Cybersikkerhed i bestyrelser

pwc

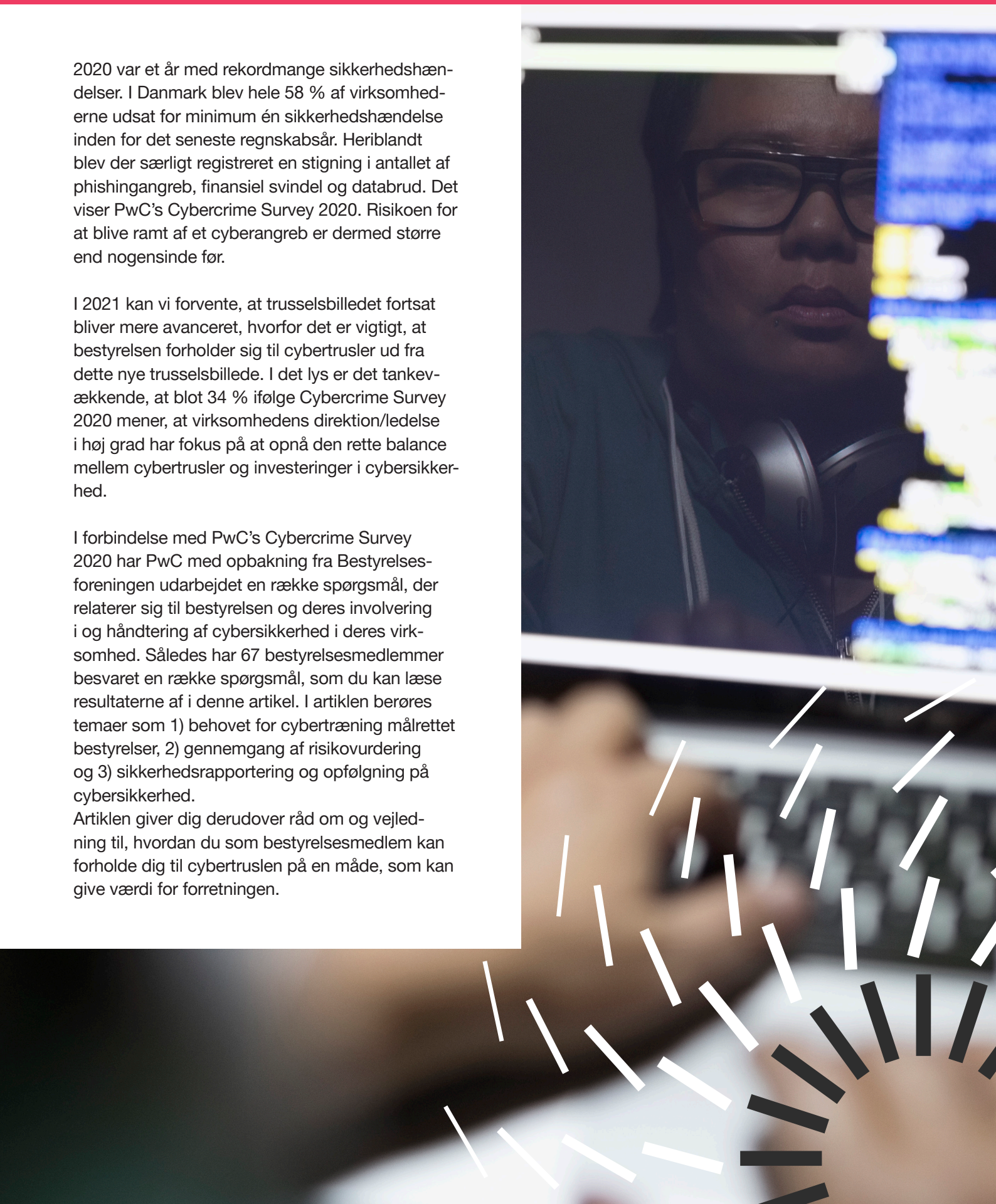
Succes skaber vi sammen ...

Sådan kan du som bestyrelsesmedlem styrke din forretnings cybersikkerhed

2020 var et år med rekordmange sikkerhedshændelser. I Danmark blev hele 58 % af virksomhederne udsat for minimum én sikkerhedshændelse inden for det seneste regnskabsår. Heriblandt blev der særligt registreret en stigning i antallet af phishingangreb, finansiel svindel og databrud. Det viser PwC's Cybercrime Survey 2020. Risikoen for at blive ramt af et cyberangreb er dermed større end nogensinde før.

