11 Grip op cybersecurity voor bestuurders en commissarissen

Sandra Konings

1. Inleiding

De kranten staan vol met berichten over cybersecurity. Ook verschijnen er regelmatig nieuwe en populaire boeken over dit onderwerp die lezen als een spannende roman en gebaseerd blijken te zijn op werkelijkheid in plaats van fictie. Belangrijke verkiezingen zoals die in Amerika lijken door externe partijen te worden beïnvloed via onder andere ongeautoriseerde toegang tot social media om de kiezer te sturen. Ook lezen we dat de cyberdreiging is toegenomen door geopolitieke spanningen, zoals de oorlog in Oekraïne. Met name in industrieën die betrokken zijn bij wapentransport, zoals grote havens en het spoor, is er sinds februari 2022 sprake van een verhoogde waakzaamheid tegen diverse soorten aanvallen, waaronder cyberaanvallen. Ook andere bedrijven hebben gevolgen op het gebied van cybersecurity ondervonden. In februari 2023 kwam het bericht naar buiten dat Europese ziekenhuizen, waaronder Nederlandse, leken te zijn getroffen door een pro-Russische hacktivistische groepering. Deze had aangekondigd websites van onder meer ziekenhuizen in landen die Oekraïne helpen in de oorlog tegen Rusland onbereikbaar te maken door overbelasting. Hierdoor konden patiënten van de getroffen ziekenhuizen het patiëntenportaal tijdelijk moeilijker en soms helemaal niet bereiken. Steeds meer organisaties lijken zich dan ook bewust te worden van hun afhankelijkheid van technologie. Daarbij brengt nieuwe technologie, zoals AI en ChatGPT, nieuwe mogelijkheden maar ook nieuwe risico's. Hoe krijg je als commissaris grip op deze risico's ook al ben je een leek op het gebied van technologie? En waarom zou je überhaupt grip op cybersecurity willen krijgen? In dit hoofdstuk geef ik antwoord op deze vragen.

Dit hoofdstuk begint met een toelichting op het begrip cybersecurity. Het is een veelomvattend begrip en er zijn wereldwijd diverse standaarden die worden ingezet om meer grip te krijgen op cybersecurity. Ik bespreek de meest gangbare standaarden en meest relevante wetgeving. Vervolgens licht ik aan de hand van recente gebeurtenissen toe waarom grip op cybersecurity noodzakelijk is en zet ik uiteen waarom cybersecurity mogelijk nog niet altijd voldoende aan bod komt in de boardroom. Het hoofdstuk eindigt met advies over hoe commissarissen grip kunnen krijgen op cybersecurity.

2. Wat wordt verstaan onder cybersecurity

2.1 Definitie van cybersecurity

Cybersecurity wordt in het Nederlands vaak aangeduid met informatiebeveiliging. Het betreft het waarborgen van het gewenste niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Deze waarborgen hoeven niet allemaal in digitale oplossingen te zijn gevat. Zij bestaan uit een verzameling van technische, procedurele en organisatorische maatregelen. Neem als voorbeeld de *beschikbaarheid* van de helpdesk van een verzekeringsmaatschappij. Stel de ICT-systemen liggen eruit met als gevolg dat de helpdeskmedewerker niets meer kan opzoeken of invoeren. Dat heeft niet tot gevolg dat de hele dienst niet beschikbaar is, immers de helpdeskmedewerker kan klanten nog steeds telefonisch te woord staan met de parate kennis in zijn hoofd en kan vervolgens de schademelding met pen op papier noteren en invoeren in het ICT-systeem zodra dat weer in de lucht is. Door dit alternatieve proces van algemene kennis in het hoofd van de medewerker, het op papier noteren van de vraag of schade, het verwerken van de notitie zodra het ICT-systeem weer in de lucht is en het eventueel terugbellen van de klant, ervaart de klant vrijwel geen uitval van beschikbaarheid van het proces van het telefonisch melden van een schade. Met het waarborgen van de beschikbaarheid van informatie wordt dan ook bedoeld dat de informatie in enigerlei vorm beschikbaar is zodat het bedrijfsproces benodigd voor de verwerking van deze informatie vrijwel onverstoord kan verlopen.

Het waarborgen van de *integriteit* van informatie betreft het garanderen van de juistheid, tijdigheid, volledigheid en onweerlegbaarheid van informatie op ieder moment gedurende opslag en gebruik. De publicatie van de jaarcijfers van een organisatie is een voorbeeld waarbij het garanderen van de juistheid van belang is. Ook is het waarborgen van integriteit noodzakelijk voor de hele financiële administratie van een organisatie. Immers, de financiële administratie moet aantoonbaar onweerlegbaar kloppen, up-to-date zijn en mag geen delen missen. Ook de integriteit van de contractadministratie moet gewaarborgd zijn, het moet onweerlegbaar aantoonbaar zijn dat het niet mogelijk is om bestaande en ondertekende contracten achteraf ongemerkt aan te passen. Om de integriteit van informatie te waarborgen wordt vaak gebruikgemaakt van technische maatregelen, zoals het toekennen van schrijf- of mutatierechten aan een beperkte groep gebruikers, of een automatische toets op bepaalde invulvelden (denk aan de automatische rekeningnummercontrole bij het online bankieren). Het is gebruikelijk, en verstandig, om deze technische maatregelen te combineren met procesmatige maatregelen, zoals het vierogenprincipe: iemand kan een financiële transactie voorbereiden, maar kan het niet zelf uitvoeren. Hiervoor is een tweede bevoegde persoon nodig die meteen een extra controle uitvoert. Om integriteitsproblemen te voorkomen worden de personen die het proces moeten uitvoeren tevens bewust gemaakt van wat er fout kan gaan en in welke situaties zij extra alert moeten zijn. Denk aan de gangbare aanvallen van CFO-fraude: iemand doet zich voor als de CFO van een organisatie en verzoekt een medewerker van de financiële administratie om met spoed een bepaald bedrag

over te maken. De organisatie is beter tegen dit type aanvallen beschermd wanneer deze medewerker dit bedrag niet zelf kan overmaken, maar er een tweede paar ogen nodig is om de transactie daadwerkelijk uit te voeren. Tevens helpt het als beide medewerkers getraind zijn op dit soort situaties en weten waar zij op moeten letten en hoe te handelen (in dit geval zelf de CFO rechtstreeks contacteren en vragen of het verzoek inderdaad van de CFO afkomstig is).

