

VELKOMMEN TIL KONFERENCE

Cyber- og informationssikkerhed på strategiske niveauer

9. november 2021



Bestyrelsesforeningens
Center for Cyberkompetencer



DANSK STANDARD

DANSK
ERHVERV



Dansk Selskab for
Virksomhedsledelse



Projekt Styrkelse af Strategiske Cyberkompetencer

- ✓ **Styrke konkurrenceevnen for danske virksomheder**
- ✓ Beskytte **virksomhedernes værdier**
- ✓ Skabe **vækst i en digital tid og udnytte den digitale transformation**
- ✓ Leve op **til bestyrelsesansvar**



DANSK ERHVERV

IT-Branchen



Dansk Selskab for Virksomhedsledelse

D I Digital



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

DS
DANSK STANDARD

VIRKSOMHEDERS VÆRDISKABELSE og TRUSSELSBILLEDET

...



World Economic Forum (Global Risk Report 2021)



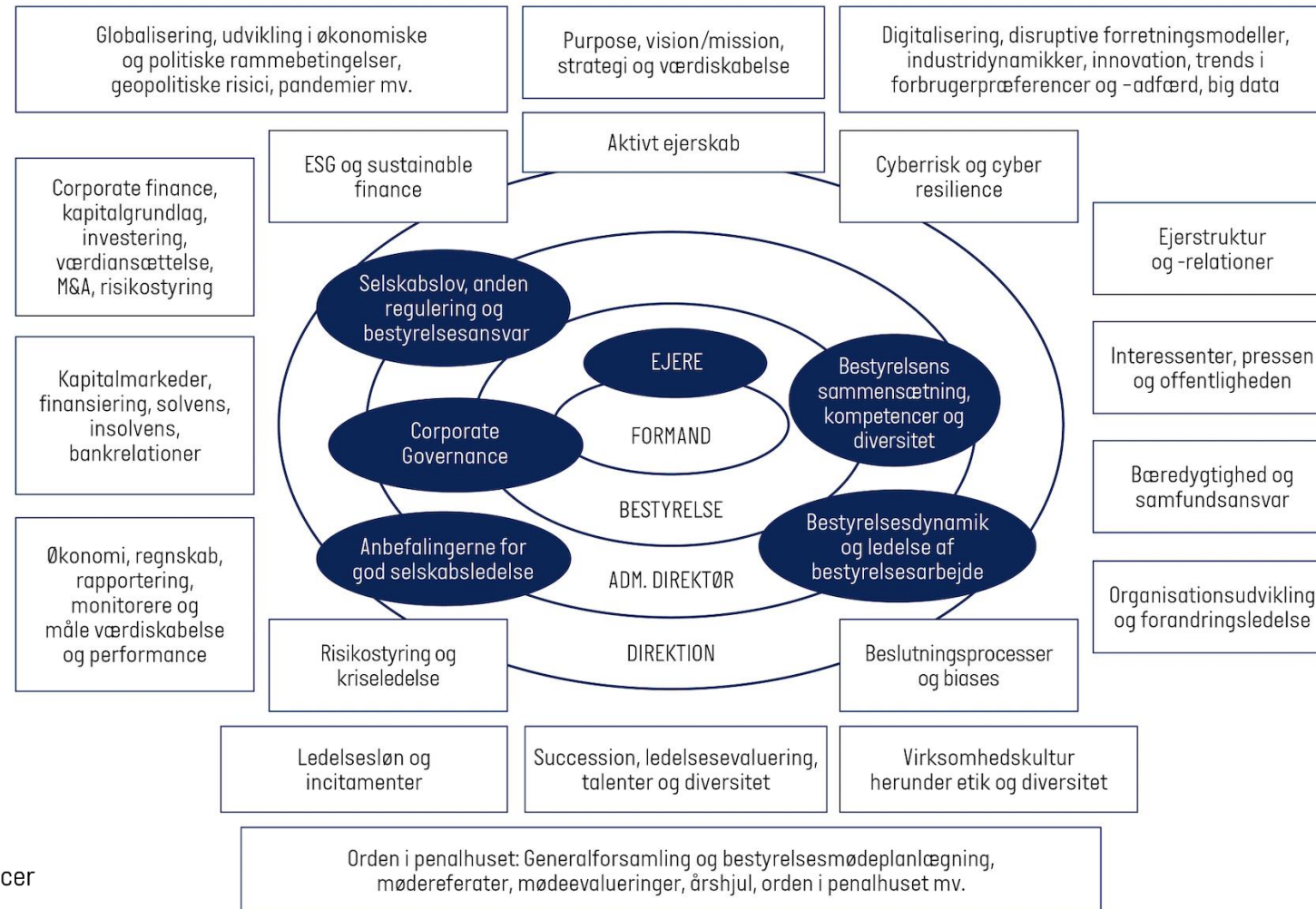
Bestyrelsesforeningens
Center for Cyberkompetencer



INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR...

360° OM BESTYRELSENS OPGAVER, PROBLEMSTILLINGER & RELATIONER



BESTYRELSENS OPGAVER og ANSVAR... og REALITET

360° OM BESTYRELSENS OPGAVER, PROBLEMSTILLINGER & RELATIONER



Strategisk og operationelt

niveau

i tæt samarbejde...



Bestyrelsesforeningens
Center for Cyberkompete



INDUSTRIENS FOND

BESTYRELSENS OPGAVER og ANSVAR... og REALITET

DoppelPaymer

Your network has been penetrated.

This link and your decryption key will expire in 21 days after your systems were infected. Sharing this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.

