Publieke reactie herziening corporate governance code

15 april 2022

Bernold Nieuwesteeg (Directeur Centre for the Law and Economics of Cyber Security // Erasmus Universiteit Rotterdam)
Willem Kuijken (Onderzoeksassistent Centre for the Law and Economics of Cyber Security // Erasmus Universiteit Rotterdam)

Transparantie over cybersecurity mogelijk 'blinde vlek'

De Monitoring Commissie Corporate Governance publiceerde op 21 februari 2022 een consultatiedocument met voorstellen voor actualisatie van de Nederlandse Corporate Governance Code (hierna: de Code). Deze publicatie vormt het startsein voor alle geïnteresseerden om een reactie uit te brengen en deel te nemen aan het publieke debat omtrent actualisatie van de Code.

Het voorstel van actualisatie voor de Code ziet op dit moment vooral op gebieden als lange termijn waardecreatie, diversiteit en de rol van aandeelhouders. *Cybersecurity* is echter nog onderbelicht in zowel de huidige Code als het voorstel voor actualisatie. In de Code wordt cybersecurity slechts eenmaal expliciet genoemd, in best practice bepaling 1.5.1.

Het belang van cybersecurity is de afgelopen jaren sterk toegenomen. Beursgenoteerde vennootschappen worden continu blootgesteld aan cyberdreigingen. Soms materialiseren deze cyberdreigingen zich in incidenten. Denk aan de cyberaanval op Maersk[1] en Randstad.[2] Een cyberaanval kan potentieel grote impact hebben op de continuïteit en winstgevend van de onderneming. Externe stakeholders moeten goed op de hoogte kunnen zijn van het cybersecurityniveau van de vennootschap. Het belang van externe transparantie rondom de cybersecuritystrategie van vennootschappen is derhalve ook toegenomen.

In deze reactie gaan wij in op de wenselijkheid van transparantie vanuit maatschappelijk en vennootschappelijk oogpunt. Vervolgens bespreken we bestaande wettelijke verplichtingen en de ontwikkelingen in Amerika. Tenslotte doen wij op basis van de huidige stand van transparantie enkele suggesties voor de Code.

[1] Economieredactie. (2018, 19 juli). Datalek bij Randstad: gegevens werkzoekenden te zien. AD.nl. https://www.ad.nl/economie/datalek-bij-randstad-gegevens-werkzoekenden-te-zien~ab481571/

[2] Greenberg, A. (2018, 22 augustus). The Untold story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Baten transparantie cybersecurity bij beursgenoteerde vennootschappen

We bespreken in deze sectie kort zowel de vennootschappelijke als de maatschappelijke baten van transparantie over cybersecurity.

Transparantie over cybersecurity kan voordelen hebben voor de relatie van de vennootschap met marktspelers zoals potentiële investeerders en klanten; regelgevende instanties, zoals de Autoriteit Persoonsgegevens alsmede een positief effect hebben op het imago extern en intern. Transparantie kan ook de bewustwording van cyberisicos en de verbetering van de situatie bevorderen binnen de organisatie.[3]

(1) Het verschaffen van publiek toegankelijke informatie over cybersecurity van de vennootschap benadrukt het belang dat de vennootschap hieraan geeft. Dit kan de relatie met investeerders en kredietverleners positief beïnvloeden, omdat informatie over risicobeheersing, waaronder cybersecurity, voor hen van belang is in hun beslissing om te interacteren met de desbetreffende onderneming. Dit geldt ook voor (potentiële) leveranciers en afnemers van de vennootschap. Een cyberincident bij de vennootschap kan van invloed zijn op de continuiteit van klanten en leveranciers (supply chain risk). Klanten en leveranciers hebben onder andere steeds vaker toegang tot delen van het IT systeem van de vennootschap.

(2) Hiernaast geeft het delen van informatie over cybersecurity een indicatie van de naleving van wet- en regelgeving. Door transparantie over cybersecurity benadrukt de vennootschap het belang van naleving van wetgeving. Het risico op schendingen van cybersecuritywetgeving - en daarmee samenhangende boetes - is daardoor kleiner.

(3) Transparantie over cybersecurity kan bewustwording van cyberrisico's vergroten en daardoor een gedragsverandering binnen de vennootschap stimuleren. Zo worden bij het opstellen van het jaarverslag de personen die verantwoordelijk zijn voor het aanleveren van de relevante cybersecuritysgegevens verplicht om samen te werken en kennis te delen met de personen belast met het opstellen van het jaarverslag. Het op regelmatige wijze delen van informatie bevordert processen voor het prioriteren, structureren en synthetiseren van die informatie. Binnen de vennootschap worden zo steeds meer personen bewust van het belang van cybersecurity.

