CYBERBEVEILIGING VOOR KLEINERE ORGANISATIES

CHECKLIST RAAD VAN BESTUUR: LEIDERSCHAP OP HET GEBIED VAN CYBERBEVEILIGING

GRONDBEGINSELEN VAN HET BEHEER VAN CYBERRISICO'S

☐ **Beoordeel als groep periodiek of de raad van bestuur de volgende vragen met 'ja' kan beantwoorden:**

- Voldoet uw organisatie aan de toepasselijke wet- en regelgeving, zoals de AVG?
- Heeft uw organisatie haar cyberblootstellingen gekwantificeerd en haar financiële veerkracht getest?
- Heeft uw organisatie een verbeterplan om te zorgen dat blootstellingen binnen uw afgesproken risicobereidheid vallen?
- Bespreekt de raad van bestuur regelmatig beknopte, duidelijke en bruikbare informatie met betrekking tot de cyberveerkracht van de organisatie die het management heeft aangeleverd?
- Heeft uw organisatie incidentresponsplannen die onlangs zijn geoefend, ook op directieniveau?
- Zijn de rollen van degenen die verantwoordelijk zijn voor het beheer van cyberrisico's duidelijk en in overeenstemming met de drie verdedigingslijnen?
- Beschikt u over een onafhankelijke validatie en waarborg van de beveiligingsmentaliteit van uw organisatie ten aanzien van cyberrisico's, bijvoorbeeld via tests, certificering of verzekering?

☐ **Als u een of meer van de bovenstaande vragen niet met 'ja' kunt beantwoorden, werk dan samen met uw CEO, CISO, relevante medewerkers binnen de organisatie en/of externe bronnen om het probleem te verhelpen.**

TOEZICHT

☐ **Zorg ervoor dat de raad van bestuur zich bewust is van zijn eindverantwoordelijkheid op het gebied van cyberrisico's en veerkracht van uw organisatie.**

☐ **Delegeer toezicht indien nodig aan een specifieke commissie.**

☐ **Wijs één bedrijfsfunctionaris aan, meestal de centrale informatiebeveiligingsfunctionaris (CISO), die verantwoording aflegt over de capaciteit van uw organisatie om cyberveerkracht en vooruitgang bij het implementeren van doelstellingen op het vlak van cyberveerkracht te bewerkstelligen.**

☐ **Ervoor zorgen dat deze functionaris standaard toegang heeft tot de raad en voldoende bevoegdheid, kennis van het onderwerp, ervaring en middelen heeft om deze taken uit te voeren.**

☐ **Bepaal jaarlijks de risicotolerantie van uw organisatie en zorg dat deze is afgestemd op uw bedrijfsstrategie en risicobereidheid.**

☐ **Zorg ervoor dat er jaarlijks een formele, onafhankelijke cyberveerkrachtbeoordeling van uw organisatie wordt uitgevoerd.**

☐ **Integreer cyberveerkracht en risicobeoordeling in de algemene bedrijfsstrategie van uw organisatie, in het risicobeheer, de budgettering en de toewijzing van middelen, met als doel ervoor te zorgen dat cyberrisico's volledig worden meegenomen in het totale operationele risico.**

☐ **Controleer risico's voor derden regelmatig.**

☐ **Houd toezicht op de opzet, de implementatie, het testen en de voortdurende verbetering van de plannen voor cyberveerkracht, zodat uw organisatie op één lijn ligt en uw CISO of een andere verantwoordelijke functionaris regelmatig verslag hierover uitbrengt aan de raad van bestuur.**

☐ **Beoordeel regelmatig uw prestaties op bovenstaande punten en win eventueel onafhankelijk advies voor continue verbetering in.**

OP DE HOOGTE BLIJVEN

- ☐ **Zorg ervoor dat alle leden die toetreden tot de raad beschikken over de juiste en actuele vaardigheden en kennis om de risico's van cyberaanvallen te begrijpen en te beheren.**
- ☐ **Vraag het management regelmatig om advies over de huidige en toekomstige risicoblootstelling van uw organisatie, relevante regelgevingsvereisten, en benchmarks voor risicobereidheid uit de branche en de maatschappij als geheel. Plan om deel te nemen aan:**
  - Regelmatige briefings over taken die voortvloeien uit nieuwe wet- en regelgeving,
  - Gezamenlijke planning en bezoeken aan de raad van bestuur en het uitvoerend comité aan collega's en leiders die beste praktijken in cyberbeveiliging toepassen,
  - Veiligheidsbriefings over de dreigingsomgeving, en
  - Uitwisselingen op directieniveau van informatie over governance en melding.
- ☐ **Herinner het management aan zijn verantwoordelijkheid om een gekwantificeerde en begrijpelijke beoordeling van cyberrisico's, bedreigingen en gebeurtenissen te geven als standaard agendapunt tijdens raadsvergaderingen.**
- ☐ **Neem regelmatig contact op met management en ander relevant personeel over ontwikkelingen in verband met lopende systemische uitdagingen, zoals kwetsbaarheden in de toeleveringsketen, gemeenschappelijke afhankelijkheden en de kloof in het delen van informatie.**

DE TOON ZETTEN

- ☐ **Zorg ervoor dat medewerkers op alle niveaus erkennen dat ze allemaal de belangrijke verantwoordelijkheid hebben om de cyberveerkracht van uw organisatie te waarborgen.**
- ☐ **Houd toezicht op de rol van het management bij het bevorderen en onderhouden van de risicocultuur van uw organisatie. Beoordeel regelmatig de doeltreffendheid van de risicocultuur van uw organisatie, rekening houdend met de impact van cultuur op veiligheid en gezondheid en voer waar nodig veranderingen door.**
- ☐ **Maak duidelijk dat van alle medewerkers wordt verwacht dat zij integer handelen en geconstateerde gevallen van niet-naleving binnen of buiten uw organisatie onmiddellijk melden.**

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org

THE WORLD BANK IBRD • IDA | WORLD BANK GROUP · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE · ICBA Independent Community Bankers of America®