KPMG

3e Cyber Security Benchmark

Aandacht in bestuurskamer neemt toe, maar is nog te versnipperd

Juni 2016

KPMG.com

Inleiding

"De uitgebreide diepgang waarmee het onderwerp Cyber Security werd besproken heeft in 2015 een kleine afname gezien. Het managen van risico's van Cyber Security wordt dit jaar wel meer dan voorgaande jaren toegeschreven aan het bestuur."

Nu Cyber Security het nieuws dagelijks beheerst, verwacht men dat Nederlands grootste ondernemingen voldoende aandacht besteden aan dit onderwerp. Maar aandacht alleen is niet genoeg. Het is ook belangrijk dat het bestuur de commissarissen en aandeelhouders voldoende informeert over risico's voor de organisatie op het gebied van Cyber Security. Gebeurt dit?

Uit een jaarlijks onderzoek van KPMG naar de berichtgeving van Cyber Security risico's in de beschikbare jaarverslagen van ondernemingen uit de AEX en Midkap blijkt dat de berichtgeving ontoereikend is. Hoewel ruim 83% van de jaarverslagen melding maakt van Cyber Security, blijkt na nader onderzoek slechts 66% dat te doen met enige mate van diepgang voor wat betreft dreigingen, risico's of maatregelen.

De ondermaatse berichtgeving is opmerkelijk. Per slot van rekening zijn bedrijven in toenemende mate afhankelijk van IT voor vitale bedrijfsprocessen, zowel op het gebied van beschikbaarheid van die IT alsook wat betreft integriteit en vertrouwelijkheid. Dit betekent in het ergste geval dat bedrijven zelfs failliet kunnen gaan als zij Cyber Security risico's onvoldoende beheersen. Een goed voorbeeld hiervan is de centrale bank van Bangladesh, waar in februari van dit jaar een bedrag van 81 miljoen dollar is gestolen door hackers.

Naast directe en meetbare schade is er bovendien veel indirecte en onmeetbare schade. Gestolen intellectueel eigendom, schade aan reputatie en toezichthouders die boetes uitdelen; het zijn slechts enkele voorbeelden.

Commissarissen en aandeelhouders alsook toezichthouders zouden moeten verlangen dat zij voldoende worden geïnformeerd over Cyber Security risico's, om tijdig bij te sturen om deze risico's adequaat te beheersen en de continuïteit van de bedrijfsvoering te waarborgen. In sommige sectoren zien we al een sterke focus op Cyber Security risico's van deze stakeholders, zoals in de financiële sector waar de DNB (en op haar beurt ook de ECB) hierover sterke verwachtingen uitspreekt.

In een publicatie van mei dit jaar mengt ook de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) zich in de discussie. Zij stellen, terecht, dat ook accountants zich moeten focussen op het onderwerp bij het vaststellen van de juistheid van de jaarrekening en de continuïteit van de bedrijfsvoering van de onderneming. De NBA legt ook duidelijk een verantwoordelijkheid voor Cyber Security in de bestuurskamer. Zoals hieronder ook is afgebeeld, wordt dit onderwerp nog te veel afgeschoven op individuele afdelingen binnen ondernemingen (vrijwel altijd de IT-afdeling), en ziet zelfs de CIO door de bomen het bos niet meer.

Wel zien we een duidelijke trend. Het onderwerp Cyber Security dringt de afgelopen jaren steeds verder door tot de bestuurskamer. Ook de diepgang kent een bescheiden stijgende lijn. Hoewel het aantal bedrijven dat uitgebreid aandacht aan Cyber Security besteedt is gedaald. Dit jaar is de aandacht voor bewustzijn en privacy wel opvallend. Privacy veelal ingegeven door de – sinds 1 januari 2016 ingevoerde – wetgeving die het melden van privacygerelateerde datalekken verplicht stelt. De aandacht voor het onderwerp bewustzijn is opvallend, en zeer positief. In onze visie, is en blijft de mens één van de zwakste schakels en een structureel terugkerende oorzaak van veel incidenten. De groeiende aandacht voor dit onderwerp, zelfs tot de bestuurstafel aan toe, wordt zodoende door ons met enthousiasme ontvangen.

Om als bestuurder de afdelingen, of als commissaris het bestuur van de onderneming de juiste vragen te stellen over de stand van Cyber Security, is het van groot belang een aantal zaken te weten, zoals:

- Wat is het dreigingsbeeld van de onderneming: **wie zijn mijn 'tegenstanders'?**
- Wat zijn de cruciale bedrijfsprocessen, applicaties of data die ik wil beschermen: **wat zijn mijn 'kroonjuwelen'?**
- Wat zijn mijn belangrijkste projecten en hoe monitor ik de effectiviteit ervan: **hoe vorderen de verbetertrajecten?**

KPMG heeft uitgebreide ervaring met het helpen beantwoorden van deze vragen en inzichtelijk te maken op bestuursniveau. Daarnaast biedt de KPMG Cyber Trends Index (http://cyber.kpmg.com) een zeer actueel en sectorgericht overzicht van trends en dreigingen op het gebied van Cyber Security. Bestuurders kunnen hierdoor dagelijks op de hoogte blijven van het externe dreigingsbeeld.

