetit og strategi

Planer, processer og beredskab

Rapportering og kontrol

Kultur og mennesker

Kompetencer og organisering

ANBEFALINGER TIL BESTYRELSEN

1. Risikovurdering og sårbarheder

Det anbefales, at:

bestyrelsen mindst to gange om året **modtager og forholder sig til en opdateret risikovurdering** på cyberområdet

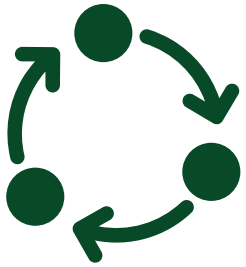
… baseret på virksomhedens vigtigste **værdier**, **teknologilandskab**, primære **sårbarheder**, sandsynlige **trusler**, **mulige tab** ved angreb og anbefaling til (yderligere) **investering**.

2. Risikoappetit og strategi

Det anbefales, at:

bestyrelsen **så ofte som relevant** og mindst én gang om året fastsætter virksomhedens **risikoappetit** indenfor cyber- og informationssikkerhed

… baseret på en **afvejning** af virksomhedens forretnings**mål** og digitaliserings**strategi**, **risikoprofil**, eksisterende **sikkerhedsbudget** og **investeringsvilje**.



3. Planer, processer og beredskab

Det anbefales, at

- bestyrelsen fører **kontrol** med, at cyber- og informationssikkerhedsrisici er fastlagt i **politikker** og håndteret i **processer** for it/fysisk **sikkerhed** og digital **adfærd**.

- bestyrelsen fører **kontrol** med, at virksomheden har **testede beredskabs- og kommunikationsplaner** for håndtering i tilfælde af alt fra hackerangreb til strømnedbrud.

4. Rapportering og kontrol

Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en **fast del af sit årshjul**, og har cybersikkerhed på **agendaen** på hvert bestyrelsesmøde

- bestyrelsen modtager **relevant rapportering** forud for hvert bestyrelsesmøde med bl.a. bl.a. aktuelt **trusselsbillede**, **sikkerhedshændelser**, resultater af sikkerheds**test** og awareness aktiviteter, **resultater** fra revisionsgennemgange, evt. **forslag** til supplerende tiltag ift. forsikringsdækning og investeringer.

ANBEFALINGER TIL BESTYRELSEN

5. Kultur og mennesker

Det anbefales, at

- virksomheden har et **træningsprogram** for **bestyrelse, direktion** og **medarbejdere** i relation til cyber- og informationssikkerhed.

- bestyrelsen går **forrest** i at understøtte en **stærk og bevidst** cyber- og informationssikkerheds**kultur** i virksomheden.

6. Kompetencer og organisering

Det anbefales, at

- mindst ét medlem af bestyrelsen har **viden om eller erfaring** med cyber- og informationssikkerhed og tilegner sig indsigt i virksomhedens tekniske og sikkerhedsmæssige fundament.

- virksomhedens sikkerhedsorganisation eller -funktion er direkte **forankret på et direktionsniveau**, der rapporterer direkte til bestyrelsen.

RELEVANTE OVERVEJELSER FOR BESTYRELSESMEDLEMMER

1. Risikovurdering og sårbarheder

- ❑ Hvad betyder det for forretningen, hvis vigtige værdier ændres, stjæles, lækkes eller hvis kritiske systemer eller andre it-services er utilgængelige i kortere eller længere tid?
- ❑ Hvem er de sandsynlige angribere, hvad er deres mål, og hvilke redskaber/teknikker bruger de til at opnå disse mål?
- ❑ På hvilke områder er virksomheden mest sårbar overfor angreb (teknologi, personale, processer), og hvor sandsynligt er angreb indenfor disse områder?
- ❑ Hvad er virksomhedens plan for risikohåndtering, inkl. investeringer?

2. Risikoappetit og strategi

- ❑ Hvor stort er budgettet for cyber- og informationssikkerhed?
- ❑ Hvor ligger virksomhedens sikkerhedsniveau- og budget sammenlignet med andre forretningsområder? Med andre virksomheder?
- ❑ Hvad er de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet?
- ❑ Baseret herpå, hvad er virksomhedens tolerance for at påtage sig cyberrisici?