Met het waarborgen van *vertrouwelijkheid* van informatie wordt bedoeld dat informatie niet in verkeerde handen valt. Beoogd wordt te voorkomen dat informatie wordt ingezien door iemand terwijl die niet voor deze persoon bestemd is. Bekende gevallen gaan vaak over datalekken van privacygevoelige informatie. Het kan zijn dat iemand van de afdeling personeelszaken per ongeluk een bijlage met alle salarisgegevens naar iedereen in de organisatie stuurt, of dat een medewerker de achterkant van een A4'tje met medische gegevens van patiënten gebruikt als boodschappenbriefje en dit briefje in het winkelwagentje van de supermarkt laat liggen (Haga Ziekenhuis, 2019). Ook aanvallen op ICT-systemen waarbij de aanvaller toegang krijgt tot informatie worden beschouwd als datalek. De aanvaller heeft immers mogelijk ongeautoriseerd toegang tot bedrijfsdata, zoals privacygevoelige data (gemeente Hof van Twente, 2020), gevoelige data van klanten of leveranciers of de geheime receptuur (intellectueel eigendom) van de organisatie. Maatregelen om ongeautoriseerde toegang tot informatie te voorkomen zijn technische preventie- en detectiesystemen, maar ook training en bewustwording. Dit betreft onder andere het checken van geadresseerden van e-mails voordat op 'Verzenden' wordt gedrukt, het sturen van een link naar een document in plaats van een bijlage (in combinatie met beheer van de toegang tot het documentbestand van de link) en de vernietiging van print-outs met privacygevoelige data.

Cybersecurity gaat dus over het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en dit wordt bereikt door een combinatie van technische, procesmatige en organisatorische maatregelen. Naast cyberrisico's in het kader van Informatie en Communicatie Technologie (ICT), zoals de werkplekautomatisering met e-mail, tekstbewerkingsprogramma's, presentatieprogramma's en bijvoorbeeld de financiële en personeelsadministratie, bestaan ook cyberrisico's ten aanzien van industriële controlesystemen, ook wel Operationele Technologie (OT) genoemd, en de inzet van Internet of Things (IoT). Deze typen technologie zijn minstens zo kwetsbaar en risicovol voor een organisatie als de ICT-systemen. Denk bijvoorbeeld aan een organisatie in de staalindustrie. In de fabriek worden grote rollen staal via katrollen langs het plafond vervoerd. De katrollen worden met software aangestuurd. Een situatie waarin een virus, aanval of fout in deze software veroorzaakt dat een grijper op een verkeerd moment een stalen rol van elf ton loslaat en deze rol vier meter naar beneden valt op de werkvloer waar net drie mensen aan het werk zijn, is een catastrofe die geen enkele bestuurder mee wil maken.

2.2 Standaarden, assurance-verklaringen en wetgeving

Sinds de start van de automatisering proberen organisaties grip te krijgen op cybersecurity. Hiervoor zijn dan ook diverse standaarden, zoals ISO 27001, ISO/IEC 62443 en assurance-verklaringen ontwikkeld, zoals SOC 1, ISAE 3402 en SOC 2. De laatste jaren zien overheden in dat ook zij een rol spelen bij het beschermen van organisaties in hun land of regio tegen cyberaanvallen en is er diverse wetgeving ontworpen.

2.2.1 Standaarden

De meest gangbare internationale standaard is ISO 27001. Tegen deze standaard kan een organisatie zich ook laten certificeren. Deze certificering moet jaarlijks bijgehouden worden. De certificering toont aan dat een organisatie ICT-security (dus niet OT-security) op een beheersbare manier heeft ingericht: er is een controlesysteem, een up-to-date beleid, bijgewerkte en geïmplementeerde processen en een cybersecurity-bewustwordingsprogramma. Voor OT-security bestaat de internationale standaard ISO/IEC 62443. Deze standaard is vergelijkbaar met ISO 27001 maar is veel omvangrijker. De risico's bij een OT-systeem zijn dan ook vele malen groter. Denk bijvoorbeeld aan een Scada-systeem in de olie- of gasindustrie. Als een van de kleppen of pompen het begeeft, kan dit een flinke milieuramp veroorzaken, of een explosie met mogelijk persoonlijk letsel. Sinds een aantal jaar is het mogelijk om tegen de ISO/IEC 62443 standaard te certificeren.