In een jaarlijks terugkerend onderzoek naar aandacht voor het onderwerp Cyber Security in jaarverslagen, heeft KPMG bovenstaande observaties gedaan. In de volgende pagina's zal dieper worden ingegaan op de specifieke onderwerpen en verschillen tussen sectoren. Het is duidelijk dat het onderwerp langzaam de bestuurstafel weet te vinden (83%), alhoewel enige diepgang van het onderwerp in het jaarverslag nog achter blijft (66%).

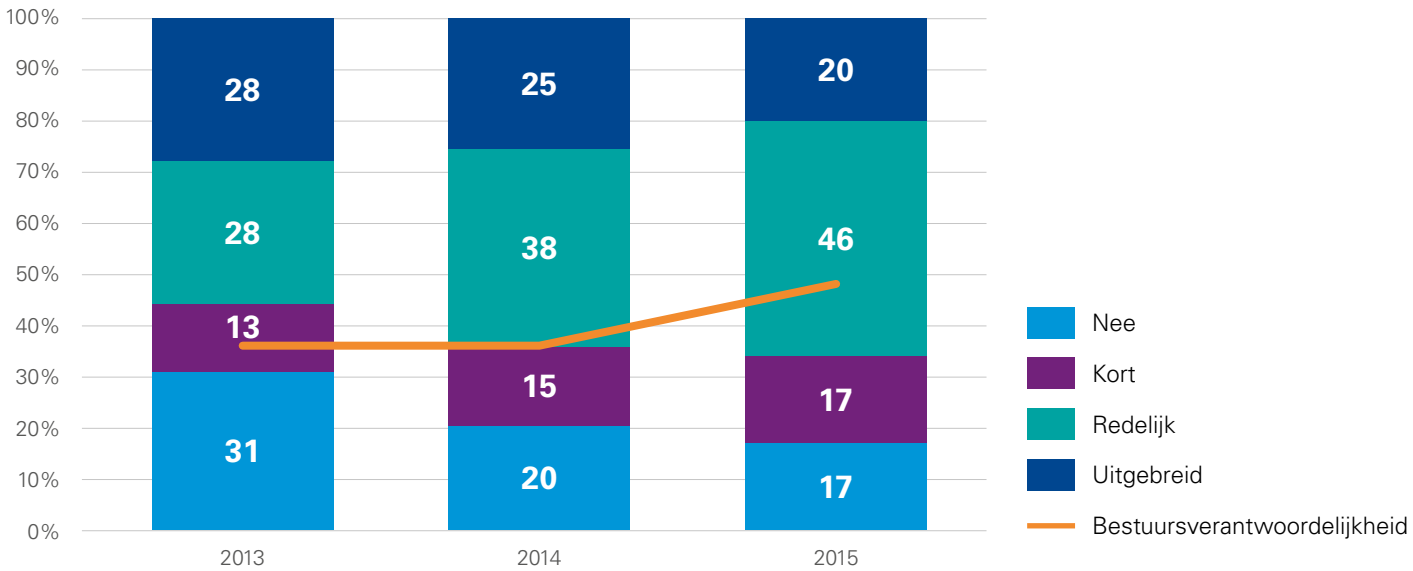
In de bestuurskamer

Zoals hierboven te zien valt, vindt Cyber Security zijn weg al wel steeds meer richting de bestuurskamer. Daar aangekomen blijft het echter een onderwerp waarvan men niet weet hoe die precies te beleggen. Commissarissen hebben moeite met de juiste vragen stellen, bestuurders vinden het veelal een IT-feestje, de meeste data privacy officers zijn nog zoekende naar hun rol binnen het onderwerp en de op dit moment hoogst verantwoordelijke voor IT (CIO) ziet intussen tussen de bomen het bos niet meer. Dit resulteert in een diffuse aanpak, en onvoldoende gerichte aandacht voor het uiteindelijke risico voor de organisatie. Dit zien we ook terug in de berichtgeving naar aandeelhouders in het jaarverslag.

Er is wel een trend waar te nemen waarin we een toename zien van het adresseren van het onderwerp in het jaarverslag. De diepgang waarmee het onderwerp Cyber Security werd besproken, heeft dit jaar echter geen vooruitgang gezien, en zelfs een kleine afname. Het managen van risico's van Cyber Security wordt dit jaar wel meer dan voorgaande jaren toegeschreven aan het bestuur.

In onderstaande figuur wordt aangegeven hoeveel jaarverslagen wat voor diepgang kenden voor het onderwerp Cyber Security. Daarnaast tonen de figuren in hoeveel procent van de jaarverslagen het risico Cyber Security als bestuursverantwoordelijkheid wordt belegd.

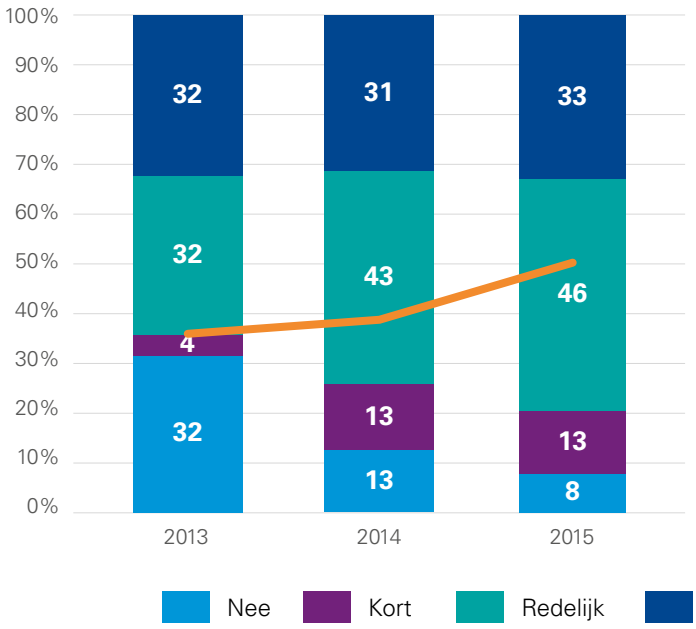
FIGUUR 1 **PERCENTAGE JAARVERSLAGEN DAT CYBER SECURITY NOEMT**



