December 2019

CYBERSIKKERHED FOR BESTYRELSER

Anbefalinger til Styrkelse af Cyberkompetencer

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

KROMANN REUMERT

CENTER FOR CYBERSIKKERHED

INDUSTRIENS FOND
FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

INDHOLD

KONTAKT

Bestyrelsesforeningens Center for Cyberkompetencer

Tom Jacobsgaard
Direktør
Mail: tj@bestyrelsesforeningen.dk

Marianne Philip
Bestyrelsesformand
Mail: mp@kromannreumert.com

Troels Ørting Jørgensen
Formand for Advisory Board
Mail: toe@bestyrelsesforeningen.dk

Kirsten Hede
Projektdirektør
Mail: khe@bestyrelsesforeningen.dk

1. Indledning

Disse anbefalinger er udarbejdet som led i projektet "*Styrkelse af strategiske cyberkompetencer i danske virksomheder*", der har til formål at øge opmærksomheden over for cyberrisici og at styrke kompetencerne inden for cybersikkerhed i danske bestyrelser og direktioner, herunder bestyrelser og direktioner i små- og mellemstore virksomheder.

Projektet er støttet af Industriens Fond, og er en del af Industriens Fonds indsats indenfor cybersikkerhed.

Projektet udføres af Bestyrelsesforeningens Center for Cyberkompetencer i samarbejde med en partnerkreds bestående af CBS, CBS Bestyrelsesuddannelserne, Aalborg Universitet (AAU), World Economic Forum, Dubex, EY, IBM, PwC, Center for Cybersikkerhed (CFCS) og Kromann Reumert.

Det er Bestyrelsesforeningens mål, at partnerkredsen løbende opdateres og kommer til at omfatte alle væsentlige rådgivere til bestyrelser, herunder bestyrelser i små- og mellemstore virksomheder.

December 2019

2. Cyberkompetencer i danske bestyrelser

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

Bestyrelser har brug for kompetencer indenfor cyber- og informationssikkerhed. Ikke kun for at håndtere risici men også for at gøre sikkerhed til en konkurrencefordel og en facilitator for virksomhedens produktudvikling og forretningsmodel.

Det er bestyrelsens opgave og ansvar at føre effektiv kontrol med virksomhedens risici – blandt andet for at beskytte og skabe afkast af den forretning, som bestyrelsen er sat til at varetage på vegne af ejerne.

Mange bestyrelser mangler dog tilstrækkelig viden og kompetencer til at kunne adressere virksomhedens risici på cyberområdet.

Risikostyring går ud på at forstå, identificere, måle, rapportere, overvåge og styre risiko. Alle risici kan ikke fjernes helt. Men ved at anvende en systematisk tilgang kan de styres. På den måde kan bestyrelsen prioritere ressourcerne der, hvor de gør mest gavn.

For at se, om kompetencerne er til stede i bestyrelsen, bør det enkelte medlem stille sig selv spørgsmålet: *"Forstår jeg virksomhedens cyberrisici, og har vi en cyberstrategi?"*

Formålet med disse anbefalinger er at klæde bestyrelsesmedlemmer på til arbejdet med en cyberstrategi og at give dem værktøjer til at sparre med og udfordre direktionen om virksomhedens cyber- og informationssikkerhed.

Bestyrelsen har brug for cyberkompetencer for at:

- ✓ Beskytte virksomhedens aktiver, forretningsprocesser og kunder.
- ✓ Skabe vækst og udnytte forretnings-muligheder i en digital tidsalder.
- ✓ Varetage sit ansvar og beslutte virksomhedens risikoprofil og investeringsvilje.

3. Udvalgte typer af cyberangreb

Cyberangreb er drevet af forskellige hensigter og metoder. Nogle har til formål at stjæle data eller spionere, andre skal afpresse penge. Nogle angreb er simple, andre er avancerede. Angreb kan komme fra f.eks. organiserede kriminelle, stater, amatører, insidere og konkurrenter. Lykkes et angreb, kan det ultimativt betyde, at virksomheden må dreje nøglen om.

Cyberangreb dækker over, at en aktør forsøger at forstyrre eller få uautoriseret adgang til data, systemer, digitale netværk eller digitale tjenester. Et vellykket angreb kan lamme hele virksomheden og tage lang tid at rydde op efter. To meget udbredte typer angreb er phishing-mails og CEO fraud (f.eks. mod bestyrelsesmedlemmer), der kan medføre store tab. Hvor et angreb kan komme fra varierer fra virksomhed til virksomhed alt efter branche, hvad virksomheden er udsat for og hvilke sårbarheder, den har. Den enkelte virksomheds risici afhænger af en konkret vurdering.