2.2.2 Assurance-verklaringen

Is een deel van de financiële verslaglegging uitbesteed, dan verdient het aanbeveling om een zogenaamde SOC 1-verklaring op te vragen bij de partij aan wie de verslaglegging is uitbesteed. SOC 1 staat voor Service Organization Control Report 1. Dit rapport is gebaseerd op de standaard Statement on Standards for Attestation Engagements no. 18 (SSAE 18) die verwijst naar AT-C 320, de Amerikaanse implementatie van de ISAE 3402 standaard. Een SOC 1-verklaring is min of meer gelijk aan de Europese ISAE 3402-verklaring. Dat is een verklaring over de interne beheersing van de financiële data van de klant door de leverancier. Naast SOC 1 kennen we ook de SOC 2-verklaring (Service Organization Control Report 2). Deze gaat verder dan puur garantie over de betrouwbaarheid van de financiële verslaglegging. SOC 2 biedt garanties over de inrichting van informatiebeveiliging voor iedere ICT-dienst geleverd door een derde partij, waaronder verwerking van data. Een SOC 2-rapport is gebaseerd op de Amerikaanse Assurance standaard AT-C 205, die min of meer het equivalent is van ISAE 3000. Het rapport heeft betrekking op de categorieën Beveiliging, Beschikbaarheid, Integriteit van processen, Vertrouwelijkheid en Privacy. Beide verklaringen, SOC 1 en SOC 2, kunnen afgegeven worden op twee manieren. Een SOC 1 (of SOC 2) type 1-verklaring toetst de opzet en het bestaan van het interne beheerssysteem en de beheersmaatregelen. Een SOC 1 (of SOC 2) type 2-verklaring is uitgebreider en toetst ook de werking van de maatregelen over

een periode van zes maanden. Steeds vaker wordt naast of in plaats van een ISO 27001 certificering gevraagd om een SOC 2 type 2-verklaring. ISO 27001 en SOC 2 gaan allebei over informatiebeveiliging, SOC 2 type 2 gaat alleen iets dieper dan ISO 27001 omdat deze de werking van de beheersmaatregelen over een bepaalde periode toetst, wat bij ISO 27001 niet het geval is.

2.2.3 Wetgeving

Naast organisaties proberen ook overheden grip te krijgen op cybersecurity en dataprotectie om de overheid zelf en de organisaties en burgers in hun land of regio te beschermen. De meest bekende wetgeving in de Europese Unie is de Algemene Verordening Gegevensbescherming (AVG). Dit is een Europese wet voor privacybescherming die van kracht is sinds 25 mei 2018 en geldt voor iedereen (alle personen en alle organisaties) die persoonsgegevens verwerkt van Europese ingezetenen. Alle Europese privacy toezichthouders, in Nederland de Autoriteit Persoonsgegevens, hebben de bevoegdheid om boetes op te leggen aan organisaties die de wet overtreden. In het kort eist de AVG dat organisaties die persoonsgegevens verwerken zich aantoonbaar houden aan zes basisprincipes: (1) rechtmatigheid, behoorlijkheid en transparantie, (2) doelbinding, (3) dataminimalisatie, (4) juistheid, (5) opslagbeperking en (6) vertrouwelijkheid en integriteit.

Hoewel er sinds 2017 veel aandacht is voor de AVG, is dit in het kader van cybersecurity niet de belangrijkste Europese wet om te kennen. De AVG gaat immers alleen om de bescherming van privacygevoelige data en niet om de bescherming van andere gevoelige data, de mate van beheersing van cyberrisico's of het voorkomen van cyberaanvallen. Daarvoor is medio 2016 de *Directive on security of network and information systems* (NIS-richtlijn) van kracht. Het doel van de NIS-richtlijn is om een hoog gezamenlijk niveau van cybersecurity te bereiken binnen alle Europese lidstaten. Europese lidstaten dienen deze richtlijn medio 2018 omgezet te hebben in lokale wetgeving, waarbij per lidstaat wordt bepaald voor wie deze wetgeving geldt. In Nederland is de NIS-richtlijn in 2018 vertaald in de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Wbni is erop gericht de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. Deze wet regelt de wettelijke taken van het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Justitie en Veiligheid en verplicht vitale aanbieders en aanbieders van essentiële diensten (AED's), uit onder andere de sectoren energie, bankwezen en drinkwater, ernstige digitale veiligheidsincidenten te melden bij het NCSC. AED's moeten deze incidenten ook melden bij hun sectorale toezichthouder. Digitale dienstverleners (DSP's) dienen ernstige digitale veiligheidsincidenten te melden bij het Computer Security Incident Response Team (CSIRT) voor DSP's. Naast de meldplicht bevat de Wbni ook een zorgplicht voor AED's en DSP's. Zij moeten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. De maatregelen moeten, gezien de stand van de techniek, zorgen voor een niveau van beveiliging dat is afgestemd op

de risico's die zich voordoen. Hierbij moet in ieder geval rekening gehouden worden met de volgende aspecten: (1) de beveiliging van systemen en voorzieningen, (2) de behandeling van incidenten, (3) het beheer van de bedrijfscontinuïteit, (4) toezicht, controle en testen en (5) inachtneming van de internationale normen. Daarbij dienen er passende maatregelen genomen te worden om incidenten die de beveiliging van de voor de verlening van de betrokken dienst gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en de gevolgen van dergelijke incidenten zo veel mogelijk te beperken, om de continuïteit van die dienst te waarborgen.

