MAB MAANDBLAD VOOR ACCOUNTANCY EN BEDRIJFSECONOMIE

Maandblad voor Accountancy en Bedrijfseconomie 97(9/10) (2023): 309–318
DOI 10.5117/mab.97.113339

Research Article

Transparantie over cybersecurity neemt toe

Peter Eimers, Abbas Shahim, Peter Kornelisse

Received 26 September 2023 | **Accepted** 15 November 2023 | **Published** 14 December 2023

Samenvatting

Cybersecurity is een randvoorwaarde voor organisaties en de samenleving om cyberrisico's te beheersen. Deze cyberrisico's kunnen zowel lokaal als wereldwijd stabiliteit en veiligheid in gevaar brengen. Het groeiend aantal cyberaanvallen, de toenemende complexiteit en de inzet van steeds meer geavanceerde digitale middelen zijn een punt van grote zorg voor alle belanghebbenden. De publieke transparantie omtrent de wijze waarop de steeds ernstiger wordende cyberrisico's worden beheerst, is dan ook van groot belang en ook steeds vaker een vereiste. Dit komt onder andere tot uiting in de risicoparagraaf van het bestuursverslag en de ontwikkelende regelgeving, zoals die van de Cybersecurity Act en de SEC over cyber disclosures.

Relevantie voor de praktijk

Beursfondsen leggen in het jaarverslag verantwoording af over hun bedrijfsactiviteiten en geven daarin blijk van een steeds grotere digitale afhankelijkheid. Daarmee neemt ook het belang van cybersecurity in het kader van de betrouwbaarheid en continuïteit van bedrijfsprocessen sterk toe. Dit vergroot de behoefte aan transparantie over cyberrisico's en kansen van cybersecurity, inclusief de manier waarop hiermee wordt omgegaan.

Trefwoorden

Cybersecurity, jaarverslagen, verslaggeving, controle

1. Inleiding

Cyberdreigingen ontwikkelen zich steeds sneller en kunnen een steeds grotere impact hebben op organisaties – en daarmee de samenleving. Hoewel het lang heeft geduurd om te beseffen dat cybersecurity niet alleen een technisch issue is en de verantwoordelijkheid van iedere belanghebbende is, is het inmiddels algemeen bekend dat cyberaanvallen zich niet langer enkel richten op grote organisaties in de publieke en in de private sector. Aansprekende voorbeelden in de afgelopen jaren, zoals de KNVB (KNVB 2023), de gemeente Hof van Twente (VNG 2021) en de Universiteit Maastricht (UM 2020) zijn slechts het topje van een ijsberg.

Bestuurders onderkennen intussen cyberrisico's als een van de voornaamste te beheersen organisatierisico's, steeds meer veroorzaakt door dreigingen zoals social engineering via phishing (een van de meest voorkomende cyberaanvallen waardoor hackers mensen misleiden om gevoelige informatie bekend te maken) en misbruik van zwakheden in IT, waaronder zero-day exploits (een ontdekte softwarefout waarvoor nog geen verbeterde software beschikbaar is, die hackers misbruiken om computersystemen aan te vallen). Steeds vaker resulteren deze dreigingen in ransomware-aanvallen en datalekken van persoonsgegevens. In het bijzonder ransomware en datalekken dragen bij tot bewustwording van de realiteit van cyberrisico's.

Cyberaanvallen treden steeds vaker op, met een steeds grotere impact en ze worden ook steeds complexer en geavanceerder. Denk hierbij aan WannaCry and NotPetya ransomware-aanvallen. Zij worden onder

andere gelanceerd door individuen, beroepscriminelen en statelijke actoren (staten of organisaties die namens staten cyberaanvallen plegen), die een significante bedreiging vormen met de potentie om de meeste schade toe te brengen (Schinagl and Shahim 2020). Veel kwaadwillenden zijn al langer actief. Hun misleidend gedrag is intussen verfijnd en hun methoden en technieken zijn van hoge kwaliteit, waardoor het lastig is om hun opzettelijke activiteiten tijdig en gericht tegen te kunnen gaan. Vooral in de laatste twee decennia hebben cyberdreigingen zich geleidelijk ontwikkeld van een abstract idee tot een zichtbaar reëel gevaar voor de samenlevingen en de wereldmarkt. In de loop der jaren is de harde les geleerd dat het cyberdreigingslandschap sneller dan ooit verergert, en dat cybersecuritypraktijken daarmee vaak niet in lijn zijn.

Cyberdreigingen worden wereldwijd als één van de belangrijkste zorgpunten beschouwd, niet alleen door cyberexperts, maar ook door business leaders (WEF 2023). De realiteit van de hedendaagse digitale wereld is dan ook dat praktisch iedereen slachtoffer kan worden. Een passende bescherming daartegen is logischerwijs van het allergrootste en strategische belang (NCTV 2023). In haar jaarlijkse rapport over cyber stelt het EU-agentschap voor cyberveiligheid (ENISA): 'In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences' (ENISA 2023).

Organisaties hebben doorgaans cybersecuritymaatregelen op basisniveau geïmplementeerd en zijn zich bewust van het feit dat een wezenlijke transformatie naar een meer integrale, proactieve en ketenbrede benadering een absolute must is. Het is vandaag de dag cruciaal om de digitale werkelijkheid te adopteren, door de aantrekkelijkheid voor aanvallers te beperken en tegemoet te komen aan de toenemende behoefte aan een nieuwe werkwijze. Deze benadering dient de veranderende cyberdreigingen het hoofd te kunnen bieden door verder te gaan dan alleen aandacht voor een compliancegebaseerde aanpak en focus op procedurele maatregelen. Onderzoek wijst uit dat bestuurders in het algemeen weinig vertrouwen hebben in het niveau van cybersecurity van hun eigen organisatie. Deze zorg wordt eveneens door de bevraagde leden van de auditcommissies genoemd als een issue dat de grootste uitdaging vormt voor organisaties (KPMG 2017).