Transparantie over cybersecurity heeft ook verschillende maatschappelijke baten:

(1) Ten eerste zijn er baten voor investeerders en schuldeisers. Investeerders en schuldeisers hebben voordeel van de toegang tot informatie over de strategie van de vennootschap met betrekking tot cyber risicomanagement en het cyberrisico. De

[3] Nieuwesteeg, B.F.H., Eijkelenboom E.V.H., Hoogerwaard, R.M. (2021). De wenselijkheid van transparantie over cyberveiligheid bij beursvennootschappen. *TvOB,* 5(1).

blootstelling aan cyberrisico is onderdeel van het totale risico dat investeerders en schuldeisers leiden.

(2) Ten tweede zijn er publieke baten voor de samenleving. Momenteel is er een brede consensus onder wetenschappers op het gebied van cyberbeveiliging dat er onvoldoende objectieve data beschikbaar is.[4] Informatie met betrekking tot cybersecurity in de jaarverslagen zou kunnen bijdragen aan het oplossen van dit tekort aan empirische data. Meer publieke data kan leiden tot:

a. Verhoogde efficiëntie en effectieve investeringen in cybersecurity, omdat organisaties informatie van andere organisaties kunnen gebruiken en het wiel niet opnieuw hoeven uit te vinden.
b. Het beter begrijpen van de dreigingsniveaus en incidenten bij beursgenoteerde vennootschappen.
c. Betere producten, zoals cyberverzekeringen.

[4] Nieuwesteeg, B.F.H. (2018, June 25). The Law and Economics of Cyber Security. EDLE - The European Doctorate in Law and Economics programme. Erasmus University Rotterdam. Geraadpleegd van: http://hdl.handle.net/1765/108963

Veranderende verplichtingen cybersecuritytransparantie in het buitenland

Tot op heden ontbreekt in Europese en nationale verslaggevingsvoorschriften het vereiste om informatie over cybersecurity openbaar te maken in de jaarlijkse financiële en niet-financiële verslaggeving.[5] In zogenoemde *soft law*, waar de Code onder valt, wordt cybersecurity slechts een enkele keer genoemd (best practice bepaling 1.5.1 in de Code.).

De IFRS (International Financial Reporting Standards) is een methode om over de grenzen
eenzelfde standaard te volgen met betrekking tot het vermelden van financiële resultaten. vennootschappen in landen die onder de IFRS vallen zijn verplicht om op deze wijze te rapporteren, anders dan de Code is hier dus geen sprake van *soft law*. In de Verenigde Staten (VS) worden beleggers beschermd door de overheidsinstelling SEC (Security and Exchange Commission). De SEC is een toezichthouder op de Amerikaanse effectenbeurzen.

De SEC heeft op 17 maart van dit jaar regels voorgesteld om de informatieverstrekking over cyberbeveiliging door beursgenoteerde vennootschappen te verbeteren en te standaardiseren.[6] Deze voorstellen betreffen het risicobeheer, de strategie, het bestuur en de rapportage over cyberbeveiligingsincidenten door beursgenoteerde vennootschappen. De wijzigingen hebben het doel om actuele rapportage over materiële incidenten op het gebied van cyberbeveiliging verplicht te stellen. De SEC stelt ook voor om periodieke informatie te vereisen over het beleid en de procedures van een bedrijf om cyberbeveiligingsrisico's te identificeren en te beheren. De rol van het management bij de tenuitvoerlegging van het cyberbeveiligingsbeleid en de cyberbeveiligingsprocedures is hierbij van belang. Ook de eventuele deskundigheid van de raad van bestuur op het gebied van cyberbeveiliging en toezicht op cyberbeveiligingsrisico's komt aan bod.

Enkele specifieke kernpunten uit het voorstel:

- *"We are proposing Item 106(b) of Regulation S-K to require registrants to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy"*
- *"Proposed Item 106(b) would therefore require registrants to disclose its policies and procedures, if it has any, to identify and manage cybersecurity risks and threats, including: operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk"*

[5] Nieuwesteeg, B.F.H., Eijkelenboom E.V.H., Hoogerwaard, R.M. (2021). De wenselijkheid van transparantie over cyberveiligheid bij beursvennootschappen. *TvOB,* 5(1).
[6] Rapport: SEC proposes rules to enhance and standardize cybersecurity-related disclosure for public companies. (2022, 17 maart). Geraadpleegd van: https://ap.lc/DLHAI

- *"Proposed Item 106(c) would require disclosure of a registrant's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing cybersecurity risks, the relevant expertise of such management, and its role in implementing the registrant's cybersecurity policies, procedures, and strategies"*

De praktijk in Nederland

De mate van transparantie omtrent cybersecurity in de jaarverslagen van beursgenoteerde vennootschappen verschilt sterk.[7] Enkele vennootschappen vermelden meer dan tien cybersecurity maatregelen, deze maatregelen zijn dan vaak zeer specifiek en technisch van aard. Andere vennootschappen vermelden een enkele of zelfs geen cybersecurity gerelateerde maatregel. Deze vennootschappen blijven vaak weinig concreet en de genoemde maatregel is meestal heel ruim omschreven (denk hierbij bijvoorbeeld aan teksten als ".. er wordt geïnvesteerd in cybersecurity om cyberrisico's te minimaliseren..."). Bovendien blijkt uit onze meest recente analyses dat vennootschappen veel verschillende type maatregelen melden. Zo worden 130 specifieke maatregelen in het jaarverslag maar door 1 of 2 beursgenoteerde vennootschappen genoemd. Dit alles maakt de transparantie van beursgenoteerde vennootschappen vaak lastig te vergelijken en te beoordelen.

