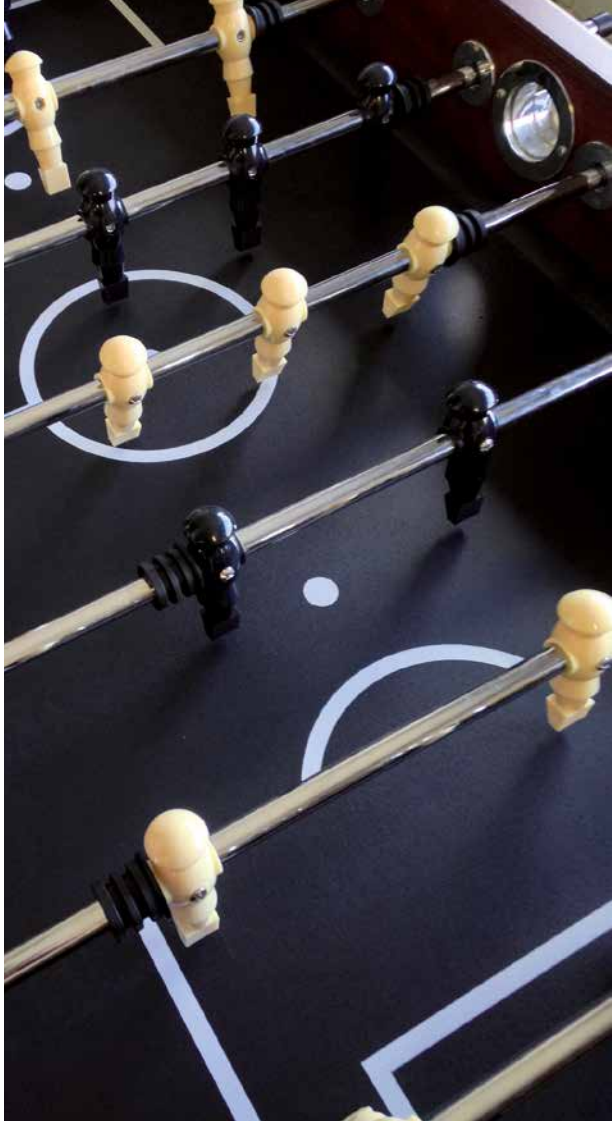


Cyber security is geen technisch probleem, maar een leiderschaps-probleem!

Drs. Dennis de Geus RE RA CISA

Cyber security wordt veelal gezien als een technisch iets. Een onderwerp waarbij techneuten de alleenheerschappij hebben. Maar is dat wel zo? Laten wij eens met een voetbalbril naar de wereld van cyber security kijken. Wat kunnen we leren als we dit doen?

Inleiding

Cyber space is overal en het domein is enorm complex. Alles en iedereen is tegenwoordig met het internet verbonden, direct of indirect. Hierdoor is een wereld ontstaan die moeilijk is in te kaderen, want alles hangt met elkaar samen (via internet of andere netwerken). Daarmee zijn veel van de producten en diensten die organisaties leveren in meerdere of mindere mate van cyber space afhankelijk. Het is dan ook niet moeilijk te stellen dat de mate van beveiliging (cyber security) van directe invloed is op de kwaliteit van dienstverlening van deze organisaties.

In de managementliteratuur is het alom geaccepteerd dat de verantwoordelijkheid voor de kwaliteit van producten en diensten niet aan één aparte afdeling uitbesteed kan worden, maar een integrale verantwoordelijkheid van het management is. In de praktijk is deze zienswijze bij verreweg de meeste organisaties als zodanig terug te vinden. Totdat ... het gaat over het kwaliteitsaspect cyber security, want dan kijkt de organisatie collectief naar de afdeling Security en ligt de primaire verantwoordelijkheid volgens het management bij de Chief Information Security Officer (CISO).

De afgelopen jaren is het cyberdomein verder ontwikkeld, zowel aan de 'goede kant' als aan de 'slechte kant'. Deze ontwikkeling heeft zowel plaatsgevonden in de diepte als in de breedte. Niet alleen zijn de cyberdreigingen geavanceerder geworden ('diepte'), maar ook is het cyberdomein uitgebreid naar onder andere de vitale infrastructuur en haar systemen ('breedte'). Deze systemen worden ook wel Industriële Controle Systemen (ICS) of SCADA-systemen genoemd. Systemen voor de aansturing van bruggen, sluizen, gastransport en robots in fabrieken zijn slechts enkele voorbeelden hiervan.