Inmiddels is Europa gaan doorpakken met het verbeteren van de digitale en economische weerbaarheid van de lidstaten en zijn op 16 januari 2023 de vervanger van de NIS-richtlijn, de NIS2-richtlijn, en de Critical Entities Resilience Directive (CER-richtlijn) in werking getreden. Europese lidstaten hebben tot 17 oktober 2024 de tijd om de NIS2-richtlijn te vertalen in lokale wetgeving en tot 17 januari 2026 om een strategie op te stellen ter verbetering van de weerbaarheid van kritieke entiteiten. Ten aanzien van NIS2 is de Nederlandse wetgeving nog in de maak. Wel kunnen organisaties zich hier alvast op voorbereiden. Zeker is dat een groter aantal organisaties onder deze wetgeving zullen vallen dan tot op heden (bij de Wbni) het geval is.[1] Daarbij richt de NIS2-richtlijn zich ook specifiek op de keten van toeleveranciers en niet alleen op de vitale organisaties zelf. Net als bij de NIS-richtlijn is er onder de NIS2-richtlijn sprake van een zorgplicht, een meldplicht en toezicht waarbij de eisen onder NIS2 flink zijn aangescherpt. Zo moeten ernstige digitale veiligheidsincidenten binnen 24 uur gemeld worden aan de eerdergenoemde instanties en moet de getroffen organisatie nu ook haar klanten informeren. De NIS2-richtlijn bevat tevens een concrete lijst aan securitymaatregelen die getroffen moeten worden. Het betreft een nadere uitwerking van de aspecten uit NIS1 aangevuld met onder andere (1) basis cybersecurity hygiëne, (2) beleid en procedures ten aanzien van versleuteling van data en (3) crisismanagement. Ook nieuw onder de NIS2-richtlijn is de rol voor bestuursorganen: zij moeten risicomanagement maatregelen goedkeuren en erop toezien dat deze daadwerkelijk geïmplementeerd worden. NIS2 stelt dat lidstaten ervoor dienen te zorgen dat bestuursorganen van essentiële en belangrijke entiteiten aansprakelijk gesteld kunnen worden indien zij verzuimen in hun plicht om de richtlijn na te leven. Daarbij dient het bestuur van de organisatie training te volgen om voldoende kennis en kunde te hebben om deze taken uit te kunnen voeren. Ter voorbereiding op de invoering van wetgeving gebaseerd op de NIS2-richtlijn kunnen organisaties (1) alvast hun processen voor incidentmanagement op orde brengen, waarbij zij voorsorteren op een melding binnen 24 uur, (2) alle risicomanagementprocessen voor informatiebeveiliging op orde brengen, bijvoorbeeld door de standaard ISO27001 te implementeren, en (3) het bestuur trainen en voorbereiden op de aankomende taken.

1 Nationaal Cyber Security Centrum van Ministerie van Justitie en Veiligheid, Wat gaat de NIS2 richtlijn betekenen voor uw organisatie – Welke sectoren en organisaties vallen onder de NIS2-richtlijn?

3. Waarom grip op cybersecurity van belang is

De laatste paar jaar wordt beheersing van cybersecurity steeds vaker opgenomen in *integrated reporting* en in duurzaamheidsverslaggeving omdat het niet beheersen van cybersecurity een steeds groter risico wordt voor een organisatie. Ook in de in december 2022 geactualiseerde versie van de Corporate Governance Code vinden we hier iets over terug. Deze Code beschrijft dat duurzame langetermijnwaardecreatie, bewustzijn van en anticiperen op ontwikkelingen in nieuwe technologieën en veranderingen in business modellen en daaraan verbonden risico's waaronder cybersecurity en dataprotectie verlangt. Ook schrijft de Code voor dat het bestuur de risico's die verbonden zijn aan de strategie en de activiteiten van de vennootschap en de met haar verbonden onderneming inventariseert en analyseert, waarbij het bestuur de risicobereidheid vaststelt en besluit welke maatregelen tegenover de risico's worden gezet. Als risico's worden genoemd risico's van informatie- en communicatietechnologie, waaronder op het gebied van cybersecurity, leveranciers- en ketenafhankelijkheden en dataprotectie.

Deze ontwikkelingen komen voort uit lering die is getrokken uit recente incidenten bij diverse organisaties. Dit heeft geleid tot financiële schade door uitval van bedrijfsprocessen, het betalen van losgeld en mogelijk ook reputatieschade. Enkele voorbeelden: In mei 2021 was Colonial Pipeline Company slachtoffer van een ransomware aanval. Dit Amerikaanse bedrijf uit Houston, Texas distribueert benzine en vliegtuigbrandstof naar met name het zuidoosten van de Verenigde Staten. Toen de aanval ontdekt werd, was het niet duidelijk of alleen de ICT-systemen of ook de OT-systemen geraakt waren. Om een grote ramp te voorkomen, heeft men snel gereageerd en binnen anderhalf uur vitale onderdelen van zowel de ICT als de OT stilgezet. Na grondig onderzoek werd de service vijf dagen later weer hervat. Het gevolg van deze aanval was een datalek van ongeveer 100 gigabyte en lange rijen bij tankstations aan de oostkust van Amerika omdat Colonial Pipeline Company niet kon leveren. American Airlines moest vluchten aanpassen met tussenlandingen om te tanken en vluchten omboeken naar andere toestellen. In juni 2017 was APM terminals slachtoffer van een virus dat niet eens specifiek voor het bedrijf was bedoeld. Het was het NotPetya virus, bedoeld om ICT-systemen van Oekraïne aan te vallen en te vernietigen. Dit virus bestaat uit software die zichzelf heel snel door ICT-systemen verspreidt en binnen enkele uren nadat het was geïntroduceerd, bevond het zich al op talloze machines in de wereld, waaronder bij APM Terminals, Mars, MSD, Raab Karcher en TNT Express. Het virus versleutelde ICT-systemen en verwijderde delen van de softwarecode. Bijna alle containerterminals van APM in de wereld waren geraakt. Het duurde ongeveer een week voordat de operatie weer terug was op normaal niveau. Wat recenter, in maart 2023, trok een ander incident onze aandacht. Nebu, aanbieder van een applicatie voor dataverzameling, was slachtoffer van een cyberaanval waarbij data zijn gelekt. Nebu is leverancier van onder andere Blauw Research dat marktonderzoek doet voor diverse klanten waaronder NS, Vodafone Ziggo en Pensioenfonds PME. Door het datalek bij Nebu zijn er mogelijk data gelekt van klanten van Blauw Research. Dit voorbeeld

geeft heel goed weer waarom het van belang is om goed zicht te houden op de afhankelijkheden van leveranciers en de waarborgen die een leverancier biedt. Dit zijn zomaar een paar voorbeelden, helaas kunnen we boeken volschrijven met alles wat er de laatste jaren is gebeurd. De verwachting is dat deze voorvallen alleen maar toe zullen nemen door mogelijkheden die Artificial Intelligence en Large Language Models bieden om meer geavanceerde aanvallen voor te bereiden.