Det anslås, at…

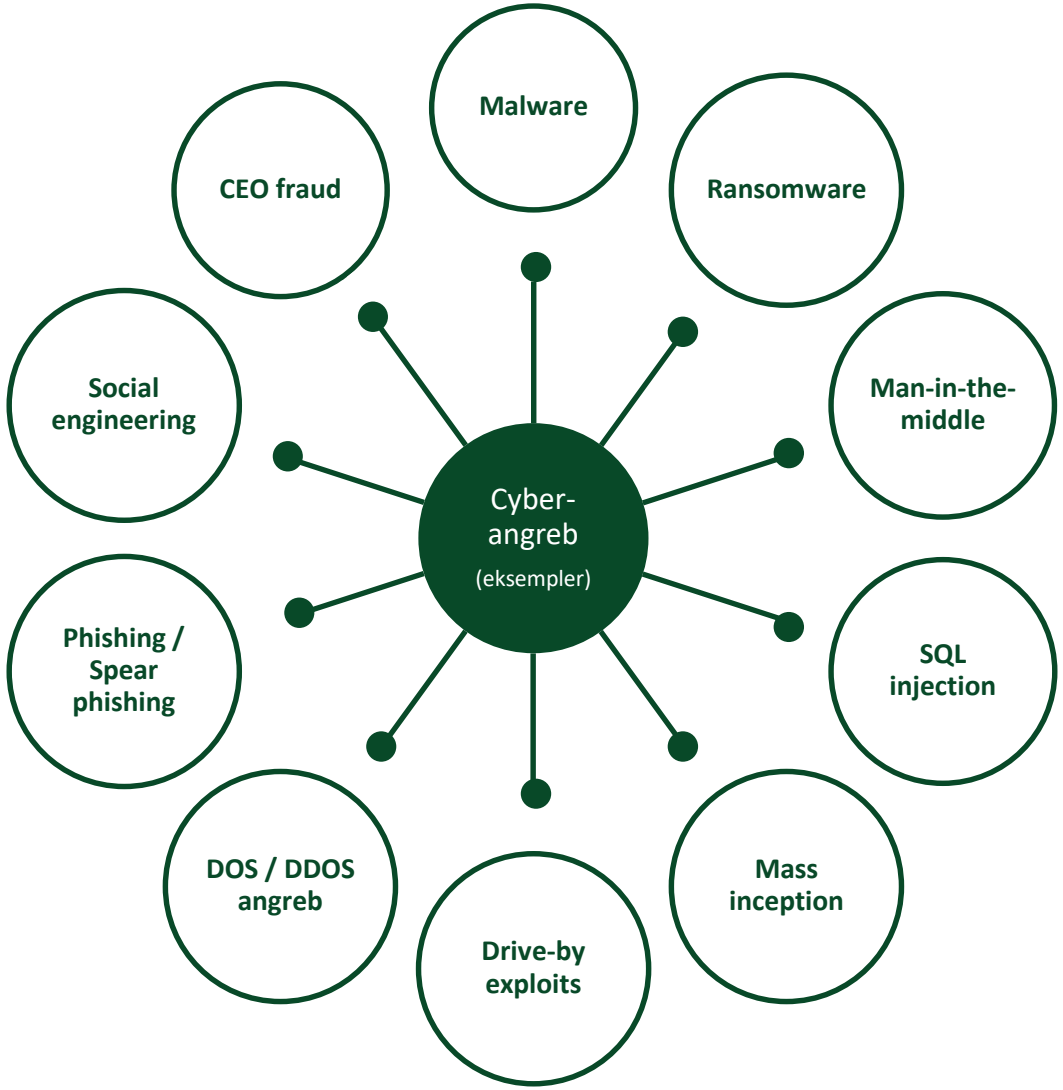
- **9** ud af **10** virksomheder har prøvet at blive hacket.
- Der sker mellem **500** og **1000** målrettede hackerangreb dagligt blot i Danmark.
- **+100.000** danske pc'er i dag er inficeret med potentielt skadelige vira.

Kilde: CSIS Security Group

De mest udsatte sektorer er bl.a.

- Finans og forsikring
- Forsyning
- Sundhed
- Transport
- Rådgivning
- Detailhandel
- Produktion

Kilder: IBM X-Force Cyber Security Intelligence Index 2019; Drooms Top 5 Industries at Risk 2019



Figuren viser eksempler på forskellige former for cyberangreb- og metoder
Ord og begreber er forklaret i ordlisten i Bilag 1.

4. Temaer i en cyberstrategi

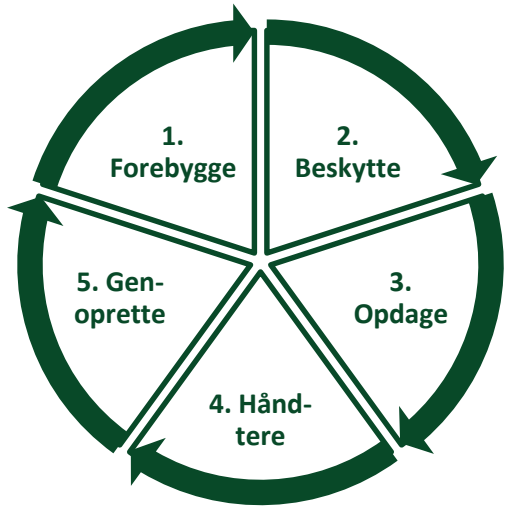
Virksomheders arbejde med cyber- og informationssikkerhed handler om mere end IT. Det handler i høj grad også om governance, ledelse, processer og mennesker. Sikkerhed er i sidste ende bestyrelsens ansvar, og bør være et vigtigt emne på bestyrelsens dagsorden. Cybertruslen er reel, og virksomheder er nødt til at have en strategi for at håndtere den.

Det overordnede formål med en cyberstrategi er **Forebygge**, **Beskytte**, **Opdage** og **Håndtere** cyberhændelser samt **Genoprette** ramte systemer, data mv. efter en hændelse.

Med dette udgangspunkt kan bestyrelsen strukturere sit arbejde med en cyberstrategi ud fra de 6 temaer vist i tabellen til højre. Hvert tema er opsummeret i en generel anbefaling (se afsnit 5), der er uddybet i 6 "værktøjskasser" med centrale overvejelser, man kan gøre sig i bestyrelseslokalet (se afsnit 6).

