Inrichting van een Cybersecurity Comité	Hebben we!		
	Ja	Nee	Gedeeltelijk
Inrichting van een Cybersecurity Comité Het instellen van een specifiek comité binnen de boardroom dat zich richt op cybersecurity, kan zorgen voor een continue aandacht voor dit onderwerp. Dit comité kan verantwoordelijk zijn voor het beoordelen van de cyberrisico's, het toezicht houden op de implementatie van beveiligingsmaatregelen en het rapporteren aan de volledige directie.			
Aanstellen van een Chief Information Security Officer (CISO): Een CISO op hoog niveau aanstellen, die rechtstreeks rapporteert aan de directie, zorgt voor een directe communicatielijn en een duidelijk aanspreekpunt voor alle zaken met betrekking tot informatiebeveiliging. Deze CISO valt niet onder een andere afdeling (IT, Finance etc.), maar beweegt onafhankelijk binnen de organisatie. Bij voorkeur met eigen budgetten en resources.			
Beleid en Procedures voor Informatiebeveiliging Het laten opstellen en onderhouden van gedetailleerde beleidslijnen en procedures voor informatiebeveiliging is essentieel. Deze moeten altijd direct kunnen duiden waarom ze relevant zijn voor het veilig stellen van de bedrijfsdoelstellingen.			
Periodieke Risicoassessments en Audits: Regelmatige beoordelingen van de cybersecurity-risico's en audits van de beveiligingsmaatregelen zorgen ervoor dat potentiële zwakke plekken tijdig worden geïdentificeerd en aangepakt.			

Permanente educatie voor Cybersecurity: Ook de directieleden moeten regelmatig worden getraind in de nieuwste cybersecurity-risico's en -dreigingen. Dit helpt om een diepgaand begrip te ontwikkelen van de risico's en de benodigde maatregelen, passend bij de bedrijfsdoelstellingen.			
Investeer in geavanceerde Beveiligingstechnologieën: Het aanschaffen van de nieuwste cybersecurity-oplossingen, zoals Endpoint Detection & Response, Intrusion Prevention Systems (IPS) en geavanceerde Threat intelligence platforms, kan helpen om de organisatie te beschermen tegen complexe cyberdreigingen. Let wel, doe dit op basis van de risicoanalyse!			
Incident Response Plan en Oefeningen: Een gedetailleerd incident response plan laten ontwikkelen en regelmatig oefenen kan helpen om de organisatie voor te bereiden op mogelijke cyberaanvallen. Dit omvat scenario-oefeningen om te testen hoe effectief het team reageert op incidenten en hoe de directie in staat is om tot de juiste Beeldvorming, Oordeelsvorming en Besluitvorming (BOB) te komen.			
Leiderschap: Transparantie, Rapportage en Communicatie: Een cultuur van transparantie creëren waarin security-kwesties en incidenten openlijk worden gerapporteerd en besproken binnen de directie. Dit helpt bij het tijdig nemen van noodzakelijke beslissingen en het bevorderen van een gedeeld verantwoordelijkheidsgevoel. Daarbij werkt dit motiverend als het gaat om het uitdragen van het juiste voorbeeld (leiderschap).			

Samenwerking met Externe Partijen: Deelname aan sectorspecifieke cybersecurity-initiatieven en samenwerking met externe deskundigen en autoriteiten kan waardevolle inzichten en ondersteuning bieden. Het delen van informatie over bedreigingen en praktijkvoorbeelden helpt bij het versterken van de algemene houding ten aanzien van informatiebeveiliging.			
Investeren in Cyberverzekeringen: Overwegen om cyberverzekeringen af te sluiten kan helpen om de financiële risico's te beperken die voortvloeien uit een mogelijke cyberaanval of datalek. Let wel dat een verzekeraar nogal wat eisen stelt aan de wijze waarop je de informatierisico's beheerst als organisatie. En in geval van een claim is de aantoonbaarheid dat je er álles aan hebt gedaan om het te voorkomen cruciaal.			