# Hoe kunnen ondernemingen zich wapenen tegen de risico's van digitalisering en hyperconnectivity?

Komen klanten nog naar een bedrijf toe als dat privacygevoelige informatie kwijtraakt? Hoeveel is een goede reputatie waard, en hoe kunnen ondernemingen zich wapenen tegen de risico's van digitalisering en hyperconnectivity? Carin Gorter, commissaris bij ING Groep, VGZ en het CBR, geeft haar visie: "Als je niet weet waar verantwoordelijkheden liggen, is het lastig toezicht houden."

"Of je nu een boek bestelt, een reis boekt of boodschappen doet bij de supermarkt: op allerlei plaatsen wordt informatie over jezelf vastgelegd. Dat is in het bedrijfsleven precies hetzelfde. Het beveiligen van assets en reputatie is niets nieuws, maar digitalisering verandert het wel."
Gorter vertelt dat jonge techneuten haar aanraadden om bij de bedrijven waar ze toezichthouder is eens te vragen wie er verantwoordelijk is voor de beveiliging van 'softe' gegevens. "Wie is verantwoordelijk voor de beveiliging van systemen, klantendata en andere kritische digitale bedrijfsgegevens? Wie is verantwoordelijk voor de kwaliteit van klantgegevens en het gebruik van zowel vaste als variabele gegevens? Wat gebeurt ermee? De vraag stellen is al de moeite waard: je weet dan of het duidelijk is wie de verantwoordelijkheden draagt. En als je niet weet waar verantwoordelijkheden liggen, is het lastig toezicht houden."

### De economische impact van ICT

"De Erasmus-universiteit deed in 2010 onderzoek naar commissarissen en ICT. De nadruk lag toen op het monitoren van ICT-projecten en op de uitval van systemen. De meerderheid van de commissarissen vond dat ze voldoende kennis in huis hadden. Maar het onderzoek ging nauwelijks over digitalisering en het vastleggen van gegevens.

Drs. Carin Gorter RA is commissaris bij ING Groep en Coöperatie VGZ, en lid van de Raad van Toezicht bij het Onze Lieve Vrouwe Gasthuis en het Centraal Bureau Rijvaardigheidsbewijzen en bestuurslid bij Schouwburg Velsen. Ze was eerder lid van de Monitoring Commissie Code Banken en bekleedde verschillende functies op het gebied van risk, control, audit en compliance bij ABN AMRO, waaronder de positie als Head of Group Compliance & Security tussen 2004 en 2008.

Ik heb mijn les in nederigheid inmiddels gehad wat betreft ICT ontwikkelingen en heb besloten dat er heel veel te leren valt. Digitalisering evolueert zo snel dat we over het idee heen moeten stappen dat 'dit ons niet kan gebeuren'. Mijn stelling is dat alles wat met het internet verbonden is gehackt kan worden. En alles is of wordt verbonden met het internet. Dat is iets om goed over na te denken in je strategische risicoanalyse: hoe staat het er bij ons voor en waar gaat het naartoe? De economische impact van ICT-ontwikkelingen is groot. Bij distributiekanalen wordt de integratie in je keten groter. We zien al dat klanten gegevens kunnen muteren, en je krijgt meer leveranciers die gekoppeld worden aan je ICT-systemen. Dat heeft veel invloed op je beveiliging en op je privacy, waarbij het complexer wordt als je grensoverschrijdend werkt en met meerdere wetgevingen te maken hebt."

'Als je niet weet waar verantwoordelijkheden liggen, is het lastig toezicht houden'

Niet iedereen schat het belang van privacy even hoog in, aldus Gorter. "Ik heb thuis twee pubers. Zij hebben een heel ander beeld van privacy en delen gemakkelijk allerlei gegevens. Die pubers zijn de medewerkers van de toekomst bij bedrijven waar wij toezicht houden. Het is nu al zo dat al meer dan de helft van alle medewerkers die nu bij een bedrijf weggaan, gevoelige data meeneemt naar hun volgende baan. Dat zijn assets van bedrijven, en dat is iets wat ons allemaal gaat raken."

