16 Cyber security: een relevant onderwerp voor iedere bestuurder

John Hermans

1. Inleiding

Dat cyber security belangrijk is voor elke organisatie, dat behoeft eigenlijk geen nadere toelichting. Vrijwel dagelijks bewijzen incidenten dat de risico's groot zijn en dat zowel individuele hackers als professioneel georganiseerde cybercriminelen actief zijn op dit gebied. Bestuurders staan dan ook voor de taak erop toe te zien dat binnen hun organisatie de juiste prioriteiten worden gesteld. Dat is voor velen echter niet eenvoudig omdat de wereld van cyber security wat ongrijpbaar is vanwege het technisch jargon en het gespecialiseerde karakter. Generalisten kunnen er maar moeilijk vat op krijgen. Bovendien is het lastig om hoofd- en bijzaken van elkaar te scheiden terwijl berichten in de media bijdragen aan een angstcultuur waarin het beeld ontstaat dat vrijwel elke organisatie een willoze prooi is. Er wordt nauwelijks onderscheid gemaakt tussen oplichters op marktplaats.nl, hackers die een website platleggen of georganiseerde criminele groepen die met een stelselmatige strategie uit zijn op het stelen van bedrijfsgeheimen (ook wel 'kroonjuwelen' genoemd). Terwijl dat onderscheid van groot belang is, want niet alle organisaties zijn even 'aantrekkelijk' voor deze verschillende typen van cybercrime.

Mede doordat begrippen door elkaar heen lopen is cyber security een lastig thema voor menig bestuurder. Dat mag echter geen excuus zijn om het thema af te schuiven naar gespecialiseerde professionals. Het is juist essentieel dat bestuurders zelf actief sturen op de aanpak van cyber security. Bestuurders staan voor de taak om in de complexiteit van dit thema gedegen afwegingen te maken en op zijn minst de juiste vragen stellen. Maar hoe doet u dat? Dit hoofdstuk geeft handvatten en brengt cyber security terug tot de basis.

2. Wat is cyber security?

Alvorens in te gaan om de rol van de bestuurder in het kader van cyber security, is het belangrijk te starten met een duidelijke definitie. Immers, in de industrie en in de media worden allerlei definities door elkaar gebruikt, hetgeen natuurlijk niet helpt om deze thematiek goed te duiden. Een goede definitie luidt als volgt: "Cyber security is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De

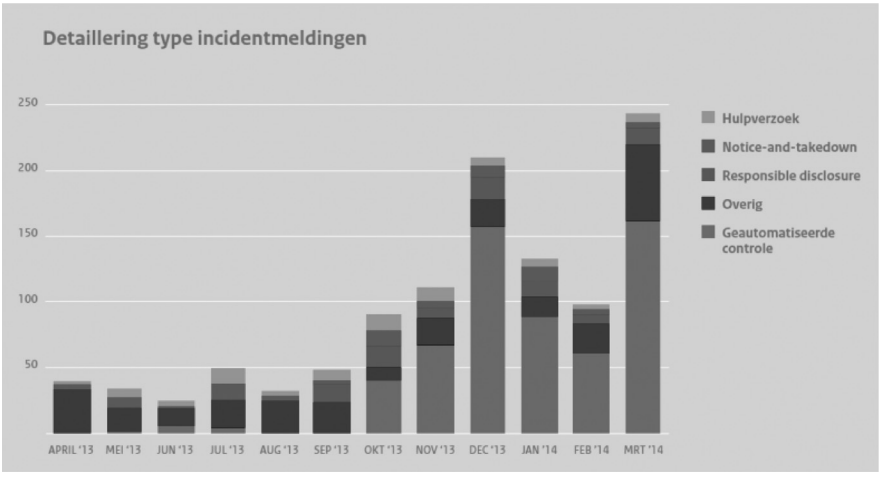
schade kan bestaan uit: aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of de integriteit van in ICT opgeslagen informatie" (bron: Nationale Cyber Security Strategy 2 – 2013). Deze verstoringen, uitval en/of misbruik kan vanuit verschillende actoren komen en hun oorsprong in de gehele keten vinden.