5 overordnede formål med en cyberstrategi

1. **Forebygge** at et cyberangreb kan lykkes.
2. **Beskytte** virksomheden mod et cyberangreb.
3. **Opdage** hvis/når et angreb sker.
4. **Håndtere** et angreb hvis/når det sker.
5. **Genoprette** eventuelt ramte systemer og data.



6 TEMAER TIL ARBEJDET MED EN CYBERSTRATEGI

Tema	Generelt
1. **Risikovurdering og sårbarheder**	Bestyrelsen har indsigt i virksomhedens sårbarheder, trusler, indvirkning af angreb og sandsynlighed for at det sker.
2. **Risikoappetit og strategi**	Bestyrelsen fastsætter virksomhedens risikoappetit baseret på forretningsmål, risikoprofil og omkostninger.
3. **Planer, processer og beredskab**	Bestyrelsen fører kontrol med, at cybersikkerhed er implementeret i testede planer og processer, bl.a. indenfor de 5 hovedområder Forebyg, Beskyt, Opdag, Håndter, Genopret.
4. **Rapportering og kontrol**	Bestyrelsen modtager relevant rapportering og har implementeret cybersikkerhed som fast del af sit årshjul.
5. **Kultur og mennesker**	Bestyrelsen går forrest i at sikre en positiv sikkerhedskultur og awareness træning af virksomhedens medarbejdere.
6. **Kompetencer og organisering**	Bestyrelsen og direktionen har de rette kompetencer til at forstå, vurdere, og håndtere cybersikkerhed.

5. Anbefalinger til bestyrelsen

Strategi

Udførelse

Mennesker

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 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.

3. Planer, processer og beredskab

Det anbefales, at

- bestyrelsen fører kontrol med, at cyber- og informationssikkerhedsrisici er håndteret i processer og politikker 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 (se eksempel på årshjul i Bilag 2).
- bestyrelsen modtager relevant rapportering forud for hvert bestyrelsesmøde med bl.a. risikovurdering, resultater af sikkerhedstest, sikkerhedshændelser, resultater fra audits, sikkerhedsbudget, forsikringsdækning, resultater fra awareness aktiviteter, og anbefalede tiltag og investeringer.

5. Kultur og mennesker

Det anbefales, at

- virksomheden har et træningsprogram for bestyrelse, direktion og medarbejdere i relation til cyber- og informationssikkerhedstræning og -awareness.
- bestyrelsen går forrest i at understøtte en cyber- og informationssikkerhedskultur 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 forankret på et direktionsniveau, der rapporterer direkte til bestyrelsen.

6. Værktøjskasse

Tema 1 – Risikovurdering og sårbarheder

Til brug for styring af cyberrisici og fastlæggelse af en overordnet cyberstrategi er bestyrelsen nødt til at have tilstrækkelig indsigt i virksomhedens overordnede teknologilandskab, vigtigste værdier, primære sårbarheder samt de mest sandsynlige trusler og konsekvenser af et cyberangreb.

Selvom bestyrelser er vant til at arbejde med risiko, sandsynlighed og konsekvens, er de færreste hjemmevante i cyber- og informationsrisici.

Indenfor cyber- og informationssikkerhed er risikovurderingen (også) omdrejningspunktet i risikostyringen, hvor risici identificeres, analyseres og evalueres.

Til at kontrollere, at bestyrelsen modtager tilstrækkelig information, kan listen til højre være til inspiration.

Bestyrelsen bør mindst to gange om året modtage en opdateret risikovurdering fra direktionen, der bl.a. beskriver:

1) Vigtigste værdier og systemer
2) Konsekvenser ved læk eller nedbrud
3) Primære sårbarheder
4) Trusler (prioriteret) og sandsynlighed
5) Plan for risikohåndtering og investeringer

Bestyrelsen kan også lade sig inspirere af World Economic Forums analyseværktøj '*Advancing Cyber Resilience Principles and Tools for Boards*' (henvisning i Bilag 4).

Ifølge PwC 2019 Annual Corporate Directors Survey svarede færre end 40% af de adspurgte ledere, at deres bestyrelse forstår virksomhedens cyberrisici.

Centrale overvejelser i et bestyrelseslokale

Værdier og systemlandskab

- Hvad er virksomhedens vigtigste værdier? Det kan være materielle aktiver (f.eks. systemer), immaterielle aktiver (f.eks. data og IP) og renommé.
- Hvor opbevares virksomhedens vigtigste data og informationer (f.eks. 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 (f.eks. 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 f.eks. Active Directory, processer der mangler eller ikke følges, manglende awareness hos medarbejdere og lign.)
- Er adgang til data og netværk begrænset til det nødvendige? (risikoen er større jo flere mennesker, der har adgang)
- Bliver sikkerhedsniveauet jævnligt testet, f.eks. gennem "red team"-angreb, firewall audits, sårbarhedsskanninger, penetrationstest, GAP analyser og lign?

Trusselsbillede og sandsynlighed

- Hvem er de sandsynlige angribere?
- Hvad er deres mål (f.eks. stjæle penge, IP, informationer, digital identitet)?
- Hvilke redskaber/teknikker bruger de til at opnå ovenstående mål (f.eks. phishing, drive-by exploits, social engineering, DDoS, malware mv.)
- Hvor sandsynlige er disse trusler overfor virksomhedens sårbarheder?

Plan for risikohåndtering og investeringer

- Hvad er virksomhedens plan for risikohåndtering, inklusive investeringer?

6. Værktøjskasse

Tema 2 – Risikoappetit og strategi

Som led i cyberstrategien bør bestyrelsen mindst én gang årligt fastlægge virksomhedens risikoappetit på cyber- og informationssikkerhedsområdet, forstået som den risiko, bestyrelsen er villig til at acceptere for at opnå virksomhedens strategiske målsætninger.