### Problemen met privacy

Gorter voorziet problemen met de nieuwe Europese privacywetgeving. "Dat gaat wringen. ICT geeft meer mogelijkheden dan ooit, terwijl mensen het minder snel doorhebben wanneer ze zich buiten de toegestane paden begeven. En de nieuwe toekomstige EU-normering is tamelijk stevig. Dus je hebt aan de ene kant een groep nieuwe medewerkers met ruime opvattingen over privacy, en aan de andere kant wetgeving met meer voorschriften en met boetes van 1 miljoen euro tot maximaal 2% van de global revenues. Die frictie moet je oplossen. Daar moeten wij als commissarissen alert op zijn, zeker omdat de regels per land kunnen verschillen. Bij het outsourcen of offshoren van ICT moet je daarom extra opletten. Overal worden bestanden gekocht voor het analyseren van big data. Maar persoonsgegevens zijn gevoelig, dus je moet goed kijken wat je binnenhaalt. Is het wel toepasselijk voor de diensten die je verkoopt, of het product dat je aanbiedt?"

### De kansen van digitalisering

Er liggen op het gebied van digitalisering duidelijke kansen voor de raad van commissarissen aldus Gorter. "Digitalisering heeft immers raakvlakken met strategievorming, besluitvorming en corporate governance. Het is een uitgelezen kans om jezelf hierin te verdiepen en ICT prominenter op de agenda te zetten. Maar het gaat te langzaam. Eens per jaar ICT bespreken is niet langer voldoende. En er zijn meer aspecten. Denk aan compliance met de wetgeving of ethische vraagstukken. Je kunt je afvragen of je bepaalde services wel wilt creëren, ook al mag het wel volgens wetgeving. De vraag is of deze diensten bijdragen aan een duurzame waardecreatie voor de klant en het bedrijf. Niet alles past bij het bedrijfsmodel.

Daarom moet je als commissaris vragen blijven stellen. Hoe is het vigerende privacybeleid en welke eisen worden op basis daarvan gesteld aan datakwaliteit en datamanagement? Hoe wordt dat vertaald in IT-controls? Hoe is de risico- en kwetsbaarheidanalyse van privacy-incidenten uitgevoerd? Hoe is de adequaatheid van de hierop van toepassing zijnde IT-controls vastgesteld? Werken legal en ICT samen aan deze problematiek? Dat zijn enkele zaken die je in het oog moet houden. Controleer de operationele effectiviteit van het beleid. Kijk buiten je keten, schakel desnoods externe deskundigen in, zoals bijvoorbeeld ethical hackers.

