Tien belangrijke inzichten voor geïnformeerd cybertoezicht

Article · August 2023

CITATIONS
0

READS
154

8 authors, including:

Freddy Dezeure
Freddy Dezeure BV
26 PUBLICATIONS **3** CITATIONS
SEE PROFILE

João Pedro Gonçalves
EQT Group
14 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Eireann Leverett
Concinnity Risks
26 PUBLICATIONS **92** CITATIONS
SEE PROFILE

Lokke Moerel
Tilburg University
38 PUBLICATIONS **89** CITATIONS
SEE PROFILE

Cyberrisico rapporteren aan raden van bestuur

Tien belangrijke inzichten voor geïnformeerd cybertoezicht

Auteurs
Freddy Dezeure
Peter Debasse
João Pedro Gonçalves
Tristan Guiheux
Éireann Leverett
Patrick Mana
Lokke Moerel
Bartosz Sygula

Recensenten
Greg Bell
Paolo Borghesi
Philippe Coffyn
Chris Deverell
Tom Gilis
Kevin Holvoet
Angelos Keromytis
Ed Millington
Dimitri Rombaut
Sam Singer

Datum: 30 augustus 2023
Versie: Definitief

Inhoudsopgave

Inleiding

In maart 2022 publiceerden we de white paper Cyberrisico's rapporteren aan Raden van Bestuur, met richtlijnen voor Chief Information Security Officers (CISO's) voor het implementeren van kwantitatieve cyberrisicometrics om cyberrisico's op bestuursniveau te rapporteren en om redelijke zekerheid te bieden dat het cyberrisico binnen de geaccepteerde risicobereidheid blijft. De white paper kreeg veel aandacht en waardering in de gemeenschap en is breed verspreid. Er is ook een verkorte versie voor bestuursleden gepubliceerd.

Sinds de publicatie hebben aanvullende wettelijke vereisten in de EU (NIS2[1] , DORA[2]) en de VS (SEC[3], NYDFS[4]) de verantwoordelijkheid en aansprakelijkheid van bestuursleden vergroot om zorgvuldig en geïnformeerd toezicht te houden op cyberrisico's in hun organisaties. Cyberrisico speelt ook een steeds grotere rol in ESG-rapportage. Sommige van deze wettelijke vereisten verwijzen expliciet naar cybermetrics (DORA, artikel 6). Er is op dit moment nog geen officiële richtlijn over wat goed toezicht door raden van bestuur inhoudt, laat staan welke strategische metrics kunnen leiden tot *geïnformeerd* toezicht.

Feedback van de gemeenschap op de inhoud van de white paper van 2022 en aanvullende inzichten hebben aangegeven dat er behoefte is aan aanvullende toelichting om de belangrijkste inzichten te benadrukken en de formulering ervan aan te scherpen. Dit document is bedoeld dat doel te dienen. Het biedt ook elementen om te voldoen aan de aanvullende wettelijke vereisten inzake informatieverstrekking aan en toezicht van de raad van bestuur.

Dit document bouwt voort op de fundamentele notie dat goed cyberrisicobeheer *evidence-based* moet zijn in plaats van te vertrouwen op intenties of aannames (vaak gebaseerd op zelfrapportage). Strategische cybermetrics zijn een essentieel onderdeel van elke succesvolle poging om cyberrisicobeheer te prioriteren en te implementeren.

Het meten van cyberrisico's op een *kwantificeerbare* manier, met behulp van gegevens van de infrastructuur, wordt nog niet op grote schaal toegepast in de industrie. Het is niet verwonderlijk dat er ook geen overeengekomen maatstaven zijn om te vergelijken tussen peers.

De huidige paper deelt 10 belangrijke inzichten van organisaties die strategische cybermetrics hebben geïmplementeerd, zodat de gemeenschap erop kan voortbouwen en ze in hun eigen omgeving kan toepassen. De inzichten worden samengevat in heldere en tot nadenken stemmende samenvattingen om de opname te vergemakkelijken. Deze aanpak kan overkomen als een generalisatie of simplificatie, maar het helps om de aandacht van CISO's en Raden van Bestuur te stroomlijnen en te focussen en uiteindelijk betere resultaten te behalen bij het beheer van en het toezicht op cyberrisico's.

---

[1] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555 (artikelen 20 en 21)
[2] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022R2554 (artikelen 5 en 6)
[3] https://www.sec.gov/news/press-release/2023-139
[4] https://www.dfs.ny.gov/system/files/documents/2022/10/rp23a2_text_20221109_0.pdf

Dit document moet worden beschouwd als een aanvulling op het witboek van 2022 en het wordt ten zeerste aanbevolen om ze samen te lezen.

Tien belangrijke inzichten

1. Bewijs in plaats van compliance

Veel organisaties gebruiken een cyberbeveiligingsraamwerk (NIST, ISO, CIS) of volgen specifieke regelgeving en normen (PCI-DSS, Solvency/Basel II), gecombineerd met externe audits en certificering. Dit is vaak een vereiste in hun activiteit, omwille van regelgeving of zakelijke redenen (verzekeringen, klanten). Deze aanpak moet echter worden beschouwd als een basislijn en niet als een wondermiddel. Ze biedt normen en beleid om na te leven, maar garandeert niet noodzakelijkerwijs dat dit voldoende is voor de specifieke bedrijfsrisico's.

Zijn de controles, als ze correct functioneren, voldoende voor een effectieve risicobeperking? Zijn ze volledig ingezet? Functioneren ze zoals bedoeld?

De meest volwassen organisaties gebruiken (continu) bewijs, door gegevens verzameld in hun infrastructuur, om de effectiviteit van hun controles vast te stellen in plaats van te vertrouwen op menselijke beoordeling, zelfrapportage en vragenlijsten die één keer per jaar worden ingevuld. Het verzamelen en bewaren van gegevens is weliswaar een belangrijke uitdaging, maar deze organisaties zijn van mening dat het de moeite waard is. Professionele beoordeling kan een onderdeel blijven bij het bieden van context in de rapportage aan het bestuur, als dit wordt ondersteund door metrics die zijn afgeleid van operationele gegevens en beveiligingsmiddelen.

2. KCI's rapporteren in plaats van alles

Raden van bestuur willen toezicht op wat belangrijk is en niet alle controles in zijn even belangrijk. De meeste raamwerken geven aan dat een beperkt aantal controles de grootste impact heeft op de risicobeperking.

Het rapporteren van Key Control Indicators (KCI's) en hun evolutie in de tijd aan de Raad van Bestuur is daarom zinvoller rapportage over alle controles. Dat betekent niet dat de CISO alle andere controles uit het oog verliest, het brengt juist in beeld wat op een bepaald moment de meeste impact heeft op risicobeperking voor een specifieke organisatie.

Verwar het concept van Key Performance Indicators (KPI's) niet met KCI's. Een CISO moet geïnteresseerd zijn in de prestaties van zijn/haar team, maar KPI's zullen niet altijd relevant zijn voor hoe goed het cyberrisico wordt beperkt. Rapportage aan de raad van bestuur vereist indicatoren die strategisch van aard zijn, die representatief zijn voor de algehele interne controleomgeving en die de risicobereidheid ondersteunen.

Gedetailleerde richtlijnen over KCI's en de effectiviteit en dekking ervan zijn te vinden in de white paper Cyberrisico's rapporteren aan Raden van Bestuur.

Hier is een voorbeeldlijst van KCI's als uitgangspunt:

KCI 1	Inventaris van activa [5]	% activa in de inventaris binnen het beleid
KCI 2	Bevoorrechte accounts	% bevoorrechte accounts beheerd binnen beleid

[5] Een nauwkeurige en volledige inventaris van bedrijfsmiddelen is van cruciaal belang, omdat het de noemer is voor veel van de KCI's

KCI 3	Tijdige patching	% patches met hoog risico binnen N uur # ontdekte bekende en misbruikte kwetsbaarheden
KCI 4	Back-up	Maximale tijd om belangrijke activa te herstellen (% van kritieke activa herstelbaar in N uur)
KCI 5	Bescherming van eindpunten	% eindpunten geconfigureerd in lijn met beleid
KCI 6	Logboeken verzamelen	% kritieke systemen aan boord voor logboekverzameling
KCI 7	Netwerkbeveiliging	% conforme belangrijke netwerkbeveiligingsconfiguraties
KCI 8	Naleving door derden	% conforme belangrijke verbindingen met derden
KCI 9	Identiteitsbeheer	% dekking van systemen die MFA gebruiken
KCI 10	Belangrijke incidenten	% grote cyberincidenten met bedrijfsimpact
KCI 11	Risicoaanvaarding	# risico geaccepteerde beleidsafwijkingen
KCI 12	Internet blootgestelde activa beveiligingsdekking	% aan internet blootgestelde bedrijfsactiva waarop beveiligingsmonitoring en regelmatige beveiligingsbeoordeling van toepassing zijn
KCI 13	Dekking kroonjuweel	% kroonjuwelen gedekt door beveiligingsmonitoring, scannen op kwetsbaarheden en regelmatige beveiligingsbeoordeling
KCI 14	Oorsprong van beveiligingsincidenten	% beveiligingsincidenten gerelateerd aan tekortkomingen van minstens één essentiële controle-indicator

3. Dreiging-geïnformeerd in plaats van statisch

Het dreigingslandschap verandert en onze controles en KCI's zouden dat ook moeten doen. Tegenstanders passen hun tactieken en technieken aan om onze verdediging te omzeilen. Ze zijn zich vaak beter bewust van onze infrastructuur en hiaten in de controle dan wij. Ze houden de publicatie van kwetsbaarheden door leveranciers in de gaten en reageren daar sneller op dan wij. Sommigen hebben voldoende middelen om geavanceerde exploits te kopen.

Om negatieve gevolgen voor ons bedrijf te voorkomen, moeten we onze controles aanpassen aan de dreiging, rekening houdend met onze specifieke omgeving en activa. Dit vereist inzicht in de tactieken, technieken en procedures van de tegenstander, prioritering en aanpassing van controles en voortdurende controle op indicators of behavior and compromise. Belangrijke ontwikkelingen moeten worden gevolgd en gerapporteerd aan de Raad. En, natuurlijk, met de juiste prioriteit opgepikt worden op technisch niveau.

4. Prioriteiten in plaats van gemiddelden

Focus houden op wat echt belangrijk is, betekent ook dat we voorzichtig moeten zijn met gemiddelden. Door een gemiddelde te nemen, kunnen afwijkingen van kritieke controles onder de radar blijven en blijven uitschieters onopgemerkt.

Daarom raden we aan om geen aggregaat te maken van de resultaten van alle honderden controles die u hebt geïdentificeerd. Het kan vanuit technisch oogpunt aantrekkelijk zijn om een percentage van de dekking van het hele raamwerk vast te stellen, maar dit uitmiddelen heeft de neiging om de belangrijkste problemen te verbergen.

Op dezelfde manier kan het uitmiddelen binnen een specifieke controle belangrijke risico's verbergen. Als een organisatie er bijvoorbeeld naar streeft om kritieke kwetsbaarheden binnen drie dagen te patchen, kwetsbaarheden met een gemiddeld risico binnen een maand en de rest binnen drie maanden, kan het gemiddelde van de patchprestaties de meest kritieke kwetsbaarheden verbergen.

Rapporteer alleen gemiddelden als dat zinvol is voor een specifieke KCI. Meer gedetailleerde richtlijnen over KCI's en dekking zijn te vinden in de 2022 white paper Cyberrisico's rapporteren aan Raden van Bestuur.

5. Hiaten rapporteren in plaats van "helemaal groen

Het is helemaal prima om de feitelijke situatie aan het bestuur te melden, inclusief de gaten die gedicht moeten worden. Ze moeten dit horen als dit de realiteit is. Het zal de organisatie ook helpen om te voldoen aan regelgevend toezicht en om de prioritering van investeringen te onderbouwen.

Bij het rapporteren van hiaten aan het bestuur moet worden uitgelegd welk risico ze met zich meebrengen en welke maatregelen worden voorgesteld om ze binnen een verwacht tijdsbestek op te lossen.

6. Ingebed in plaats van losgekoppeld

De impact van het melden van cyberrisico's aan de raad zal worden vergroot door degenen die ze beheren (operators, managers) toegang te geven tot de status van de controles. We noemen dit de "democratisering van de metrics".

Het rapporteren van cyberrisico's aan de raad van bestuur stuurt de organisatie. Wat als belangrijk wordt gerapporteerd, zal onvermijdelijk (gelukkig) als belangrijk worden ervaren door het bestuur en binnen de organisatie. De gerapporteerde KCI's moeten daarom zinvol zijn vanuit het perspectief van risicobeheer en de werkelijke status van het risico zichtbaar maken.

De onderliggende gegevens voor de KCI's moeten worden verzameld uit de systemen die de controles implementeren. Het implementeren van gekoppelde dashboards op alle niveaus van de organisatie, met de granulariteit die nodig is om inzicht te geven aan de managers van de controles, zorgt voor transparantie, vergroot het eigenaarschap en maakt het mogelijk om het systeem te verfijnen.

7. Transparantie van afwijkingen in plaats van acceptatie

U moet overwegen specifieke afwijkingen van belangrijke controles zichtbaar maken door ze te rapporteren aan het bestuur. Deze afwijkingen kunnen het gevolg zijn van risicoacceptatie of beleidsovertredingen (opzettelijk of onopzettelijk).

De meeste organisaties hebben een proces dat afdelingen toestaat af te wijken van het beveiligingsbeleid door "het risico te accepteren". In plaats van deze

afwijkingen onder de radar te houden, zou het verstandig zijn om ze te rapporteren. Het zichtbaar maken van afwijkingen kan de organisatie helpen om zich te richten op de belangrijkste controles die zijn ontworpen om het risico te beperken en binnen de risicobereidheid te blijven.

Het monitoren van afwijkingen is vooral nuttig om inzicht te krijgen in de volwassenheid van de organisatie met risicomanagementprocessen en -cultuur. Meer volwassen organisaties hebben de neiging om "risicoaanvaarding" als laatste van de beschikbare opties te behandelen, niet als eerste.

Het proces van het documenteren van deze afwijkingen stelt ons ook in staat om drempels te identificeren die onrealistisch zijn, bijvoorbeeld het patchen van alle kwetsbaarheden met een budget van 1% van de ARR. Door de afwijkingen te bespreken, kan de hele organisatie toewerken naar drempelwaarden voor risicoacceptatie die praktischer en realistischer zijn.

8. Risicobereidheid in plaats van nul risico

We kunnen dit niet vaak genoeg herhalen, een organisatie moet op bestuursniveau bepalen wat een acceptabel niveau van cyberrisico is. Nul risico is een onmogelijk en waarschijnlijk zelfs onwenselijk doel. Dat is in wezen risicovermijding in plaats van 'efficiënt omgaan met risico's'. In veel organisaties is risicobereidheid al vastgelegd binnen de algemene bedrijfsrisicoprocessen. Als dit voor cyber nog niet het geval is, moet de CISO de raad van bestuur vragen de risicobereidheid voor cyber vast te stellen:

- Hoeveel zijn we bereid te verliezen als het cyberrisico werkelijkheid wordt? Denk aan dagen downtime, diefstal van intellectuele eigendomsrechten, verlies van PII, reputatieschade...
- In welke mate willen we dat het risico wordt beperkt? Nul risico is een onmogelijk doel. De cyberrisicobereidheid zal naar verwachting schommelen tussen hoog en gemiddeld, gezien de evolutie van het dreigingslandschap en de beschikbare technologie.
- Welke middelen willen we beschikbaar te stellen voor mitigatie?
- Willen we het resterende cyberrisico verzekeren of zelf verzekeren?

Een kwantitatieve benadering van cyberrisicobereidheid is momenteel moeilijk te realiseren en is eerder uitzondering dan norm. De Risk Appetite Statement (RAS) is meestal gebaseerd op een kwalitatieve benadering die onderliggende kwalitatieve en kwantitatieve elementen combineert. Het niveau van de RAS wordt door het bestuur vastgesteld in termen van Laag, Gemiddeld, Hoog. Vaak wordt het vastgesteld door verschillende risicodomeinen te vergelijken en te prioriteren. Het is eerder een kalibratie van de verschillende domeinen. De eigenlijke onderbouwing van de RAS is een echte uitdaging. Het vereist een cascade van indicatoren vanaf het technische/operationele niveau tot het management- en strategische niveau.

Hoewel moeilijk, is het bespreken van cyberrisico's in termen van zakelijke impact in cijfers nuttig en het doel is niet perfectie. Vergis je eerst in deze getallen en laat de leidinggevenden toewerken naar het beantwoorden van deze vragen op een herhaalbare manier. Ze moeten zich bewust worden van cyber als bedrijfsrisico en er op dezelfde manier mee omgaan.

9. Het verhaal vertellen - risicoverbinding met diensten

Een CISO moet het cyberverhaal in een bedrijfscontext vertellen om de boodschap succesvol te kunnen brengen. Hiervoor moet hij/zij inzicht hebben in de status van de controles en hun impact op het risicoprofiel dat wordt aangestuurd door zakelijke diensten.

Een belangrijke doelstelling voor organisaties die streven naar echte volwassenheid van hun risico- en controleomgeving is het vermogen om inzicht te krijgen:

- hoe hun zakelijke diensten (bijv. een lening verstrekken of handel drijven) het inherente cyberrisicoprofiel beïnvloeden (bijv. de noodzaak om vertrouwelijke klantgegevens veilig op te slaan)
- en vice versa, hoe het inherente cyberrisico deze diensten kan beïnvloeden (bijv. een gebrek aan veilige opslag voor afgeschermde klantgegevens kan leiden tot onbedoelde openbaarmaking van gegevens of de toegang tot gegevens veel gemakkelijker maakt voor kwaadwillende actoren).

De organisatie moet begrijpen welke IT-middelen en processen hun zakelijke diensten ondersteunen (bijv. welke systemen nodig zijn om een lening te verstrekken). Dit maakt het mogelijk om het inherente cyberrisico te profileren en te meten.

De volgende stap is ervoor te zorgen dat cybercontroles worden toegepast op de IT-middelen en processen via geautomatiseerde methoden (bijv. "controles als code"), zodat de effectiviteit duidelijk kan worden gemeten via belangrijke controle-indicatoren (bijv. zoals eerder vermeld KCI5 % eindpunten geconfigureerd in lijn met beleid).

Met deze aanpak kan de CISO de raad van bestuur een duidelijk verhaal geven over hoe de huidige status van restrisico's en tekortkomingen in de controle het bedrijf kunnen beïnvloeden en context bieden om de risicobereidheid met succes te beheren en relevante investeringsbeslissingen te nemen.

10. Uniformeer cyberregelgeving - pas selectieve 'gold-plating' toe

De meeste hedendaagse en opkomende cyberregelgeving wereldwijd heeft overlappende vereisten. Een CISO moet alle regelgeving die relevant is voor zijn/haar organisatie op de verschillende geografische locaties en verschillende sectoren implementeren door mappings te gebruiken om de implementatie ervan te harmoniseren.

Deze aanpak maakt het mogelijk om dezelfde logica en redenering toe te passen bij het aanpakken van vergelijkbare risico's en controles, ongeacht de regelgeving waar de focus op ligt, met een aanzienlijke verlaging van de overhead voor de CISO en de technische teams.

Er bestaan echter altijd uitzonderingen. Sommige voorschriften kunnen specifieke controles voorschrijven die uniek zijn voor een bepaalde entiteit en mogelijk een uitdaging vormen om te handhaven. In dergelijke gevallen kan men kiezen voor een 'gold-plating' strategie, waarbij deze controles worden

geïsoleerd, uitsluitend voor die entiteit. Deze selectieve toepassing minimaliseert overbodig werk voor andere entiteiten binnen de organisatie en maakt het mogelijk om een alomvattende cyberbeveiligingsstrategie en rapportage te handhaven.

De rapportagelijn(en) van de CISO

Een CISO is belast met het bepalen en onderhouden van de visie, de strategie en het programma van de organisatie om informatie- en technologiemiddelen te beveiligen. De CISO moet autonoom en onafhankelijk kunnen handelen (bijv. DORA art. 6.4[6]). Traditioneel rapporteert de CISO aan een C-suite executive, zoals de Chief Information Officer (CIO), Chief Operating Officer (COO), Chief Finance Officer (CFO) of zelfs de CEO. Hoewel deze structuur wijdverbreid is, kunnen CISO's zich in een tegenstrijdige positie bevinden wanneer de betreffende C-suite executive ook verantwoordelijk is voor andere functies waarbij beslissingen moeten worden genomen over afwegingen tussen naleving van beveiligingsnormen en operationele efficiëntie, enzovoort.

Om te voorkomen dat de CISO geïsoleerd optreedt, moet er een balans zijn tussen de belangen van de interne stakeholders en het beperken van het cyberrisico. Een organisatie kan een Information Security Steering Committee (SteerCo) oprichten met het mandaat om operationele beslissingen te nemen, beveiligingsrisico's en belangrijke controles te bewaken, metrics overeen te komen, budgetten te sanctioneren, de beveiligingsstrategie te valideren en de effectieve implementatie ervan te bewaken.

De doeltreffendheid van de SteerCo staat of valt met de deelname van relevante leden van de C-suite, zoals de Chief Risk Officer (CRO), Chief Operating Officer (COO), Chief Compliance Officer (CCO), Chief Information Officer (CIO), Chief Financial Officer (CFO), Legal Counsel en natuurlijk de CISO. Een minder frequente maar besluitvaardige SteerCo heeft de voorkeur boven frequente SteerCo-vergaderingen met beperkte beslissingsbevoegdheid.

De rapportage van cyberrisico's aan de raad van bestuur zou de taak moeten zijn van de CISO, idealiter in overeenstemming, of op zijn minst in volledige transparantie, met de SteerCo. De CISO zou een onafhankelijke rapportagelijn moeten hebben naar de raad van bestuur of een van zijn subcommissies, zoals het auditcomité. De frequentie van de rapportage van cyberrisico's aan de raad moet in verhouding staan tot de materialiteit van het risico voor de organisatie, maar een kwartaalrapportage zou een goede praktijk zijn, indien gecombineerd met een escalatieproces in geval van nood.

Dit model combineert effectieve beslissingsbevoegdheid met robuust en effectief bestuur.

Product, portfolio, supply chain cyberrisico

De principes die zijn beschreven in onze white papers voor het rapporteren van cyberrisico's aan raden van bestuur kunnen eenvoudig worden omgezet en uitgebreid naar *product cyberrisico* (hoe goed zijn uw producten beschermd?),

[6] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022R2554 (artikel 6)

portfolio *cyberrisico* (wat zijn de belangrijkste controles die u wilt opleggen aan uw portfoliobedrijven en hoe wilt u de naleving van deze belangrijkste controles meten?) en *supply chain cyberrisico* (belangrijkste bedrijfsmiddelen, afhankelijkheid, belangrijkste controles en hoe de naleving te meten en te rapporteren). De KCI's kunnen op deze gebieden verschillen, waarbij nog steeds vergelijkbare principes worden gebruikt.

Vergelijken met peers

We hebben een aanzienlijke mate van overeenstemming gevonden over de principes die in dit witboek worden beschreven binnen een sectoroverschrijdende groep van veertig organisaties die gedurende een periode van twee jaar elk kwartaal bijeenkwamen in een CISO-werkgroep.

We hopen dat het delen van deze praktijken binnen de bredere gemeenschap de weg vrijmaakt om praktijken (en resultaten) te vergelijken met collega's en zelfs om deze principes te gebruiken in de interactie met toezichthouders.