Een robuust en volwassen risicobeheersingsmechanisme voor cybersecurity dient dan ook operationeel te zijn om de blootstelling aan de huidige, evenals de opkomende en ingewikkelde cyberbedreigingen te kunnen verminderen. De auditfunctie (zowel de internal auditor als de openbaar accountant) kan hierbij een belangrijke rol spelen door het bieden van zekerheid en advies. De verwachting is dat deze ondersteuning voornamelijk focust op het beschermen tegen de cyberbedreigingen ten behoeve van elk relevant facet van de bedrijfsvoering, waaronder bij de inrichting van multilayered defenses (implementatie van een diversiteit aan securitymaatregelen op verschillende niveaus), veilige configuraties van hardware en software op mobiele apparaten, bevoorrechte toegang, preventie van gegevensverlies, leveranciersmanagement, incident response, veilige codering en de directe relatie tussen cybersecurity en organisatierisico's (Shahim et al. 2022).

Deze bijdrage belicht de ontwikkelingen op het gebied van transparantie over cybersecurity vanuit een maatschappelijk perspectief, zowel vanuit regelgeving als vanuit andere ontwikkelingen (hoofdstuk 2). In hoofdstuk 3 is de opzet van ons onderzoek onder de jaarverslagen 2022 van de AEX-fondsen beschreven, hoofdstuk 4 bevat de analyse naar aanleiding van het uitgevoerde onderzoek. Deze bijdrage wordt afgesloten in hoofdstuk 5 met een conclusie en een reflectie.

2. Regels en verwachtingen over openbaarmaking van informatie over cybersecurity door organisaties

Op basis van artikel 391.1 BW2 moet het bestuursverslag een beschrijving geven van de voornaamste risico's en onzekerheden waarmee de rechtspersoon wordt geconfronteerd. De Nederlandse Corporate Governance Code ziet het als taak van de Audit Commissie (als onderdeel van de raad van commissarissen) om toezicht op het bestuur te houden inzake de toepassing van informatie- en communicatietechnologie door de vennootschap, waaronder risico's op het gebied van cybersecurity (MCCGC 2016). Toezichthouders, ketenpartners, bestuurders en management hebben een steeds grotere behoefte om geïnformeerd te worden en betrokken te zijn bij het beheersen van cyberrisico's. Dit blijkt bijvoorbeeld uit ontwikkelende regelgeving van de SEC en de EU, de security-eisen die aan businesspartners worden gesteld met toenemende verantwoordingsvereisten, en de belangstelling die bestuurders en management steeds meer tonen voor het onderwerp cybersecurity.

Openbaarmaking van (financiële) informatie aan het publiek in lijn met wet- en regelgeving is geen nieuw fenomeen. Voor het borgen van transparantie hebben organisaties veelal specifieke processen ingericht met behulp waarvan relevante financiële informatie openbaar wordt gemaakt. De nieuwe regelgeving van SEC (SEC 2023) vraagt echter om aanvullende transparantie van financiële informatie betreffende cyberrisico's.

Gezien het belang van cybersecurity tonen steeds meer belanghebbenden interesse in de openbaarmaking van cyberrisico's en daarmee gepaard gaande informatie over cybersecurity. Was de behoefte voor het delen van informatie over cyberrisico's eerst met name intern gericht bij het interne management en de bestuurders, thans zien wij een toenemende interne en externe behoefte om te worden geïnformeerd. Al in 2016 schreef de NBA haar publieke management letter 'Cybersecurity: Van Hype naar Aanpak' (NBA 2016), waarin aandacht werd gevraagd voor de sterk groeiende risico's rond cybersecurity. Concrete praktische aanbevelingen stonden in deze publicatie:

- Stel als bestuurder de juiste vragen.
- Breng de kroonjuwelen in kaart.
- Besteed ook aandacht aan cultuur en gedrag.
- Vergroot de digitale weerbaarheid.
- Zorg voor voldoende cyber kennis bij de controle.

Vanuit de interne behoefte onderkennen wij dat bestuurders in het algemeen worden geïnformeerd over beveiligingsincidenten en de voortgang van het verbeteren van cybersecurity. De externe behoefte is op dit moment nog met name gericht op informatie over cybergerelateerde incidenten, in het bijzonder als deze het onderstaande betreffen:

- persoonsgegevens;
- continuïteit van de bedrijfsvoering;
- het publiekelijk bekend worden van vertrouwelijke informatie;
- derde partijen.

In jaarverslagen zien wij over de afgelopen jaren een toename van opgenomen cybersecurity-elementen. Een recent onderzoek in de Verenigde Staten naar de toelichtingen in de jaarverslagen bij de Fortune 100 wijst uit dat er in de afgelopen jaren een gestage en significante groei is in het aantal toelichtingen in het kader van cybermanagement en toezicht (EY 2023). Transparantie gaat echter verder dan jaarverslagen alleen. Wij zien op dit moment verschillende vormen van eisen over het delen van aspecten van cybersecurity met belanghebbenden. Zie hiervoor Tabel 1. Hierin is met name Nederlandse/Europese wet- en regelgeving opgenomen, aangevuld met Amerikaanse. Deze Amerikaanse regelgeving, vanuit de SEC, is weliswaar alleen van belang voor in de Verenigde Staten aan de beurs genoteerde organisaties, maar deze regelgeving straalt daarnaast ook af op Nederland als het gaat om verwachtingen in de markt. In tabel lichten wij de transparantievereisten voor Nederland, Europa en de VS toe.

Tabel 1. Overzicht van eisen in het kader van aspecten van cybersecurity*.

Wijze van communicatie (voorbeelden)	Incidenten en kwetsbaarheden	Cyber-risicomanagement, strategie en governance	Cybersecurity-maatregelen
Aan RvC en RvB		• SEC	• NIS2 voor essentiële en belangrijke entiteiten • DORA • SEC
Aan Toezichthouders (bijvoorbeeld Nationaal Cybersecurity Centrum, Autoriteit Persoonsgegevens)	• AVG/GDPR • NIS2 • DORA		
Aan publiek via jaarverslag	• SEC	• De Nederlandse Corporate Governance Code • SEC	
Aan publiek via publicatie	• CRA	• SEC	

* de genoemde afkortingen worden toegelicht in de hiernavolgende paragrafen.