Vroeger waren deze ICS niet aan internet verbonden, maar bevonden zij zich vaak in een 'stand-alone' omgeving. Meer en meer zien we dat deze systemen met het internet verbonden worden, onder meer om beheer op afstand uit te kunnen voeren. Daarnaast maakten deze ICS tot voor enkele jaren gebruik van zelf ontwikkelde protocollen en systemen, terwijl op dit moment vaak gebruik wordt gemaakt van systemen die wel bij een groot deel van de hackerscommunity bekend zijn. Kortom, deze systemen zijn beter toegankelijk voor een grotere groep mensen die weten hoe ze deze ICS-omgevingen kunnen beïnvloeden.

Drs. D. de Geus RE RA CISA
is senior manager bij
KPMG Advisory N.V.
degeus.dennis@kpmg.nl

Zolang cyber security als een puur technische aangelegenheid wordt gezien, worden organisaties niet veiliger

De combinatie van deze ontwikkelingen is een reden tot zorg. Immers, de breedte en diepte van het speelveld neemt toe, terwijl een belangrijk deel van de spelers langs de zijlijn toekijkt hoe 'de afdeling Security' probeert de wedstrijd te winnen. Het is toch een technisch probleem en zij zijn de specialisten!

En hierin zit ook gelijk de kern van het probleem. Cyber security wordt gezien als een technisch IT-probleem, met een onmogelijke spagaat als gevolg. Een spagaat veroorzaakt doordat aan de ene kant de medewerkers van de organisatie hun rol op security onvoldoende pakken en door anderzijds de druk op de noodzakelijke reductie van investeringen in security. Immers, het is onderdeel van IT en het jaarlijkse IT-budget moet naar beneden.

Zolang de perceptie blijft bestaan dat cyber security een puur technische aangelegenheid is, gaan organisaties niet veiliger worden. Laten we daarom eens naar cyber security kijken vanuit de analogie met het voetbal.

Cyber security in voetbaltermen

We staan op het punt om de tweede helft te beginnen en als 'supporter', maar ook als 'liefhebber/hobbyist' zouden wij graag wat wijzigingen in de selectie en speelwijze voorstellen. Het doel is hier het verkrijgen van de heilige drieeenheid in security: Mens, Proces en Techniek in balans.

1. De rol van Bondscoach wordt actief ingevuld door het bestuur van de organisatie

Net als bij voetbal wordt het succes op het speelveld van de cyber security bepaald door de voorbereiding van de organisatie. Door al vanaf het begin van het seizoen goed te kijken wie de tegenstanders zullen zijn, kan de Bondscoach bepalen welke typen spelers hij in het komende seizoen nodig gaat hebben en wat de samenstelling van het team gaat zijn.

In het speelveld van cyber security is het feitelijk weinig anders. Het bestuur dient, samen met deskundigen, te bepalen welke tegenstanders de organisatie in het cyberdomein zou kunnen treffen (threat landscape) en waar deze tegenstanders op uit kunnen zijn (kroonjuwelen).

Belangrijk is om niet te vergeten dat security geen doel op zich is, maar dat het een essentiële factor is in het realiseren van de organisatiestrategie. Het goed bepalen van de strategische securityrisico's is waar het hier om gaat. Welke cyber-securityrisico's zouden nu wezenlijk de realisatie van de organisatiestrategie kunnen belemmeren? Wat is de top 10 securityrisico's?

Op basis van deze top 10 securityrisico's kan gekeken worden waar de eigen organisatie kwetsbaar is (risk assessment) en kunnen zo de lijnen voor verbetering worden uitgezet. Belangrijk hier is dat niet alleen gekeken wordt naar de technische aspecten, maar naar het geheel van mensen, processen, governance en techniek.

Kroonjuwelen

Wat moet ik nu precies beschermen? Dit is een veelgestelde vraag. Om hier inzicht in te krijgen kunnen de volgende vragen gesteld worden:

- Welke informatiesystemen zijn voor mijn organisatie van essentieel belang?
- Het wegvallen van welke data zou grote financiële of reputatieschade veroorzaken?
- In welke gegevens zouden concurrenten en/of criminele organisaties zeer geïnteresseerd zijn?