Risikoappetitten er redskabet til at koble de strategiske målsætninger sammen med den operationelle drift.

Risikoappetitten fastsættes bl.a. ud fra virksomhedens forretningsmål, risikobillede og omkostninger ved at investere i et højere sikkerhedsniveau.

Risikoappetitten kan udtrykkes som en overordnet målsætning (f.eks. at der skal være en "lav risiko" for, at virksomheden kan blive misbrugt til datalæk, eller at sikkerhedsniveauet som minimum skal opretholdes ved outsourcing).

Risikoappetitten kan også være målbar (f.eks. en minimum tilgængelighed på kritiske systemer eller forbud mod at opbevare følsomme data udenfor Danmark).

Bestyrelsesmedlemmer skal være påpasselige med at undervurdere risikoen, særligt hvis de ikke forstår den, da det kan give et skævt billede af den reelle risikoappetit.

Til at fastsætte risikoappetitten og føre tilsyn med virksomhedens eksponering kan bestyrelsen bruge listen til højre til inspiration.

Ifølge Deloitte Cyber Risk Landscape Report 2019 mente halvdelen af de adspurgte ledere, at deres virksomhed kan vende tilbage til 'business as usual' i løbet af et par dage. Mere end 1/3 mente, at det kun vil tage en dag. De mindre virksomheder var mest optimistiske.

Centrale overvejelser i et bestyrelseslokale

Strategi

- Hvad er virksomhedens overordnede strategi og forretningsmål?
- Hvad er virksomhedens digitaliseringsstrategi?

Risikobillede

- Hvad er det centrale i risikovurderingen fra direktionen *(se 'Risikovurdering og sårbarheder' i Tema 1)*, herunder på hvilke områder er virksomheden mest sårbar overfor angreb, hvor sandsynligt er angreb på virksomheden indenfor disse områder, og hvad er de potentielle konsekvenser ved et angreb, f.eks. økonomisk, samfundsmæssigt og for renommeét?
- Har virksomheden kritisk infrastruktur eller er den i øvrigt underlagt regulatoriske krav, der påvirker risikoappetitten?
- Er virksomheden på vej til at investere i ny teknologi og services (f.eks. mere IoT og cloud), der ændrer risikobilledet og kræver ny investering i sikkerhed?
- Har virksomheden legacy-systemer (dvs. ældre systemer der skal udskiftes)? Hvis ja, er der en plan for udfasning eller isolering af programmer og operativsystemer, der ikke længere supporteres eller opdateres?

Omkostninger

- Hvor stort er budgettet for cyber- og informationssikkerhed?
- Hvor ligger virksomhedens sikkerhedsniveau- og budget sammenlignet med andre virksomheder?
- Hvad er de potentielle omkostninger forbundet med at investere i en opgradering af sikkerhedsniveauet?

Risikoappetit

- På baggrund af en samlet vurdering, hvad er virksomhedens tolerance for at påtage sig cyberrisici, herunder toleranceværdien for de enkelte risici, f.eks. risikotype, produkttype, kunder, strategi, målsætninger mv.?

Udmøntning

- Er risikoappetitten udmøntet som rammer i virksomhedens interne politikker, f.eks. for operationel risici, compliance risici, markedsrisici, likviditetsrisici, forsikringsrisici, outsourcing mv. ?

6. Værktøjskasse

Tema 3 – Planer, processer og beredskab

Det ikke er et spørgsmål om, hvorvidt virksomheden bliver ramt, men et spørgsmål om hvornår. Alle virksomheder bør derfor have et velafprøvet beredskab. Det er vigtigt, at bestyrelsen spørger ind til, og om der foreligger velafprøvede planer og processer til at håndtere cyber- og informationssikkerhedshændelser.

Selvom virksomheden allerede har sikkerhedspolitikker og beredskabsplaner, er det ikke sikkert, at de tager højde for, hvordan virksomheden forebygger, beskytter, opdager og håndterer en sikkerhedshændelse og genopretter systemer efter et angreb.

Sikkerhedshændelser kan have store omkostninger til udredning, genopretning, driftstab, kompensation til kunder mv. Det er derfor vigtigt, at have dokumenterede og testede politikker, processer og beredskabsplaner, som medarbejderne er trænet i, for at kunne forebygge og håndtere et angreb effektivt.

Til at føre kontrol med om virksomheden har etableret et passende sikkerhedsniveau og beredskab, eventuelt baseret på anerkendte standarder, kan bestyrelsen bruge listen til højre til inspiration.

Hvis virksomheden ikke følger en standard eller et rammeværk for styring af informationssikkerhed, kan det overvejes at anvende f.eks. ISO27001, der er en statslig sikkerhedsstandard, det har været obligatorisk at følge for statslige institutioner siden 2014.

Ifølge PwC 2019 Annual Corporate Directors Survey svarede 53 % af respondenterne, at bestyrelsen var tryg ved virksomhedens plan for håndtering af sikkerhedshændelser.

Centrale overvejelser i et bestyrelseslokale

Processer og politikker

- Har virksomheden nedskrevne it-sikkerhedspolitikker, som direktionen aktivt støtter, og som medarbejderne er trænet i? F.eks. politikker for, hvor ofte it-sikkerhedsniveauet skal testes/opgraderes (såsom at firewall audits skal udføres månedligt eller at nye applikationer skal gennemgå code review, før de udrulles), politikker for opførsel for medarbejdere, leverandører og kunder mv..
- Er sikkerhed tænkt ind i virksomhedens forretningsprocesser?