2.1. Cyber-disclosures in Europa

Op basis van de cybersecurity act (EU 2019) worden eisen gesteld aan cyber security en geeft Europa een kader voor de certificering van producten, processen en diensten op het gebied van cyberveiligheid. Hierin past ook het mandaat van het EU-agentschap voor cyberveiligheid, ENISA. Wet- en regelgeving wordt van kracht voor financiële instellingen (DORA 2023), evenals voor essentiële (zoals energie en transport) en andere belangrijke entiteiten, zoals afvalverwerking (NIS2) (EU 2022a). NIS2 is de opvolger van de NIS (Wet Beveiliging Netwerk- en Informatiesystemen), die vanaf 2018 al van kracht was. Ook zal voor producten met digitale elementen in de nabije toekomst meer disclosure worden vereist op basis van de Cyber Resilience Act (CRA) (EU 2022b).

Deze wet- en regelgeving zet kracht bij om cyberrisico's expliciet te beheersen en vereist ook het nemen van bestuurlijke verantwoordelijkheid. Voor financiële instellingen en essentiële entiteiten zal proactieve monitoring door toezichthouders gelden, voor belangrijke entiteiten zal met name worden gesteund op zelfcontrole en monitoring door de toezichthouder als daartoe aanleiding bestaat, bijvoorbeeld bij cyber-gerelateerde incidenten. DORA en NIS2 vereisen expliciet dat relevante cyber-gerelateerde incidenten binnen een dag worden gemeld bij de van toepassing zijnde toezichthouders. Het niet voldoen aan DORA en NIS2 kan hoge boetes tot gevolg hebben.

2.2. Cyber-disclosures in de VS

De regelgeving in de Verenigde Staten is explicieter dan in Europa. Zo heeft de Securities and Exchange Commission (SEC 2023) regels aangenomen die registranten verplichten om:

- materiële cyberbeveiligingsincidenten die zij ervaren binnen vier werkdagen openbaar te maken, en
- op jaarbasis materiële informatie over hun cybersecurity-risicomanagement, -strategie en -governance in jaarverslagen op te nemen.

De disclosure-vereisten richten zich op het beschermen van beleggers tegen de schade die een inbreuk op cybersecurity kan veroorzaken. Daarom verwachten beleggers openbaarmaking van actuele en consistente informatie van de ondernemingen, waaraan hun financiële middelen zijn toevertrouwd. Hiermee worden de ondernemingen verantwoordelijk gesteld om transparantie te verschaffen over de wijze waarop cybersecurityrisico's door hen worden gemanaged. De SEC heeft deze

transparantieverplichtingen vastgesteld voor zowel Amerikaanse als buitenlandse ondernemingen met een beursnotering in de Verenigde Staten ('foreign private issuers').

Het is de verwachting dat deze vereisten vanuit de Verenigde Staten ook in Europa de aandacht zullen krijgen. Deze regelgeving raakt de aan de beurs in de VS genoteerde ondernemingen in Nederland, en daarmee kunnen deze ondernemingen ook een voorbeeldfunctie vervullen betreffende de mate waarin cyber dislosure kan plaatsvinden. Om die reden zijn de volgende drie disclosure-eisen van de SEC ook voor Nederlandse beursgenoteerde ondernemingen relevant:

1) Openbaarmaking van incidenten:
   - Maak elk cyberbeveiligingsincident bekend waarvan is vastgesteld dat het materieel is, tenzij onmiddellijke openbaarmaking een aanzienlijk risico voor de nationale of openbare veiligheid zou vormen.
2) Informatieverschaffing over cybersecurity-risicomanagement, strategie en governance:
   - Maak risicomanagement en strategie bekend, waaronder processen voor het beoordelen, identificeren en beheren van materiële risico's van cybersecurity-bedreigingen, evenals de materiële effecten van risico's als gevolg van cybersecurity-bedreigingen en eerdere cybersecurity-incidenten. Dit betreft onder andere cyber-risico's in relatie tot externe dienstverleners.
3) Governance:
   - Toezicht op het bestuur, evenals de rol van het management betreffende risico's van cyberbeveiligingsbedreigingen, en processen waarbij het management wordt geïnformeerd over – en toezicht houdt op – cyberbeveiligingsincidenten.

2.3. Overige initiatieven

De beroepsorganisatie van IT-auditors heeft in 2023 een consultatiedocument uitgebracht met een verslaggevingsstandaard voor verantwoording IT-beheersing (NOREA reporting initiative) (NOREA 2023). Het document biedt een handvat aan het management van een organisatie om zich met een IT-beheerverslag te verantwoorden en belanghebbenden te informeren. De opzet hiervan is dat dit leidt tot een IT-verslag (NOREA 2023) en een IT-verklaring, waarbij analoog aan de jaarrekening door een organisatie de IT-aspecten, zoals IT-beheersing en cybersecurity, worden beschreven, en waarover de IT-auditor een bepaalde mate van zekerheid afgeeft.

Disclosure wordt ook geassocieerd met de opzet van een proces waarmee feiten en informatie over een thema publiekelijk bekend worden gemaakt. Een voorbeeld van een initiatief dat in de praktijk kan worden gebracht is de inrichting van een 3-lines of defense voor cybersecurity. In verband hiermee staan op dit moment twee thema's in het algemeen centraal, te weten: kunstmatige intelligentie (AI) en vendor risk management. Bestuurders bediscussiëren dit idee en zijn mede op zoek naar een modelmatige disclosure van cyber-gerelateerde informatie, zodat zij gerichte acties kunnen nemen.

2.4. Accountant en cyber

2.4.1. Werkzaamheden door de accountant

In de NBA publieke management letter over cyber wordt erkend 'dat de controlerend accountant een beperkte verantwoordelijkheid heeft tot het onderzoeken van en rapporteren over cyberrisico's in relatie tot het auditrisico in relatie tot de jaarrekeningcontrole' (NBA 2016). De accountant verklaart in de controleverklaring dat de jaarrekening een getrouw beeld geeft van vermogen, resultaat, kasstromen en andere toelichtingen. Onderdeel van de controle is dat de accountant op zoek gaat naar risico's op materiële afwijkingen in de jaarrekening als gevolg van fraude of fouten. In de vernieuwde controlestandaard 315 die sinds 2022 van toepassing is, wordt uitgebreid stilgestaan bij mogelijke materiële afwijkingen die te maken hebben met IT. Standaard 315 stelt dat de accountant inzicht dient te verwerven in de informatieverwerkingsactiviteiten van de entiteit (NBA 2023b Standaard 315.25a). Hierbij schenkt de accountant aandacht aan 'de complexiteit van de beveiliging over de IT-omgeving, inclusief kwetsbaarheid van de IT-applicaties, databases, en andere aspecten van de IT-omgeving voor cyberrisico's, vooral wanneer er webgebaseerde transacties zijn of transacties waarbij externe interfaces betrokken zijn' (NBA 2023b Standaard 315, bijlage 5 onderdeel 4).