Actoren variëren van georganiseerde misdaad, staten, hacktivisten, eigen medewerkers tot onderzoeksjournalisten, waarbij iedere actor andere motieven en belangen heeft alsook meer of minder middelen (in termen van geld en technologische hulpmiddelen) heeft. Immers, een staat die op zoek is naar intellectueel eigendom heeft andere motieven, in dit geval economisch gewin, dan een onderzoeksjournalist, die de overtuiging heeft dat het zijn of haar taak is om aan te tonen dat een organisatie niet goed met cyber security omgaat en dat daardoor de privacy van bijvoorbeeld burgers in het geding komt.

3. Relevantie voor bestuurskamer

Eerste vraag die je als lezer zou kunnen stellen, is waarom dit thema relevant is voor de bestuurskamer, voor Raden van Bestuur en/of Raden van Commissarissen. Cyber security is immers niet nieuw. Echter, het stijgende aantal zoals in Figuur 1 weergegeven in de cijfers van het Nationaal Cyber Security Centrum (NCSC – juni 2014) en de ernst van de incidenten zijn zodanig toegenomen dat cyber security een substantieel risico kan vormen voor een organisatie. Een organisatie loopt niet immers alleen een financieel risico door fraude en inkomstenderving, maar zeker ook risico ten aanzien van verlies van imago (reputatieschade) alsook het publiek worden van intellectueel eigendom.

***Figuur 1*: Incidentmeldingen van cyber security**



Daarnaast is, gelet op de verregaande digitalisering van de meeste organisaties, het beveiligen van de meest belangrijke informatie ('kroonjuwelen') van organisaties ook van strategisch belang. Een organisatie kan het zich eenvoudig niet veroorloven om bijvoorbeeld intellectueel eigendom te verliezen waardoor de organisatie strategische marktvoordeel denkt te behalen.

Ten slotte heeft het thema cyber security door het sterk stijgende aantal spraakmakende incidenten aandacht vanuit de klanten, media en ook de toezichthouders. Klanten maken zich terecht zorgen door dit stijgende aantal incidenten en vragen zich af hoe hun informatie wordt beschermd door de organisatie. Het stijgende aantal incidenten blijft niet onopgemerkt door de media, die zeker niet terughoudend is met het publiceren over al deze incidenten en organisaties publiekelijk ter verantwoording roept over de mate van bescherming van bijvoorbeeld klantgegevens. Ook toezichthouders, zoals bijvoorbeeld De Nederlandsche Bank, roeren zich op dit onderwerp door enerzijds aandacht van bestuurders te vragen voor dit thema en anderzijds thematische onderzoeken te doen op de maatregelen die een organisatie treft ten aanzien van cyber security.

4. Risicoprofiel als startpunt

Dit alles maakt dat het thema cyber security aandacht verdient in de bestuurskamer, echter wel in de juiste context. Organisaties moeten zich niet gek laten maken. De media schetsen regelmatig een ongenuanceerd beeld van cyber security alsof veel organisaties een haast willoos slachtoffer zijn van cybercriminelen. Daarbij wordt alles over één kam geschoren en dat leidt bij bedrijven hier en daar tot angst die niet op feiten is gebaseerd. Een MKB-bedrijf heeft een heel ander profiel dan een multinational en over veel van de in de media genoemde incidenten hoeft een MKB-bedrijf zich dan ook weinig zorgen te maken.

De waarheid ligt dan ook genuanceerder dan het beeld in de media. De risico's zijn wel degelijk beheersbaar. Cybercriminelen zijn geen onoverwinnelijke genieën, en het ontbreekt overheden en ondernemingen zeker niet aan kennis om cybercrime te bestrijden. Maar we moeten ons wel realiseren dat 100% veiligheid een illusie is en dat het najagen van die 100% niet alleen tot frustratie zal leiden maar mogelijk ook tot schijnzekerheid.