De zaken die bij het beantwoorden van deze vragen naar boven komen, kunnen aangemerkt worden als de te beschermen kroonjuwelen. Naast een passend niveau van basisbeveiliging, richten de cyber-defencemaatregelen zich met name hierop.

Deze top 10 is een goede eerste stap naar een vorm waarbij de securityrisico's als onderdeel van een geïntegreerd risicobeheersingsraamwerk worden beheerst. Want hoewel er veelal een zweem van mystiek om het geheel van cyber security hangt, is het gewoon één van de risico's die samenhangt met de activiteiten van de organisatie. Het is dan ook logisch dat de Bondscoach verantwoordelijk is voor het adequaat managen van deze risico's, een rol waarvoor hij/zij adequate stuurinformatie kan, mag en moet verlangen. Je kan dus ook stellen dat cyber security gewoon een aspect van risicomanagement is.

2. De Bondscoach zorgt voor de opstelling van een breed team

Het volgende voorstel is dat de Bondscoach zorgt voor de opstelling van een breed team. Een team waarbij eenieder goed op de hoogte is van zijn/haar eigen verantwoordelijkheden in het team. Elkaar actief aanspreken op deze verantwoordelijkheden en het nakomen hiervan is essentieel.

In het voetbal zien we dat er bij succesvolle teams sprake is van een excellente samenwerking over alle rollen heen: spelers, assistent-trainers, verzorgers, technische staf tot en met degenen die verantwoordelijk zijn voor het veld. De Bondscoach is de drijvende kracht hierachter.

Hoe anders is het vaak in het cyberdomein! Vanuit de bestuurskamer wordt cyber security veelal gepositioneerd als een IT-technisch iets, wat vooral aan de specialisten overgelaten moet worden. Natuurlijk kan het zo zijn dat bestuurders vinden dat ze onvoldoende kennis van deze materie hebben, maar dat mag geen excuus zijn om het onderwerp niet serieus te nemen.

Ook ten aanzien van cyber security geldt dat in alle geledingen men zijn of haar rol dient te pakken. Laten we hier eens nader op inzoomen.

In werkelijkheid zit de oorzaak van veel cyberincidenten niet in de techniek, maar in de aspecten van mens en aansturing. Wie kent er niet de situatie waarin de afdeling Marketing, onder druk van de marktontwikkelingen, snel even een nieuwe website bij het hostingbedrijfje op de hoek laat opzetten en hosten. Het gevolg is vaak een slecht beveiligde website met klantgegevens, een uitnodiging voor hackers alom.

Cyber security is een integraal onderdeel van de kwaliteit van dienstverlening van een organisatie. En zoals kwaliteit niet de verantwoordelijkheid van de afdeling Kwaliteitscontrole is, kan security net zo min alleen de verantwoordelijkheid zijn van de afdeling Security. In de opstelling van een breed team is het dan ook noodzakelijk dat er gewerkt gaat worden volgens het 'three layers of defence'-model. Volgens dit model ligt de primaire verantwoordelijkheid bij business en IT-management en vervult de afdeling Security de tweedelijnsverdediging, zijnde faciliteren en monitoren. De derde lijn (toezicht) ligt bij de auditfunctie.

In de praktijk blijkt de implementatie van dit model, hoewel noodzakelijk, wel wat voeten in de aarde te hebben. Zij raakt onder meer targetsetting, managementrapportage, opleidingen & trainingen, methodiek van risicobeheersing en beloningsbeleid. Hieruit blijkt wederom dat een succesvolle strategie voor cyber security begint en eindigt in de bestuurskamer.

In de eerste stap zijn de strategische securityrisico's bepaald. In deze stap is het van belang om deze risico's te beleggen bij het verantwoordelijke lijnmanagement. De afdelingen Inkoop, Marketing & communicatie, Verkoop, IT, HR, etc., allemaal hebben ze een primaire verantwoordelijkheid voor security. Het is aan de Bondscoach om de risico's aan de juiste afdelingen te alloceren en te zorgen dat er periodiek gerapporteerd wordt over de te nemen en genomen acties om deze risico's te mitigeren. Deze rapportage zou bij voorkeur via de reguliere managementrapportages dienen plaats te vinden. Gelijk aan de rapportage over de ontwikkelingen in het marktaandeel, debiteurenrisico's en de omzet.