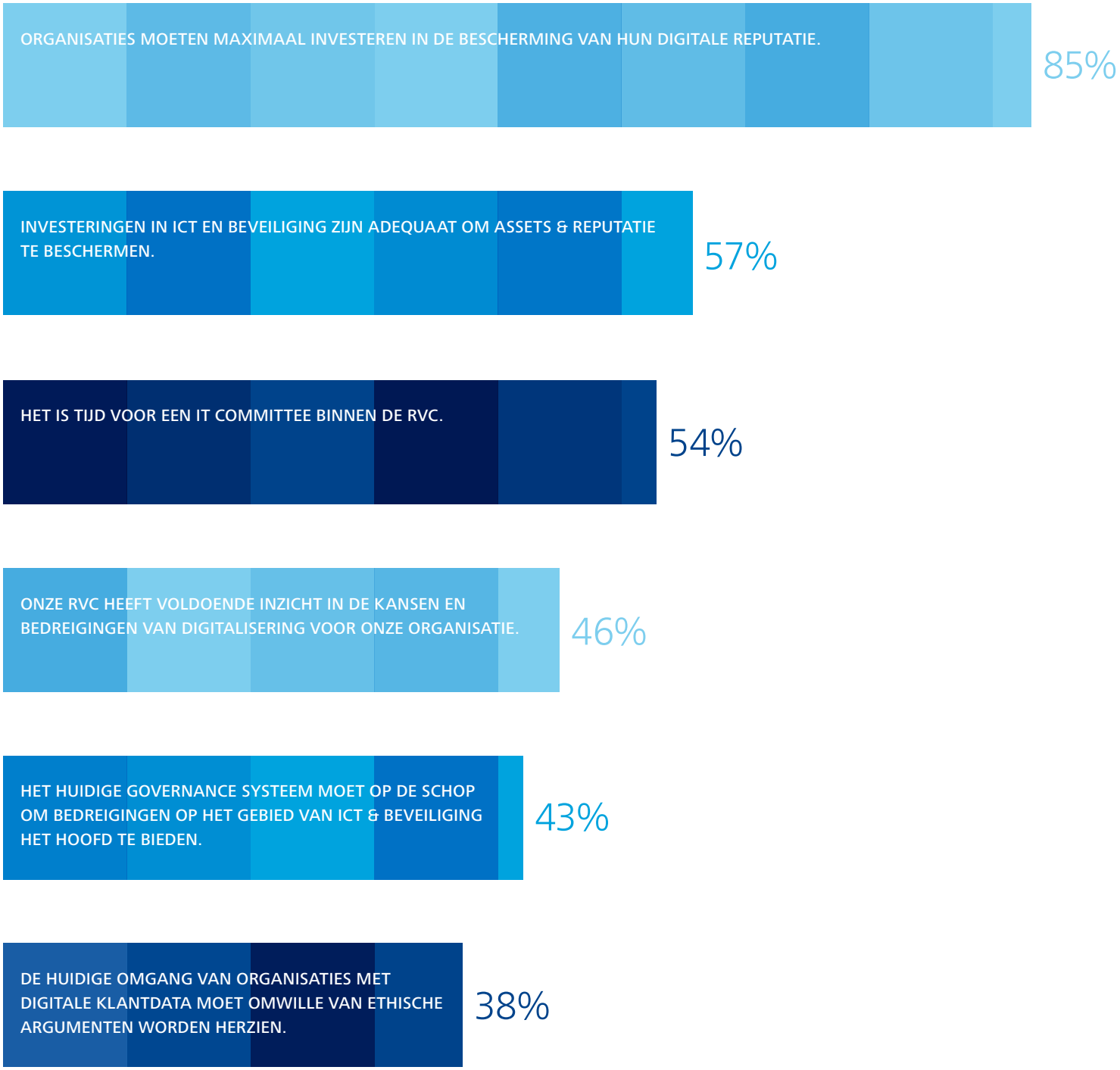
De kernvraag is: wie is verantwoordelijk, wat wordt er met gegevens gedaan en hoe zorgen we ervoor dat de informatie niet uit de organisatie verdwijnt op een manier die we niet willen? Dat zijn kwesties die ons aan de beheerskant altijd al bezighielden, maar die een nieuwe dynamiek hebben gekregen."

# ‘Alles wat met internet is verbonden kan gehackt worden’

Carin Gorter,
commissaris
ING Groep

### Wij zijn IT eens

Voorafgaand aan het commissarissendebat over 'Digitalisering en de verantwoordelijkheden van de RvC', hebben we een zestal stellingen aan de deelnemers voorgelegd. Via deze stellingen peilen we de opinie van de commissarissen over onderwerpen die tijdens de bijeenkomst besproken worden. De stellingen die de meeste controverse oproepen zijn vervolgens in het daadwerkelijke debat behandeld. Onderstaand treft u de uitkomsten van de opiniepeiling over het acteren van commissarissen met betrekking tot de digitale agenda.



### Stellingen

Stelling: Onze raad van commissarissen heeft voldoende inzicht in de kansen en bedreigingen van digitalisering voor onze organisatie.
"Inzicht is in grote lijnen weten hoe het zit", zegt de eerste spreker. "Je hoeft dus geen expert te zijn. Zo bekeken heeft de raad van commissarissen waar ik in zit voldoende inzicht. Het onderwerp staat regelmatig op de agenda en we vragen door".
"Ik denk dat we wel weten wat de kansen en bedreigingen zijn", reageert een commissaris. "Maar weten we ook hoe we problemen kunnen oplossen? De awareness zie ik wel, maar er is niet altijd zicht op de aanpak. Je kunt niet op hoofdlijnen besturen als je de details niet begrijpt. Als het er echt op aankomt, is het hinderlijk om te werken met een organisatie die zich onvoldoende in digitalisering heeft verdiept."
"We weten op dit moment nog niet wat digitalisering allemaal gaat inhouden", aldus een ander. "Dus in algemene zin hebben we er niet voldoende zicht op."

