Cybersikkerhed i bestyrelser

Få gode råd til at opnå et højere niveau af cybersikkerhed

Ruslands invasion af Ukraine har skabt et fornyet trusselsbillede i Vesten, og Center for Cybersikkerhed har senest i januar 2023 hævet trusselsniveauet for cyberaktivisme som følge af krigen. I seneste årlige vurdering af truslerne mod Danmark vurderer Forsvarets Efterretningstjeneste desuden, at cyberkriminalitet og cyberspionage udgør alvorlige trusler mod det danske samfund. De alvorligste cybertrusler mod Danmark kommer fra russisk og kinesisk cyberspionage og fra cyberkriminalitet, der er udført af organiserede kriminelle netværk i udlandet.

I **PwC's Cybercrime Survey 2022** angiver hele 73 % af de adspurgte, heriblandt både repræsentanter fra ledelse og fagfolk, at deres stigende bekymring for cybertrusler i nogen eller høj grad skyldes konflikten mellem Rusland og Vesten.

Organiserede kriminelle anses fortsat for at være blandt de største cybertrusler. De cyberkriminelle udvikler i stigende grad deres kompetencer og begynder at tage nye angrebsmetoder i brug. Derfor er cybersikkerhed et anliggende for virksomhedens bestyrelse, som har ansvaret for at vurdere virksomhedens risici og beslutte på hvilket niveau, virksomheden skal beskytte sig mod cybertrusler.

Rapporten Cybercrime Survey 2022 er baseret på svar fra flere end 500 ledere og fagfolk. Denne artikel er baseret på besvarelserne fra de 64 bestyrelsesmedlemmer, der deltog i undersøgelsen. De har svaret på spørgsmål målrettet bestyrelsesmedlemmer.

Det er bestyrelsens ansvar at sikre værdiskabelse og konkurrenceevne samt at beskytte virksomhedens værdier både på kort og lang sigt (jf. selskabslovens § 115). Bestyrelsen er ansvarlig for virksomhedens strategi og for at følge op på strategien. Dette gælder også, når det kommer til cybersikkerhed, da en cyberhændelse i værste fald kan påvirke såvel virksomhedens bundlinje som evnen til at nå strategiske mål.

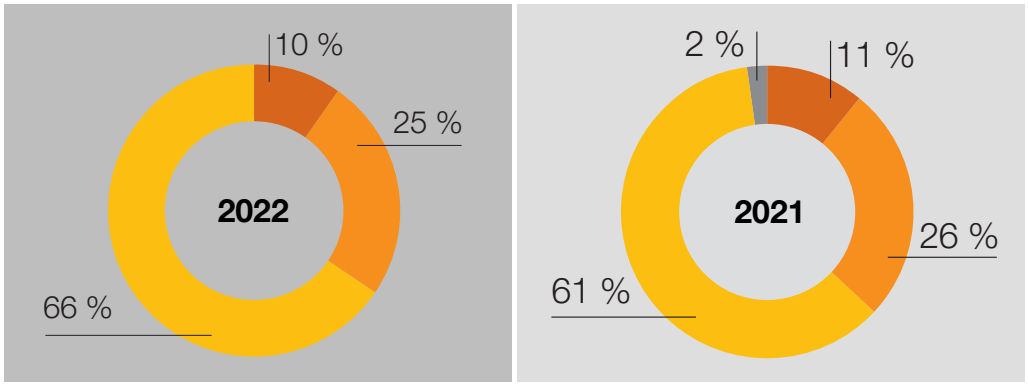
> Vores kunder bruger mere og mere energi på at sikre sig, at dem, de samarbejder med, har styr på interne kontroller samt de erklæringer, der er krav på. Nogle af vores største kunder forlanger, at der er styr på det."
>
> Rikke Stampe Skov, CEO i Impero og bestyrelsesmedlem i Penneo

Data fra PwC's Cybercrime Survey 2022 indikerer altså, at der er en direkte relation mellem niveauet af cybersikkerhed og virksomhedens omsætning. Dette understøttes af Rikke Stampe Skov, CEO i Impero og bestyrelsesmedlem i Penneo. Rikke Stampe Skov udtaler sig om, hvorvidt hun kan mærke et øget fokus på it-sikkerhed internt såvel som eksternt for virksomhederne: *"Vores kunder bruger mere og mere energi på at sikre sig, at dem de samarbejder med har styr på interne kontroller samt de erklæringer, der er krav på. Nogle af vores største kunder forlanger, at der er styr på det."*

Behov for cybertræning og uddannelse målrettet bestyrelser

PwC's Cybercrime Survey 2022 viser, at kun 10 % af bestyrelsesmedlemmerne modtager træning i cyber- og informationssikkerhed. Dette billede er stort set uændret sammenlignet med 2021, og der er ligesom sidste år plads til forbedring.