Beredskabsplaner

- Er der planer for reetablering af systemer og data (Disaster Recovery Plans og Technical Recovery Plans)?
- Er der planer for, hvordan forretningen kan fortsætte i tilfælde af manglende adgang til systemer, programmer og data (Business Continuity Plans og IT Service Continuity Plans)?
- Beskriver planerne, hvem der skal involveres i en krisesituation, f.eks. kommunikation, økonomi, ledelse, jura, responsteamet og it-specialister?
- Beskriver planerne hvordan forretningen kan fortsætte i en krisesituation?
- Er der indgået aftale med eksterne ressourcer og specialister, som kan tilkaldes for at støtte interne teams?
- Har planerne procedurer for orientering og eskalering, f.eks. hvornår bestyrelsen skal orienteres?
- Hvad er procedurerne for at kommunikere med myndighederne, f.eks. politi, tilsyn, Erhvervsstyrelsen (virk.dk)?
- Hvornår og hvordan vil man orientere andre interessenter – f.eks. leverandører eller individer, hvis personoplysninger er kompromitteret?
- Bliver planerne øvet og testet regelmæssigt?
- Hvad er resultatet af seneste test, og har det ført til forbedringer?
- Bliver planerne justeret i lyset af angreb, der har ramt andre virksomheder?

6. Værktøjskasse

Tema 4 – Rapportering og kontrol

Bestyrelsen skal modtage forståelig og målbar rapportering om cybertrusler, - risici og sikkerhedshændelser for at kunne føre kontrol med virksomhedens cybersikkerhed og integrere arbejdet med cybersikkerhed som en naturlig del af sin tilsyns- og kontrolopgave.

Tilstrækkelig og relevant rapportering er altafgørende, da bestyrelsen ikke kan udfylde sin tilsynsopgave uden at forstå de potentielle trusler og risici.

Bestyrelsen bør tænke rapporteringen ind i sit årshjul. Et eksempel på hvordan dette kan gøres er vist i Bilag 2.

Den specifikke rapportering, bestyrelsen bør modtage, og hvor ofte, er delvist afhængig af den enkelte virksomhed.

Der findes ikke en standard for rapportering på cyber- og informations-sikkerhedsområdet, som der f.eks. gør for finansiel rapportering, og rapporteringen kan nemt blive subjektiv.

Det er derfor vigtigt, at bestyrelsen beder om en konsistent rapportering, og at bestyrelsen får information nok til at forstå, hvad der ligger bag det, der rapporteres, og hvordan det stemmer med den overordnede cyberstrategi.

Til at vurdere, om bestyrelsen modtager tilstrækkelig information, kan listen til højre være til inspiration.

Ifølge PwC 2019 Annual Corporate Directors Survey svarede 66 % af respondenterne, at bestyrelsen modtager meningsfuld rapportering på cyberområdet.

Centrale overvejelser i et bestyrelseslokale

Rapportering

- Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed fra direktionen, f.eks. om:
  - Top 5-10 væsentligste cyberrisici samt udvikling/trends siden sidst
  - Resultater fra test af beredskabsplaner og kritiske systemer
  - Sikkerhedshændelser og konsekvenser heraf
  - Status på implementering af sikkerhedstiltag
  - Eventuelle fravigelser fra de af bestyrelsen fastsatte risikotolerancer
  - Resultater fra interne og eksterne audits
  - Sikkerhedsbudget og sammenligning med markedet
  - Forsikringer og hvilke udgifter/tab de dækker ved et cyberangreb
  - Anbefalinger til forbedringer og investeringer forbundet hermed

Årshjul

- Har bestyrelsen implementeret cybersikkerhed som en fast del af et årshjul, der sikrer opfølgning og kontrol som en fast del af bestyrelsens arbejde, og sikrer rette rapportering i rette tid?
- Et eksempel på et årshjul med cyberaktiviteter er vist i Bilag 2.

Audit og revision (på sikkerhed)

- Får virksomheden udarbejdet revisorerklæringer i forhold til it sikkerhed, f.eks. ISAE3402 eller ISAE3000?
- Stiller virksomheden krav om, at dets kunder eller leverandører får udarbejdet disse erklæringer?
- Er der findings fra disse audits, og hvis ja, en plan for udbedring?

Tilsynsmyndigheder

- Er virksomheden i en branche eller sektor, der kræver løbende dialog og forventningsafstemning med nationale myndigheder (f.eks. virksomheder der leverer kritisk infrastruktur)?
- Har virksomheden en proces for opbevaring og gennemgang af data til brug for eventuelle tilsynsbesøg?

6. Værktøjskasse

Tema 5 – Kultur og mennesker

Strategier og planer er én ting, men hvis de ikke følges af ledelse og medarbejdere, er man lige vidt. Medarbejderne er én af de vigtigste kilder til et højt sikkerhedsniveau, da der ikke skal mere end én uopmærksom medarbejder til at trykke på et forkert link.

Der er et behov for træning og awareness programmer for medarbejderne i danske virksomheder, både i forhold til at dele viden, øge viden og ændre adfærd.

Den eksplosive vækst i phishing-mails, malware og ransomware, der er rettet mod ledelse og medarbejdere, stiller ikke bare store krav til virksomhedens sikkerhedsforanstaltninger men også til den digitale adfærd.

Det kan synes banalt, men for hackere er det meget nemmere at komme ind via (dårlige) IT-vaner, end at skulle hacke sig ind via den "digitale hoveddør".

Der er behov for, at bestyrelsen går forrest i at støtte op om en kultur i virksomheden, hvor sikkerhed kan diskuteres åbent, hvor medarbejderne kan rapportere fejltagelser og brud på sikkerheden, og hvor man lærer af sine fejl.