I 2021 kan vi forvente, at trusselsbilledet fortsat bliver mere avanceret, hvorfor det er vigtigt, at bestyrelsen forholder sig til cybertrusler ud fra dette nye trusselsbillede. I det lys er det tankevækkende, at blot 34 % ifølge Cybercrime Survey 2020 mener, at virksomhedens direktion/ledelse i høj grad har fokus på at opnå den rette balance mellem cybertrusler og investeringer i cybersikkerhed.

I forbindelse med PwC's Cybercrime Survey 2020 har PwC med opbakning fra Bestyrelsesforeningen udarbejdet en række spørgsmål, der relaterer sig til bestyrelsen og deres involvering i og håndtering af cybersikkerhed i deres virksomhed. Således har 67 bestyrelsesmedlemmer besvaret en række spørgsmål, som du kan læse resultaterne af i denne artikel. I artiklen berøres temaer som 1) behovet for cybertræning målrettet bestyrelser, 2) gennemgang af risikovurdering og 3) sikkerhedsrapportering og opfølgning på cybersikkerhed.
Artiklen giver dig derudover råd om og vejledning til, hvordan du som bestyrelsesmedlem kan forholde dig til cybertruslen på en måde, som kan give værdi for forretningen.

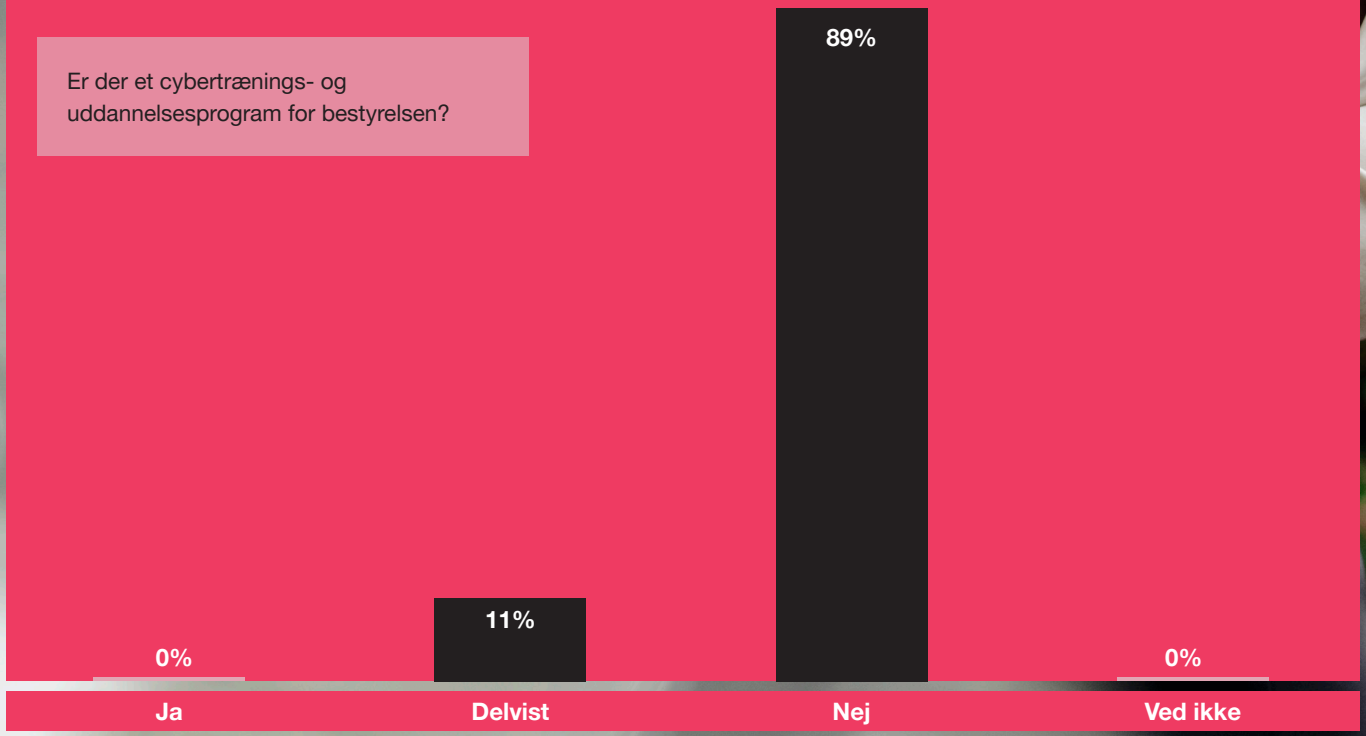


Behov for cybertræning og uddannelse målrettet bestyrelser

I undersøgelsen svarer hele 89 % af bestyrelsesmedlemmerne, at der ikke eksisterer et cybertrænings- og uddannelsesprogram for bestyrelsen. Det er på trods af, at awareness-træning er essentielt i forhold til at skabe en bedre forståelse for digitale trusler og risici i virksomheden, som kan have større eller mindre konsekvenser for virksomheden, kunder eller borgere.