Modtager bestyrelsen træning i cyber- og informationssikkerhed?

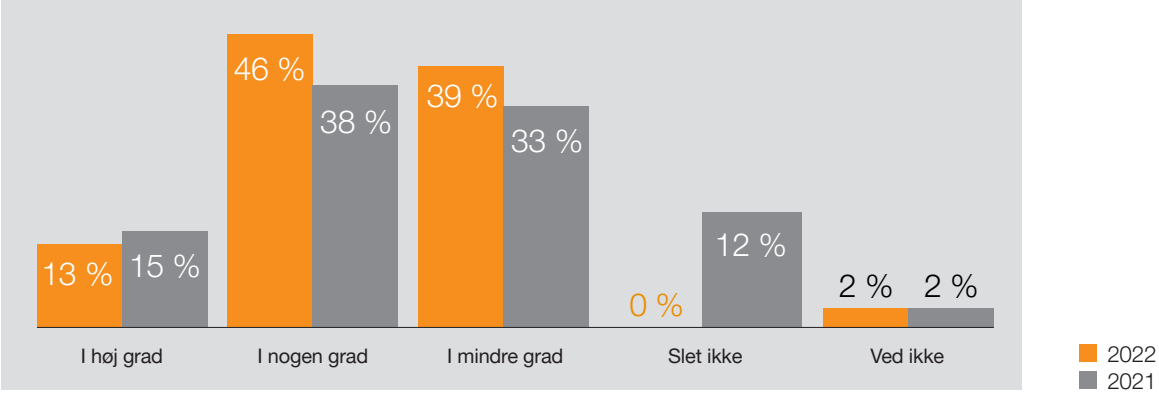


> Det er afgørende at have den nødvendige viden og kompetenceprofil for at definere en specifik risiko, politik og kultur, så det reelt afspejles i den operationelle hverdag. Hvis kompetencerne ikke findes internt, eller man er i tvivl om best practice, så er det oplagt at få eksperter ind og bistå."
>
> Ulrik Ross, CEO og bestyrelsesformand

Samtidig viser undersøgelsen, at 39 % vurderer, at sammensætningen af bestyrelsens kompetencer i mindre grad eller slet ikke giver dyb nok viden om cyber- og informationssikkerhed, hvoraf dette tal var 45 % i 2021. Der er dermed sket en forbedring sammenlignet med sidste år hvad angår sammensætningen af bestyrelsens kompetencer.

Bestyrelsesmedlemmers viden om cyber- og informationssikkerhed kan forbedres ved at sætte cyber- og informationssikkerhed højere på agendaen og ved at få inspiration fra eksterne parter. Vigtigheden i forståelsen af eget kompetenceniveau bekræftes af Ulrik Ross, CEO og bestyrelsesformand i den finansielle sektor, der som privatperson udtaler følgende: *"Det er afgørende at have den nødvendige viden og kompetenceprofil for at definere en specifik risiko, politik og kultur, så det reelt afspejles i den operationelle hverdag. Hvis kompetencerne ikke findes internt, eller man er i tvivl om best practice, så er det oplagt at få eksperter ind og bistå."*