Bovenstaande voorbeelden hadden financiële impact op de getroffen organisaties. Er is in sommige gevallen losgeld betaald om toegang tot versleutelde ICT-systemen te krijgen, in alle gevallen zijn er kosten gemaakt om delen van ICT-systemen opnieuw op te bouwen en er is omzetschade geleden doordat bedrijfsprocessen dagen werden stilgelegd. Al deze kosten samen kunnen hoog oplopen. Een organisatie loopt dan ook financiële risico's als cybersecurity onvoldoende is ingericht. In het voorbeeld van het metaalbedrijf kwam naar voren dat zelfs flink persoonlijk letsel of overlijden van medewerkers een gevolg kan zijn van onvoldoende beheerste cybersecurity. Het is goed voor te stellen dat een aanval op of een onbedoeld virus bij een gas- of oliemaatschappij desastreuze gevolgen kan hebben voor het milieu en mensen in het getroffen gebied. Het is dus van belang om als commissaris hier grip op te krijgen. Daarbij stelt wetgeving, zoals de AVG, de Wbni en de NIS2-richtlijn, eisen aan organisaties en daarmee aan het bestuur. Bij het niet naleven van de wet volgen vaak boetes en soms andere sancties. Tevens zien we dat journalisten steeds meer kennis hebben over cybersecurity en de zorgplicht van organisaties. Juiste en tijdige berichtgeving kan reputatieschade voorkomen of zelfs bijdragen aan een goede reputatie. Grip krijgen is dus eigenlijk niets anders dan zicht krijgen op de actuele cybersecurity-risico's in zowel ICT, OT als IoT en begrijpen wat er gedaan wordt of moet worden gedaan om die risico's te reduceren tot een acceptabel niveau. Het betekent ook grip hebben op de externe rapportage en communicatie mocht het toch fout gaan.

4. Komt cybersecurity voldoende aan bod komt in RvC vergaderingen?

Digitale vernieuwingen komen versneld op ons af en dat vraagt aandacht en visie van het bestuur en de RvC van organisaties. Op basis van gesprekken met commissarissen, directeuren internal audit en directeuren risicomanagement van verschillende organisaties rijst de hypothese dat er nog steeds onvoldoende diepgaand op cybersecurity-risico's wordt ingegaan tijdens RvC (commissie)vergaderingen. Dit zou kunnen komen doordat er onvoldoende kennis in de RvC's aanwezig is om cyberrisico's daadwerkelijk goed te kunnen inschatten en behandelen. Daarbij wordt cybersecurity vaak gezien als een wat lastig en technisch gedetailleerd onderwerp. Het wordt vooral lastig als het de commissarissen persoonlijk raakt. Dat gebeurt bijvoorbeeld wanneer de organisatie eist dat informatiedeling met en tussen de leden van de RvC alleen nog mag plaatsvinden via een afgeschermd portaal (het liefst met twee-factor-authenticatie voor toegang) en via het e-mailadres van de

organisatie. Dit betekent dat commissarissen die actief zijn bij verschillende organisaties, meerdere portalen, e-mailadressen en digitale kalenders moeten bijhouden en soms ook meerdere authenticatiemechanismen moeten toepassen. Voor het gemak – ook al moeten zij onderkennen dat zij werken met gevoelige data en niet kunnen uitleggen wanneer er iets mocht voorvallen dat deze data door hun toedoen op straat komen – forwarden de commissarissen dan de organisatie-email en alle kalenderafspraken naar hun privé-emailadres en privékalender. Het liefst communiceren zij onderling ook buiten de organisatie om via hun privé-emailadressen en wisselen zij chatberichten uit via publieke chatapps zoals whatsapp. Bij organisaties waar dit speelt, is er duidelijk onvoldoende bewustzijn van cyberrisico's en de potentiële impact van cyberincidenten op de organisatie waarop toezicht gehouden wordt.

Natuurlijk proberen RvC's hier iets aan te doen. Men stelt steeds vaker een commissaris met digitale kennis en ervaring aan. Zo is uit onderzoek in 2019[2] al gebleken dat destijds 76% van de beursgenoteerde NV's ten minste één commissaris had met digitale kennis en ervaring. 'Digitale kennis en ervaring' was in dit onderzoek echter een breed begrip. In hoeverre kan iemand die in het verleden succesvol een digitale transformatie heeft geleid daadwerkelijk doorvragen op cybersecurity-risico's in de ICT of OT-omgeving? En iemand die hoofd personeelszaken was bij een ICT-organisatie? Beide profielen worden in het genoemde onderzoek gekenmerkt als een profiel met digitale kennis en ervaring, maar om echt grip te krijgen op cyberrisico's lijkt het aantrekken van deze profielen niet voldoende. Men komt vaak niet verder dan het stellen van de volgende vragen: 'Hoe goed zijn wij beschermd tegen ransomware aanvallen? Doen we wel eens een test op dit vlak?' En ook: 'Als we een phishing test doen, geven we de gebruiker dan ook terugkoppeling op zijn actie?' Af en toe wordt gevraagd hoeveel de organisatie uitgeeft aan cybersecurity. Dit is een logische vraag, maar met welk antwoord is de commissaris tevreden? Om echt de goede vragen te stellen lijkt het verstandig om er een cybersecurity-expert erbij te halen of één of twee keer per jaar in te huren.