Det er PwC's erfaring, at bestyrelser har behov for og efterspørger oplysning om cybersikkerhed. Vi har i det seneste år foretaget flere cyber-præsentationer, herunder egentlige træningsforløb omkring cyber-beredskab relateret til de hændelsesforløb, som virksomheder skal igennem f.eks. ved et phishing/ransomware-angreb. Den viden, som bestyrelsesmedlemmerne opnår ved disse forløb, sætter dem i stand til at prioritere sikkerhedstiltagene.

Er der et cybertrænings- og uddannelsesprogram for bestyrelsen?

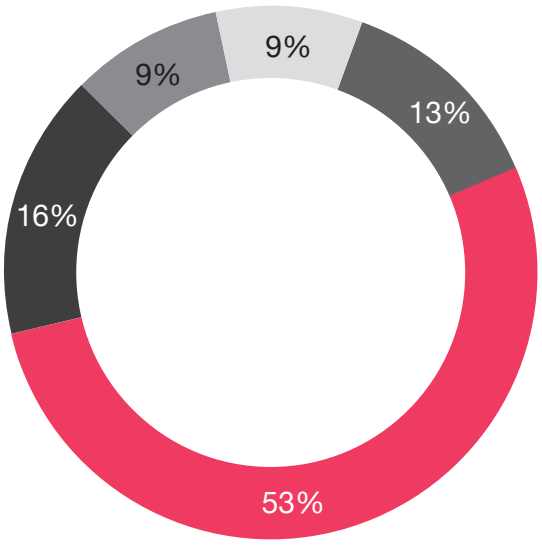


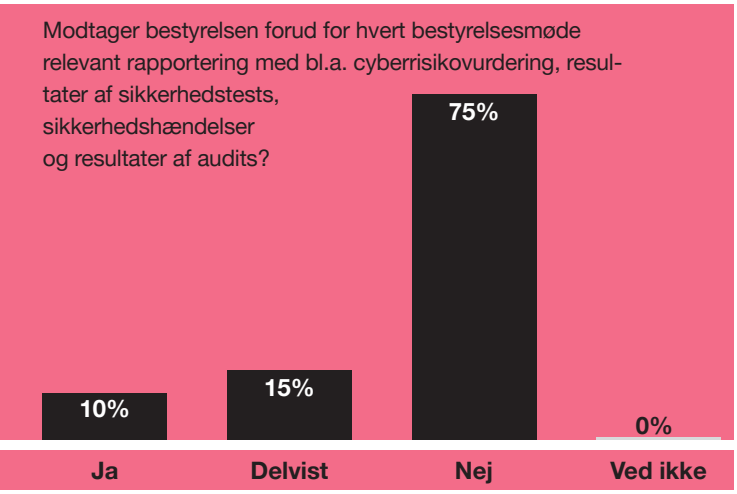
Behov for gennemgang af risikovurdering på cyberområdet

PwC's Cybercrime Survey 2020 har ligeledes undersøgt, hvor ofte bestyrelsen modtager og behandler en opdateret risikovurdering på cyberområdet. Cirka halvdelen af bestyrelsesmedlemmerne (53 %) svarer, at denne proces udføres mindst én gang årligt. Dog svarer hele 25 % at de aldrig eller mindre end én gang om året modtager og behandler en opdateret risikovurdering relateret til cybersikkerhed.

Det er PwC's erfaring, at den rapportering, som mange virksomheder foretager omkring cyber- risici, ofte "drukner" i den almindelige risikorapportering. Cybertruslen udvikler sig hurtigere end mange andre af virksomhedens trusler. Derfor anbefaler PwC, at bestyrelsen sikrer en relevant prioritering af cybertruslen herunder arbejder med en opdateret risikovurdering relateret til cybertrusler for at sikre, at virksomheden løbende forholder sig proaktivt til og prioriterer aktuelle risici relateret til cybersikkerhed.

Hvor ofte modtager og behandler bestyrelsen en opdateret risikovurdering på cyberområdet?