All files on each host in your network have been encrypted with flawless algorithm. Backups were either encrypted or deleted and backup disks were formatted.

There is no working decryption software that may solve this.

Do not rename the encrypted or informational text files. Do not move the encrypted or informational text files. This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data. So if you decide not to pay, we would share it. It may harm your business reputation.

Online chat

RobbinHood ransomware.

days and we've worked on your systems to gain full access to your company and bypass all of your protections. If you don't pay in the specified duration, the price increases **\$10,000** each day after the period. After 10 days your files will be removed automatically and you won't be able to get your data back. We're watching you, if you want to know who we are, upload your files to virustotal or services like that, don't call FBI or other security organizations. For security of **your systems**, don't recover your computer, don't rename your files, it will damage your files. All procedures are repeated more times or somethings like that we won't talk more, all we know is MONEY. If you don't care about yourself we will destroy your time and **hurry up!** Tik Tak, Tik Tak, Tik Tak!

your files?

encrypted by a strong encryption with **RSA-4096** ciphers. The private key can be found here: [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

In summary you can't read or work with your files. But with our help you can recover them. It's **impossible** to recover your files without private key and our unlocking software (You can google: Baltimore city, Greenville city and RobbinHood ransomware)

Just pay the ransomware and end the suffering then get better cybersecurity

How to get private key or unlocking software?



BESTYRELSENS OPGAVER og ANSVAR... og REALITET

Man. 15. mar. 23.33

Jeg har behov for at komme i kontakt med jer ASAP. Vi er blevet hacket udefra ser det ud til, og står uden adgang til al IT. At betale løsesum (beløb er ukendt) er en reel overvejelse nu. Vi er i en situation hvor vi ikke har drift adskillige dage fremadrettet. De har taget al tilgængelig backup. Vi kigger ind i vores værste mareridt!!!

JS



Ikke BESTYRELSENS BRILLER... men hvad så?



BESTYRELSENS OPGAVER og ANSVAR... og REALITET

COCKTAILS

ELDERFLOWER SOUR Homemade Elderflower vodka	125
ITALIAN SPRITZ Aperitivo, Gin, Pink Grapefruit	115
APEROL SPRITZ Aperol, Prosecco	105
HUGO Elderflower, Prosecco, Mint	
BELLINI Peach, Prosecco	
BLOODY MARY Vodka, Tomato, Celery, Tabasco	
ESPRESSO MARTINI Espresso, Vodka, Kahlua	
PAPER PLANE Aperol, Vodka, Lemon	

BIRRA

CARLSBERG	58
INDIA PALE ALE, BREWMASTER'S	68
KRONENBOURG BLANC	68
PORETTI NO 4, BIRRIFICIA ANGELO	68
GRIMBERGEN DOUBLE AMBRE	68

NEGRONI Campari, Gin, Vermouth	125
GODFATHER Scotch, Amaretto	115
ICE TEA Dark rum, Earl Grey, Peach	125
PINK PALOMA Tequila, Pink Grapefruit, Lime	115
BERGAMOTTO Gin, Bergamot, Lemon	115



BESTYRELSENS OPGAVER og ANSVAR... og REALITET



CYBERSIKKERHED FOR BESTYRELSER

Anbefalinger til Styrkelse af Cyberkompetencer

Denne publikation udgør ikke og kan ikke erstatte professionel rådgivning. Bestyrelsesforeningen eller dens samarbejdspartnere påtager sig ikke ansvar for tab som følge af handlinger eller undladelser baseret på publikationens indhold. Alle rettigheder forbeholdes.

BESTYRELSESFORENINGEN
Fokus på værd skabe se, ledelse og governance
Bestyrelsesforeningens Center for Cyberkompetencer

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

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 forretningsmål og digitaliseringsstrategi, risikoprofil, eksisterende sikkerhedsbudget og investeringsvilje.

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. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest og awareness aktiviteter, resultater fra revisionsgennemgange, evt. forslag til supplerende tiltag ift. forsikringsdækning og investeringer.

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 er direkte forankret på et direktionniveau, der rapporterer direkte til bestyrelsen.

3. Planer, processer og beredskab

- 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 cybersikkerhed?

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 indgået aftale med eksterne, som kan tilkaldes for at støtte interne teams?

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 informationssikkerhedskultur i virksomheden.

Har bestyrelsen forrest i at understøtte en stærk og bevidst cyber- og informationssikkerhedskultur, 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 eksternt 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- og informationssikkerhed?
- Rapporterer denne sikkerhedsfunktion direkte til de rigtige på ledelsesniveau?
- Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- Har virksomheden de rette tekniske kompetencer inhouse, eller er der behov for eksternt hjælp?

Dagens program

9:10

De aktuelle cyberudfordringer – organisationernes cyberstrusselsbillede
Eva Leisner, Center for Cybersikkerhed

9:30

Standarder som et værdifuldt værktøj til at systematisere virksomhedens arbejde med cyber- og informationssikkerhed
Henriette Rolskov, COOP

9:55

Ledelsens ansvar i forhold til cyber- og informationssikkerhed
Michael Ørnø, Statens IT

10:20

Pause

10:35

Bestyrelsens ansvar i forholdt til cyber- og informationssikkerhed
Søren Skibsted, Kromann Reumert

11:00

Hvordan kan D-mærket bidrage til at styrke danske virksomheders modstanddygtighed?
Mikael Jensen, D-mærket

11:20

Afrunding og tak for i dag



Bestyrelsesforeningens
Center for Cyberkompetencer

INDUSTRIENS FOND