De laatste tijd zien we regelmatig dat de CISO (Corporate Information Security Officer) wordt uitgenodigd om toelichting te geven over de laatste stand van zaken in bijvoorbeeld de Audit & Risk Commissie. Dit is begrijpelijk omdat deze commissie grip wil houden op de risico's van de organisatie. Maar ook daar zien we organisaties worstelen. Omdat in de Audit & Risk Commissie vaak niemand met een diepgaande technische achtergrond deelneemt, heeft de CISO veelal moeite om de vaktechnische kennis te vertalen naar organisatierisico's. De CISO draagt vaak alleen bij aan het op peil houden of brengen van informatiebeveiliging in procesessen en de organisatie rondom ICT en heeft nauwelijks tot geen zicht op OT en IoT. We komen dan in de situatie waarbij de Audit & Risk Commissie namens de RvC wat eenvoudige algemene vragen stelt aan de CISO om grip te krijgen op cybersecurity-risico's en gedetailleerde technische antwoorden terugkrijgt die

2 J. Oehmichen & H. van Ees, 'Over de digitale expertise van de Nederlandse RvC', in: M. Lückerath-Rovers, H. van Ees, M. Kaptein & I.W. Wuisman (red.), *Jaarboek Corporate Governance 2019-2020*, Deventer: Kluwer 2019.

alleen over ICT gaan. Het is voor de Audit & Risk Commissie een onmogelijke puzzel om met deze informatie goed zicht te krijgen op de risico's in ICT, OT en IoT en op mogelijke financiële schade, reputatieschade en kans op menselijk letsel. Ook de discussie over welke schade nog acceptabel is, is moeilijk te voeren als de commissarissen en de expert een andere taal spreken.

Al met al lijkt het erop dat de echte vragen om grip te krijgen op cybersecurity nog onvoldoende gesteld worden in de RvC. Wellicht komt dit doordat cybersecurity geassocieerd wordt met technologie en dan met name ICT. Doorgaans is er weinig kennis over dit onderwerp bij de leden van de RvC en gaat men ervan uit dat de ICT-directeur de zaakjes wel goed voor elkaar heeft. Buiten het feit dat iedereen, ook de ICT-directeur, blind kan zijn voor de eigen aanpak en toezicht daarom benodigd is, weten we nu ook dat cybersecurity niet alleen gaat over ICT, maar ook over OT en IoT. Tevens speelt diverse wet- en regelgeving een rol. Het lijkt daarom verstandig om zowel de ICT-directeur *als* de Operationeel directeur *en* directeur Juridische zaken te bevragen over de mate waarin cybersecurity-risico's binnen ICT, OT en IoT worden beheerst. Deze directeuren kunnen zich laten adviseren door de CISO mits die een voldoende vertaalslag kan maken naar organisatierisico's of door een externe cybersecurity-expert die deze vertaalslag wel kan maken.

5. Hoe grip te krijgen op cybersecurity

Het is voor een commissaris mogelijk om grip te krijgen op cybersecurity zonder echt diep inhoudelijke technische kennis te hebben. In deze paragraaf worden de zes belangrijkste aandachtspunten besproken waarop commissarissen kunnen doorvragen en wordt ingegaan hoe dit toezicht te organiseren. Dit betreft (1) inzicht hebben in de cyberrisico's, (2) investeringen in cybersecurity, (3) weerbaarheid van de organisatie, (4) key performance indicatoren, (5) zekerheid (*assurance*) en (6) cybersecurity in producten en diensten.

5.1 Zes belangrijkste aandachtspunten voor commissarissen

5.1.1 Inzicht hebben in de cyberrisico's

Als eerste is het van belang om een actueel inzicht te hebben in de risico's die de organisatie loopt op het gebied van cybersecurity. Vraag hiervoor om een high-level overzicht van de kwetsbaarheden in de ICT, OT en IoT. Wat is het plan om deze kwetsbaarheden te mitigeren? Wat zijn de belangrijkste assets of kroonjuwelen? Hoe worden deze beveiligd? Vraag ook aan welke wetgeving de organisatie moet voldoen. Verkrijg inzicht in de eisen op het gebied van cybersecurity van klanten, beloften aan klanten en eisen van de verzekeraar. Wordt er al volledig aan deze (wettelijke) eisen en beloften voldaan? Indien dat niet het geval is, wat is het plan om dit te verbeteren? Welke risico's zijn ontstaan uit recente fusies of overnames en welke uit de verkoop van bedrijfsonderdelen? Wat is het plan om ook deze risico's

te mitigeren? Wat is de zogenaamde *risk appetite*, in andere woorden, welk risico wordt acceptabel geacht? Wanneer is de risk appetite voor het laatste vastgesteld? Loopt de uitvoering van alle plannen zoals hierboven beschreven op schema? Hoe vaak worden de plannen geactualiseerd? Tegen welke uitdagingen loopt de organisatie aan op het gebied van cybersecurity?