Een van de aanwezigen herkent de problemen.
"Je weet namelijk niet precies wat er gebeurt in je marketingafdeling en je verkoopafdeling. Afdelingen hebben de vrijheid gekregen om databestanden binnen te halen en te combineren. Maar dan zit je je op een dag toch af te vragen wat je privacygewijs als bedrijf nu gedaan hebt. Digitalisering gaat niet over de ICT-kant, maar over de businesskant van het vraagstuk. Met name het tempo waarin veranderingen impact hebben op strategische elementen maakt het lastig. Daarom hebben wij in de raad van commissarissen bewust iemand zitten die knowhow heeft op dit gebied."

"Ik heb de indruk dat de RvC de kansen en bedreigingen van digitalisering overschat", werpt een van de aanwezigen tegen. "Er is een tijd geweest dat er ICT-directeuren zitting hadden in raden van bestuur en raden van commissarissen. Dat is fout. Je hebt toch ook geen directeur voor water of voor gas? ICT is een hulpmiddel om zaken te doen, en niets meer. Ik vind niet dat er sprake is van voldoende inzicht, maar juist van te veel." Daar is niet iedereen het mee eens. "Als je praat over problemen gerelateerd aan IT, praat je altijd over die van eergisteren. Digitalisering als kans wordt niet begrepen in RvC's en besturen."

## 'De wet maakt onze digitale snelweg niet veiliger'

**Wat is de belangrijkste bedreiging die binnen nu en drie jaar op ons af komt?**
Gorter: "Dat we in een transitieproces zitten en niet weten hoe en in welke mate zaken geregeld moeten worden. Data worden al dan niet bewust gelekt of ontvreemd. We zijn ons nog niet in voldoende mate bewust van de risico's en hoe we ons daartegen kunnen beschermen. Kennis over waar de risico's liggen is essentieel voor een raad van commissarissen."
Lenting plaatst een kanttekening: "Als toezichthouder moet je weten waar de risico's liggen, maar je hoeft ze niet te inventariseren. Daar is de raad van bestuur voor."
"Het merendeel van de bedrijven heeft het in de boardroom wel gehad over de DDoS-aanvallen", zegt Gorter. "Wat in het verleden is gebeurd, daar kun je je tegen wapenen. Maar er komt een hele generatie enthousiaste, creatieve en innovatieve afgestudeerden de werkvloer op. Die gaan iets nieuws verzinnen. We komen in een crunch-fase waarin de wetgever strenger wordt, terwijl de situatie eigenlijk niet te remmen is. In die tussenfase loop je als bedrijf relatief meer risico's."
Lenting: "Ik denk dat de Europese privacywetgeving niet gaat werken. De wet maakt onze digitale snelweg niet veiliger. Wij kunnen dat zelf wel, als we maar beseffen dat we in een glazen huis zitten."

**Is het haalbaar om te komen tot een internet dat veiliger en betrouwbaarder is?**
De lat ligt hoog, denkt Gorter. "De huidige transitiefase is niet binnen tien jaar opgelost. Maar ik denk wel dat het kan. Wie dat moet gaan doen? Een sterke geest met heel veel geld."
Beter omgaan met de bestaande techniek helpt ook, benadrukt Lenting. "Dit weekend is mijn dochter van zes via de iPad op internet gekomen, terwijl ik dacht dat ik een verdraaid goed wachtwoord op dat ding had gezet. Dus ben ik haar uit gaan leggen hoe ze veilig op de digitale snelweg kan rijden. Dat kan geen wet voor mij regelen. Ook bedrijven hebben een maatschappelijke verantwoordelijkheid."
Gorter is het daarmee eens. "Het helpt zeker om medewerkers te trainen in internetveiligheid. Als commissaris kun jij vragen hoe dit bij het bedrijf gebeurt en de mate waarin. En je moet het aantoonbaar goed regelen."

**Hoe zorg je dat er awareness voor dit onderwerp ontstaat?**
Gorter: "Dat lukt niet met één maatregel. Het begint bij de profielschets van de commissaris. Zoek naar mensen die digitalisering als bagage hebben. School je bij, en investeer daar tijd in. Stel vragen en ga in dialoog met het bestuur."
Meten is weten, vindt Lenting. "Is alles getest? Zijn er preventieve hackers in je bedrijf geweest? Als jouw onderneming kan aantonen dat er degelijk getraind is op veiligheid en dat er reguliere updates zijn geweest, krijg je korting op eventuele boetes."

‘We weten wel wat de kansen en bedreigingen zijn. Maar weten we ook hoe we problemen kunnen oplossen?’