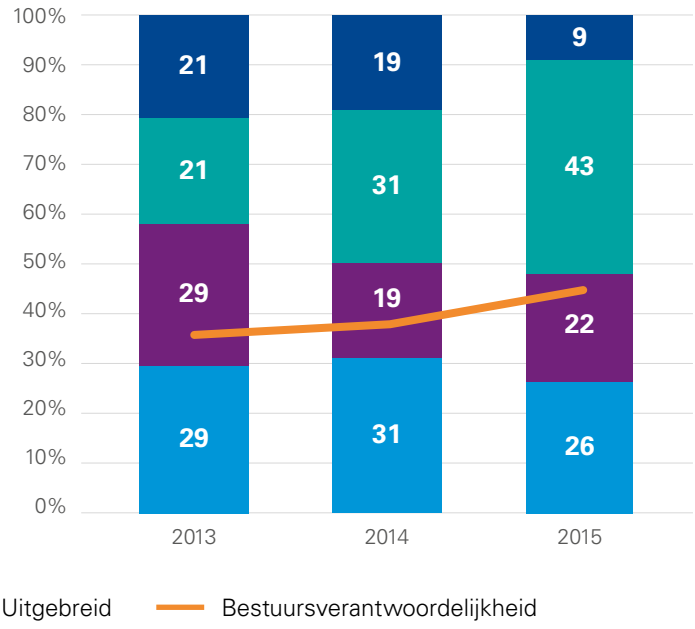
"Nieuwkomers in de AEX en Midkap beschrijven risico's en maatregelen uitgebreider dan oudgedienden. Ook in beleggen van de bestuursverantwoordelijkheid doen zij het beter."

Wanneer we de AEX (25 grootste ondernemeningen) en de Midkap (volgende 25) splitsen, zien we dat er een duidelijk verschil merkbaar is tussen de grootste ondernemingen, en de daaropvolgende. Met name opvallend, is het aantal bedrijven in de Midkap dat het onderwerp niet behandelt. Dat aantal is al drie jaar redelijk stabiel. Ook de diepgang kent een fors verschil.