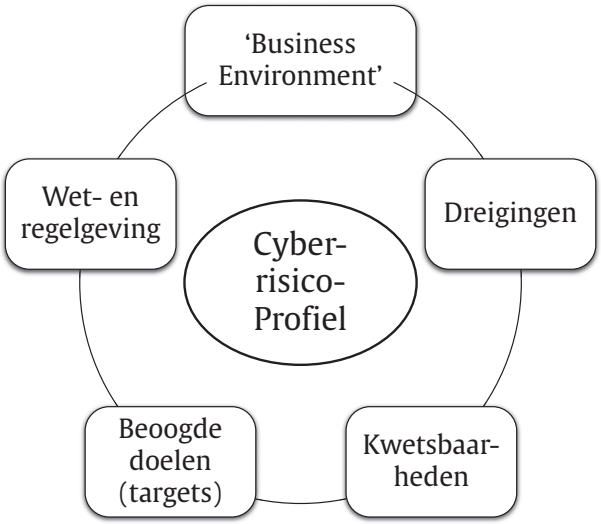
In feite moeten we cyber security gaan beschouwen als '*business as usual'*. Als een thema dat op dezelfde wijze aandacht verdient als bijvoorbeeld het risico op brand of fraude. Dit zijn thema's die gestructureerd worden aangepakt door het management, vanuit een risk-managementperspectief en dus niet met de gedachte een systeem te bouwen dat 100% waterdicht is. Veel organisaties moeten op een andere manier naar cyber security gaan kijken. Ze moeten niet redeneren vanuit angst voor wat er buiten gebeurt, maar redeneren vanuit eigen kracht. Vanuit de juiste overwegingen over risico's en het karakter van de eigen organisatie, in lijn met

het risicoprofiel van een organisatie. Startpunt van de verkenning van het cyber risico van een organisatie is dan ook het bepalen van het risicoprofiel van uw organisatie? Relevante vragen om het risicoprofiel te bepalen zijn vragen zoals 'hoe interessant is uw organisatie voor potentiële cybercriminelen?', 'hoe afhankelijk is uw organisatie van de dienstverlening van andere organisaties?', en ten slotte 'hoeveel risico wilt u als organisatie lopen?'.

Om het risicoprofiel te bepalen is een model – zoals afgebeeld in Figuur 2 – hanteerbaar die de onderstaande vijf aspecten belicht:

1. Wat is de 'business environment' van een organisatie? In welke markten is een organisatie actief, wat is de mate/afhankelijkheid van digitalisering van de dienstverlening van de organisatie? Hoe verbonden is een organisatie met anderen, die mogelijkerwijs een additioneel risico in dit kader kunnen opleveren?
2. Voor welke groep cybercriminelen en waarom is een organisatie een aantrekkelijk doelwit ('dreigingen'), en wat zijn de middelen die door de aanvaller ingezet kunnen worden ingezet?
3. Welke kwetsbaarheden binnen een organisatie kunnen door cyber criminelen worden gebruikt? Denk hierbij niet alleen aan technische kwetsbaarheden, maar zeker ook aan het menselijk handelen.
4. Wat zijn relevante doelwitten ('targets') binnen de organisatie, maar zeker ook binnen de keten waarin een organisatie actief is?
5. Wat zijn de vereisten van wet- en regelgeving ten aanzien van cyber security? In dit kader worden zowel in Nederland als buiten Nederland nieuwe regelgevingen ontwikkeld die mogelijkerwijs voor uw organisatie relevant zijn.

***Figuur 2*: Risicomodel cyber security**



Op basis van het analyseren van de genoemde vijf aspecten is een organisatie in staat te bepalen wat haar risicoprofiel is, alsmede ook te bepalen hoeveel risico een organisatie wenst te lopen ('risk appetite') en de juiste set van maatregelen te treffen. Immers, 100% veiligheid bestaat niet en is ook niet wenselijk.

5. Maatregelen

De cyberrisico's kunnen en moeten worden gemitigeerd door het inzetten van maatregelen en het instaat zijn om te kunnen reageren wanneer een organisatie onder vuur ligt van een cyberaanval. Maar hoe de juiste set van maatregelen te selecteren?