5.1.2 Investeringen in cybersecurity

Ten tweede helpt het om een idee te hebben van de totale jaarlijkse investering in cybersecurity. Vraag hoeveel budget er jaarlijks wordt besteed aan cybersecurity voor ICT en vergelijk dit met het totale ICT-budget. In september 2016 pleitte Herna Verhagen[3], CEO van PostNL, voor het doen van significante investeringen bij zowel de overheid als het bedrijfsleven om cybersecurity in Nederland op peil te brengen en te houden; het budget voor cybersecuritymaatregelen zou ongeveer tien procent van het jaarlijkse ICT-budget moeten bedragen. Anno 2023 is tien procent toch wel iets aan de hoge kant; benchmark is om circa vijf procent van het jaarlijkse ICT-budget aan cybersecuritymaatregelen te besteden. Het gaat dan om preventieve maatregelen ter voorkoming van cyberincidenten, maar ook om maatregelen om incidenten en aanvallen tijdig te detecteren, dus een (uitbesteed) team dat systemen monitort met geavanceerde software. Zodra iets gedetecteerd wordt, moet er meteen een proces opgestart worden om snel te handelen om de impact op de organisatie beperkt te houden. Zie hiervoor het voorbeeld van Colonial Pipeline Company. Tijdens de ransomware aanval was niet duidelijk of dit alleen ICT of ook OT betrof. De organisatie besloot geen enkel risico te willen lopen en heeft meteen niet alleen de ICT-systemen, maar ook een aantal OT-systemen stilgelegd. De cybersecurity investeringen betreffen onder andere salarissen voor personeel, salarissen voor inhuur van krachten, contracten voor uitbesteding, contracten voor detectie, preventie en response software, contracten voor reguliere testen, certificeringskosten, kosten voor het kopen of maken van trainingen en bewustwordingscampagnes, lidmaatschapsbedragen voor het deelnemen aan kennisinstituten en het ontvangen van nieuwe dreigingsinformatie en de kosten voor de cybersecurityverzekering. Is deze verzekering afgesloten? Wat is de dekking?

5.1.3 Weerbaarheid van de organisatie

Een van de aspecten van de beheersing van cybersecurity is de mate waarin de organisatie weerbaar is. Een cyberincident of cyberaanval is immers niet voor honderd procent te voorkomen. Natuurlijk is het verstandig om flink te investeren in preventie, maar dan nog loopt iedere organisatie kans om getroffen te worden. Dan is het van belang om een goed monitoring-detectie-response-mechanisme geïmplementeerd te hebben. En om voldoende te leren van incidenten in het verleden. Vraag twee keer per jaar wat de meest relevante incidenten de afgelopen zes maanden zijn geweest, hoe de organisatie daarop geacteerd heeft en wat de geleerde lessen

3 H. Verhagen, *De economische en maatschappelijke noodzaak van meer cybersecurity. Nederland digitaal droge voeten*, 2016.

zijn. Hebben deze lessen gezorgd voor een bijstelling van het verbeterplan dat is opgesteld aan de hand van de risico's? Welke incidenten verwacht de organisatie in de toekomst en waarom? Denk aan modellen waarmee cyberincidenten voorspeld kunnen worden op basis van de rol die de organisatie speelt in de maatschappij en recente maatschappelijke ontwikkelingen. Of denk aan nieuwe technologische ontwikkelingen zoals Large Language Models en quantum computing.

5.1.4 Key performance indicatoren

Vraag eens wat de key performance indicatoren zijn voor cybersecurity. Kijk goed of er naast ICT ook aandacht is voor OT en IoT. Zijn er alleen indicatoren opgesteld voor technische aspecten, of komen ook organisatorische aspecten aan bod, zoals beleid, procedures, werkinstructies en menselijk gedrag? Vraag hoe deze indicatoren tot stand zijn gekomen, zijn zij afgeleid van een internationale standaard, klanteisen, wetgeving of benchmark? Hoe scoort de organisatie op deze indicatoren? Hoe verhoudt zich dat tot de benchmark, klanten en andere organisaties in dezelfde branche? Als een indicator (nog) niet wordt gehaald, hoe erg is het dan dat dit niet op orde is? Wat is het plan om deze indicator wel (weer) te gaan halen? Is dit opgenomen in het verbeterplan?

5.1.5 Zekerheid (assurance)

Een vijfde aandachtspunt is de mate van zekerheid (assurance) over de betrouwbaarheid van de inrichting van cybersecurity. Bekijk als eerste eens hoe de governance van cybersecurity is ingericht. Het is gebruikelijk om dit in een zogenaamd 'three lines of defense'-model in te richten. De eerste 'line of defense' betreft de maatregelen die door de eerste lijn getroffen moeten worden als normaal onderdeel van hun bedrijfsprocessen. Denk daarbij aan ICT-maatregelen getroffen door de ICT-organisatie, OT-maatregelen door operations en financiële maatregelen zoals vier-ogen voor het uitvoeren van transacties door de financiële afdeling. De tweede 'line of defense' ziet erop toe dat de eerste lijn zijn taken goed uitvoert, houdt cyberrisico's op organisatieniveau bij naar aanleiding van de laatste ontwikkelingen en formuleert het cybersecuritybeleid. De derde 'line of defense' is de interne auditfunctie. Als de eerste en tweede lijn goed functioneren kan de derde lijn volstaan met het controleren van de tweede lijn. Indien er een externe auditor is aangesteld, wordt zij vaak beschouwd als de vierde 'line of defense'. Vraag vervolgens eens om het auditplan van de interne auditor. Worden alle aspecten (ICT, OT, IoT, processen, organisatie) goed afgedekt? Worden openstaande punten tijdig en afdoende opgepakt? Realiseer je dat het externe IT-auditrapport, als onderdeel van de financiële jaarcontrole door de externe auditor, niet het gehele ICT, OT en IoT landschap afdekt. Vaak zijn alleen de financiële ICT-systemen in scope. Vraag door over de leverancierselectie voor cybersecuritydiensten. Het is niet onverstandig om een gelaagd model te kiezen waarbij wordt voorkomen dat de slager zijn eigen vlees keurt. Is er inmiddels een sterke afhankelijkheid van één leverancier, toets dan of de securitydiensten bij een andere leverancier worden afgenomen. Het bestaan van

een ISO 27001 certificaat of een SOC 2(liefst type 2)-verklaring kan ook een goede aanwijzing zijn dat cybersecurity in de kern in orde is. Let wel, dit is een goede indicatie, maar zeker niet voldoende en kan niet de andere vragen uit deze paragraaf vervangen. Er zijn diverse voorbeelden van cyberincidenten en datalekken waarbij de getroffen partijen een ISO 27001 certificaat hadden en toch financiële schade en reputatieschade opliepen. Overweeg om buiten ISO 27001 en SOC 2 ook eens een andere onafhankelijke externe toets te laten uitvoeren, bijvoorbeeld op de key performance indicatoren of de geleerde lessen uit incidenten om meer zekerheid te krijgen over de betrouwbaarheid van de inrichting van cybersecurity.