3. Planer, processer og beredskab

- ❑ Har virksomheden nedskrevne it-sikkerhedspolitikker, som direktionen aktivt støtter, og som medarbejderne er trænet i?
- ❑ Foreligger der beredskabs- og kommunikationsplaner – både elektronisk og på papir – til at håndtere sikkerhedshændelser?
- ❑ Beskriver planerne hvordan forretningen kan fortsætte i tilfælde af manglende adgang til de vigtigste it-systemer og it-services, hvem der skal involveres i en krisesituation, og hvordan der sker reetablering af it-systemer og it-services?
- ❑ Angiver planerne en handlingsplan for de første 24 timer efter en sikkerhedshændelse, herunder hvem der har ansvaret for at føre minutrapport?
- ❑ Bliver planerne øvet og testet regelmæssigt?
- ❑ Hvad er resultatet af seneste test, og har det ført til ændringer?
- ❑ Bliver planerne justeret i lyset af angreb, der har ramt andre virksomheder?
- ❑ Er der aftaler indgået med eksterne, som kan tilkaldes for at støtte interne teams?

4. Rapportering og kontrol

- ❑ Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed (risici, status, investeringer, anbefalinger mv.) fra direktionen?
- ❑ Er cyber- og informationssikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?

5. Kultur og mennesker

- ❑ Er der et trænings- og uddannelsesprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- ❑ Foregår der et samarbejde på tværs af organisationen, hvor der deles viden?
- ❑ Opfordrer virksomheden sine tekniske specialister til at udveksle viden og erfaringer med medarbejdere fra lignende organisationer?
- ❑ Går bestyrelsen forrest i at understøtte en stærk og bevidst cybersikkerhedskultur, f.eks. ved selv at anvende VPN, password managers og flerfaktor godkendelse?

6. Kompetencer og organisering

- ❑ Har mindst ét bestyrelsesmedlem kompetencer og erfaring indenfor cyber- og informationssikkerhed? Hvis ikke, får bestyrelsen intern eller ekstern rådgivning og/eller sparring på området? F.eks. fra rådgivere eller en komité?
- ❑ Deltager bestyrelsen aktivt i diskussioner om cyber- og informationssikkerhed?
- ❑ Er bestyrelsen opmærksom på, at dens medlemmer selv kan være et oplagt mål for cyberangreb?
- ❑ Hvor i organisationen (person/funktion) ligger ansvaret for cyber- & informationssikkerhed?
- ❑ Rapporterer denne sikkerhedsfunktion direkte til rigtigt på ledelsesniveau?
- ❑ Er der allokeret tilstrækkelig ressourcer og de rette tekniske kompetencer til at løfte opgaven?
- ❑ Har virksomheden de rette tekniske kompetencer inhouse, eller er der behov for ekstern hjælp?

...TJEKLISTEN

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

… HVIS DU VIL GØRE LIDT EKSTRA

Værdier og systemlandskab:

- Hvad er virksomhedens vigtigste værdier? Det kan være materielle aktiver (fx systemer), immaterielle aktiver (fx data og IP) og andet (fx renommé).
- Hvor opbevares virksomhedens vigtigste data og informationer (fx i cloud, hos ekstern leverandør, indenfor eller udenfor Danmark?)
- Hvilke it systemer og –services er de mest kritiske?
- Hvem er virksomhedens vigtigste leverandører og samarbejdspartnere?
- Hvilke kontrol- og sikkerhedssystemer har virksomheden implementeret (fx overvågning, AI på adgangskontroller, multi faktorautentificering)?
- Bliver disse oversigter løbende vedligeholdt – og af hvem?

Konsekvenser ved en sikkerhedshændelse:

- Hvad betyder det for forretningen, hvis vigtige værdier ændres, stjæles, lækkes eller hvis kritiske systemer eller andre it-services er utilgængelige i kortere eller længere tid?

Sårbarheder:

- Hvor er virksomheden mest udsat for sikkerhedsbrud? (Sårbarheder kan ligge i systemer og programmer som fx Active Directory, processer der mangler eller ikke følges, uvidenhed hos medarbejdere eller lignende)
- Er adgang til data og netværk begrænset til det nødvendige? (risikoen større jo flere mennesker, der har adgang)
- Bliver sikkerhedsniveauet jævnligt testet, f.eks. gennem ”red team”-angreb, firewall audits, sårbarhedsskanninger, penetrationstest, GAP analyser eller lignende?
- Har selskabet legacy-systemer (dvs. ældre systemer der skal udskiftes)? Og hvis ja, er der udarbejdet en plan for udfasning eller isolering af programmer og operativsystemer, der ikke længere supporteres eller opdateres?