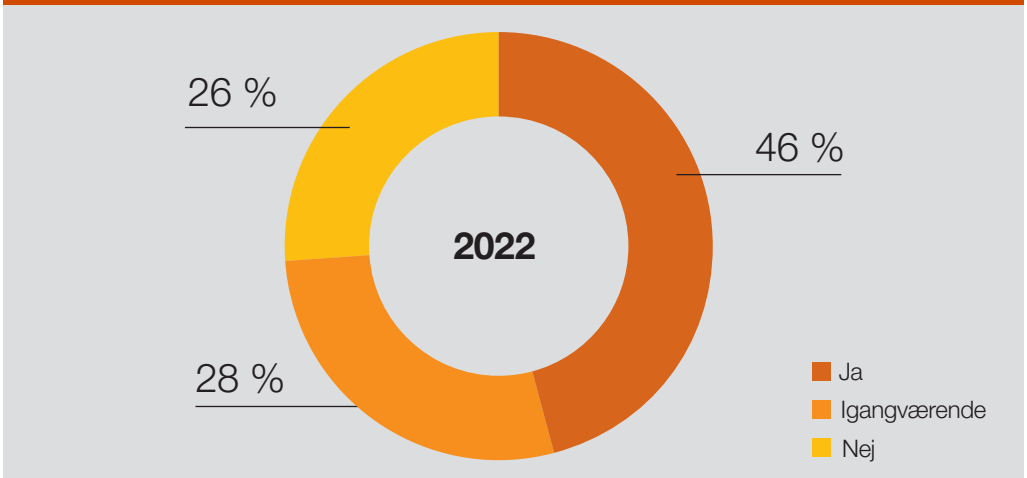
I hvilken grad vurderer du, at sammensætningen af bestyrelsens kompetencer giver dyb nok viden om cyber- og informationssikkerhed?



Behov for en styrket indsats i bestyrelsesarbejdet

PwC har spurgt bestyrelsesmedlemmer, om deres virksomhed har etableret en længerevarende handlingsplan/et program for cyberområdet*. Næsten halvdelen (46 %) af bestyrelsesmedlemmerne angiver, at deres virksomhed har etableret en plan/et program, mens 28 % er i gang med at etablere dette. 26 % har ikke en plan/et program og er ikke gået i gang med dette. Ifølge undersøgelsen er cybersikkerhed i stigende grad en tilbagevendende del af bestyrelsesarbejdet. Men selvom der er fremgang at spore, er der fortsat mange virksomheder, hvor der ikke er tilstrækkelig styring på området.

Har din virksomhed etableret en længerevarende handlingsplan/et program for cyberområdet*?



Trods den øgede indsats i bestyrelsesarbejdet understreger Rikke Stampe Skov det centrale i erfaring fra tidligere angreb, når bestyrelsen skal tage stilling til cyberrisici. I den forbindelse udtaler Rikke Stampe Skov: *"Man kan ikke som bestyrelse negligere tidligere angreb; derfor skal virksomheden forholde sig til de risici, der eksisterer for virksomheden."*

* Definition:

En længerevarende handlingsplan/et program for cyberområdet defineres som et sæt af dokumenterede aktiviteter, der over en periode bringer virksomhedens cybersikkerhed op på et acceptabelt niveau.

> Man kan ikke som bestyrelse negligere tidligere angreb; derfor skal virksomheden forholde sig til de risici, der eksisterer for virksomheden."
>
> Rikke Stampe Skov, CEO i Impero og bestyrelsesmedlem i Penneo

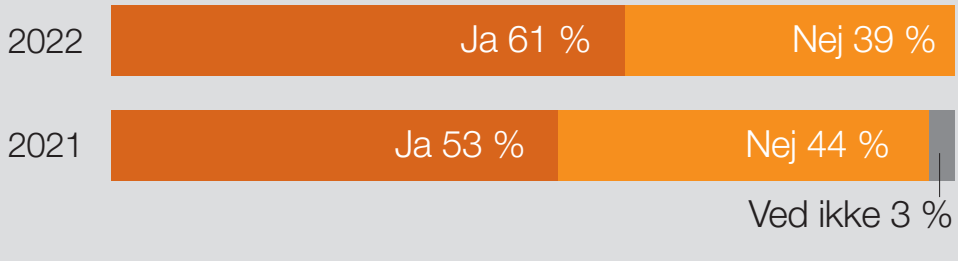
> It-direktøren besøger os to gange årligt med henblik på at kigge ind i opgaven om at minimere risici. Sideløbende modtager vi ekstern rapportering med det formål at belyse kritiske punkter. Bestyrelsens opgave efterfølgende er at holde rapporten op imod de interne processer."
>
> Kim Frimer, Bestyrelsesmedlem i logistikvirksomheden Frode Laursen A/S