FIGUUR 2 **PERCENTAGE JAARVERSLAGEN AEX DAT CYBER SECURITY NOEMT**

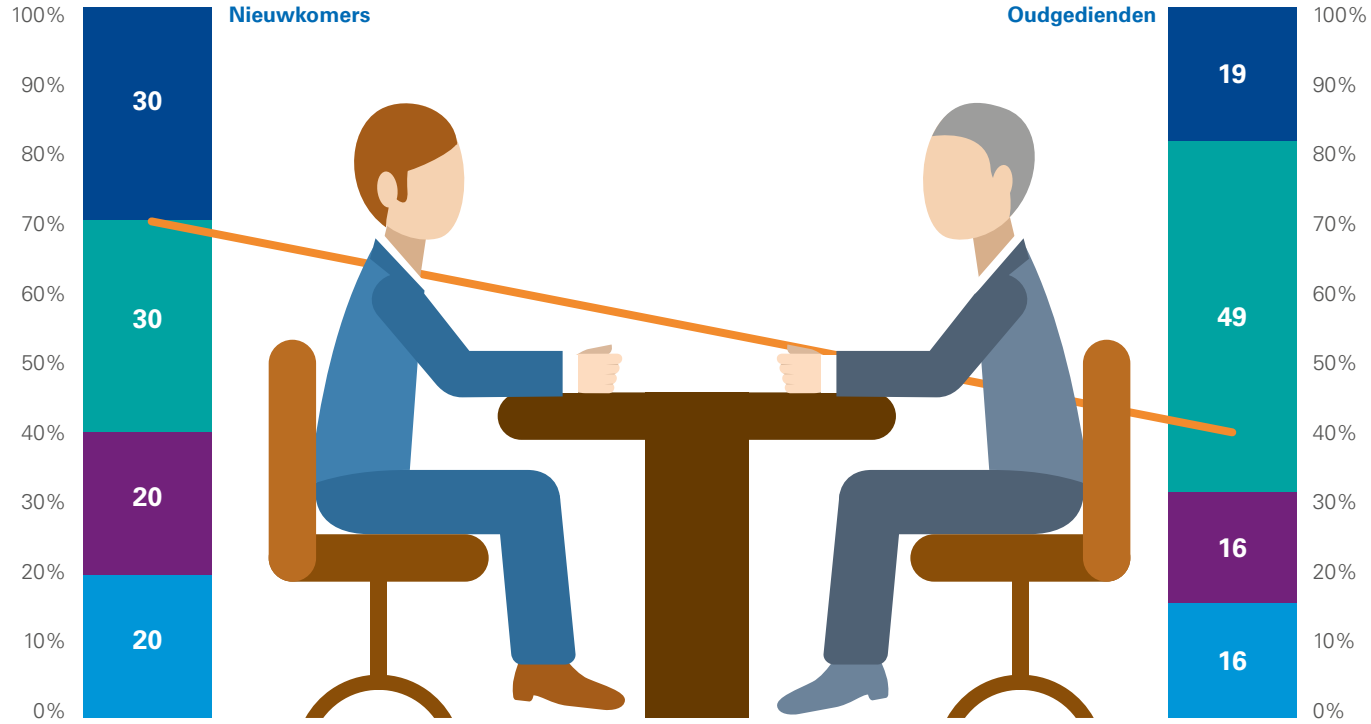


FIGUUR 3 **PERCENTAGE JAARVERSLAGEN MIDKAP DAT CYBER SECURITY NOEMT**



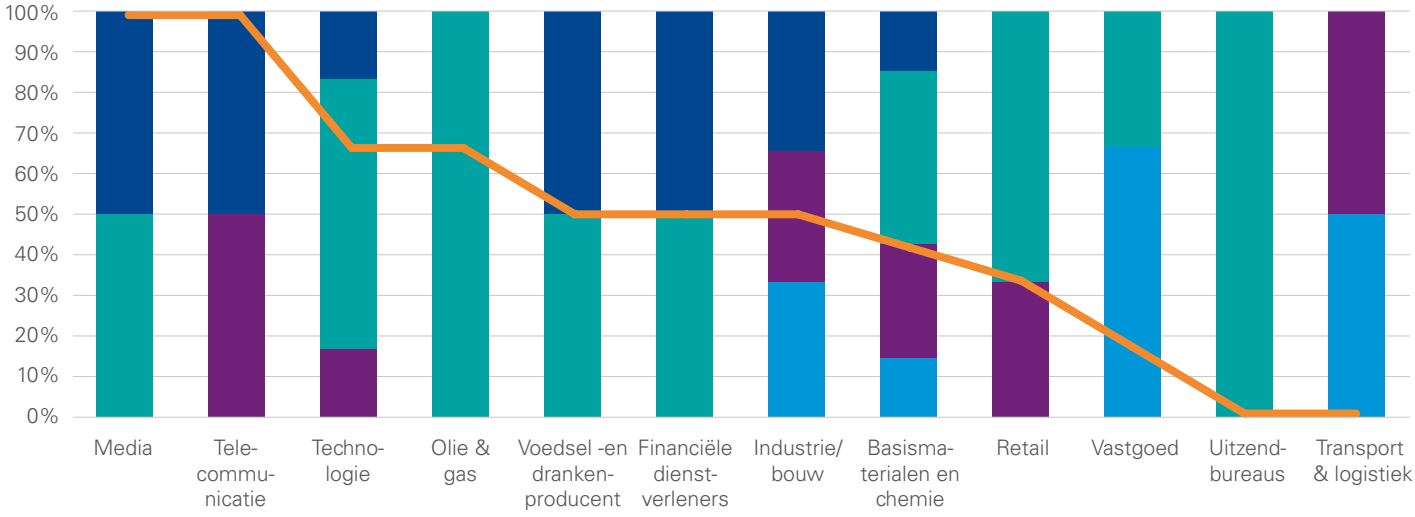
Wanneer nieuwkomers in de AEX en Midkap vervolgens worden afgezet tegen oudgedienden, valt op dat zij zowel op de diepgang van Cyber Security als het toeschrijven van bestuursverantwoordelijkheid meer aandacht voor dit onderwerp hebben.

FIGUUR 4 **VERSCHIL IN NOEMEN CYBER SECURITY NIEUWKOMERS EN OUDGEDIENDEN**



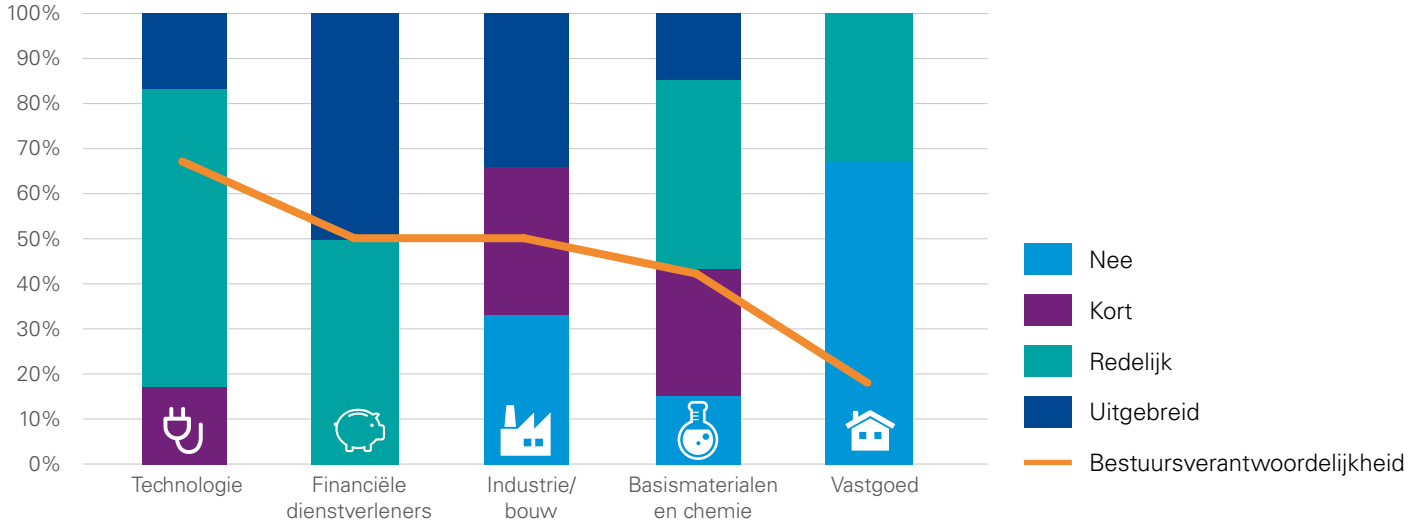
Verschillende sectoren zijn in verschillende mate afhankelijk van IT. Daarnaast kennen bedrijven in deze sectoren verschillende waarde toe aan kroonjuwelen van de organisatie. Het is dan ook niet verwonderlijk om een groot verschil te zien tussen het aantal bedrijven binnen een sector dat Cyber Security meeneemt in het jaarverslag, de diepgang en de bestuursverantwoordelijkheid.