Trusselsbillede og sandsynlighed:

- Hvem er de sandsynlige angribere, og hvilke mål kunne de tænkes at gå efter i virksomheden?
- Hvor sandsynlige er disse trusler er overfor de virksomhedens sårbarheder?
- Tager risikoanalyserne højde for nye teknologier og services (f.eks. øget brug af IoT og cloud)?

HANDS-ON …APPENDIKS

APPENDIKS

…OVERSKUELIGHED

Akut tjekliste – GODE RÅD *(illustrativt og vejledende)*

Appendiks 3. Akut checkliste ved cyberhændelser

Tabellen til højre viser et eksempel på en akut checkliste ved en cyberhændelse.

Checklisten er illustrativ:

- ✓ Alle sikkerhedshændelser er forskellige
- ✓ Der findes ikke én tjekliste, der dækker alle situationer
- ✓ Det er vigtigt at kunne være fleksibel i reaktionen

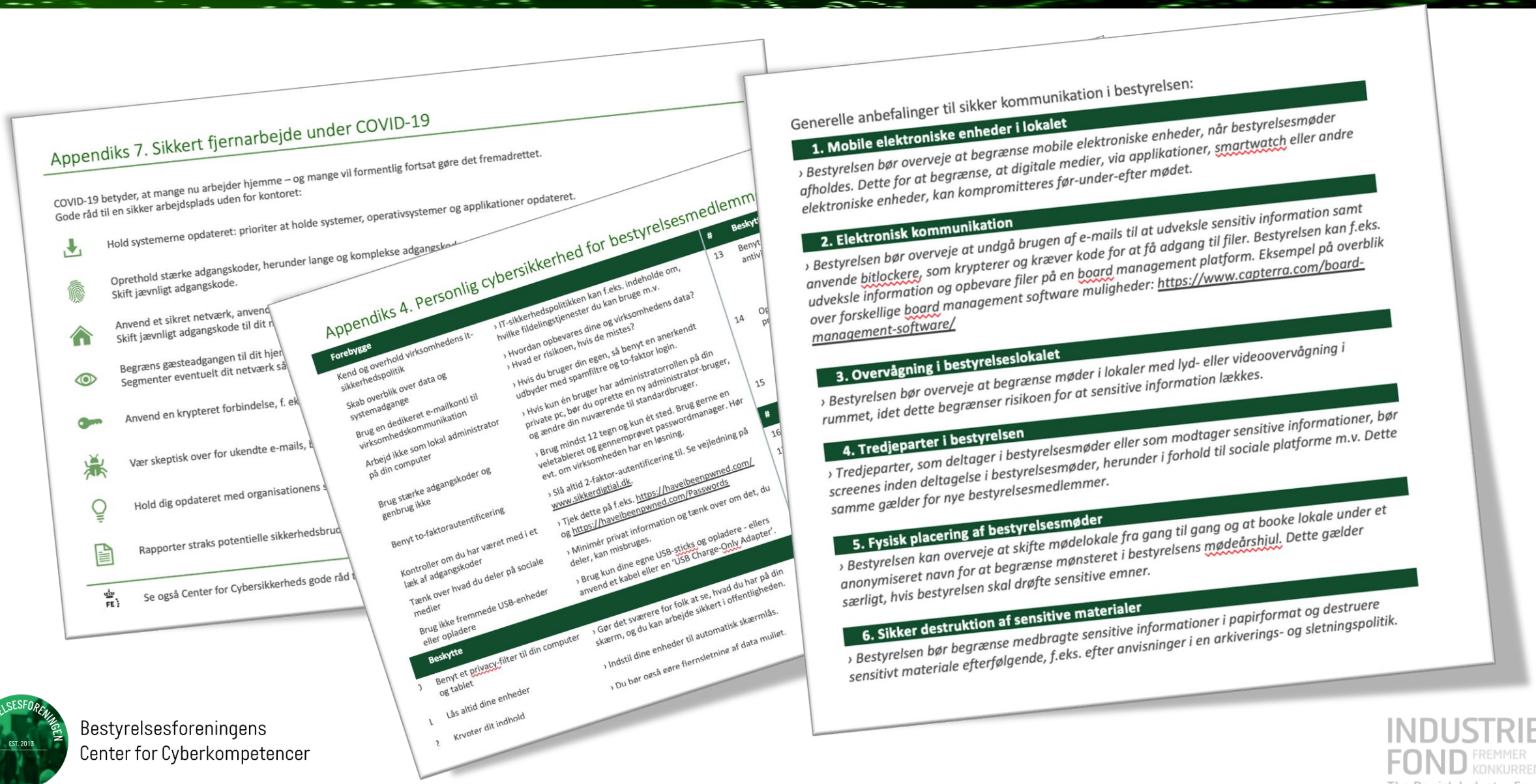
Det vigtigste arbejde sker *før,* virksomheden bliver ramt, bl.a. ved etablering af en *incident response* plan, sikring af backup og evt. indgåelse af aftale med en ekstern sikkerhedspartner, der kan hjælpe.

