HANDLEIDING DIRECTIENIVEAU: LEIDERSCHAP IN CYBERBEVEILIGING

TOEZICHT

Als het hoogste leiderschapsniveau binnen uw organisatie heeft de raad van bestuur de eindverantwoordelijkheid voor het beheersen van cyberrisico's en moet daarom toezicht houden op de strategie, het beleid en de activiteiten van de organisatie op dit gebied. De raad van bestuur moet specifiek:

- De eindverantwoordelijkheid nemen voor het toezicht op cyberrisico en veerkracht, hetzij als volledige raad of door het delegeren van toezicht aan een specifieke commissie van de raad van bestuur.
- Eén bedrijfsfunctionaris aanwijzen, meestal de centrale informatie beveiligingsfunctionaris (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 beheren. 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.
- Jaarlijks de risicotolerantie van uw organisatie bepalen en zorgen dat deze is afgestemd op uw bedrijfsstrategie en risicobereidheid.
- Ervoor zorgen dat er jaarlijks een formele, onafhankelijke cyberveerkrachtbeoordeling van uw organisatie wordt uitgevoerd.
- Toezicht houden 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.
- Cyberveerkracht en risicobeoordeling in de algemene bedrijfsstrategie van uw organisatie, in het risicobeheer, de budgettering en de toewijzing van middelen integreren, met als doel ervoor te zorgen dat cyberrisico's volledig worden meegenomen in het totale operationele risico. Controleer risico's voor derden regelmatig.
- Regelmatig uw prestaties op bovenstaande punten beoordelen en eventueel onafhankelijk advies voor continue verbetering inwinnen.

OP DE HOOGTE BLIJVEN

De effectiviteit van het toezicht op cyberrisico's door de raad van bestuur hangt af van de aanwezige kennis van het onderwerp bij de leden en het op de hoogte zijn van actuele informatie.

- Ervoor zorgen 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.
- Het management regelmatig om advies vragen over de huidige en toekomstige risicoblootstelling van uw organisatie, relevante regelgevingsvereisten, en benchmarks voor risicobereidheid uit de branche en de maatschappij als geheel. Daarnaast houdt de raad regelmatig briefings over de laatste ontwikkelingen met betrekking tot bedreigingen en het regelgevingsklimaat, plant en overlegt samen met collega's en leiders in de cyberbeveiliging en wisselt op directieniveau informatie over governance en rapportage uit.
- Het management herinneren aan zijn verantwoordelijkheid om een gekwantificeerde en begrijpelijke beoordeling van cyberrisico's, bedreigingen en gebeurtenissen te geven als standaard agendapunt tijdens raadsvergaderingen.
- Zorg ervoor dat iedereen op de hoogte is van voortdurende uitdagingen voor systemen, zoals kwetsbaarheden in de toeleveringsketen, wederzijdse afhankelijkheden en het onvoldoende delen van informatie.

DE TOON ZETTEN

Naast het senior management moet de raad van bestuur de kernwaarden, risicocultuur en verwachtingen van uw organisatie met betrekking tot cyberveerkracht vaststellen en uitdragen.

- Een cultuur bevorderen waarin medewerkers op alle niveaus hun belangrijke verantwoordelijkheden voor het behoud van cyberveerkracht in uw organisatie kennen. Het goede voorbeeld geven.
- Toezien op de rol van het management bij het bevorderen en onderhouden van de risicocultuur van uw organisatie. De risicocultuur promoten, bewaken en beoordelen, rekening houdend met de impact van cultuur op veiligheid en gezondheid en waar nodig veranderingen doorvoeren.
- Duidelijk maken dat van alle medewerkers wordt verwacht dat zij integer handelen en geconstateerde gevallen van niet-naleving binnen of buiten uw organisatie onmiddellijk melden.

Grondbeginselen van het beheer van cyberrisico's

Bevestig dat u de volgende vragen met ja kunt beantwoorden:

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

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
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