[7] Eijkelenboom E.V.A., Nieuwesteeg, B.F.H., (2021). An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law & Security Review, 40.

Concrete rol van cybersecurity in herziening van de corporate governance code

Wij zien een aantal uitdagingen omtrent cybersecuritytransparantie in het jaarverslag.

- In de analyses met betrekking tot jaarverslagen van beursgenoteerde vennootschappen in Nederland zien we dat de verschillen vooralsnog groot zijn en dat vennootschappen lastig te vergelijken zijn. Enkele vennootschappen bespreken wel de rol van het management en de raad van bestuur bij cybersecurity en schetsen ook wel kort het beleid hieromtrent. Het blijft echter vaak abstract.
- Ook zijn de meeste specifieke maatregelen technisch van aard en lijken de meeste maatregelen enigszins willekeurig in het jaarverslag terecht gekomen te zijn.
- In Amerika komt hoogstwaarschijnlijk dwingende regelgeving omtrent transparantie.

De Code zou een bijdrage kunnen leveren aan het faciliteren van transparantie omtrent cybersecurity op een wijze die externe stakeholders faciliteert en tegelijkertijd baten heeft voor de vennootschap als zodanig. Duidelijke richtlijnen met betrekking tot cybersecuritytransparantie in de code kunnen ervoor zorgen dat de vennootschappen een stuk meer op een lijn komen te liggen en dieper ingaan op hun beleid en procedures omtrent cybersecurity. Zeer specifieke technische cybersecuritymaatregelen hoeven dan niet meer genoemd te worden.

Op welke wijze zou de code *effectieve* vormen van transparantie voor beursgenoteerde vennootschappen kunnen stimuleren?

Transparantie is geen doel op zich. Vennootschappen delen op dit moment een selectie van specifieke technische maatregelen. Dit draagt onvoldoende bij aan bovenstaande doelen en zou dus geen onderdeel moeten zijn van het jaarverslag. Het doel van transparantie is o.a. om intern beleid te prioriteren en externe stakeholders op hoog aggregatieniveau een indicatie te geven. Transparantie over de volgende thema's zou bij kunnen dragen aan het genereren van de vennootschappelijke en maatschappelijke baten. Deze thema's sluiten ook aan bij de punten die in de SEC filing worden genoemd.

- **Interne governance.** Dit behelst het proces met betrekking tot de interne rapportage. Op welke wijze wordt gerapporteerd aan het bestuur? En aan wie binnen het bestuur?
- **Externe kennisdeling en leiderschap**. Op welke wijze deelt de vennootschap kennis over cybersecurity naar externe stakeholders, bijvoorbeeld in de keten?
- **Het cyberrisico**. Een omschrijving van de ordegrootte van cyberrisico en de wijze waarop het risico is afgedekt. Liefst zo concreet mogelijk.

De Code zou ook richtlijnen kunnen geven over wat juist niet genoemd hoeft te worden in het kader van cybersecuritytransparantie. Te denken valt dan aan specifieke technische maatregelen, dreigingen of incidenten.

Concreet tekstvoorstel:

Wij zoeken aansluiting in de toelichting van best practice bepaling 1.1.1. ESG-doelen omvatten tevens cybersecurity

Onder: *Vennootschappen formuleren als onderdeel van hun strategie voor lange termijn waardecreatie een heldere strategie op het gebied van ESG. Ter zake worden concrete doelstellingen geformuleerd (best practice bepaling 1.1.1);*

Cybersecurity
Cybersecurity is onderdeel van ESG. Vennootschappen zijn transparant over de interne governance (de wijze van rapportage over cybersecurity), externe kennisdeling (o.a. in de keten), de ordegrootte van het cyberrisico en de afdekking ervan. Cybersecurity transparantie is in ontwikkeling. Het SEC voorstel voor transparantie kan als leidraad dienen alsmede het paper reporting cyber risks to boards.[8]

En eventueel:

Transparantie over cybersecurity heeft maatschappelijke baten. Dat betekent echter niet dat specifieke cybersecurity 'controls' en dreigingen publiek gedeeld hoeven te worden, wanneer de risicos en kosten van het delen niet opwegen tegen de baten voor o.a. investeerders en klanten. Bovendien is het jaarverslag niet het medium om zeer tijdsspecifieke maatregelen te delen.

[8] Aanpassing SEC: https://www.sec.gov/rules/proposed/2022/33-11038.pdf en Dezeure, Freddy & Webster, George & Moerel, Lokke. (2022). Cyberrisico's rapporteren aan raden van bestuur. Bestuursuitgave. Geraadpleegd van: https://ap.lc/EyXT9