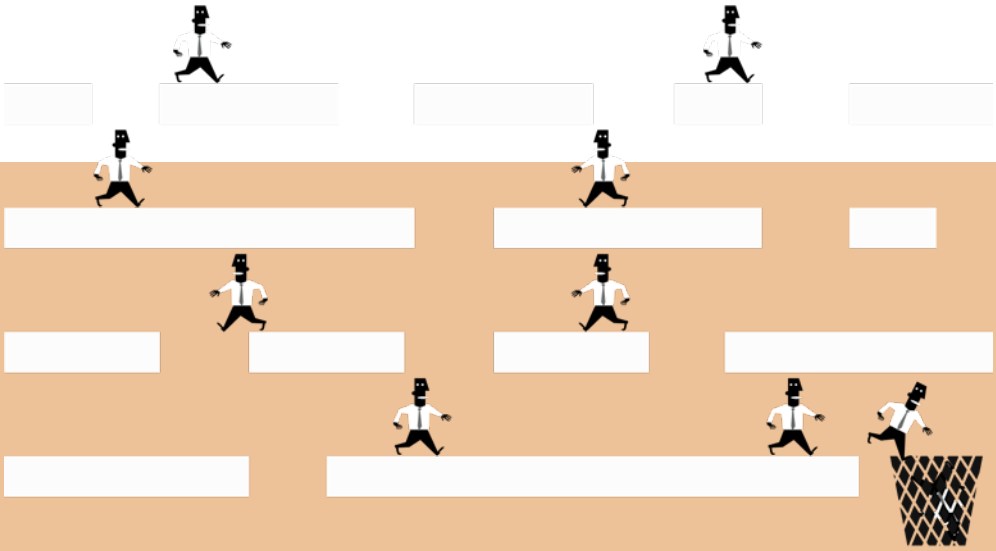
SPELEN BESTUURDERS EN COMMISSARISSEN WEL GENOEG COMPUTERGAMES?

Cyberaanvallen op bedrijven veroorzaken wereldwijd enorme financiële verliezen als gevolg van een gebrek aan bewustzijn van cyberrisico's bij organisaties. Het begrijpen van cybersecurityrisico's is cruciaal voor bedrijfsdirecteuren.

In 2022 publiceerden Nigel Phair en Hooman Alavizadeh (beiden werkzaam bij de University of New South Wales in Australië) een studie waarin zij de cybersecurityvaardigheden analyseren van de directeuren die worden vermeld in de top 100 Australian Securities Exchange (ASX 100), rekening houdend met de marktkapitalisatie[1].
Door de achtergrond en vaardigheden van de niet-uitvoerende bestuursleden van ASX 100-bedrijven te analyseren, konden zij vaststellen dat slechts 1,8 procent van de niet-uitvoerende directeuren kennis en ervaring heeft op het gebied van cybersecurity. Interessant is dat een meerderheid van de directeuren (ongeveer 78 procent) noch kennis heeft van technologie, noch van cybersecurity. Bovendien heeft slechts 7 procent van de ASX 100-bedrijven ten minste één directeur met kennis en ervaring op het gebied van cyber en technologie.

Verrassend
Deze resultaten zijn verrassend, want bestuurders en commissarissen zijn verantwoordelijk voor het toezicht op de activiteiten van de bedrijven waaraan zij leidinggeven of toezicht houden. Dat schept verplichtingen, die bijvoorbeeld in de Australische Corporations Act van 2001 als volgt zijn verwoord. 'Als directeur moet u volledig op de hoogte zijn van wat uw bedrijf doet, inclusief de financiële positie, managers en personeel ondervragen over hoe het bedrijf presteert, en een actieve rol spelen in directievergaderingen.' Volledig op de hoogte zijn van wat het bedrijf doet, houdt ook in dat bestuurders en commissarissen kennis van zaken moeten hebben op het gebied van ICT en cyberrisico's.

Steeds belangrijker
Bovendien wordt deze aandacht voor een goede bescherming tegen cyberaanvallen steeds belangrijker. Een actueel voorbeeld is het advies uit 2022 van het Australian Cyber Security Centre aan alle Australische organisaties om dringend een verbeterde cybersecurityhouding aan te nemen. 'Na de aanval op Oekraïne is er wereldwijd een verhoogde dreiging van cyberaanvallen, en het risico op cyberaanvallen op Australische netwerken, zowel rechtstreeks als onbedoeld, is toegenomen.'
Ook de snelheid waarmee bedrijven meer en nieuwe technologie zoals AI gebruiken, neemt toe. Goede cybersecurity is vereist om de organisatie te beschermen, samen met de bedrijfsgegevens en de personen die toegang hebben tot die gegevens. Omdat de 'toon aan de top begint', is het hebben van adequaat geschoolde en ervaren bestuurders en commissarissen steeds meer een fundamentele vereiste.