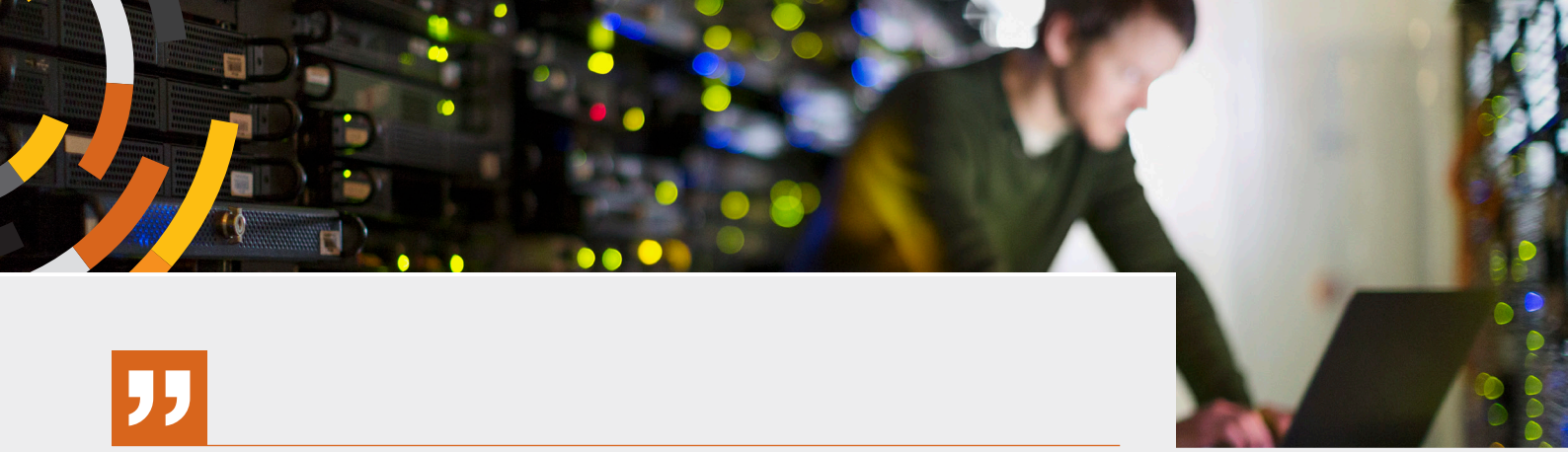
Desuden svarer 39 % af bestyrelsesmedlemmerne, at de ikke har cybersikkerhed som en fast del af årshjulet, mens 61 % angiver, at de har. Årshjulet er med til at sikre, at cybersikkerhed prioriteres og er på virksomhedens agenda. Vi ser en lille forbedring sammenlignet med sidste år.

Denne vigtige fremgang bekræftes af Kim Frimer, bestyrelsesmedlem i logistikvirksomheden Frode Laursen A/S, der både er i dialog med it-direktører og samtidig benytter rapportering fra eksterne partnere som udtaler: *"It-direktøren besøger os to gange årligt med henblik på at kigge ind i opgaven om at minimere risici. Sideløbende modtager vi ekstern rapportering med det formål at belyse kritiske punkter. Bestyrelsens opgave efterfølgende er at holde rapporten op imod de interne processer."*

På den måde bliver cybersikkerhed prioriteret som en fast del af årshjulet med optimal kommunikation internt såvel som eksternt.

Har bestyrelsen cybersikkerhed som en fast del af sit årshjul?