Deze aandacht voor beveiliging is geen doel op zich: 'Dergelijke risico's hoeven niet noodzakelijkerwijs invloed te hebben op de financiële verslaggeving, aangezien de IT-omgeving van een entiteit ook IT-applicaties en aanverwante gegevens kan omvatten die betrekking hebben op operationele of nalevingsbehoeften (…)' (NBA 2023b Standaard 315, bijlage 5, art 19).

2.4.2. Rapportage door de accountant

Nederland kent al decennia de verplichting voor de externe accountant tot rapporteren over de betrouwbaarheid en continuïteit van gegevensverwerking op basis van het Burgerlijk Wetboek (BW 2 Titel 9):

> *De accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.*

Dit artikel stelt dat voor zover bevindingen inzake betrouwbaarheid en continuïteit zijn gedaan, deze dienen te worden gerapporteerd aan de raad van commissarissen. Cyberrisico's kunnen daar onderdeel van zijn. Uit de wetsgeschiedenis blijkt dat de accountant met betrekking tot betrouwbaarheid en continuïteit van de geautomatiseerde

gegevensverwerking geen actieve onderzoekplicht heeft in het kader van de jaarrekeningcontrole. Zo kan de accountant kiezen voor een gegevensgerichte controleaanpak die 'om de computer heen' controleert. Gezien de sterk toegenomen afhankelijkheid van IT binnen ondernemingen sinds deze wetsbepaling, kan de accountants steeds minder vaak voor een controleaanpak kiezen die de risico's van automatische gegevensverwerking negeert.

Naast deze specifiek benoemde wettelijke rapportageplicht aan de raad van commissarissen, heeft de accountant bij organisatie van openbaar belang (OOB) de plicht om in een uitgebreide controleverklaring in het jaarverslag aandacht te schenken aan de controleaanpak en de kernpunten van de controle ('key audit matters'). Kernpunten zijn 'aangelegenheden die, in de professionele oordeelsvorming van de accountant, het meest significant waren bij de controle van de financiële overzichten van de huidige verslagperiode. Kernpunten van de controle worden geselecteerd uit de aangelegenheden die zijn gecommuniceerd met de met governance belaste personen' (NBA 2023a, Standaard 701.8). Dit betekent dus dat cybersecurity in bepaalde omstandigheden voor de accountant aanleiding is om daarover te rapporteren in de controleverklaring.

Intussen wordt van de publieke accountant verwacht dat deze op de algemene vergadering ook mondeling een toelichting geeft omtrent de uitgevoerde jaarrekeningcontrole. In NBA-handreiking 1118 (NBA 2023a) wordt expliciet aangegeven dat dit ook cybersecurity kan betreffen.

2.5. Reflectie vanuit de praktijk

Assurance inzake cybersecurity beperkt zich niet tot jaarverslagen en beperkt zich ook evenmin tot accountants. Dit is niet voorbehouden aan accountants. Een voorbeeld hiervan is 'ISAE 3402': Assurancerapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie.[1] Dit betreffen rapportages over serviceorganisaties aangaande de uitbestede diensten met een reikwijdte die relevant wordt geacht voor de jaarrekeningcontrole van gebruikersorganisaties. Een sprekend voorbeeld hiervan is de uitbesteding van de salarisadministratie, die met behulp van de software van een derde partij wordt gevoerd. Ook zien wij in de markt alternatieven, zoals:

- AICPA SOC2, waarbij zogenaamde Trust Services Criteria worden afgedekt. Deze betreffen confidentiality, integrity, availability, security en privacy. SOC2 security is de meest voorkomende IT-rapportage in de praktijk met name als het om clouddiensten gaat (Boer 2013);
- AICPA SOC for Cybersecurity, waarbij de volgende informatiesets worden gepresenteerd: Management description, Management Assertion, and the practitioner's opinion. Deze rapportage is nog niet zo populair als de bovenstaande SOC2-rapportage (AICPA 2017).

Wij (als auteurs die betrokken zijn bij cybersecurity) merken in de praktijk dat belanghebbenden steeds vaker een grotere bijdrage verwachten van organisaties en accountants betreffende het transparant maken van de cyberrisico's en cyberrisicobeheersing van organisaties. Het belangrijkste doel van disclosure in hun optiek is inzichtverschaffing in de organisatie van cybersecurity, om investeerders en andere belanghebbenden te helpen tot de juiste besluitvorming te komen. In de jaarverslagen wordt onder meer stilgestaan bij de wijze waarop cyber-gerelateerde risico's worden beheerst. Hierbij past een storyline die dwars door de bedrijfsactiviteiten loopt en aandacht heeft voor de onderkende risico's, de genomen maatregelen, de monitoring door de raad van commissarissen en – waar relevant – de rapportage van bevindingen door de accountant.

Waarnemingen

In aanvulling op het bovenstaande hebben wij de volgende beelden op basis van onze ervaringen in de praktijk betreffende de transparantie door ondernemingen en het rapporteren door de accountant over cybersecurity:

1. **Compliance-benadering ten behoeve van disclosure**. Disclosure van cybercompliance is geen "silver bullet" voor de aantoonbare beheersing van cybersecurityrisico's. Het risico van deze benadering is dat de navolging van de regels het doel wordt en niet het transparant maken van het cyberrisico. Het rapporteren van expliciete risico-inschattingen vindt minder plaats dan het bekendmaken van generieke cybersecuritymaatregelen.
2. **Technische kennis van board members**. In jaarverslagen wordt in een aantal gevallen specifieke cyber-ervaring bij een of enkele C-level-bestuurders aangegeven. In het algemeen is de digitale kennis van bestuurders doorgaans onvoldoende om de impact van cyberrisico's te kunnen bepalen. Dit vraagt om specifieke training voor topmanagers, evenals specifieke cyber-ervaring bij een of enkele board members.
3. **Onderzoeken van de effectiviteit van cybermaatregelen**. De inzet van digitale middelen (zoals hulpmiddelen voor geautomatiseerde securityvalidatie) laat nog steeds te wensen over bij het onderzoeken van – en rapporteren over – de effectiviteit van cybersecurity-maatregelen. Het komt nog steeds voor dat de cyber-gerelateerde activiteiten op een procesmatige manier en met documentatiebestudering worden beoordeeld, zonder met voldoende diepgang instellingen te onderzoeken, handmatig of geautomatiseerd met tooling. Hierdoor kunnen de uitkomsten van onderzoeken afwijken van de cybersecurity-realiteit. Op basis van ontwikkelende vereisten zoals van DORA, verwachten wij een toename van penetratietesten, waarbij ook specifieke tooling wordt ingezet om de effectiviteit van cybermaatregelen te testen.
4. **Rol van de accountant**. De accountant wordt geacht zich comfortabel te voelen bij een cybergesprek en in staat te zijn om de juiste expertise in te schakelen waar nodig. Dit vergt kennisuitbreiding en een

intensievere samenwerking met de cyberspecialist en met de IT-auditor om de technische en organisatorische cyberbeheersmaatregelen boven water te kunnen halen en de connectie te kunnen maken met bedrijfsrisico's.

3. Onderzoek jaarverslagen 2022

Voor dit onderzoek hebben wij de jaarverslagen over 2022 van de 25 AEX-fondsen onderzocht, waarop de specifieke cyberregelgeving vanuit Europa of de VS betrekking heeft. In Tabel 2 zijn de fondsen gerangschikt. Daarbij zijn de in hoofdstuk 2 beschreven ontwikkelingen als startpunt genomen. Ons eerste filter was het zoekwoord 'cyber', omdat dit een algemeen begrip is dat andere varianten als 'cybersecurity' en 'cybercrime' ook afdekt. Aanvullend is gezocht naar 'digital security', 'law & regulation', 'GDPR' 'DORA', 'NIS' en 'Cyber Resilience Act'.

Volgend op de vorige hoofdstukken van deze bijdrage is gezocht naar antwoorden op de volgende vragen:

1. Wordt cyber gezien als een integraal onderdeel van de bedrijfsactiviteiten, onder andere in de risicoparagraaf? Wordt de link gelegd tussen cyber en ESG?
2. Wordt duidelijk welke maatregelen er zijn genomen ter mitigering van de onderkende risico's?
3. In hoeverre zijn de toezichthoudende organen aangehaakt?
4. In hoeverre vindt validatie plaats door de externe accountant?
5. Wordt de van toepassing zijnde wet- en regelgeving benoemd?

4. Onderzoek van AEX-jaarverslagen

In de 25 jaarverslagen varieerde het aantal keren dat 'cyber' (en dus ook de samengestelde woorden met daarin cyber) voorkwam enorm, van 4 tot 77. Na een eerste analyse bleek dat deze kwantitatieve meting geen inhoudelijk representatieve weergave was van de aandacht voor cyber in de afzonderlijke jaarverslagen. Als alternatief hebben wij een kwalitatief onderzoek uitgevoerd waarin wij een indeling hebben gemaakt naar activiteiten, risico's, maatregelen, governance en rapportage van bevindingen. In die laatste categorie is ook gekeken naar de betrokkenheid van interne en externe accountants. Het overzicht van de vindplaatsen van 'cyber' in de jaarverslagen 2022 is weergegeven in Tabel 2.

4.1. Cyber als onderdeel van de bedrijfsactiviteiten

In algemene zin valt op dat de aandacht voor cyber in het jaarverslag een sterke diversiteit kent. Aan de ene kant van het spectrum bevinden zich onder andere ABN-AMRO, Aegon, ASR, ING, KPN, NN, Relx en Wolters Kluwer, waarbij de ondernemingen cyber zien als integraal

Tabel 2. Overzicht van vindplaatsen over cyber in de jaarverslagen 2022 van de 25 AEX-fondsen.

		Management report		Riskmanagement			Supervisory Board report		Auditor's report	
		Bedrijfs-activiteiten	ESG	Risico's	Maatregelen	Learning/ Awareness	Competenties van RvC leden	(Belangrijk) thema RvC/audit commissie	Audit aanpak	KAM
1	ABN Amro	•	•	•	•	•		•		•
3	Aegon	•	•	•	•	•		•	•	
4	Ahold	•		•	•	•	•	•		
5	Akzo			•	•	•		•		
7	Arcelor Mittal			•	•	•		•		
8	ASMI		•	•	•	•	•	•	•	
6	ASML			•	•	•		•		
9	ASR	•	•	•	•	•		•		
2	Ayden			•		•		•		
10	Besi	•		•		•		•		
11	DSM		•	•	•	•		•		
12	Exor			•			•			
13	Heineken			•	•			•		
14	IMCD		•	•	•	•	•	•		
15	ING	•	•	•	•	•		•	•	•
16	KPN	•	•	•	•	•	•	•		•
17	NN	•	•	•	•	•		•	•	
18	Philips		•	•	•	•				
19	Prosus	•	•	•		•		•		
20	Randstad	•	•	•	•	•	•	•		
21	Relx	•	•	•	•	•		•		
22	Shell			•	•	•	•	•		
23	UMG		•	•	•	•		•		
24	Unilever			•	•			•		
25	Wolters Kluwer	•	•	•	•	•		•		•
	Totaal	**12**	**15**	**25**	**21**	**22**	**7**	**23**	**4**	**4**

onderdeel van de waardepropositie en van daaruit in het hele verslag aandacht schenken aan cyber. Aan de andere kant van het spectrum bevinden zich ondernemingen die cyber weliswaar aanstippen, maar waarbij uit het verslag niet blijkt wat de echte impact van cyber is voor de onderneming. Een voorbeeld hiervan is Exor. Daar tussenin zien we ondernemingen die cyber zien als risico en vervolgens aandacht schenken aan de diverse aspecten van cyber. In een aantal gevallen blijft de lezer van het jaarverslag in het ongewisse over de diepgang c.q. concreetheid van acties en meldenswaardige specifieke omstandigheden in 2022. Voorbeelden hiervan zijn Ayden, Besi en Prosus.