Bestuur is verantwoordelijk

Dat beheersing van risico's op het terrein van cybersecurity de verantwoordelijkheid van het bestuur is en niet alleen van de IT-afdeling, werd in 2018 al onderschreven door Ray Rothrock, James Kaplan en Friso van der Oord in het artikel *The Board's Role in Managing Cybersecrity Risks* in *MIT Sloan Management Review*[2], en in het artikel van David Larcker, Peter Reiss en Brian Tayan, *Critical Update Needed: Cybersecurity Expertise in the Boardroom*, gepubliceerd op SSRN van het Rock Center for Corporate Governance[3].

In het SSRN-artikel geven de auteurs duidelijk aan waarom aandacht in het bestuur voor cybersecurity juist nu belangrijk wordt. In de afgelopen jaren zijn de kosten en het aantal cyberaanvallen op bedrijfsgegevens toegenomen. Tegelijkertijd werd duidelijk dat een breed scala aan gegevens – niet alleen klantgegevens, maar ook bedrijfsgegevens – het doelwit zijn van dergelijke aanvallen. Welke stappen kunnen de raad van bestuur en het management nemen om zich voor te bereiden en te reageren op cyberdreigingen? Welke praktische maatregelen kunnen zij nemen om deze te verminderen of te voorkomen?

Cyberexpertise geen vereiste

Uit observaties blijkt dat bedrijven maar weinig governanceveranderingen doorvoeren als reactie op grote cyberaanvallen. Senior executives worden zelden ontslagen. Hun beloningspakketten worden zelden verminderd of geherstructureerd om gegevensbescherming te belonen. Cyberexpertise is geen centrale kwalificatie of vereiste voor de meeste bestuursleden. Waarom niet? Zien de bestuurders en commissarissen de omvang en ernst van cyberdreigingen niet? Of geloven ze dat ze voldoende beleid hebben om ermee om te gaan?

Cyberaanvallen vormen een groot risico voor organisaties: de kosten van een inbreuk zijn hoog, de verscheidenheid aan aanvallen is breed en de technologische vraagstukken zijn geavanceerd. Het MIT-artikel bespreekt de rol van bestuurders en commissarissen in aanvulling op de afdeling informatietechnologie (IT) bij het beheren van cybersecurityrisico's. Zij beschrijven onder andere de implicaties van het (on)vermogen van bedrijven om het risico op de reputatie van het bedrijf, de aandelenkoersen en de professionele reputatie van bestuurders te beheersen, het gebrek aan managementinfor-

matie voor het bestuur om de cybersecurity van het bedrijf te beoordelen, en het belang van een grotere veerkracht voor een effectieve beheersingsstrategie van cyberrisico's.

Aansprakelijkheidsrisico's

Aan de hand van een aantal cases beschrijft Benjamin Edwards in het artikel *Cybersecurity Oversight Liability*[4] de aansprakelijkheidsrisico's op het gebied van cybersecurity voor bestuurders. De veranderende cybersecurity-omgeving vormt nu een aanzienlijke uitdaging voor corporate governance. Hoewel sommige datalekken op het gebied van cybersecurity wellicht onvermijdelijk zijn, overwegen rechtbanken steeds vaker of de leidinggevenden en bestuurders van een bedrijf aansprakelijk kunnen worden gesteld omdat zij te kwader trouw handelden en nalieten om goed toezicht te houden op de gang van zaken van de onderneming. Edwards bespreekt de implicaties van recente bedrijfscases en moedigt bedrijfsbesturen aan om te erkennen dat in een omgeving vol toenemende bedreigingen, een adequate reactie het toewijzen van daadwerkelijke middelen en aandacht aan cybersecurity-kwesties vereist. Het artikel wordt afgesloten met een belangrijke waarschuwing: De SEC heeft in oktober 2018 een rapport gepubliceerd waarin cybersecurity wordt verbonden met de verplichtingen van beursgenoteerde vennootschappen voor een effectief interne controle en risicobeheersingssysteem om cyberrisico's te beheersen.