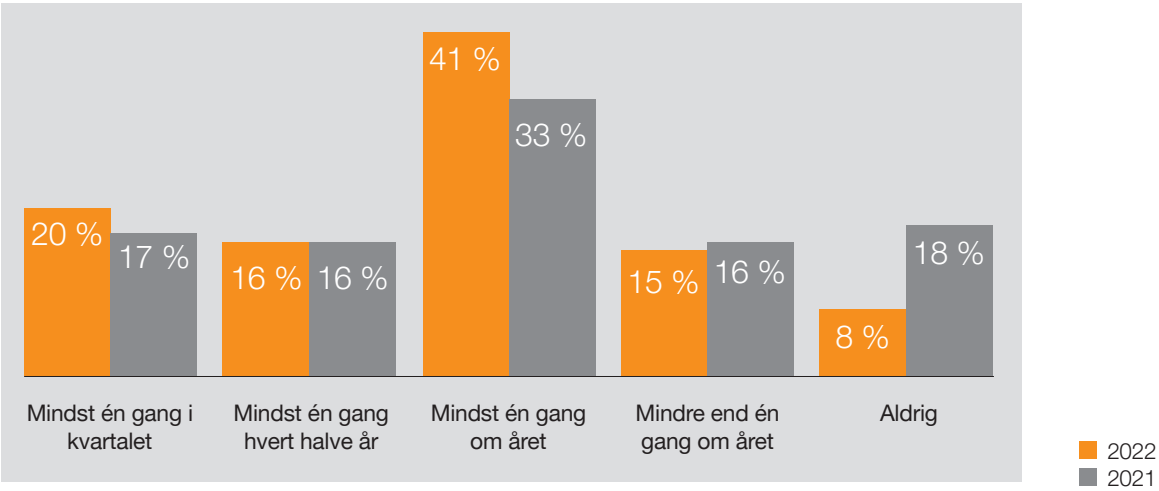
I bund og grund så er cybersikkerhed et område, der hele tiden udvikler sig. Vi bliver mere digitale, og derfor bliver vi mere eksponeret."

Anders K. Bønding, Bestyrelsesmedlem i Sanistål

Behov for sikkerhedsrapportering og kontrol

Når bestyrelsesmedlemmer bliver spurgt til håndtering af information af cyberrisici, angiver 23 % af bestyrelsesmedlemmerne, at de mindre end én gang om året eller aldrig behandler information om cyberrisici. Der er sket en lille forbedring sammenlignet med sidste år vedrørende behandling af information om cyberrisici. Den stigende digitalisering i den operationelle hverdag, og det deraf følgende dynamiske trusselsbillede, betyder, at virksomheder bliver mere eksponeret. Dette understreges af Anders K. Bønding, bestyrelsesformand i Sanistål, der udtaler: *"I bund og grund så er cybersikkerhed et område, der hele tiden udvikler sig. Vi bliver mere digitale, og derfor bliver vi mere eksponeret."*

Hvor ofte modtager og behandler bestyrelsen information om cyberrisici?



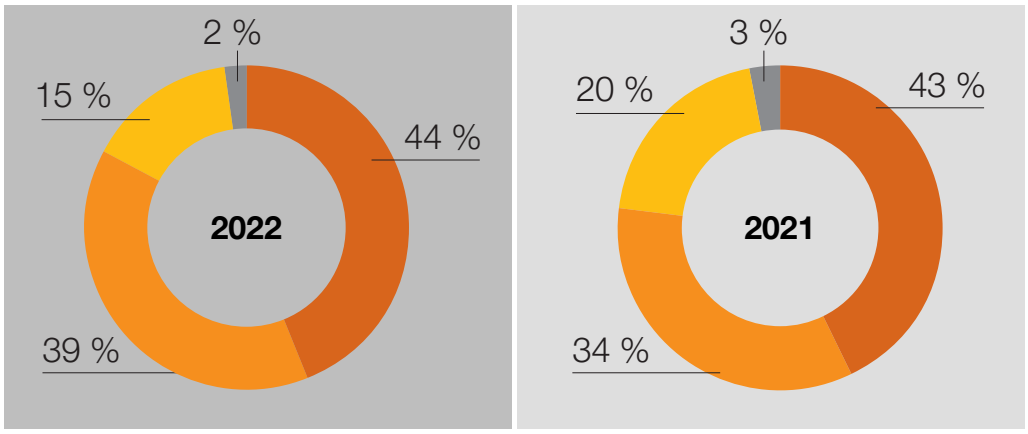
Cyberrisiko er en megatrend, som bestyrelsen skal forholde sig til. Det er vigtigt, at virksomheder forstår, at cyberrisici er et bestyrelsesansvar og ikke isoleret hører til i en it- eller finansafdeling."