Arbejdet med awareness kan foregå på forskellige niveauer, f.eks. i form af at dele viden internt, øge kendskab/viden og ændre adfærd.

Som forberedelse til at sparre med og udfordre direktionen indenfor digital adfærd, kan listen til højre til være til inspiration.

Ifølge PwC 2019 Cybercrime Survey udgør ansattes/insideres ubevidste handlinger fortsat den største cybertrussel. 54% af respondenterne angav, at virksomheden rent faktisk testede sine medarbejdere i awarenesstræning mv.

Centrale overvejelser i et bestyrelseslokale

- **Uddannelse, træning og awareness**
- Er der et træningsprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- Er der et uddannelsesprogram for, at medlemmer af bestyrelse, direktionen og medarbejdere løbende modtager uddannelse i cyberrisici, f.eks. gennem deltagelse i eksterne arrangementer, konferencer og seminarer med fokus på cyberrisiko, cyberkriminalitet, og trends og udvikling indenfor virksomhedens branche?

Nøglepersoner

- Baggrundstjekker virksomheden nøglepersoner ved ansættelse?
- Modtager nøglepersoner målrettet træning og uddannelse indenfor cybersikkerhed?
- Er der er specifikt cybersikkerheds awareness program for nøglepersoner eller personer med kritiske funktioner, f.eks. en rejsepolitik I relation til bestemte lande eller en politik for nøglepersoners brug af sociale medier, BYOD (bring your own device)?

Kultur og videndeling

- 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 for at drage fordel af the ‘wisdom of the crowd’ indenfor forebyggelse?
- Benytter den IT ansvarlige sig af netværk og eksterne samarbejder, der kan styrke viden og kompetencer?
- Understøtter ledelsen en positiv sikkerhedskultur, f.eks. ved løbende at informere om cybersikkerhedsstrategien, typen af trusler, og hvordan virksomheden er beskyttet?

6. Værktøjskasse

Tema 6 – Kompetencer og organisering

Bestyrelsesmedlemmer forventes i dag at være i stand til at forholde sig til væsentlige forhold i relation til virksomhedens sikkerhed, og at kunne medvirke til at stille spørgsmål til direktionen og forholde sig til svarene.

Bestyrelen behøver ikke kende cyber- og informationssikkerhed i detaljer, men mindst ét medlem bør have indsigt i virksomhedens tekniske og sikkerheds-mæssige fundament og være i stand til at sparre på lige fod med direktionen.

Cyber- og informationssikkerhed er for vigtigt og komplekst til, at forståelsen ligger hos få hænder, og IT er for kritisk og risikoen for stor til, at bestyrelsen ikke holder sig tæt på området.

Bestyrelsen er i sidste ende ansvarlig for at sikre, at de rette kompetencer er til stede i bestyrelsen og virksomheden – uanset uddelegering og outsourcing.

Indtil de rette kompetencer er til stede, må bestyrelsen sikre sig, at både bestyrelsen, ledelsen og organisationen faktisk har eller har adgang til de nødvendige kompetencer og ressourcer på cyberområdet – om nødvendigt gennem aftaler med eksterne samarbejdspartner og specialister.

Til at vurdere om de rette kompetencer og rolledeling er på plads, kan bestyrelsen bruge listen til højre til inspiration.

Ifølge PwC 2019 Annual Corporate Directors Survey svarede 36 % af respondenterne, at bestyrelsen havde tilstrækkelige kompetencer på cyberområdet.

Centrale overvejelser i et bestyrelseslokale

Bestyrelsen

- Har mindst ét bestyrelsesmedlem kompetencer og erfaring med cyber- og informationssikkerhed, f.eks. cybersikkerheds- og risikovurderingsprocesser, leverandørstyring, sikkerhedskrav og lignende?
- Er cybersikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- Holder bestyrelsen sig løbende orienteret om de cybertrusler og aktører, der truer virksomheden, deres metoder og motivation?
- Deltager bestyrelsen aktivt i diskussioner om cybersikkerhed?
- Modtager bestyrelsen løbende træning og uddannelse i cybersikkerhed?
- Er bestyrelsen opmærksom på, at den selv kan være et oplagt mål for cyberangreb (f.eks. CEO fraud)?

Direktionen

- Har virksomheden en sikkerhedsorganisation forankret på direktionsniveau, f.eks. CEO, CFO eller CIO?
- Rapporterer denne funktion direkte til bestyrelsen eller gennem en anden rapporteringsproces?

Organisationen

- Hvor i organisationen (person/funktion) ligger ansvaret i øvrigt for cyber- og informationssikkerhed?
- Bør andre forretningsområder involveres i arbejdet med cybersikkerhed, f.eks. ledere af afdelinger, der udvikler vores produkter og services?
- Hvem rapporterer denne sikkerhedsfunktion til?
- Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?

Eksterne

- Har virksomheden de rette tekniske kompetencer inhouse eller er der behov for ekstern hjælp?
- Har bestyrelsen brug for hjælp til tilsynsopgaven fra rådgivere eller en komité?
- Kan bestyrelsen have gavn af at få eksterne eksperter til at præsentere trends og best practices for at give cybersikkerhed et ekstra perspektiv?

Bilag 1. Ordliste – eksempler på udvalgte ord og begreber inden for cybersikkerhed

Botnet: Et botnet er et netværk af kompromitterede computere, der styres af en tredjepart. Et botnet bliver skabt ved, at computere med internetadgang bliver inficeret med malware, hvorefter den, der kontrollerer botnettet, kan anvende det til f.eks. at udføre DDoS-angreb, phishing-angreb (spam), distribuere malware, mine bitcoins osv.