Brennan Ackerman concludeert in zijn artikel *The Fiduciary Duties of the Board of Directors: Cybersecurity Potential Liability and Preventative Actions*[5] enigszins geruststellend voor bestuurders van Delaware vennootschappen dat een rechtszaak op basis van de zorgplicht tegen de raad van bestuur in geval van een cyberinbreuk waarschijnlijk niet zal slagen. Voor cybersecurity zou de raad van bestuur op basis van de business judgment rule grove nalatigheid moeten tonen door onopzettelijk het probleem niet te erkennen, ondanks de publiciteit die het kreeg. Om aan zijn plicht van loyaliteit te voldoen in de context van een cybersecurityrisico's, moet een raad van bestuur relevante risico's bespreken, een rapportagesysteem implementeren waarbij zij op de hoogte wordt gesteld van belangrijke cybersecurity-ontwikkelingen en interne controles invoeren. Een raad van bestuur kan waarborgen implementeren om zich te beschermen tegen een cyberinbreuk en tevens een responsplan ontwikkelen dat in werking wordt gesteld bij een cyberinbreuk. Tegelijkertijd is de bewijslast waarover de eiser moet beschikken om aan te tonen dat een bestuurslid de plicht van loyaliteit heeft geschonden, hoog.

Oplossing

Ondanks alle grote risico's die bedrijven lopen op het gebied van cybersecurity, lijkt de oplossing voor de hand te liggen. Het artikel *Board effectiveness and cybersecurity disclosure*[6] van Nadia Smaili, Camélia Radu en Amir Khalili in het *Journal of Management and Governance* in 2022 analyseert in een longitudinale studie de 60 grootste Canadese beursgenoteerde bedrijven. Zij concluderen dat uiteindelijk een effectieve Board (bestuurders en commissarissen) een positieve invloed heeft op de beslissing van bedrijven

om cybersecurity-informatie openbaar te maken. Ten slotte hebben onafhankelijkheid en financiële expertise van commissarissen een positieve invloed op de hoeveelheid informatie die openbaar wordt gemaakt.

In de studie *Board of directors' attributes and aspects of cybersecurity disclosure*, later in 2022 gepubliceerd in het *Journal of Management and Governance* concluderen Sylvie Héroux en Anne Fortin[7] dat aangezien cybersecurity een kritiek risico is voor ondernemingen, openbaarmaking van cybersecurity belangrijk is voor financiële toezichthouders, financiële analisten, aandeelhouders en andere belanghebbenden. Organisaties staan voor uitdagingen bij het beslissen of, wat en wanneer cybersecuritygerelateerde informatie moet worden bekendgemaakt. De belangrijkste bevindingen van hun studie geven aan dat de aanwezigheid van een cybersecuritycommissie in het bestuur (en raad van commissarissen) essentieel is voor meer cybersecurity-openbaarmaking. Overigens hebben ook zonder zo'n cybersecuritycommissie IT-expertise van commissarissen, het aantal jaren lidmaatschap van de raad van commissarissen en de onafhankelijkheid van de leden, het aandeel vrouwelijke leden en de leeftijd van de commissarissen een positieve invloed op de mate van totale cybersecurity-openbaarmaking, in het bijzonder over de beheersing van cybersecurityrisico's.

Preventie

De ontwikkeling van het gebruik van computers, (informatie)technologie, artificial intelligence gaan hard en bedrijfsgegevens worden steeds waardevoller voor bedrijven. Bestuurders en commissarissen die goed op de digitale toekomst zijn voorbereid, plaatsen het belang van goede cybersecurity hoog op de agenda en richten de organisatie daarop in. Preventie is beter dan reactief zijn op het terrein van cyberrisico's. Vraag af en toe eens aan een medebestuurder of collega-commissaris wat haar of zijn ervaringen met online computergames zijn.

Samenstelling

Stefan Peij (Governance University), **Remko Renes** (Nyenrode Business Universiteit) en **Pieter-Jan Bezemer** (Edith Cowan University, Australië).

Noten

1. Phair, Nigel; Alavizadeh, Hooman (2022). *Journal of Risk Management in Financial Institutions* Autumn 2022, Vol. 15 Issue 4, p 429-436, 8p.
2. The Board's Role in Managing Cybersecrity Risks' in *MIT Sloan Management Review*. Winter 2018, Vol. 59 Issue 2, p12-15.
3. David Larcker, Peter Reiss en Brian Tayan, 'Critical Update Needed: Cybersecurity Expertise in the Boardroom'. gepubliceerd op SSRN van het Rock Center for Corporate Governance (https://ssrn.com/abstract=3074594.
4. Benjamin P. Edwards. (2019) *Cybersecurity Oversight Liability*, 35 Ga. St. U. L. Rev. 663.
5. Ackerman, B. (2019). The Fiduciary Duties of the Board of Directors: Cybersecurity Potential Liability and Preventative Actions. *Wayne State University Journal of Business Law*, 2, 12-32.
6. https://doi.org/10.1007/s10997-022-09637-6.
7. https://doi.org/10.1007/s10997-022-09660-7