Ulrik Ross, CEO og bestyrelsesformand

54 % af bestyrelsesmedlemmerne angiver, at de ikke/kun delvist fører kontrol med, at virksomheden har testede beredskabsplaner i tilfælde af hændelser. Ulrik Ross udtaler: *"Cyberrisiko er en megatrend, som bestyrelsen skal forholde sig til. Det er vigtigt, at virksomheder forstår, at cyberrisici er et bestyrelsesansvar og ikke isoleret hører til i en it- eller finansafdeling."*

Behandling af information om cyberrisici og kontrol med, at beredskabsplaner er testede, skal bidrage til, at bestyrelsen kan tage stilling til virksomhedens risikoappetit og evne til at håndtere cyberhændelser. Disse tal er delvist uændret sammenlignet med besvarelser i 2021.

Fører bestyrelsen kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering i tilfælde af hackerangreb, strømnedbrud mv.?

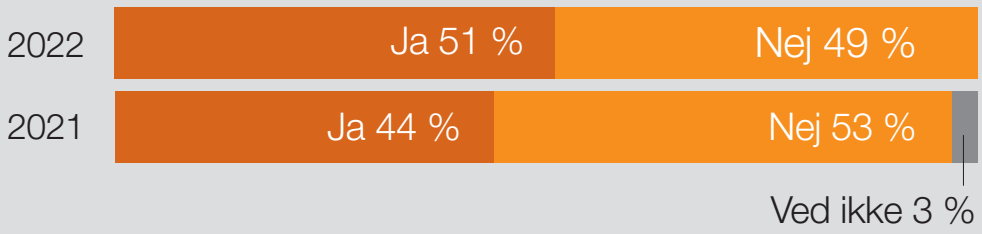


Et tilstrækkeligt videngrundlag er forudsætningen for, at bestyrelsen kan håndtere virksomhedens cybersikkerhed hensigtsmæssigt. Alligevel er det kun halvdelen (51 %) af bestyrelsesmedlemmerne, som angiver, at de mindst én gang om året modtager en an-

> Lad være med at undervurdere cybertruslen. Rapportering skal bruges til at forstå, hvad der kan ske, og hvor meget skade det giver."
>
> Kim Frimer, Bestyrelsesmedlem i logistikvirksomheden Frode Laursen A/S

vendelig rapport vedrørende cybersikkerhed. Vi ser en lille fremgang sammenlignet med sidste år. Et nøgleord i forbindelse med rapportering er anvendelighed. Kim Frimer kommenterer: *"Lad være med at undervurdere cybertruslen. Rapportering skal bruges til at forstå, hvad der kan ske, og hvor meget skade det giver."*

Modtager bestyrelsen mindst én gang årligt en anvendelig rapport vedrørende cybersikkerhed?



I forbindelse med anvendelighed af en rapport vedrørende cybersikkerhed udtaler Ulrik Ross følgende: *"Der er to sider af en cyberrapport. En officiel side, hvor man kun i grove træk vil ud og fortælle omverdenen om hvilke, sikkerhedssystemer og politikker man benytter grundet sikkerhed. Samtidig en uofficiel side, hvor vi skal have så meget viden som overhovedet muligt for at tage de bedste beslutninger omkring cyberrisici. Det er god kutyme for en bestyrelse at inddrage cyberrisici som en del af årshjulet, hvor man kan certificere it-sikkerhedsniveauet inden for forskellige revisionspraksisser."*

Der eksisterer altså en balance mellem anvendeligheden af og eksekveringen på rapporten, samtidig med at man gerne vil minimere eksponeringen af, hvad man som virksomhed foretager sig.