Een volgende stap in het borgen van security in de lijn is het koppelen van deze risico's en verantwoordelijkheden aan persoonsgebonden doelstellingen. Hiermee kan een link gelegd worden met het beloningsbeleid van de organisatie, waardoor de verantwoordelijkheid voor security echt komt te liggen waar die hoort. In de eerste lijn!

3. Een nauw samenspel tussen de Bondscoach en de Technisch Directeur

Er komt een nauw samenspel tot stand tussen de Bondscoach en de Technisch Directeur (CISO) omtrent technische analyses (zwakheden in de verdediging), nieuwe spelvormen (governance) en benodigde faciliteiten (mensen en middelen voor security in de tweede lijn).

De Technisch Directeur is in staat door zijn ruime ervaring het bestuur te adviseren op dit domein. Doordat hij vanuit zijn rol niet wordt opgeslokt door de dagelijkse

Een succesvolle strategie voor cyber security begint en eindigt in de bestuurskamer

operaties is hij in staat de ontwikkelingen in de markt te analyseren en door te vertalen naar de eigen organisatie. Hij acteert als gelijkwaardige gesprekspartner richting de Bondscoach en brengt het belangrijke 'outside in perspective'.

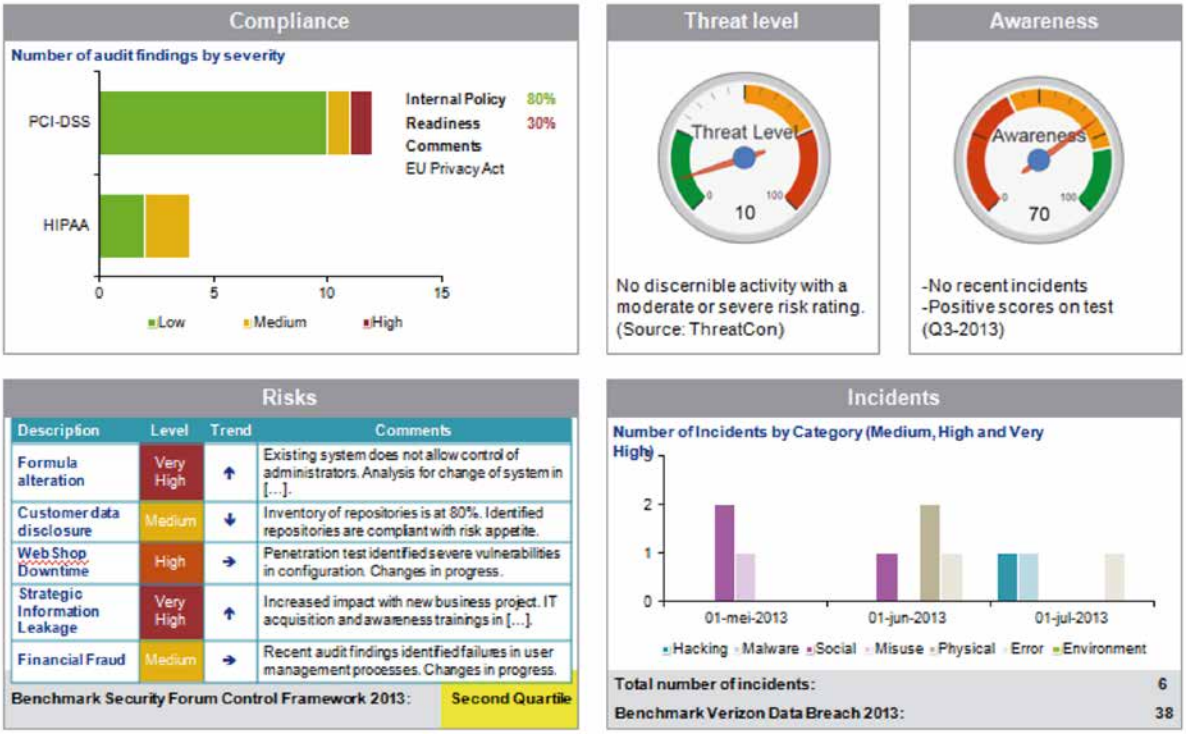
Het is de rol van de CISO om, naast het bepalen van de kaders (securitybeleid), het bestuur te voorzien van de benodigde expertise. Zoals hen informeren over ontwikkelingen in het cyberdomein, belangrijke gebeurtenissen en incidenten bij andere organisaties en nieuwe wet- en regelgeving. Daarnaast heeft de CISO een adviserende taak over zaken als de benodigde security governance en wat er in de organisatie nodig is aan mensen en middelen op het securityvlak.