5.1.6 Cybersecurity in producten en diensten

Ten slotte is het belangrijk om te toetsen in hoeverre cybersecurity wordt geborgd in het eindproduct van een organisatie. De voorgaande vijf aspecten gingen met name over de borging van cybersecurity in de interne bedrijfsprocessen en systemen om uitval en datalekken te voorkomen en integriteit te garanderen. Het is daarnaast ook van belang om te zorgen voor een voldoende mate van cybersecurity in de te leveren producten en diensten. Dit om te voorkomen dat een klant al haar fabrieken voor twee dagen moet sluiten omdat er in software in een robotmachine geleverd door een leverancier een virus blijkt te zitten dat schade kan veroorzaken bij de klant. Vraag de directeur operations in hoeverre er wordt getoetst dat zogenaamde ‘embedded software’ in fysieke machines die worden verkocht aan klanten virusvrij is. Welke afspraken worden hierover gemaakt in de juridische contracten? Welke beloften doet de organisatie aan klanten over updates bij nieuwe ontwikkelingen op het gebied van cybersecurity?

5.2 Organiseren van toezicht

In de in december 2022 geactualiseerde Corporate Governance Code staat dat het bestuur de effectiviteit van de opzet en de werking van de interne risicobeheersings- en controlesystemen met de auditcommissie bespreekt en daarover verantwoording aflegt aan de RvC. Veelal worden cybersecurity-risico’s besproken met de audit en riskcommissie. Voor organisaties in de digitale dienstverlening kan overwogen worden om naast de audit en riskcommissie, die zich richt op algemene en financiële risico’s, een aparte veiligheidscommissie in te richten die zich richt op digitale weerbaarheid. Het is tevens van belang om zowel het bestuur als de voltallige RvC regulier bij te spijkeren over nieuwe ontwikkelingen in cyberrisicomanagement die van strategisch belang zijn, zoals beschreven in de Europese NIS2-richtlijn.

6. Conclusie

Cybersecurity-risico’s kunnen niet genegeerd worden bij het bespreken van risico’s en het houden van toezicht op een organisatie. De vele praktijkvoorbeelden waarover de laatste jaren in de kranten te lezen was, laten zien dat cybersecurityincidenten een

aanzienlijke financiële- of reputatie-impact kunnen hebben. Dat is waarschijnlijk ook de reden dat de recent geactualiseerde Corporate Governance Code beschrijft dat ontwikkelingen in nieuwe technologieën en veranderingen in business modellen en daaraan verbonden risico's zoals cybersecurity en dataprotectie vragen om bewustzijn van en anticiperen door het bestuur. Ook zien we dat centrale overheden, zoals de Europese Commissie, komen met aangescherpte wetgeving voor organisaties.

De commissaris kan er bijna niet aan ontkomen om regulier of ten minste bij essentiële ontwikkelingen zich te laten bijpraten over strategisch risicomanagement op het vlak van cybersecurity zoals ook de nieuwe Europese NIS2-richtlijn voorschrijft. Het wordt dan meteen duidelijk dat cybersecurity niet alleen gaat om ICT-systemen, maar ook om OT-systemen zoals robots in een fabriek of pompen van een oliemaatschappij en om IoT, zoals bewakingscamera's. Daarbij zijn maatregelen om een cyberincident te voorkomen of om de impact beperkt te houden lang niet altijd puur technologisch. Maatregelen kunnen ook een herontwerp van een bedrijfsproces inhouden, of een aangepaste procedure of werkinstructie. Tevens speelt de menselijke factor bij vrijwel ieder cyberincident een rol, dus werken aan bewustwording bij en opleiding over gewenst handelen door medewerkers, klanten en leveranciers is een essentieel onderdeel van het totale maatregelenpakket.

De commissie die door de RvC wordt aangewezen om zicht te houden op cybersecurity-risico's kan meer grip krijgen door de volgende zes aandachtspunten te bespreken met de algemeen directeur (CEO), de ICT-directeur, de operationeel directeur, de juridisch directeur en indien aanwezig de security officer (CISO): actuele cybersecurity-risico's en risicomanagement, jaarlijkse cybersecurity investeringen in verhouding tot de totale ICT-investering, recente incidenten en de lering die daaruit is getrokken, key performance indicatoren, de mate waarin zekerheid (assurance) wordt verleend, en de borging van cybersecurity in het eindproduct dat de organisatie levert.

Het verdient aanbeveling om nog voordat een incident zich voordoet te bepalen welke berichtgeving uitgestuurd wordt ten tijde van een incident. In het huidige tijdperk waar journalisten gebrand zijn op transparantie en de zorgplicht van een organisatie kan het soms zelfs beter zijn om meteen naar buiten te komen met de melding van een incident en achteraf te verklaren dat het gelukkig meeviel, dan een incident te verzwijgen totdat het later alsnog aan het licht komt, waarbij duidelijk wordt dat de organisatie het destijds bewust heeft verzwegen.