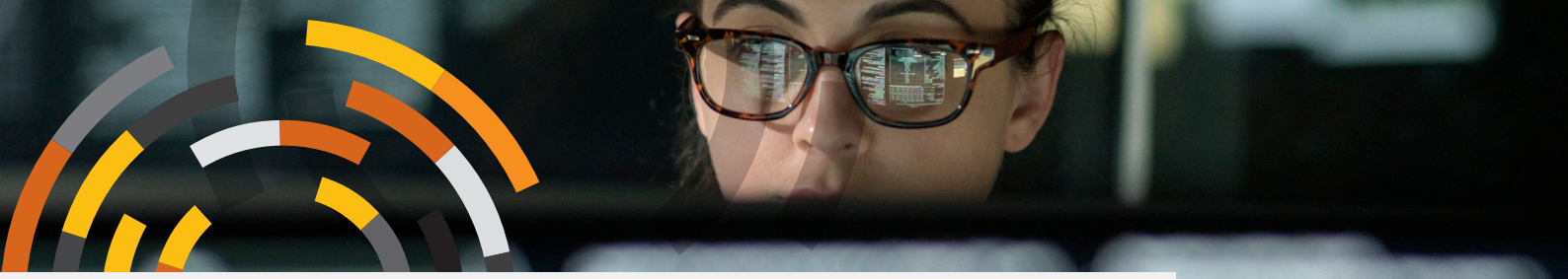
PwC anbefaler

Bestyrelsen bør minimum årligt modtage en risiko- og sårbarhedsvurdering af virksomheden fra direktionen. Desuden bør bestyrelsen minimum årligt tage stilling til virksomhedens risikoappetit. Her godkender bestyrelsen den samlede risikostrategi inklusive de specifikke aktiviteter, som virksomheden ønsker at igangsætte for at forbedre processer, styrke arkitekturen, øge god adfærd, forbedre beredskabet og dermed reducere det samlede risikobillede. Det anbefales desuden, at cybersikkerhed er en fast del af bestyrelsens årshjul, og at det er på agendaen på bestyrelsesmøder. For at opretholde virksomhedens evne til at håndtere konkrete hændelser bør bestyrelsen yderligere mindst én gang om året kontrollere, at virksomhedens beredskabsplaner er opdaterede. Der bør jævnligt gennemføres træningsforløb med fokus på cyber- og informationssikkerhed, som er målrettet bestyrelsesmedlemmer, og som kan styrke deres viden om og kompetencer i relation til cybersikkerhed.

Gode råd

De konkrete valg og metoder afhænger altid af den enkelte virksomhed, men overordnet set er det en god idé, at bestyrelsen:

- sikrer, at virksomheden har et overblik over risici og har igangsat et cyberprogram med rapportering om fremdrift til bestyrelsen
- etablerer et træningsforløb til bestyrelsesmedlemmer i relation til cyber- og informationssikkerhed (fx anbefales det, at mindst ét medlem har relevant viden om eller erfaring med cyber- og informationssikkerhed)
- implementerer cybersikkerhed som en fast del af årshjulet, har cybersikkerhed på agendaen på bestyrelsesmøder og modtager relevant rapportering om cyberhændelser.



Om undersøgelsen

Rapporten Cybercrime Survey 2022 er baseret på svar fra flere end 500 ledere og it-fagfolk. Denne artikel er baseret på besvarelserne fra 64 bestyrelsesmedlemmer, der deltog i undersøgelsen.

I 2022-udgaven af undersøgelsen har de 64 bestyrelsesmedlemmer i Danmark – primært tilhørende den private sektor og SME-segmentet (små og mellemstore virksomheder) – besvaret en række cyberrelaterede spørgsmål. Du kan læse mere om Bestyrelsesforeningens konkrete anbefalinger på **www.bestyrelsesforeningen.dk**.

Undersøgelsen bygger på onlinebesvarelser indsamlet i perioden maj-august 2022. **Læs mere om PwC's Cybercrime Survey 2022**.

PwC har desuden udarbejdet en udførlig CFO-guide, der klæder direktionen på til at oversætte cybertruslen til et relevant risikobillede for forretningen. **Læs den her**.

Kontakt

Kontakt en af PwC's eksperter for en dialog om resultaterne af denne undersøgelse eller en uforpligtende snak om dine konkrete udfordringer og behov. Du kan også læse mere om vores ydelser inden for cyber- og informationssikkerhed på **www.pwc.dk/cyber**.

PwC's eksperter inden for cyber- og informationssikkerhed.

Mads Nørgaard Madsen

Partner
Leder af Technology & Security
T: 2811 1592
M: mads.norgaard.madsen@pwc.com

Peter Brock Madsen

Partner
Cyberrisikostyring
Technology & Security
T: 2056 8505
M: peter.brock.madsen@pwc.com

William Sharp

Partner
Cyber Operationel Technology
Technology & Security
T: 4040 1074
M: william.sharp@pwc.com

Christian Kjær

Partner
Cyberberedskab
Technology & Security
T: 5132 1270
M: christian.kjaer@pwc.com