In dit kader is een aantal overwegingen relevant:

- *Focus op uw 'kroonjuwelen'*: Aangezien het onmogelijk is alles te beschrijven, vereist cyber security gerichte aandacht op de bescherming van de meest relevante informatie van een organisatie. Het is dan ook van belang dat een organisatie bepaalt wat haar 'kroonjuwelen' zijn die beschermd dienen te worden.
- *De mens blijft de zwakste schakel:* het hebben van technische systemen ter bescherming, om op te sporen en te reageren op een aanval is belangrijk, maar in veel organisaties is de mens de zwakste schakel. De mens kan ook de grootste troef worden voor de verdediging, mits juist geïnformeerd en opgeleid.
- *Verschuiving van preventieve maatregelen naar detectieve maatregelen:* daar waar de organisatie in het verleden met name steunden op preventieve maatregelen teneinde een incident te voorkomen, zien we op dit moment veel meer aandacht voor het kunnen detecteren van een aanval, om direct en adequaat te kunnen reageren. Zo zien we bij veel organisaties een stijgend gebruik van technische monitoringsvoorzieningen om vreemd verkeer te kunnen detecteren en te analyseren.
- *Aandacht op reactievermogen van een organisatie:* zoals aangeven, is het naar onze mening een kwestie van tijd voordat een organisatie slachtoffer is van een cyberincident. In plaats van een willoos slachtoffer te zijn, kan een organisatie zich hierop voorbereiden. Het is dan ook zaak dat een organisatie in haar crisisplannen het afhandelen van cyberincidenten opneemt. Tevens is het zaak een protocol op te stellen dat gebruikt wordt in de communicatie tijdens een dergelijk cyberincident.
- *Samenwerking is vereist:* naast het kunnen reageren op incidenten is het zaak op de hoogte te zijn en te blijven van nieuwe bedreigingen en te leren van de afhandeling van incidenten bij andere organisaties. Om dit te faciliteren zijn er verschillende niveaus organisaties actief om hierin te ondersteunen: enerzijds op nationaal niveau (bijvoorbeeld het Nationale Cyber Security Centrum), op sectoraal niveau in de zogenoemde ISAC's en soms informele samenwerkingsverbanden, bijvoorbeeld een groep CISO's binnen een bepaalde industrie. Teneinde een proactieve aanpak van cyber security te bewerkstelligen, is een actieve participatie van een organisatie aan dergelijke netwerken vereist en kan het de organisatie helpen bij het verbeteren van de weerbaarheid van de

eigen organisatie. Immers, een incident bij een andere organisatie, is een dreiging voor de eigen organisatie!

6. Technologie alleen is niet het antwoord

Technologie is niet het antwoord op cyber security. Het antwoord is gelegen in een integrale benadering voor cyber security, met aandacht voor zowel de zachtere elementen zoals governance, cultuur en gedrag, als de meer hardere elementen als technologie.

In een dergelijke integrale benadering voor cyberrisicomanagement dient aandacht te worden gegeven aan de volgende aspecten:
- Leiderschap en governance: bestuurders van een organisatie dienen in woord en daad te laten zien dat ze zich eigenaar voelen van het thema en laten zien dat ze de ermee samenhangende risico's adequaat willen managen.
- Gedrag van de mens: cyber security heeft niet (alleen) te maken met de juiste technische maatregelen, maar ook met het creëren van een cultuur waarin mensen alert zijn en zich bewust zijn van hoe zij kunnen bijdragen aan veiligheid.
- Information Risk Management: een adequate aanpak voor alomvattend en effectief risicomanagement ten aanzien van informatievoorziening, ook in relatie tot partnerorganisaties.
- Business Continuity & Crisis Management: een goede voorbereiding op eventuele incidenten en het vermogen de impact van deze incidenten te minimaliseren. Dit omvat onder meer crisis- en stakeholdermanagement.
- Operations & Technologie: de implementatie van controle- en beheersingsmaatregelen in de organisatie om risico's van cyber security te identificeren en de impact van incidenten te minimaliseren.
- Wet- en regelgeving: het voldoen aan wet- en regelgeving ten aanzien van informatiebeveiliging.

Het toepassen van dit holistische model levert organisaties het volgende op:
- Het minimaliseren van het risico dat een organisatie wordt getroffen door een cyberaanval van buiten en het minimaliseren van de eventuele gevolgen van een succesvolle aanval.
- Betere beslissingen op het gebied van cyber security: de informatievoorziening over maatregelen, aanvalspatronen en incidenten wordt daartoe geoptimaliseerd.
- Heldere communicatielijnen over het thema cyber security. Iedereen kent zijn verantwoordelijkheden en weet wat er moet gebeuren als er (vermoedens van) incidenten zijn.
- Een bijdrage aan een betere reputatie. Een organisatie die goed is voorbereid en goede afwegingen over het thema cyber security heeft gemaakt kan op vertrouwenwekkende wijze communiceren over dit thema.
- Het verhogen van de kennis en competenties over cyber security.