Cyber wordt door 15 fondsen betrokken in ESG: zowel op het gebied van de stakeholdersdialogen als bij de bepaling van de (dubbele) materialiteit: vanuit impact- en financieel perspectief. Opvallend is dat uit de stakeholdersanalyse bij IMCD blijkt dat cyber niet hoog in de materialiteitsmatrix staat, maar dat er toch relatief veel aandacht is voor cyber in het kader van riskmanagement (moderate risk met high impact). Prosus besteedt in het ESG-hoofdstuk uitgebreid aandacht aan cyber resilience. Een voorbeeld van het verankeren van cyber in ESG vinden wij in het jaarverslag van Wolters Kluwer, waarin cybermaturity onderdeel is van het Remuneration Report door de raad van commissarissen over het bestuur. Daarin wordt zowel over de mate van verbetering van cybermaturity als de cybermaturity-score zelf gerapporteerd als onderdeel van de niet-financiële KPI's (zie Figuur 1).

4.2. Cyberrisico's en maatregelen

Alle 25 AEX-fondsen benoemen risico's uit hoofde van cybersecurity. Bij 6 fondsen wordt cyber genoemd onder strategische risico's (of equivalent key risk of top risk): ASML, ASR, ING, NN, Philips en Unilever. In totaal 12 andere fondsen benoemen cyber als een operationeel risico. De overige fondsen laten het in het midden, door geen toewijzing naar strategisch of operationeel risico te maken. ASML en ASMI koppelen het cyberrisico aan het bewaken van de IP, 'de kroonjuwelen van de onderneming' (NBA 2016). ASML en ASR benoemen specifiek outsourcing als een aandachtsgebied waar het cyberrisico kan spelen. Bij een aantal fondsen blijft dit op het niveau van benoemen, bij andere fondsen wordt concreet toegelicht wat er kan gebeuren als het risico zich voordoet en welke maatregelen daartoe getroffen zijn. Een voorbeeld van een AEX-fonds uit deze laatste groep is Heineken (zie Figuur 2).

Figuur 1. Rapportage over maturity cybersecurity (Wolters Kluwer, Annual Report 2022, p. 103).

ESG objective	Measure	Weighting %	Description of target and how it is measured
Secure systems and processes	Indexed cybersecurity maturity score	3,33%	The annual target is based on a company-wide program designed to maintain cybersecurity at or above the industry standard benchmark for high-tech companies. The cybersecurity maturity score is assessed annually by a third party, based on the National Institute of Standards and Technology (NIST) framework. For 2023, the minimum payout requires the score to be in line with the industry standard for high-tech companies.

Figuur 2. Vermelding maatregelen tegen cyberrisico's (Heineken Annual Report 2022, p. 38).

Information security
What could happen? HEINEKEN's business increasingly relies on technology, both in the office environment and in the industrial control domain of its breweries. Failure of our systems as well as cybersecurity incidents could lead to business disruption, loss of confidential information, unauthorised access to our data, as well as a breach of data privacy regulations. All of this might lead to financial or reputational damage.
Recent developments HEINEKEN's digital footprint is expanding rapidly, in line with the strategy to become the best-connected brewer. Our Company is and will be more connected with our customers, consumers, suppliers and employees than ever. Attacks are becoming more sophisticated and potential consequences are more punitive and destructive in nature. A growing number of attacks, most notably increasing cases of malware and phishing are actively blocked by our Cyber Defense Operations (CDO) team. Geopolitical tensions have led to an increase of hacktivism as well as a slow increase of cyber warfare activities. Both will increase the likelihood of a cyber incident. We observe an increase in cyberattacks on our customers as well as key suppliers leading to security of supplies concerns. On top of this, regulations continue to place stricter security requirements on data processing by HEINEKEN and its ecosystem of partners.
What are we doing to manage this risk? Cybersecurity remains a top priority within HEINEKEN. All functions collaborate closely to act promptly and aligned in case of cyber incidents at HEINEKEN or one of our suppliers or customers. The portfolio of cybersecurity initiatives, which is evaluated regularly, is executed to address cybersecurity threats in both our office systems and Industrial Control Domain. Our Cyber Defence and Operations teams monitor and act upon cyberattacks 24/7 globally. Our main focus is to enhance the resilience of the current and future technology landscape of HEINEKEN, while continuously increasing employee security/privacy awareness.

Een ander voorbeeld is ASML, dat een Cyber Defense Center heeft gecreëerd en een 'Information security and cyber resilience programme' heeft lopen. Dat is niet voor niets: zo meldt ASML maar liefst 2800 cybersecurity-incidenten die zijn onderkend en ondervangen. Ook KPN is transparant over kwetsbaarheden en incidenten.

4.3. Cyber en toezichthoudende organen

Cyber heeft de aandacht van elke raad van commissarissen[2]: bij 7 fondsen wordt bij de profielen van de leden cyber als een van de competenties genoemd. In de meeste verslagen van de raad van commissarissen wordt in meerdere of mindere mate verwoord dat het thema op de agenda heeft gestaan: bij 23 van de 25 fondsen wordt cyber in het commissarissenverslag als een van de besproken thema's genoemd. Alleen bij Exor en Philips wordt dit niet expliciet genoemd. Bij een aantal jaarverslagen blijft dit beperkt tot een bespreekpunt, in andere verslagen wordt meer diepgang verwoord door presentaties van het bestuur, de internal auditor of de dialoog met de externe accountant. Ook wordt in meerdere verslagen vermeld dat er deep dives zijn uitgevoerd met en voor de Audit Commissie en de raad van commissarissen.

4.4. Validatie door de externe accountant

In de 25 jaarverslagen van de AEX-fondsen is bij 4 fondsen door de externe accountant cyber in de controleverklaring genoemd in de paragraaf over de controleaanpak. Bij 4 fondsen is een key audit matter verwoord waarin cybersecurity aan bod komt, inclusief de reflectie daarop voor de controle-aanpak: ABN-AMRO, ING, KPN en Wolters Kluwer. In deze key audit matter gaat de accountant specifiek in op de werkzaamheden rond cybersecurity. Gezien de importantie van cybersecurity voor de bedrijfsvoering van deze fondsen is dat ook goed te verklaren. Dit blijkt onder andere uit de bespreking van cyber in de bedrijfsvoeringsparagrafen en niet alleen in de riskmanagementparagrafen in de betreffende jaarverslagen.