CEO fraud: "Direktørbedrageri" der går ud på at franarre en virksomhed oplysninger eller udbetale penge ved at udgive sig som direktør af virksomheden. Anvender ofte (spear)phishing-teknikker (f.eks. e-mail) og social engineering.

DDoS-angreb: Står for Distributed Denial of Service og er et overbelastningsangreb. Hackere udnytter kompromitterede computere (et botnet) til at generere usædvanligt store mængder datatrafik mod en hjemmeside (webserver) eller et netværk, så hjemmesiden eller netværket ikke er tilgængeligt for legitim trafik, mens angrebet står på.

Drive-by exploits: Et udtryk for, at den ramte virksomhed ikke var målet for kampagnen, men blot blev ramt ved et hændeligt uheld.

Malware: Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting der, hvor de er installeret. Begrebet dækker over alle kategorier af skadelige programmer herunder virus og orme som f.eks. spyware, ransomware, botnets og trojanske heste. Antivirusprogrammer bekæmper som oftest ikke kun vira, men flere forskellige typer malware.

Man-in-the-middle: Angreb, hvor en skadelig enhed eller person placerer sig mellem to enheder, eksempelvis mellem brugeren og routeren. Dermed får mellemmanden adgang til al data, brugeren afsender.

Mass interception: Massiv overvågning af tele- og internetaktivitet, eksempelvis gennem logning af internetsessioner. Udføres af stater, men kan også ved hjælp af en ekstensive netværk af overvågningsprogrammer bruges af it-kriminelle til at indhente enorme mængder data om adfærd.

Phishing/spear phishing: Phishing er forsøg på via social engineering at manipulere en person til i god tro at videregive personlige oplysninger eller klikke på inficerede filer eller links til falske hjemmesider. Phishing-mails sendes ofte bredt ud til mange modtagere. Spear phishing adskiller sig særligt ved at være målrettet den enkelte modtager og anvende teknikker fra social engineering. E-mails er typisk udformet, så de virker særligt relevante, overbeisende og troværdige for modtageren ved f.eks. at anvende navn, personspecifikke informationer eller relevante filer, der er opdaget ved forudgående rekognoscering.

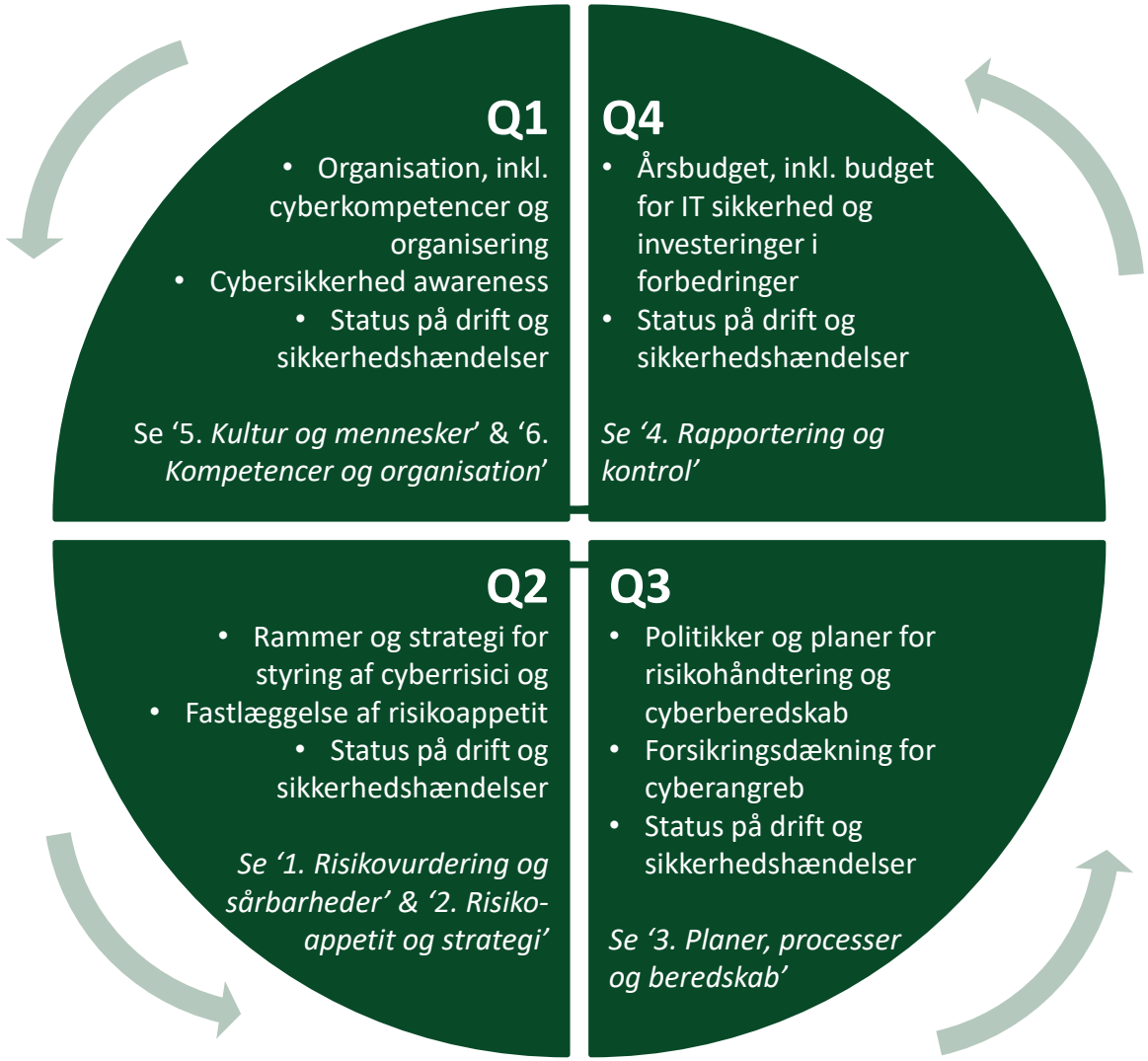
Ransomware-angreb: Ved et ransomware-angreb bliver data og systemer på offerets computer holdt som gidsel, da de krypteres og derved bliver utilgængelige. Den ansvarelige bag angrebet kræver en løsesum typisk i form af kryptovaluta (f.eks. Bitcoin), for at give adgang til data igen. Som regel vil den ansvarlige bag angrebet installere malware ved hjælp af phishingmails. De fleste ransomware-angreb lykkes, fordi brugeren snydes til at klikke på et link eller en vedhæftet fil i en e-mail, men ransomware-angreb kan også ske via sms eller et reklamebanner på en hjemmeside. Der findes mange varianter af ransomware. Målrettede ransomwareangreb forsøger at ramme f.eks. administrative netværk i specifikke virksomheder og myndigheder.