FIGUUR 5 **SECTOROVERZICHT PERCENTAGE JAARVERSLAGEN DAT CYBER SECURITY NOEMT**



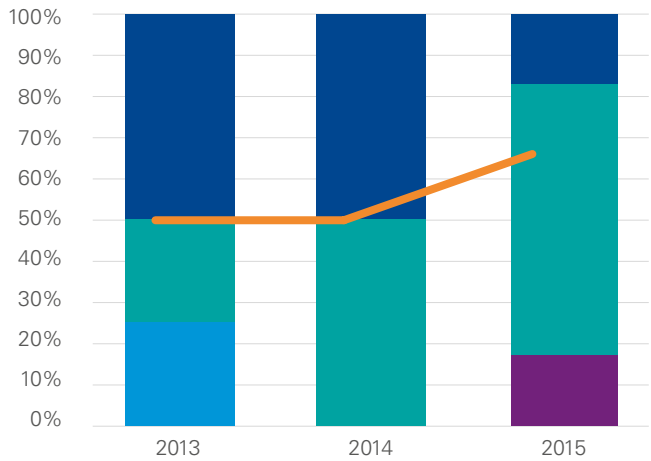
Vooral binnen de grotere sectoren (meer dan drie bedrijven in de statistieken) is goed te zien wat het betekent om in een bepaalde sector werkzaamheden te verrichten. Hier valt duidelijk te zien dat bedrijven in de technologie en financiële dienstverleningssector aandacht besteden aan dit onderwerp, alsmede het toeschrijven van bestuursverantwoordelijkheid. Een sector als vastgoed heeft duidelijk minder met het onderwerp. Hieronder zullen we de vijf sectoren die het meest vertegenwoordigd worden in de statistieken, nog nader toelichten.

FIGUUR 6 **OVERZICHT PERCENTAGE JAARVERSLAGEN DAT CYBER SECURITY NOEMT GROOTSTE SECTOREN**



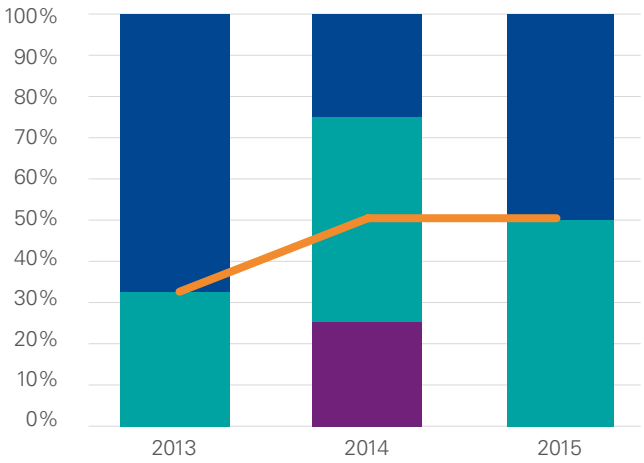
TECHNOLOGIE

In de technologiesector heeft elke onderneming het onderwerp meegenomen in het jaarverslag na 2013. Wel zien we dat de diepgang van het onderwerp achteruitgang kent. Dit zou te maken kunnen hebben met aandacht voor andere opkomende trends in die sectoren, zoals Big Data en Internet of Things. Opvallend is de stijgende lijn voor bestuursverantwoordelijkheid, welke goed te verklaren is door recente incidenten.