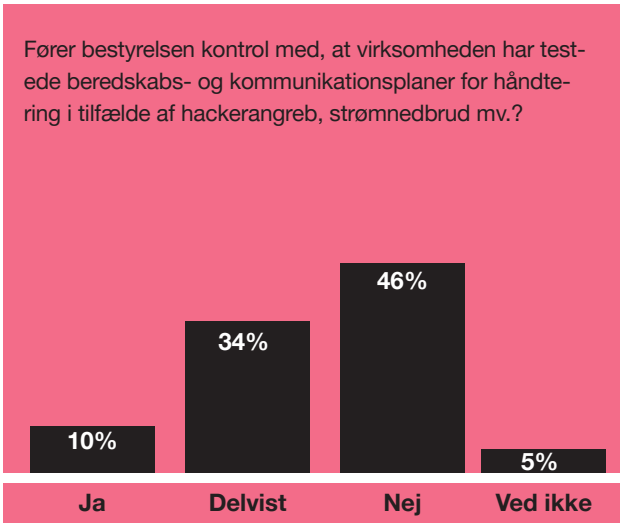


Behov for sikkerhedsrapportering og opfølgning på cybersikkerhed

75 % af bestyrelsesmedlemmerne svarer, at bestyrelsen ikke modtager relevant sikkerhedsrapportering forud for hvert bestyrelsesmøde. Modtagelse af relevant rapportering om blandt andet trusler, risici og hændelser i relation til cybersikkerhed er imidlertid essentielt for at kunne føre tilsyn og kontrol med implementering af cybersikkerhed i virksomhedens processer og politikker.

Størstedelen af bestyrelsesmedlemmerne svarer, at de delvist (46 %) eller slet ikke (15 %) fører kontrol med, at virksomheden har testede beredskabs- og kommunikationsplaner for håndtering af hackerangreb, strømnedbrud mv.

PwC's erfaring er, at mange virksomheder oplever, at cyberhændelser kan få en stor konsekvens på virksomhedens økonomi, image og mulighed for at levere deres services. Det er derfor vores anbefaling, at bestyrelsen modtager rapportering fra direktionen så de i relevant omfang kan følge op på de sikkerhedstiltag der prioriteres og igangsættes, således at de besluttede tiltag har den nødvendige fremdrift.



Opsummering

Når du som bestyrelsesmedlem vil udbygge din viden om cybersikkerhed og aktivt går i gang med at forbedre dig på området, er det vigtigt at være grundigt forberedt på, hvordan det skal foregå. Nedenstående råd og anvisninger er blot tre ud af mange måder, hvorpå man som som bestyrelsesmedlem kan sikre sig, at man er forberedt på cybertruslen.

1. Træningsforløb omkring cyber-beredskab relateret til de hændelsesforløb, som virksomheder skal igennem ved f.eks et phishing/ransomware-angreb, sætter bestyrelsesmedlemmer i stand til at prioritere de rette sikkerhedstiltag.
2. For at sikre, at virksomheden løbende forholder sig proaktivt til og prioriterer aktuelle risici relateret til cybersikkerhed, bør bestyrelsen arbejde med en opdateret risikovurdering relateret til cybertrusler.
3. Bestyrelsen bør følge op på de tiltag, virksomheden planlægger at udføre, og sikre, at de valgte sikkerhedstiltag reelt minimerer risikoen for et cyberangreb, og at de har den nødvendige fremdrift.

Om undersøgelsen

Med opbakning fra Bestyrelsesforeningen har 67 bestyrelsesmedlemmer, primært tilhørende den private sektor og SME-segmentet (små og mellemstore virksomheder), deltaget i PwC's Cybercrime Survey 2020. Respondenterne har besvaret en række spørgsmål, der baserer sig på Bestyrelsesforeningens anbefalinger til styrkelse af cyber-kompetencer i bestyrelser. Du kan læse mere om Bestyrelsesforeningens konkrete anbefalinger her www.bestyrelsesforeningen.dk

Analysen bygger på onlinebesvarelser indsamlet i perioden oktober-december 2020. Læs mere om PwC's Cybercrime Survey 2020 på www.pwc.dk/cybercrime20. 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 www.pwc.dk/cfocyberguide.

Om PwC

I PwC arbejder vi for at styrke tilliden i samfundet og være med til at løse væsentlige problemstillinger. Det gør vi med udgangspunkt i vores viden inden for revision, skat og rådgivning. Vores kunder kommer fra alle dele af erhvervslivet og den offentlige sektor, og vi er ca. 2.500 medarbejdere og partnere, som brænder for at gøre en positiv forskel for kunder og kolleger. Globalt er vi over 280.000 PwC'ere i 155 lande, og i Danmark er vi markedsledende. Mød os over hele landet. Vi er der, hvor du er.

Kontakt

Vi vil meget gerne i dialog med dig om resultaterne af denne undersøgelse. Kontakt en af PwC's eksperter for en uforpligtende snak om dine konkrete udfordringer og behov. Du kan 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
Security & Technology
2811 1592
mads.norgaard.madsen@pwc.com

Jørgen Sørensen
Partner
Security & Technology
2494 5254
jorgen.jgs.sorensen@pwc.com

Christian Kjær
Partner
Security & Technology
3945 3282
christian.kjaer@pwc.com