Efter en kritisk hændelse kommer ofte en lang proces med at sikre, at angrebet er ordentlig elimineret, systemer er genetableret (ofte fra backup), og alle sårbarheder er udbedret.

På bl.a. https://sikkerdigital.dk/virksomhed/naar-skaden-er-sket findes overordnet hjælp til nogle af de mest almindelige typer hændelser.

#	Akut checkliste	Eksempler
1	**Undgå panik og bevar roen**	› Betal ikke de kriminelle
2	**Få overblik over problemet**	› Bed om en root cause analyse
3	**Begræns den akutte skade**	› Isoler hændelsen hvis muligt › Afbryd forbindelsen til internettet › Afbryd forbindelsen til netværket › Sluk ikke for computerne › Skift password › Kontakt banken (ved økonomisk svindel)
4	**Brug Incident Response planen**	› Processen for hændelseshåndtering ligger typisk hos systemejerne
5	**Få kvalificeret ekstern hjælp**	› Fra bl.a. sikkerhedseksperter, jurister og leverandører
6	**Prioritér indsatsen**	› Hvad er der sket og hvad er ramt? › Hvad er konsekvensen for forretningen? › Implementer en plan for forretnings kontinuitet › Er der kompromitteret persondata? › Fokus: Er der (stadig) en backup, der virker?
7	**Kommunikér klart og løbende**	› Intern underretning til ledelse og medarbejdere › Ekstern kommunikation til samarbejdspartnere og presse
8	**Foretag nødvendige anmeldelser**	› Politianmeldelse › Anmeldelse til Datatilsynet (ved tab af persondata) › Anmeldelse til andre myndigheder (særlig i kritiske sektorer)
9	**Husk dokumentation af forløbet**	› Minutlog og revisionsspor mm.
10	**Sørg for bevissikring**	› Få kvalificeret ekstern hjælp til bevissikring › Pas på ikke at ødelægge beviser › Kopi af inficerede maskiner til efterforskning › Sikring af logfiler
11	**Følg op på udbedringsplan**	› Etablering af overvågning og evt. sikkerhedskontroller så yderligere forsøg på kompromittering opdages

Øvrige Appendix – GODE RÅD *(eksempler)*



Appendiks 7. Sikkert fjernarbejde under COVID-19

COVID-19 betyder, at mange nu arbejder hjemme – og mange vil formentlig fortsat gøre det fremadrettet.
Gode råd til en sikker arbejdsplads uden for kontoret:

- Hold systemerne opdateret: prioriter at holde systemer, operativsystemer og applikationer opdateret.
- Opretholdstærke adgangskoder, herunder lange og komplekse adgangsko
  Skift jævnligt adgangskode.
- Anvend et sikret netværk, anvend
  Skift jævnligt adgangskode til dit n
- Begræns gæsteadgangen til dit hjer
  Segmenter eventuelt dit netværk så
- Anvend en krypteret forbindelse, f. ek
- Vær skeptisk over for ukendte e-mails,
- Hold dig opdateret med organisationens
- Rapporter straks potentielle sikkerhedsbrud