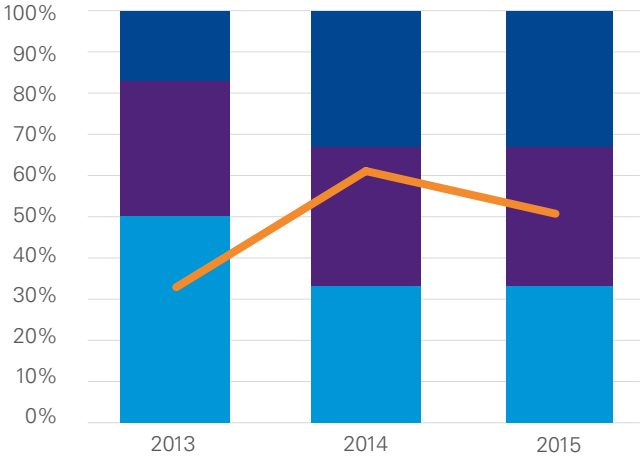
FINANCIËLE DIENSTVERLENERS

Financiële dienstverleners zijn door wet- en regelgeving gebonden aan rapportages over Cyber Security, zodoende zien we ook dat het onderwerp bij alle organisaties in deze sector in het jaarverslag terug te vinden is. De diepgang van het onderwerp toont wel een schommelend beeld. Een verklaring hiervoor zou kunnen liggen in de wisselende wet- en regelgeving waar financiële dienstverleners mee te maken krijgen in verslaglegging. Ook wisselende interesse voor het onderwerp Legacy-systemen in het jaarverslag, kan hier een rol spelen. Toenemende interesse voor het onderwerp privacy in jaarverslagen over 2015 ligt aan de basis voor de stijging van diepgang dit jaar. Opvallend is dat 50% van de bestuurders niet verantwoordelijk wordt geacht voor Cyber Security, waar hun bedrijfscontinuïteit volledig afhankelijk is van IT.



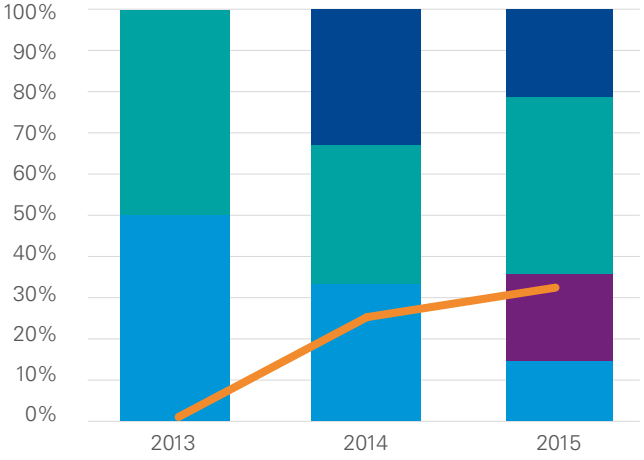
INDUSTRIE/BOUW

In de industrie- en bouwsector zijn enkele organisaties zeer stabiel in uitgebreide beschrijvingen van Cyber Security in het jaarverslag alsmede toeschrijving van bestuursverantwoordelijkheid. Andere organisaties in die sector schommelen tussen het meenemen van het onderwerp. Opvallend is, dat als organisaties ervoor kiezen het onderwerp mee te nemen, zij het ook in minimaal de helft van de gevallen opnemen als bestuursverantwoordelijkheid. Het ligt in de natuur van dit soort organisaties om risico's in het jaarverslag op te nemen als bestuursverantwoordelijkheid, gedreven door risico's rondom gezondheid, veiligheid en omgeving (HSSE).



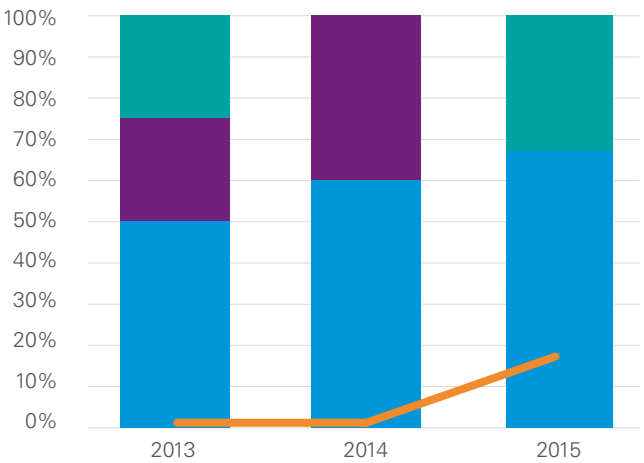
BASISMATERIALEN EN CHEMIE

In de sector basismaterialen en chemie wordt het besef van het intellectueel eigendom waarover zij beschikken steeds belangrijker. Dit verklaart een stijgende lijn in het meenemen van het onderwerp. In zekere mate is er ook een stijging wat betreft de diepgang waarin risico's en maatregelen worden beschreven in het jaarverslag. Bestuursverantwoordelijkheid moet van ver komen, maar is bezig aan een langzame klim.



VASTGOED

In de vastgoedsector is het gebruik van IT veel lager, en daarmee de afhankelijkheid van IT voor bedrijfscontinuïteit een minder grote zorg. Dit is ook duidelijk terug te zien in ietwat variërende, maar continue lage scores voor het meenemen van het onderwerp, de diepgang alsook de bestuursverantwoordelijkheid.