Social engineering: Et udtryk for, at man udnytter sociale interaktioner og psykiske kneb til at narre en person eller en virksomhed til at udlevere informationer, give adgang til systemer eller overføre penge til dem.

SQL injection: Angreb rettet mod databaselaget i software, som udnytter en sårbarhed i håndtering af input og databasekald. Databasekaldet manipuleres gennem inputtet (typisk ved brug af specialtegn) til at opnå en anden effekt end den tilsigtede - for eksempel at afsløre, hvem der har administratorrettigheder.

Der findes forskellige definitioner af centrale begreber inden for cyber- og informationssikkerhed. Udvalgte begreber fremgår i dette bilag.
Mere information kan bl.a. findes i CFCS's dynamiske ordliste her: https://fe-ddis.dk/CFCS/PUBLIKATIONER/ORDFORKLARING/Pages/default.aspx

Bilag 2. Årshjul – Eksempel på cyber-delen



Bilag 3. Tjekliste til centrale overvejelser i et bestyrelseslokale

Sammenfatning af spørgsmålene i punkt 6, tema 1-6

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 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?
- ❑ 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?

4. Rapportering og kontrol

- ❑ Modtager bestyrelsen med faste intervaller rapporter om virksomhedens cybersikkerhed (risici, status, investeringer, anbefalinger mv.) fra direktionen?
- ❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af et 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 positiv sikkerhedskultur?

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?
- ❑ Er cyber- og informationssikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ 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?
- ❑ Hvem rapporterer denne sikkerhedsfunktion til?
- ❑ 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 ekstern hjælp?

Bilag 4. Referencer og baggrundsmateriale

Center for Cybersikkerhed	> Cyberforsvar der virker: (https://fe-ddis.dk/cfcs/publikationer/Documents/Cyberforsvar%20der%20virker%20-%202017_110117.pdf) > CFCS: Ordforklaringer: (https://fe-ddis.dk/CFCS/PUBLIKATIONER/ORDFORKLARING/Pages/default.aspx) > CFCS: Cybertruslen mod Danmark: (https://fe-ddis.dk/cfcs/publikationer/trusselsvurderinger/Pages/default.aspx)
Deloitte	> Cyber Risk Landscape Report 2019: (https://cyber.deloitte.dk/artikler/artikler-it-sikkerhed/cyber-risk-landscape-report-2019/)
Digitaliseringsstyrelsen	> Sikkerdigital.dk (https://sikkerdigital.dk/virksomhed/) > Vejledning i it-risikostyring og vurdering: (https://sikkerdigital.dk/media/10382/vejledning-it-risikostyring-og-vurdering.pdf)
Erhvervsstyrelsen	> Styrket digital sikkerhed i virksomhederne: (https://erhvervsstyrelsen.dk/styrket-it-sikkerhed-i-virksomhederne)
IBM	> IBM X-Force Threat Intelligence Index 2019 (https://www.ibm.com/security/data-breach/threat-intelligence)
Industriens Fond	> Projekt for Styrkelse af Strategiske Cyberkompetencer: (https://www.industriensfond.dk/Styrkelse-af-Strategiske-Cyberkompetencer)
National Cyber Security Centre (UK)	> Board Toolkit (https://s3.eu-west-1.amazonaws.com/ncsc-content/files/board_toolkit_final.pdf)
PwC	> Hvordan kan din bestyrelse være effektiv i håndteringen af cyberrisici? (https://www.pwc.dk/da/nyt/publikationer/bestyrelseshaandbogen-2019/bestyrelse-haandteringen-af-cyberrisici.html) > 2018 Global State of Information Security: (https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html) > 2019 Annual Corporate Directors Survey: (https://www.pwc.com/us/en/services/governance-insights-center/assets/pwc-2019-annual-corporate-directors-survey-full-report-v2.pdf.pdf) > 2019 Cybercrime Survey: https://www.pwc.dk/da/publikationer/2019/11/cybercrime-survey-2019.html
World Economic Forum	> Advancing Cyber Resilience Principles and Tools for Boards: (http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf) > Ten Ways the C-Suite Can Protect their Company against Cyberattack: (https://www.weforum.org/press/2019/10/ten-ways-the-c-suite-can-protect-their-company-against-cyberattack/)