– Het benchmarken van de organisatie op het gebied van cyber security in relatie tot peers.

7. Rol van commissarissen

Commissarissen zullen zich wellicht afvragen wat hun rol in deze dient te zijn. De Raad van Bestuur is verantwoordelijk voor het vaststellen, uitvoeren, monitoren en waar nodig bijstellen van het algehele risicobeleid van de organisatie. De Raad van Commissarissen dient echter minimaal één keer per jaar het risicobeleid goed te keuren alsmede toezicht te houden op het door het Raad van Bestuur gevoerde risicobeleid. Kortom, commissarissen hebben een belangrijke rol in het vaststellen van het risicoprofiel van een organisatie en in het vaststellen en toezicht houden op het gevoerde risicobeleid. Dus ook voor cyberrisico's, immers, deze kunnen van strategisch belang zijn voor de organisatie.

Om commissarissen een handreiking te geven om deze rol goed te vervullen sluit ik af met een overzicht van aandachtspunten en vragen (zie Tabel 1).

***Tabel 1*: Handreiking voor commissarissen**

Hoe de cyber risk appetite en prioriteitstelling te bepalen?	– Wat is uw organisatierisicobereidheid voor downtime, verlies van gegevens en privacy-incidenten, hoe je 'risk appetite' te stellen, en hoe dit te monitoren? – Wat zijn de 'kroonjuwelen' die de hoogste niveaus van bescherming nodig hebben? Welke bedrijfsprocessen zijn cruciaal voor het voortbestaan van de organisatie?
Hoe bent u georganiseerd ten aanzien van cyber security?	– Wat is de inrichting van de 'first- and second-line defense' ten aanzien van cybersecurity? – Hoe wordt over het cyberrisico security gerapporteerd? – Hoe vindt de coördinatie plaats tussen de verschillende verantwoordelijke bedrijfsfuncties ten aanzien van cyber security.
Investeert u voldoende in cyber op dit moment? En krijgt u voldoende 'value for money'?	– Wat zijn de geplande investeringen op het gebied van cyber security voor de komende drie jaren? – Is dit voldoende om afdoende beschermd te zijn op deze dreiging (in lijn met uw risk appetite)? – Hoe verhouden uw investeringen zich ten aanzien van cyberinvesteringen van uw peers?

Hoe veilig/weerbaar is de organisatie nu?	– Wat waren de meest relevante beveiligings- en privacy-incidenten waarin uw organisatie (of diens peers) in de laatste twaalf maanden? – Wat waren de 'lessons learned'? – Wat doet de organisatie nu anders om te voorkomen dat deze incidenten wederom kunnen ontstaan?
Wordt de organisatie veiliger of onveiliger?	– Welke KPI's staan op uw cyberrisicodasboard? – Behaalt uw organisatie de gestelde cyberrisicodoelstellingen? – Hoe verhouden zich de cyberrisico KPI's ten opzichte van uw concurrenten?
Hoe beheerst u het risico ten aanzien van uw externe leveranciers en andere ketenpartners?	– Hoe zorgt u dat uw externe leveranciers en diens leveranciers alsook andere ketenpartners uw organisatie niet blootstellen aan een onaanvaardbaar cyberrisico?
Op welke wijze is cyber security geborgd in uw producten en diensten?	– Op welke wijze is cyber security geborgd in de: – huidige producten en diensten? – ontwikkeling van nieuwe producten en diensten?

8. Conclusie

Een bestuurder kan niet meer om het thema cyber security heen. Het aantal en de ernst van de incidenten, de media-aandacht, maar ook de aandacht van toezichthouders en klanten, vereisen dat cyber security één van de thema's is die in de strategisch risicoagenda van de meeste organisaties opgenomen dient te worden. Natuurlijk met de juiste nuance, in lijn met het risicoprofiel van een organisatie en op basis van een gedefinieerde *risk appetite*. Eigenlijk '*risk management as usual*'. En dat zit toch bij de meeste bestuurders in de genen?