Nee
Kort
Redelijk
Uitgebreid
Bestuursverantwoordelijkheid

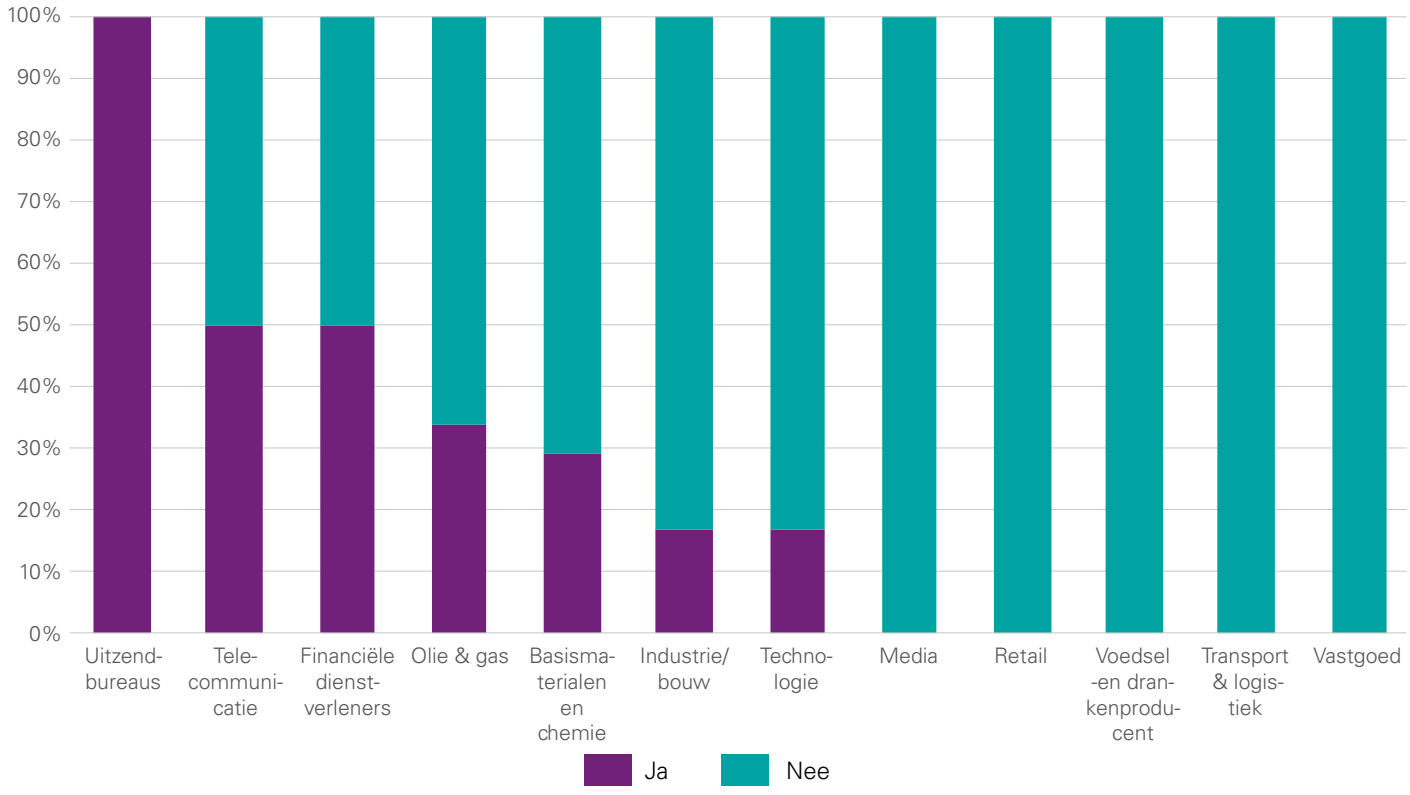
Bewustzijn

Het verhogen van bewustzijn van Cyber Security onder medewerkers wordt door professionals al jaren genoemd als één van de belangrijkste investeringen die organisaties kunnen doen. Vrijwel elke bekende cyberaanval van de laatste jaren begon met uitbuiting van een menselijke fout.

Onderdeel van een succesvol programma om bewustzijn voor Cyber Security binnen de organisatie te verhogen kan bestaan uit het testen van het bewustzijn. KPMG voert regelmatig dit soort testen uit, waarbij we bijvoorbeeld phishing e-mails inzetten, USB-sticks verspreiden of fysiek proberen het pand van de organisatie binnen te komen. Na zo'n test volgt er vaak een bewustwordingstraining, waarin wordt teruggegrepen op de uitgevoerde test.

Dit jaar is de uitgebreide aandacht voor bewustzijn, met name in de sectoren uitzendbureaus, telecommunicatie en financiële dienstverleners opvallend. Bewustzijn is een onderwerp dat in elke organisatie, onafhankelijk van de sector, een belangrijk thema zou kunnen zijn. Dat verklaart ook waarom bij sectoren waar een grotere aandacht voor Cyber Security is, niet per definitie meer aandacht voor bewustzijn hoeft te zijn.