De specifieke aandacht door de accountant voor cyber in een key audit matter bij KPN is zichtbaar vanaf het jaarverslag 2016. Bij NN geeft KPMG aan dat de key audit matter over betrouwbaarheid van IT general controls en cybersecurity controls uit de controleverklaring van 2021 niet meer is opgenomen in 2022, omdat bevindingen minder significant waren in 2022. In die controleverklaring 2021 was de argumentatie voor de key audit matter als volgt verwoord: *'Taking into account group's dependency on the reliability and continuity of IT and the increasing frequency and severity of cyber incidents in the environment where the group operates, we considered the reliability of IT general controls and cybersecurity controls a key audit matter.'*

4.5. Cyber vanuit de invalshoek van wet- en regelgeving

Tabel 3 bevat een samenvatting van de verwijzingen naar wet- en regelgeving in de jaarverslagen 2022 over cyber.

Tabel 3. Verwijzingen naar wet- en regelgeving.

	GDPR/ privacy	NIS/ NIS2	DORA	SEC m.b.t. cyber
Term genoemd	8	1	2	1
Term genoemd met onderliggende risico's en maatregelen	13	0	0	0
Totaal genoemd	21	0	2	1
Niet genoemd	4	24	23	24
Totaal	**25**	**25**	**25**	**25**

In de jaarverslagen wordt in 21 verslagen de van toepassing zijnde privacyregelgeving, in generieke termen of specifiek GDPR, genoemd. In 13 verslagen wordt de term genoemd en wordt ingegaan op de daaruit volgende risico's en maatregelen. In 8 aanvullende gevallen wordt alleen de term genoemd. In 4 gevallen (Ahold, Akzo, Besi en Unilever) wordt geen verwijzing gemaakt naar de geldende privacyregelgeving. Omdat de privacyregelgeving in 2018 is ingegaan, lijkt het na een paar jaar dus gemeengoed om hier ook expliciet aandacht aan te geven in het bestuursverslag. Alleen KPN maakt melding van de aankomende NIS2-regelgeving. DORA wordt genoemd door Aegon en ASR, terwijl Adyen, ABN AMRO, ING en NN deze niet expliciet benoemen. ASR en KPN maken melding van de aangekondigde Cyber Resilience Act. Van de

Figuur 3. Key audit matters en werkzaamheden rond cybersecurity (KPN Integrated Annual Report 2022, p. 181).

Key audit matter	Our audit approach	Key observations
Reliability of IT systems, including security, cybercrime and data privacy		
At KPN, processes are highly automated and KPN continuously invests in simplification and improvement of IT systems. Reliability and security of IT systems are thereby high on the of agenda of KPN and for that purpose KPN's internal control framework includes several controls to ensure, inter alia, proper identity, access and change management of its IT systems. The reliability of IT systems, including security, cybercrime and data privacy is considered a key audit matter as it is key for KPN's activities and financial reporting.	As part of our audit, we have reviewed the quality of KPN's IT systems and the controls embedded therein with a purpose to express an opinion on the financial statements. With respect to cybersecurity, we obtained an understanding KPN's security and privacy organization as well as cyber risk management in relation to KPN's cyber threat landscape. For this purpose, we performed our own procedures and reviewed and tested the work done by KPN Risk Management and KPN Audit. Since this is highly specialized work, our audit team includes IT specialists.	In a few instances with respect to our IT general control testing, we identified situations where controls needed improvement. KPN has setup remediation procedures that we have also reviewed and tested with satisfactory results.

Tabel 4. Samenvatting onderzoek jaarverslagen.

	Activiteiten	Risico's	Maatregelen	Governance	Rapportage bevindingen
Aspecten	- Koppeling met ESG (stakeholdersdialoog en materialiteit) - Samenwerking (partnering en outsourcing) - Effect impact regelgeving	Onderdeel strategische en operationele risico's met dimensies kans en impact	(Awareness) training	- Expertise Board leden (RvB en RvC) - Besprekingen in vergaderingen van audit commissies en RvC - Rol internal audit	- Rapportage over concrete incidenten - Reflectie externe accountant over aanpak, werkzaamheden en uitkomsten
Aansprekende voorbeelden	KPN - Waarde propositie - Partnering ASR - effect regelgeving - effect outsourcing Randstad - Relatie met persoonsgegevens Wolters Kluwer - Cyber maturity als KPI voor remuneratie	NN - Strategic risk assessment	DSM Training ASML - Cyber Resilience Programma	Prosus - Competenties board leden Heineken - Deep dive sessie met AC en RvC NN en Unilever - Werkzaamheden internal audit	ING - Transparantie over attack KPN - Transparantie over vulnerabilities en incidenten - KAM in controleverklaring

7 fondsen uit de AEX die ook in de VS zijn genoteerd, wordt alleen door Aegon in het jaarverslag specifiek ingegaan op de aangekondigde SEC-regelgeving met betrekking tot cyber. Deze analyse is samengevat in Tabel 4, waarin ook aansprekende voorbeelden zijn genoemd.

5. Conclusie

Er is een diversiteit aan aandacht voor cybersecurity in het jaarverslag, zowel in omvang als diepgang. Regelmatig wordt cybersecurity genoemd, maar vaak meer als formeel punt zonder specifieke diepgang of expliciete betekenis. Een aantal ondernemingen benoemt de relevantie voor business en de bedrijfsactiviteiten. Een aantal ondernemingen vermeldt cybersecurity als onderdeel van ESG. De raad van commissarissen (en daarbinnen de Audit Commissie) is in veel gevallen zichtbaar aangehaakt. Specifieke dreigingen worden (slechts) beperkt genoemd, zoals risico's vanuit derde partijen, terwijl dit bij alle organisaties een wezenlijk groeiende en grote dreiging is. De meeste ondernemingen benoemen een beveiligingsmaatregel, zoals trainingen voor beveiligingsbewustzijn, maar ze benoemen dan niet andere beveiligingsdomeinen, zoals secure software development. Hiermee wordt de schijn van sterke maatregelen gegeven, maar er ontbreekt transparantie van beveiligingsmaatregelen in de breedte.

Bij vier ondernemingen heeft de accountant in de controleverklaring als onderdeel van de key audit matters aandacht gegeven aan cybersecurityrisico's en de daaruit volgende controlewerkzaamheden. Kennelijk beschouwen accountants cyberrisico's in veel gevallen niet als onderwerp van grote aandacht voor de jaarrekeningcontrole, dat vervolgens aanleiding geeft tot het formuleren van een key audit matter.

Gezien de geschetste ontwikkelingen vanuit wet- en regelgeving, de erkenning van uitdagingen in de bedrijfsvoering en een vergroot ESG-bewustzijn, is het onze verwachting dat het thema cyber in de jaarverslagen een verder groeiende aandacht zal krijgen. Transparantiegerelateerde activiteiten (traceerbare communicatie van de feiten naar de belanghebbenden) worden gedreven door de wet- en regelgeving alsmede door cyberbewuste leiders. Meer transparantie zal op termijn resulteren in een betere beheersing van cybersecurityrisico's.

- **Prof. dr. PWA Eimers RA – Peter** is hoogleraar Audit & Assurance aan de Vrije Universiteit en partner bij EY.
- **Prof dr. A. Shahim RE – Abbas** is hoogleraar IT Auditing aan de Vrije Universiteit en Global ESG partner bij Eviden (voormalig Atos).
- **Ir. P. Kornelisse RE – Peter** is partner bij EY en hoofddocent IT Auditing aan TIAS.

Noten

1. Deze internationale assurancestandaard is in Nederland als vertaling uitgegeven als Standaard 3402 door NBA en als Richtlijn 3402 door NOREA.
2. Of de Board of Directors voor die fondsen waar sprake is van een one-tier Board.

Literatuur

- AICPA (2017) SOC for Cybersecurity: A backgrounder. https://www.aicpa-cima.com/resources/download/learn-about-soc-for-cybersecurity
- AP [Autoriteit Persoonsgegevens] (2023) AVG Algemeen. https://autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen [geraadpleegd in september 2023]
- Boer JC (2013) Nieuwe ontwikkelingen IT-gerelateerde Service Organization Control-rapportages: SOC2 en SOC3, Compact, Nummer 2, KPMG, 2013.
- EY [Ernst & Young LLP] (2023) What cyber disclosures are telling shareholders in 2023, EY Center for Board Matters. https://www.ey.com/en_us/board-matters/what-cyber-disclosures-are-telling-shareholders-in-2023
- DORA [Digital Operational Resilience Act] (2023) European Insurance and Occupational Pensions Authority, Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- EU [European Union] (2019) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). https://eur-lex.europa.eu/eli/reg/2019/881/oj
- EU [European Union] (2022a) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive [EU] 2016/1148 (NIS 2 Directive). https://www.nis-2-directive.com
- EU [European Union] (2022b) EU Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- ENISA (2023) ENISA Threat landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- Heineken (2023) Annual Report 2022. https://www.theheinekencompany.com/sites/theheinekencompany/files/Investors/financial-information/results-reports-presentations/Heineken-NV-Annual-Report-2022-23_02_2023.pdf
- KNVB (2023) Informatie cyberinbraak KNVB, 12 september 2023. https://www.knvb.nl/info/68084/informatie-cyberinbraak-knvb
- KPMG [KPMG International Cooperative] (2017) Is everything under control? Audit committee challenges and priorities, 2017 Global audit committee pulse survey, KPMG's Audit Committee Institute.
- KPN (2023) Integrated Annual Report 2022. https://ir.kpn.com/files/doc_financials/2022/ar/KPN_Integrated_Annual_Report_2022_20230224.pdf
- MCCGC [Monitoring Commissie Corporate Governance Code] (2016) De Corporate Governance Code. https://www.mccg.nl/de-code
- NCTV [Nationaal Coördinator Terrorismebestrijding en Veiligheid] (2023) Cybersecuritybeeld Nederland. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland
- NBA (2016) Van Hype naar Aanpak, Publieke management letter over Cybersecurity. https://www.nba.nl/themas/kennis-delen-en-pml/van-hype-naar-aanpak/
- NBA (2023a) Handreiking 1118 Het optreden van de externe accountant in de algemene vergadering van aandeelhouders, versie 27 februari 2023. https://www.nba.nl/siteassets/wet--en-regelgeving/nba-handreikingen/1118/nba-handreiking-1118-definitief-20230227.pdf
- NBA (2023b) Handleiding Regelgeving Accountancy, daarin opgenomen de NV COS met individuele controlestandaarden (individueel aangeduid als 'Standaard').
- NOREA (2023) Consultatie verslaggevingstandaard verantwoording IT-beheersing (NOREA Reporting Initiative). https://www.norea.nl/nieuws/consultatie-verslaggevingstandaard-verantwoording-it-beheersing-norea-reporting-initiative
- Schinagl S, Shahim A (2020) What do we know about information security governance? "From the basement to the boardroom": Towards digital security governance. https://research.vu.nl/en/publications/what-do-we-know-about-information-security-governance-from-the-ba
- SEC [Securities and Exchange Commission] (2023) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure
- Shahim A, Rahali A, Van Praat J [red.] (2022) Research in cybersecurity: An IT audit and advisory perspective. Vrije Universiteit, School of Business and Economics.
- UM [Universiteit Maastricht] (2020) Reactie Universiteit Maastricht op rapport FOX-IT, 5 februari 2022. https://www.maastrichtuniversity.nl/nl/file/foxitrapportreactieuniversiteitmaastrichtnl10-02pdf
- VNG (2021) Bestuurlijke lessen uit de hack bij Hof van Twente, 20 april 2021. https://vng.nl/nieuws/bestuurlijke-lessen-uit-de-hack-bij-hof-van-twente
- WEF [World Economic Forum] (2023) Global Cybersecurity Outlook 2023 – Insight report January 2023. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
- Wolters Kluwer (2023) Annual Report 2022. https://assets.contenthub.wolterskluwer.com/api/public/content/7ecf79d725094df588fddb8b58370a0c?v=0723f0d6