Om deze rol goed in te kunnen vullen is het ook van belang dat de CISO en zijn team goed in de organisatie gepositioneerd zijn. Immers, hij moet vrij kunnen praten over de securityprestaties van alle businessunits en afdelingen, inclusief IT. Korte rapportagelijnen aan het bestuur zijn hier dan ook het uitgangspunt!

In de praktijk zien we helaas vaak dat de afstand tussen het bestuur en de CISO groot is. Gepositioneerd binnen de IT-afdeling verliest de CISO al snel de ruimte om onafhankelijk te kunnen opereren en wordt zijn toezichthoudende rol op de technische component van cyber security verzwakt. Idealiter is de positie van de CISO en zijn team zodanig dat hij zijn adviserende en toezichthoudende rol over de breedte van de organisatie kan uitvoeren. Dit betekent dat hij/zij een onafhankelijke positie dient te hebben van alle risico-eigenaren onder het bestuur. Op deze wijze kan hij/zij de meeste waarde leveren aan het bestuur in zijn taak de organisatie te behoeden voor de gevolgen van cyber-securityrisico's.

4. De Technisch Directeur neemt het initiatief in het verzorgen van frequente analyses over de competitie en de eigen speelwijze, als input voor de Bondscoach

De meerwaarde van de Technisch Directeur ligt onder meer in de onafhankelijke analyses die hij voor de Bondscoach kan verzorgen. Vanuit zijn rol is hij in staat een blik van buitenaf te geven op de speelwijze van de club, en de individuele spelers. Hij kan dit plaatsen in de context van de nationale en internationale competities. Gevraagd en ongevraagd advies vanuit de één team-gedachte.



Figuur 1. **Cyber dashboards kunnen voorzien in de noodzakelijke goede stuurinformatie.**

De oorsprong van veel cyber-incidenten is terug te voeren op menselijk handelen

Goede stuurinformatie is essentieel voor het bestuur om de verantwoordelijkheid voor cyber security te kunnen dragen. Het is de rol van de CISO om te zorgen dat deze informatie met de juiste diepgang en regelmaat op het bureau van de bestuurders ligt. De kunst is hier om geen lijvig technisch document neer te leggen, maar een 1-pager met Key Performance Indicators (KPI's) die relevant zijn vanuit het businessperspectief. Zo'n cyber dashboard dient zich te richten op de top 10 strategische securityrisico's en de relevante ontwikkelingen in het cyberdomein. De informatie moet op zo'n wijze gepresenteerd worden dat het bestuur er zijn acties op kan bepalen.

De waarde van een dergelijk cyber security dashboard wordt bepaald door de actualiteit en relevantie. De laatste factor komt voort uit de wijze waarop inzicht wordt gegeven aan de informatiebehoefte van bestuur en management. Uiteraard is hier de koppeling met de top 10 strategische risico's van belang, maar het dashboard dient ook informatie te geven omtrent ontwikkelingen in het dreiginglandschap, compliance met wet- en regelgeving, belangrijke incidenten, het niveau van awareness in de organisatie en ontwikkelingen in securityrelevante projecten.

De actualiteit vereist een dynamische aanpak. De ontwikkelingen in het cyberlandschap kenmerken zich immers door een hoog tempo van verandering. Systemen die vandaag nog veilig zijn kunnen morgen kwetsbaar zijn door een nieuw ontdekt beveiligingslek. Een goed cyber dashboard maakt daarom ook zoveel mogelijk gebruik van geautomatiseerde metingen van de feitelijke situatie. Een voorbeeld hiervan is het monitoren van kwetsbaarheden in systemen. Op de markt zijn verschillende systemen verkrijgbaar voor het geautomatiseerd in kaart brengen van patchlevels en compliance met best practices voor systeembeveiliging. De uitkomsten van zo'n compliancescan kunnen worden vertaald in een stoplicht op het dashboard. De samenhang van de verschillende stoplichten voor de verschillende KPI's geeft het bestuur een scherp en actueel inzicht in de digitale weerbaarheid van de organisatie.

5. Het stimuleren van een cultuur waarin alle betrokkenen zich gezamenlijk verantwoordelijk voelen en zijn voor het succes van het gehele team

Het stimuleren van een cultuur waarin alle betrokkenen zich gezamenlijk verantwoordelijk voelen en zijn voor het succes richt zich op het gehele team, te weten de spelers, de fans (medewerkers), de stadionbeheerder (IT) en anderen. De Bondscoach en de Technisch Directeur voelen zich en zijn gezamenlijk verantwoordelijk voor het succes van het gehele team. Dit betekent ook dat betrokkenen die hun rol niet conform afspraak invullen dit in hun beloning kunnen voelen.

Eerder is het belang van het 'three lines of defence'-model aangegeven en is gemeld dat de oorsprong van veel cyberincidenten terug te voeren is op menselijk handelen. De digitale weerbaarheid van een organisatie is dan ook sterk afhankelijk van het bewustzijn van alle medewerkers inzake de digitale risico's. In de praktijk horen we veel organisaties zeggen een cyber-awarenessprogramma te hebben. Helaas blijkt dit veelal niet meer dan een eenmalige e-learning. Dit is net zo realistisch als wanneer je verwacht dat een persoon, na het zien van de voetbaldocumentaire Johan Cruijff – Nr. 14, ineens een volleerd voetballer is.

Het creëren van echte awareness en een cultuur waarin eenieder zich verantwoordelijk voelt voor de digitale veiligheid van de organisatie vergt een continue aanpak. Een aanpak waarin er vanuit leiderschap, voorbeeldgedrag, beloning en training voor gezorgd wordt dat het onderwerp continu en op een positieve wijze onder de aandacht blijft. Voor het opzetten van een gedegen awarenessprogramma adviseren wij veelal in drie fasen te werken:

1. *Informeren*
   Het overbrengen van nut en noodzaak met betrekking tot cyber security. Wat zijn de risico's, waarom is het belangrijk en wat is de rol van de medewerker hierin. In begrijpelijke taal uitleggen, waarbij de relevantie voor de individuele medewerker centraal staat.
2. *Confronteren*
   'Wie niet horen wil moet maar voelen' – dit oud-Hollands spreekwoord is ook prima toepasbaar op cyber security. Immers, mensen die ervaren hoe geraffineerd cybercriminelen te werk gaan zullen zich veel meer bewust zijn van de valkuilen en wat veilig gedrag inhoudt. Belangrijk is wel dat een aanpak gekozen wordt waarin personen niet beschadigd raken.
3. *Uitdagen*
   Hoe zorg je ervoor dat veilig gedrag een onderdeel wordt van het normale werken, van de gedragingen van de medewerkers? Door te zorgen dat medewerkers elkaar gaan aanspreken op onveilig gedrag. De derde stap van een goed awarenessprogramma is er dan ook op gericht

om dit te realiseren. Dit kan vanuit verschillende positieve incentives worden ingestoken, zoals beloning en competitie.

De vraag hoe cyber security is ingebed in het management-developmentprogramma van de organisatie wordt meestal met een stilzwijgen beantwoord. Terwijl dit toch een prima manier is om de verantwoordelijkheid voor dit belangrijke onderwerp echt in de organisatie te verankeren. Wij zouden de HR-afdelingen van organisaties dan ook echt adviseren om te bezien hoe cyber security is ingebed in hun eigen HR-programma's. Immers, het realiseren van het benodigde bewustzijn door de gehele organisatie heen vergt veelal een cultuurverandering. En dit is een rol waarin zeker kansen liggen voor HR-afdelingen.

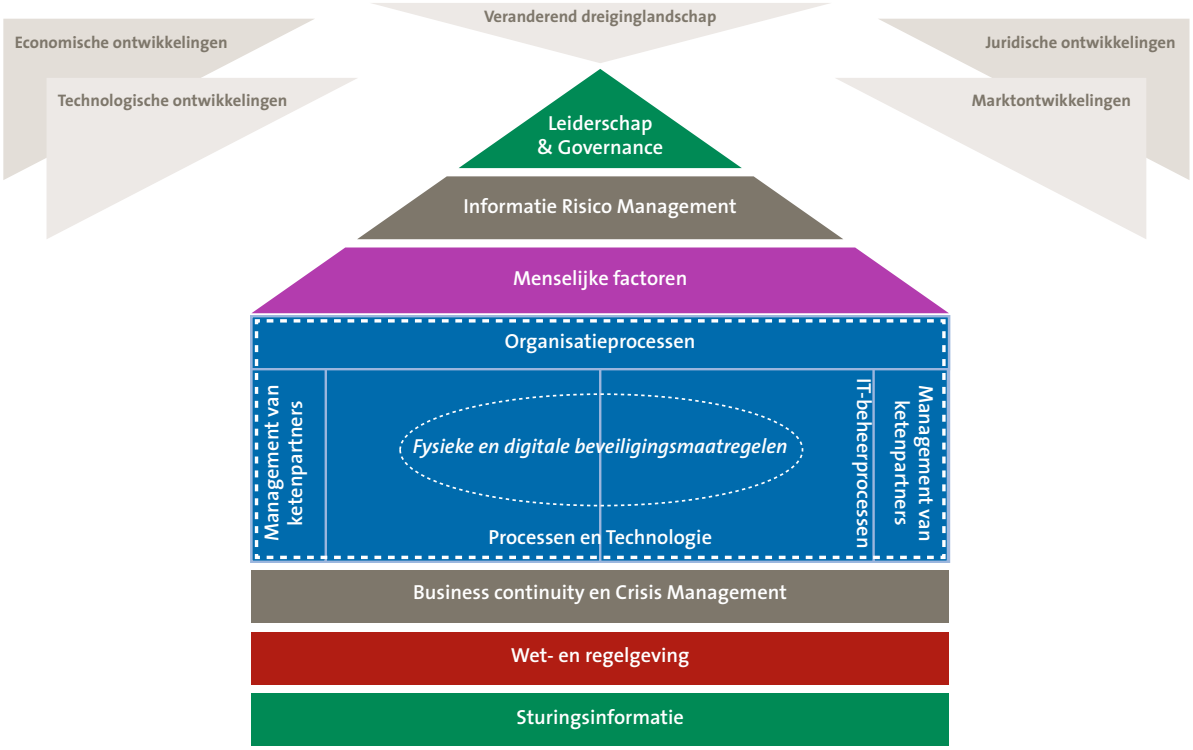
Tot slot

Rond cyber security hangt nog veelal de zweem van een complex onderwerp voor technisch specialisten, een onderwerp dat vooral ver van de bestuurskamer moet blijven. Met dit artikel willen wij illustreren dat de verantwoordelijkheid voor cyber security onterecht wordt beschouwd als een technisch probleem, een probleem dat vooral bij de 'Technisch Directeur' neergelegd moet worden. Ja, voor bepaalde elementen is specialistische kennis nodig, maar bovenal is cyber security een onderwerp dat een integraal onderdeel van de bedrijfsvoering dient te zijn. Een onderwerp dat met de risicobril bekeken moet worden en dat, net als kwaliteit, de verantwoordelijkheid van het management is. Pas wanneer cyber security op integrale wijze benaderd wordt kan het proces van cybertransformatie ingezet worden, een proces waarin een organisatie op een verantwoorde wijze naar het gewenste volwassenheidsniveau wordt gebracht. Een proces dat van strategisch belang is voor organisaties en dat zelfs kan bijdragen aan het verhogen van het onderscheidend vermogen van organisaties.

Kortom, cyber security is geen technisch probleem, maar een leiderschapsprobleem. Wil de echte Bondscoach nu opstaan!

Over de auteur

Drs. D. de Geus RE RA CISA is senior manager bij KPMG Advisory N.V. Zijn visie is dat cyber security een waarde creërende factor voor organisaties kan zijn, mits vanuit een integraal perspectief geïntegreerd. Vanuit een ruime praktijkervaring als IT security professional helpt hij organisaties het gewenste niveau van cyber resilience te realiseren.



Figuur 2. **Een integrale benadering van cyber security voorkomt dat dit wordt gezien als een puur technisch probleem.**