FIGUUR 7 **SECTOROVERZICHT PERCENTAGE JAARVERSLAGEN DAT BEWUSTZIJN NOEMT**



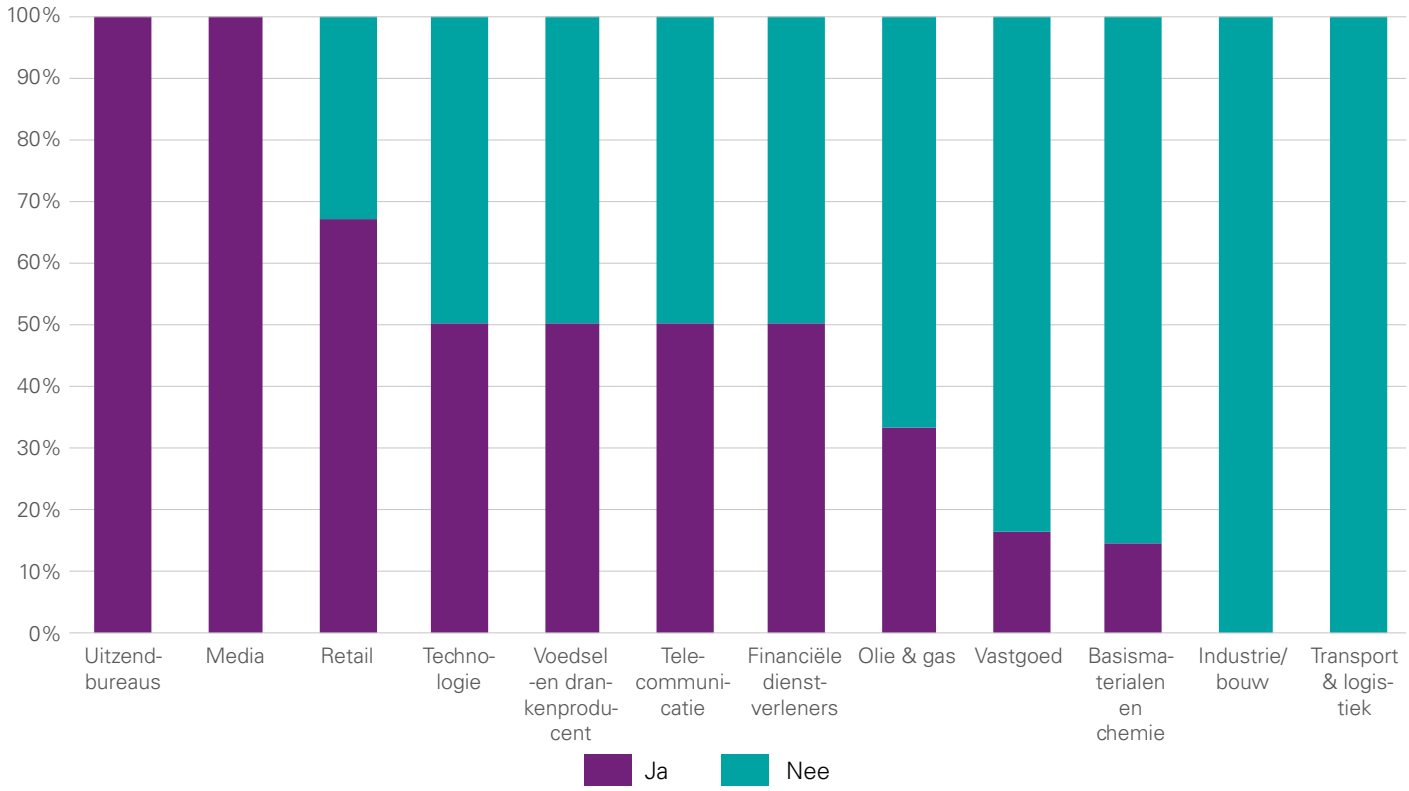
Privacy

Sinds 1 januari 2016 zijn organisaties verplicht om datalekken te melden bij de Autoriteit Persoonsgegevens. Boetes op schending van privacy zijn verhoogd en kunnen nu om verschillende redenen worden opgelegd. Voor veel organisaties betekent dit dat zij hun privacy op orde dienen te hebben. Met name voor de grote organisaties, met veel internationale vestigingen, is dat een uitdaging. Ongetwijfeld heeft dit gezorgd voor een toename in het adresseren van privacy in jaarverslagen.

In ons werk komen wij veel organisaties tegen die moeite hebben met het lokaliseren van de privacygevoelige data die zij verwerken. Naast een veelheid aan systemen, applicaties en databases, zijn er veel eindgebruikers die over uittreksels van die data beschikken. KPMG helpt organisaties in het lokaliseren van al dit soort privacygevoelige data, en helpt in het beschermen van die data.

Anders dan bij bewustzijn, is privacy een onderwerp dat nogal kan variëren per sector. Het is bijvoorbeeld niet verwonderlijk dat de uitzendbranche, die van nature veel privacygevoelige data verwerkt, hoog scoort op het benoemen van risico's gerelateerd aan privacy en privacyprogramma's die gestart zijn.

FIGUUR 8 **SECTOROVERZICHT PERCENTAGE JAARVERSLAGEN DAT PRIVACY NOEMT**



Contact

John Hermans
Partner
KPMG Cyber, EMA Lead Cyber Security
E: hermans.john@kpmg.nl
https://nl.linkedin.com/in/jamhermans
@jhermans_kpmg

Dennis van Ham
Director
KPMG Cyber, Corporate Clients
E: vanham.dennis@kpmg.nl
https://nl.linkedin.com/in/dennis-van-ham-406132
@dennisvanham

Ton Diemont
Senior manager
KPMG Cyber, Cyber in de boardroom
E: diemont.ton@kpmg.nl
https://nl.linkedin.com/in/tondiemont
@TonDiemont

Ruud Verbij
Consultant
KPMG Cyber, Cyber in de boardroom
E: verbij.ruud@kpmg.nl
https://nl.linkedin.com/in/ruud-verbij-37ba43a

Met contributies van Stijn van Winsen, Roy Kreuse en Max Kerkers.

KPMG on social media

Download on the App Store

KPMG app

http://www.kpmg.com/nl/cyber
http://cyber.kpmg.com

Cyber in de Boardroom

Connecting the dots