Gorter haakt in op de kansen van digitalisering. “Met name op strategisch gebied zijn de kansen en bedreigingen nog niet voor iedereen duidelijk. Digitalisering kan organisaties in potentie maken en breken. Je wilt als commissaris niet bedolven worden onder de details, maar je wilt wel de hoofdthema’s kunnen volgen. Ik geloof dat we ons in de jongere generatie moeten verdiepen, en ervan leren.”
“Wat mij opvalt, is dat er vooral wordt gesproken over bedreigingen”, zegt Gerrie Lenting, Partner bij Deloitte en verantwoordelijk voor dienstverlening op het gebied van Reputation & Financial Crime bij Deloitte Risk Services. “Dat moet ook wel, maar ik mis de discussie over de kansen. Vraag je af wat je met digitalisering kunt, dan zie je vanzelf hoe je de bedreigingen kunt aanpakken.”

Stelling: Het huidige governancesysteem moet op de schop om bedreigingen op het gebied van ICT en beveiliging het hoofd te bieden.
“Je kunt alles wel op de schop nemen als het even niet is wat het zou moeten zijn”, vindt een commissaris. “Er is al zo veel geregeld in het governancesysteem dat digitalisering daar niet ook nog bij hoeft. Het gaat erom hoe je de verantwoordelijkheden verdeelt. Daar hoeft het systeem niet per se voor op de schop. Je moet accenten leggen. Zo zou een auditcommissie meer tijd kunnen uittrekken voor ICT.”

“De auditcommissie wordt een beetje gebruikt als vuilnisbak”, zegt een ander. Hij pleit voor een aparte commissie die zich bezighoudt met digitalisering, als onderdeel van de RvC. Maar ook dat idee stuit op bedenkingen. “Weer een commissie vind ik geen goed idee; dat ontslaat de RvC van de verantwoordelijkheid om een integrale visie te ontwikkelen. Wel moet je meer kennis in huis halen, bijvoorbeeld door een digitaliseringsexpert aan te stellen als commissaris.”
Ook de volgende spreker heeft geen behoefte aan een aparte commissie. “Ik heb goede resultaten gezien als digitalisering wordt ondergebracht bij de audit- en riskcommissie. Digitalisering brengt duidelijk een ‘operational risk’ met zich mee. Daarvoor hoef je alleen de profielschets aan te passen.

Wat kunnen jongeren nu precies beter? Als je kijkt naar de inhoud van Twitter en Facebook mis je niks. Ja, ze zijn sneller en hebben meer techniekkennis. Maar hebben we techniekkennis in een RvC nodig om een bedrijf tijdig en adequaat te ondersteunen met strategische beslissingen?"

"Een RvC hoort op ieder moment de expertise in huis te hebben die relevant is voor de business", vat een ander samen. "Die kennis is niet statisch, dat kan veranderen, ook in het huidige governancesysteem. Het is geen technisch vraagstuk. Je moet iemand hebben in de RvC die beseft wat digitalisering kan doen. Die nadenkt over big data analysis en zich realiseert wat de mogelijkheden en onmogelijkheden zijn."

Gorter geeft haar indruk van de verschillende mogelijkheden. "Het huidige governancesysteem moet voldoende consistent en resistent zijn om het af te vangen. Je kunt kijken of je de kennis zelf in huis hebt, je kunt kennis via nieuwe mensen binnenhalen, maar je kunt kennis ook extern inhuren. Als het om strategie gaat moet de hele RvC daarbij betrokken zijn, niet alleen een subcommissie. Een van de dingen die het governancesysteem wel ingewikkeld gaat maken is de hyperconnectivity. Als je als bedrijf een beslissing neemt en je bent connected met al je leveranciers, is het wel jouw verantwoordelijkheid om te bedenken wat dat betekent voor de ander. Die bewustwording betekent een verbreding van de governance."

"Ik heb mijn twijfels over de effectiviteit van het melden van datalekken.", zegt Lenting. "Je kunt beter – naar analogie van de bancaire wereld – digitalisering veiliger maken door proactief op te treden. Mogelijk verdachte activiteiten moet je melden aan een instantie. Daar kunnen we als toezichthouder in governanceperspectief veel meer mee dan met alleen repressieve meldingen."

'Een RvC hoort op ieder moment de expertise in huis te hebben die relevant is voor de business'