Se også Center for Cybersikkerheds gode råd t

Appendiks 4. Personlig cybersikkerhed for bestyrelsesmedlemm

#	Forebygge	
13	Kend og overhold virksomhedens it-sikkerhedspolitik	› IT-sikkerhedspolitikken kan f.eks. indeholde om, hvilke fildelingstjenester du kan bruge m.v.
14	Skab overblik over data og systemadgange	› Hvordan opbevares dine og virksomhedens data? › Hvad er risikoen, hvis de mistes?
15	Brug en dedikeret e-mailkonti til virksomhedskommunikation	› Hvis du bruger din egen, så benyt en anerkendt udbyder med spamfiltre og to-faktor login.
16	Arbejd ikke som lokal administrator på din computer	› Hvis kun én bruger har administratorrollen på din private pc, bør du oprette en ny administrator-bruger, og ændre din nuværende til standardbruger.
17	Brug stærke adgangskoder og genbrug ikke	› Brug mindst 12 tegn og kun ét sted. Brug gerne en veletableret og gennemprøvet passwordmanager. Hør evt. om virksomheden har en løsning.
	Benyt to-faktorautentificering	› Slå altid 2-faktor-autentificering til. Se vejledning på www.sikkerdigtial.dk.
	Kontroller om du har været med i et læk af adgangskoder	› Tjek dette på f.eks. https://haveibeenpwned.com/Passwords og https://haveibeenpwned.com/
	Tænk over hvad du deler på sociale medier	› Minimér privat information og tænk over om det, du deler, kan misbruges.
	Brug ikke fremmede USB-enheder eller opladere	› Brug kun dine egne USB-sticks og opladere - ellers anvend et kabel eller en 'USB Charge-Only Adapter'.
	Beskytte	
	Benyt et privacy-filter til din computer og tablet	› Gør det sværere for folk at se, hvad du har på din skærm, og du kan arbejde sikkert i offentligheden.
	Lås altid dine enheder	› Indstil dine enheder til automatisk skærmlås.
	Krypter dit indhold	› Du bør også gøre fjernsletning af data muligt.

Generelle anbefalinger til sikker kommunikation i bestyrelsen:

1. Mobile elektroniske enheder i lokalet

› Bestyrelsen bør overveje at begrænse mobile elektroniske enheder, når bestyrelsesmøder afholdes. Dette for at begrænse, at digitale medier, via applikationer, smartwatch eller andre elektroniske enheder, kan kompromitteres før-under-efter mødet.

2. Elektronisk kommunikation

› Bestyrelsen bør overveje at undgå brugen af e-mails til at udveksle sensitiv information samt anvende bitlockere, som krypterer og kræver kode for at få adgang til filer. Bestyrelsen kan f.eks. udveksle information og opbevare filer på en board management platform. Eksempel på overblik over forskellige board management software muligheder: https://www.capterra.com/board-management-software/

3. Overvågning i bestyrelseslokalet

› Bestyrelsen bør overveje at begrænse møder i lokaler med lyd- eller videoovervågning i rummet, idet dette begrænser risikoen for at sensitive information lækkes.

4. Tredjeparter i bestyrelsen

› Tredjeparter, som deltager i bestyrelsesmøder eller som modtager sensitive informationer, bør screenes inden deltagelse i bestyrelsesmøder, herunder i forhold til sociale platforme m.v. Dette samme gælder for nye bestyrelsesmedlemmer.

5. Fysisk placering af bestyrelsesmøder

› Bestyrelsen kan overveje at skifte mødelokale fra gang til gang og at booke lokale under et anonymiseret navn for at begrænse mønsteret i bestyrelsens mødeårshjul. Dette gælder særligt, hvis bestyrelsen skal drøfte sensitive emner.

6. Sikker destruktion af sensitive materialer

› Bestyrelsen bør begrænse medbragte sensitive informationer i papirformat og destruere sensitivt materiale efterfølgende, f.eks. efter anvisninger i en arkiverings- og sletningspolitik.

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

ÅRSHJUL – CYBERSIKKERHED *(eksempel)*

1. kvartal

- Organisation, herunder cyberkompetencer og organisering
- Cybersikkerhed awareness
- Status på drift og sikkerhedshændelser

Se vejledning

5 – Kultur og mennesker

6 – Kompetencer og organisering

2. Kvartal

- Rammer og strategi for styring af cyberrisici
- Fastlæggelse af risikoappetit
- Status på drift og sikkerhedshændelser

Se vejledning

1 – Risikovurdering og sårbarheder

2 – Risikoappetit og strategi

3. Kvartal

- Politikker og planer for risikohåndtering og beredskab
- Forsikringsdækning for cyberangreb
- Status på drift og sikkerhedshændelser

Se vejledning

3 – Planer, processer og beredskab

4. Kvartal

- Årsbudget, herunder budget for IT-sikkerhed og investeringer i forbedringer
- Status på drift og sikkerhedshændelser

Se vejledning

4 – Rapportering og kontrol

BESTYRELSENS KOMPAS

PARTNER

LEDER

KONTROL

GÅ IKKE
I VEJEN…

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

www.bestyrelsesforeningen.dk

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

TAK FOR I DAG
Lad os sammen styrke cybersikkerheden i danske virksomheder

Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation