Risicorapport Cyberveiligheid 2021

Risico's en kansen in balans brengen met betere beslissingen

Cyberrisico's zijn diep geworteld. Neemt uw organisatie de juiste beslissingen over uw cyberbeveiligingsbudget?

Aon's Risicorapport Cyberveiligheid 2021 beantwoordt deze vraag.

Inhoudsopgave

Voorwoord

Leiders wereldwijd staan nu meer dan ooit onder toenemende druk. Inkomsten zijn gedaald, er is gesneden in budgetten en de voortdurende druk om te transformeren leidt ertoe dat organisaties een inhaalslag moeten maken in het spel van cyberveiligheid. Dit alles betekent dat er moeilijkere beslissingen genomen moeten worden in steeds complexere omgevingen.

In 2020 overtrof de snelheid van digitale veranderingen in alle bedrijfstakken die van de cyberbeveiliging. Organisaties verschoven hun focus om te kunnen blijven bestaan en mee te komen met de versnelde digitalisering. De meeste cyberdreigingen waarmee organisaties vandaag de dag worden geconfronteerd, zijn niet nieuw. Verbonden apparaten, ransomware en dreigingen van binnenuit (insider threat) zijn altijd aanwezig. Nieuw is de door COVID-19 veroorzaakte en versnelde verandering in de aard van het zakendoen, waarmee het cyberrisico exponentieel is toegenomen. Dit werd duidelijk door een sterke stijging in het aantal en de ernst van ransomware-incidenten in combinatie met kwetsbaarheden in de keten en bij servicepartners.

Succesvolle cyberaanvallen die eind 2020 en begin 2021 in de publiciteit kwamen - waaronder Mimecast, SolarWinds, Accellion en Microsoft Exchange - brachten kwetsbaarheden aan het licht die verband houden met het samenwerken met derden. Ransomware werd hét cyberrisico voor verzekeraars en verzekerden aangezien de activiteit enorm groeide; vanaf het eerste kwartaal van 2018 tot het vierde kwartaal van 2020 steeg dit risico met 400%. Verzekeraars die hun cyberverzekeringsportefeuilles voornamelijk verliesgevend zagen worden door ransomware, erkenden de noodzaak om de premie van de cyberverzekeringen te verhogen en de eisen voor het afsluiten van de verzekering te verzwaren.

De uitdagingen zijn ingrijpend. Organisaties wereldwijd bevinden zich niet in een staat van digitale transformatie. Deze term impliceert namelijk een begin, midden en einde. Wat organisaties wél doormaken, is een digitale evolutie waarin dagelijks nieuwe risico's opduiken.

Het is een evenwichtsoefening tussen risico's en kansen waardoor klanten zich constant afvragen: 'Hoe kunnen we weloverwogen beslissingen nemen over ons cyberbeveiligingsbudget zodat we veranderende bedrijfsmodellen kunnen ondersteunen en tegelijkertijd onze mensen, klanten, partners en balans beschermen?

In deze context schreven we Aon's Risicorapport Cyberveiligheid 2021: Risico's en kansen in balans brengen met betere beslissingen, onze jaarlijkse analyse van de stand van zaken rondom cyberrisico's. Het rapport concentreert zich op vier belangrijke risico's die op dit moment kritiek zijn, namelijk: nieuwe dreigingen verkennen, ken uw partners, focus op maatregelen en perfectioneer de basis. Het rapport sluit af met een discussie over opkomende risico's. Met behulp van onze toonaangevende gegevens, analyses en deskundige inzichten willen we met dit rapport organisaties helpen hun volwassenheid rondom cyberrisico's te evalueren en betere beslissingen over ondernemingsrisico's te nemen.

Nieuw dit jaar is het inzicht vanuit Aon's Cyber Quotient Evaluation (CyQu), een cyberrisicobeoordeling die de volwassenheid van cyberrisico's evalueert in negen kritieke domeinen. CyQu helpt organisaties cyberdreigingen te begrijpen door zowel een commerciële bril als door de bril van informatiebeveiliging. De gegevens voor 2020 vertellen ons dat organisaties in verschillende regio's, sectoren en omzetgroottes gemiddeld onder de basislijn presteren en alleen een basisniveau scoren wat betreft cybervolwassenheid en voorbereiding.

Zo geven slechts twee op de vijf organisaties aan voorbereid te zijn om nieuwe dreigingen aan te kunnen, die het gevolg zijn van de snelle digitale evolutie. Nog verontrustender is dat slechts 17% van de organisaties meldt dat ze over adequate

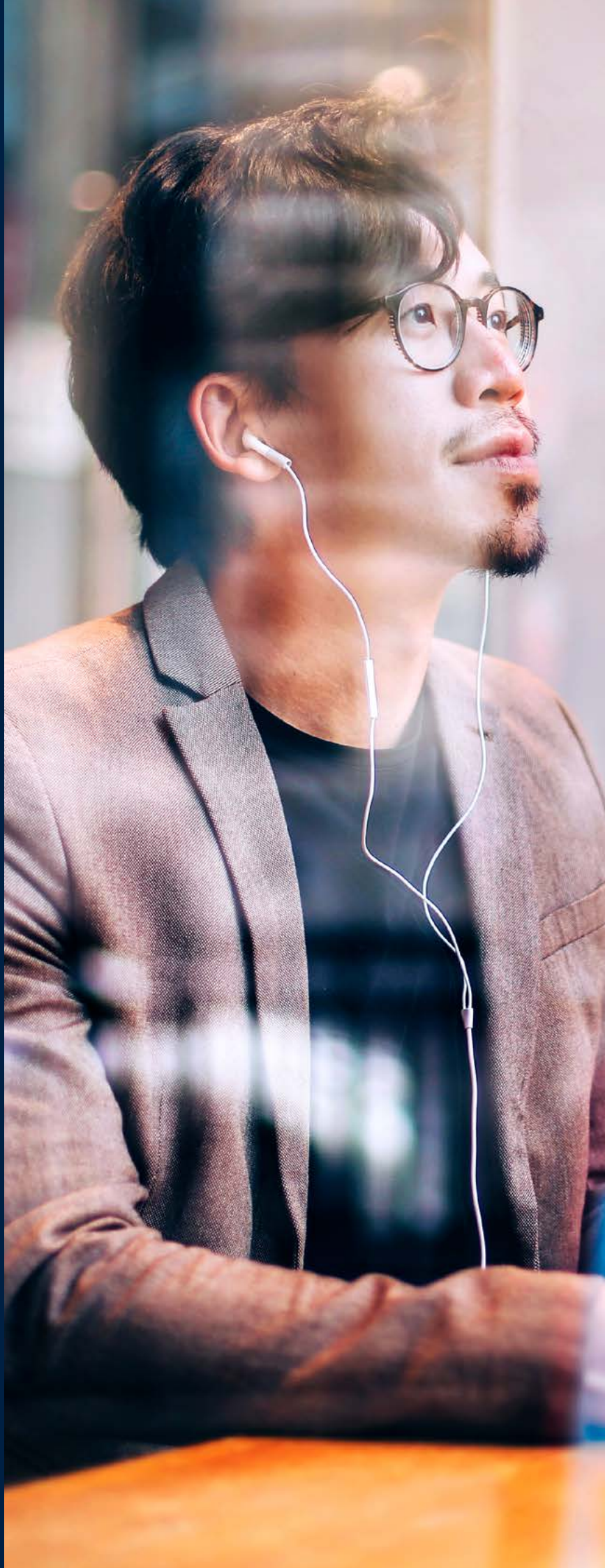
beveiligingsmaatregelen voor hun applicaties beschikken. Als we kijken naar de risico's van derden, meldt slechts 21% van de organisaties dat ze basismaatregelen hebben genomen om zicht te houden op belangrijke leveranciers en verkopers. Over het algemeen vertellen de CyQu-gegevens ons dat cyberrisicomanagementprocedures en -maatregelen niet geformaliseerd zijn en dat het risico reactief en ad hoc beheerd wordt.

Organisaties hebben in 2021 (en daarna) nog veel werk voor de boeg om de controle door regelgevende instanties, verzekeraars, partners en klanten te doorstaan. Dit rapport begeleidt organisaties naar het nieuwe beter - het beheren van cyberrisico's als een ondernemingsrisico.

Methodiek

Trendgegevens over de volwassenheid van cyberbeveiligingsmaatregelen komen uit Aon's Cyber Quotient Evaluation (CyQu). Dit is een online self-assessment platform voor cyberrisico's. 996 organisaties hebben hun gegevens gedeeld. Deze organisaties vertegenwoordigen 20 sectoren en zijn verspreid over Noord-Amerika, Europa, het Midden-Oosten en Afrika, en Azië-Pacific. Er werden meer dan 111.552 datapunten geregistreerd. Het inzicht in de trends is vastgesteld door middel van de negen beveiligingsdomeinen en de 35 kritieke controlegebieden die de CyQu-methodologie vormen.

Cyberrisico thema's



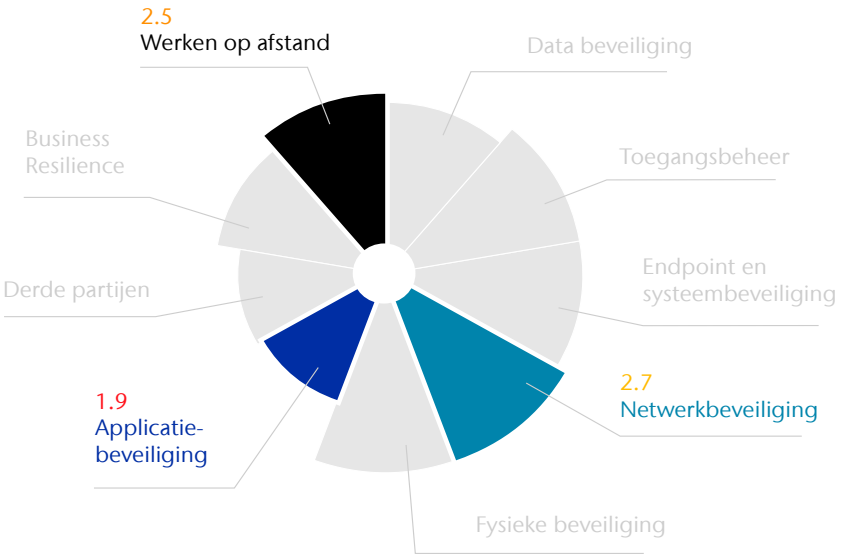
Nieuwe dreigingen verkennen: snelle digitale evolutie

Aan de kant, CTO, CIO en CFO! COVID-19 trad in 2020 toe tot de C-suite en leidde tot grote veranderingen; bedrijven werden gedwongen om snel externe werkplekken te organiseren en digitaal klantcontact mogelijk te maken.

Elk punt voor een gelijkmatige en strategische digitale agenda werd aan de kant geschoven om te kunnen overleven. Misschien is uw organisatie snel overgestapt naar de cloud. Onder tijd- en kostendruk verplaats je met 'lift and shift' je bestaande architectuur snel naar een nieuwe cloudomgeving. Maar misschien denkt u nu dat deze strategie - hoe noodzakelijk op dat moment ook - aanzienlijke beveiligingsnadelen met zich meebracht en misschien zelfs de vele voordelen van de cloud tenietdeed. Of misschien heeft uw organisatie de pandemie wel doorstaan, maar roept het bestuur nu op tot meer innovatie; dringt het bijvoorbeeld aan tot de inzet van kunstmatige intelligentie (AI) om slimmere beslissingen te nemen. Verandering lijkt constant te zijn geworden en dat is ook zo. Organisaties bevinden zich in een proces van digitale evolutie. Het voortdurende streven naar innovatie - denk aan Internet of Things (IoT), Internet of Bodies (IoB) en Smart City initiatieven - zal in 2021 nog meer cyberrisico's opleveren. Organisaties die in deze omgeving opereren, worden opgeroepen om de verwachte voordelen van een digitale agenda af te wegen tegen het cyberrisico dat ze introduceren met de implementatie van nieuwe technologieën of bedrijfsmodellen. Als onderdeel van een organisatiebrede aanpak is het essentieel om de cyberrisico's en dreigingen te identificeren, risico's zo nodig te mitigeren door middel van de beste cyberbeveiligingsaanpak, voorbereid te zijn op incidenten, te overwegen welk deel van het risico overgedragen wordt via een verzekering en vervolgens de huidige en beschikbare polissen te bekijken om ervoor te zorgen dat nieuwe risico's zijn gedekt.

> Organisaties worden uitgedaagd om de nieuwe dreigingen te verkennen die voortkomen uit een snelle, digitale evolutie.

Belangrijkste risico's die voortkomen uit snelle digitale evolutie



CyQu score

Initieel
1 - 1.9

Basis
2 - 2.5

Beheerd
2.6 - 3.4

Geavanceerd
3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is een cyberrisicobeoordeling die de risicovolwassenheid beoordeelt op negen kritieke domeinen. Deze domeinen zijn onderverdeeld in 35 kritieke controlegebieden.

Werken op afstand

CyQu wereldwijd gemiddelde | 2.5 (Basis)

Hiermee kunnen gebruikers op een veilige manier op afstand toegang krijgen tot bedrijfssystemen en gegevens. Dit zodat ze hun taken en verantwoordelijkheden na kunnen komen buiten de werkomgevingen van het bedrijf.

Werken op afstand is blijvend, maar slechts 40% van de organisaties geeft aan over adequate thuiswerkstrategieën te beschikken om deze nieuwe situatie te beheren.

Deze maatregelen houden in:

- Connectiviteit op afstand
- Authenticatie en identiteit
- Kwetsbaarheid van apparaten & monitoring Bedrijfscontinuïteit op afstand
- Veiligheidsbewustzijn op afstand

Applicatiebeveiliging

CyQu wereldwijd gemiddelde | 1.9 (Initieel)

Beschermt applicaties tegen bedreigingen door maatregelen of controles te vereisen.

Dit tijdens elke fase van de levenscyclus van de applicatie-ontwikkeling.

Zie pagina 34 voor beschrijving van de score.

Slechts 17% van de organisaties geeft aan dat ze adequate beveiligingsmaatregelen voor hun applicaties hebben genomen die passen bij het snelle tempo van de digitale evolutie.

Deze maatregelingen houden in:

- Trainen van ontwikkelaars
- Beveiligde ontwikkeling
- Software management

Dicht de gaten

Organisaties die de applicatiebeveiligingsrisico's niet adequaat beheren, zouden moeten overwegen om alle ontwikkelaars training te geven op het gebied van applicatiebeveiliging, en penetratietesten uit te voeren op kritieke digitale services.

Netwerkbeveiliging

CyQu wereldwijd gemiddelde | 2.7 (Beheerd)

Levert infrastructuurdiensten, waaronder netwerkbeveiliging, fysieke aanwezigheid, cloud, opslagbeheer en operaties.

Zie pagina 35 voor beschrijving van de score.

Wat positief is te noemen is dat 60% van de organisaties aangeeft voldoende netwerkbeveiligingsmaatregelen te hebben getroffen om nieuwe digitale technologie te beheren.

Netwerkbeveiliging omvat:

- Netwerkomgeving
- Draadloze verbindingen
- Netwerkpenetratietests
- Netwerkcapaciteit

Ken je partners : Het risico van derden

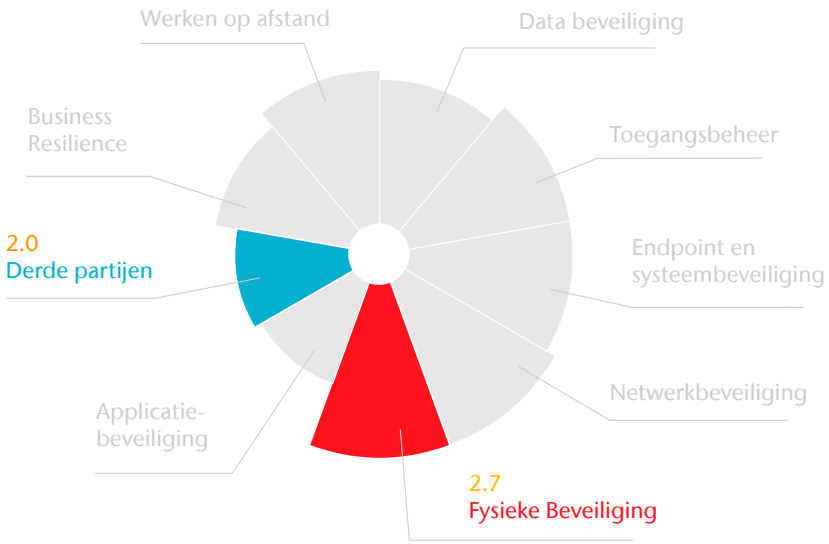
Het is nu de tijd om dubbel in te zetten op uw beveiliging. U kunt verwachten dat er dit jaar zwaardere lijnen worden getrokken. Organisaties zullen cyberrisico's die voortvloeien uit hun toeleveringsketens opnieuw en met grotere bezorgdheid evalueren.

> Organisaties zijn niet klaar voor het adresseren en beheersen van risico's van derde partijen.

Als aan bepaalde normen niet kan worden voldaan, worden er geen contracten getekend. De redenering is simpel. Er is slechts één slecht verdedigde achterdeur nodig om het voortbestaan van een bedrijf in gevaar te brengen - recentelijk nogmaals duidelijk gemaakt door het legacy file-sharing programma van Accellion en SolarWinds' Orion netwerkbeheersoftware die de gehele keten in gevaar brachten. Profit, non-profit, educatieve instellingen, de overheid: alle organisaties zijn met elkaar verbonden. COVID-19 dwong organisaties tot meer afhankelijkheid van derden omdat ze zich haastten om aan de digitale eisen te voldoen. De opmars van CPU's en hybride computerchips met softwarecomponenten brengt ook nieuwe risico's met zich mee. Als één versie van een chip gecompromitteerd is, heeft een hacker opeens potentieel toegang tot duizenden organisaties. Zelfs wanneer dit allemaal al bekend is, hebben organisaties moeite om de kwetsbaarheid en veiligheid van hun toeleveringsketens daadwerkelijk te beoordelen. De statistische benadering, waarbij organisaties vertrouwen op niet-geverifieerde en niet-geteste antwoorden uit een risicobeoordeling van 500 vragen, is misschien niet langer voldoende.

Dus, wat kan uw organisatie doen? Een review van de broncode van derden kan een optie zijn, maar stuit waarschijnlijk op bezwaren en gaat voor velen te ver. Misschien worden assessments en certificeringen door betrouwbare, neutrale derde partijen de best practice. Een uitgebreide beoordeling van de maatregelen, gecombineerd met risicokwantificering en verzekeringsplanning, is een begin. Maar het beheren van risico's van derden vereist een model wat continue zekerheid biedt, met continue scans en opsporing van dreigingen, bijvoorbeeld via 'red teaming'. Organisaties moeten ook voorbereid zijn om te reageren en moeten de juiste partner voor incident respons te kiezen. De kwaliteit varieert namelijk, en verzekeraars tonen minder flexibiliteit voor de inzet van niet-gecontracteerde of vooraf geaccepteerde partners.

Belangrijkste risico's die voortkomen uit de toeleveringsketens



CyQu score

Initieel
1 - 1.9

Basis
2 - 2.5

Beheerd
2.6 - 3.4

Geavanceerd
3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is een cyberrisicobeoordeling die de risicovolwassenheid beoordeelt op negen kritieke domeinen. Deze domeinen zijn onderverdeeld in 35 kritieke controlegebieden.

Derde partijen

CyQu wereldwijd gemiddelde | 2.0 (Basis)

Bewaakt relaties met derden om ervoor te zorgen dat de geleverde services voldoen aan het gedefinieerde beveiligingsbeleid.

Zie pagina 35 voor beschrijving van de score.

Een alarmerend lage 21% - oftewel één op de vijf organisaties - meldt te beschikken over adequate maatregelen om zicht te hebben op kritieke leveranciers en partners.

- Deze maatregelingen houden in:
- Contracten met derde partijen
- Due diligence
- Overzicht met derde partijen

Dicht de gaten

Organisaties die de risico's van derden niet goed onder controle hebben, moeten een reeks van maatregelen uitvoeren op het gebied van due diligence, onboarding en contractrisicobeheer. Voer bijvoorbeeld beoordelingen over de genomen cyberbeveiligingsmaatregelen uit bij derden tijdens de controlefase en onboarding-processen. En eis van derden dat ze akkoord gaan met het Service Level Agreement (SLA) om periodiek beoordelingen, penetratietests, bedrijfscontinuïteitsbeheer en responseoefeningen uit te voeren.

Fysieke beveiliging

CyQu wereldwijd gemiddelde | 2.7 (Beheerd)

Zie pagina 35 voor beschrijving van de score.

Positief te noemen is dat 60% van de organisaties aangeeft over adequate fysieke beveiligingsstrategieën te beschikken.

Deze maatregelingen houden in:

- Fysieke toegang
- Fysieke penetratietesten
- Sabotage en Wijzigen
- Omgeving

Focus op maatregelen: ransomware

COVID-19 gooide brandstof op een reeds brandend vuur, want het aantal en verschillende soorten ransomware-aanvallen is in 2020 explosief toegenomen.
Cyberverzekeraars rapporteerden een stijging van 336% in claims van begin 2019 tot 2020.

De bedrijfskosten in relatie tot ransomware zullen naar verwachting oplopen tot 20 miljard dollar in 2021. Ransomware is niet langer beperkt tot het eenvoudige model van 'betalen om te ontsleutelen'. Gegevens kunnen worden gebruikt voor afpersing, worden misbruikt of zelfs gewist. Bedrijfsonderbreking als gevolg daarvan is zeer waarschijnlijk. Eind 2020 werd bij zeven van de tien ransomware-aanvallen gedreigd ontvreemde gegevens te lekken en in sommige gevallen de gestolen gegevens te veilen. Ook werden er meer gegevens vernietigd, waarbij servers of clusters van gegevens permanent gewist werden. Bovenop dit risico van ransomware zullen we ook in 2021 criminelen zien die door buitenlandse staten worden gefinancierd bij het hacken van privé-ondernemingen vanuit staatsbelang. De meest ernstige dreiging blijft komen vanuit Advanced Persistent Threats (APT's), wat weer een nieuwe uitdaging en een aanzienlijke nalevingslast met zich meebrengt: bijvoorbeeld het extra risico dat komt kijken bij betaling als op deze 'bad actor' een overheidssanctie voor betalingen en onderhandelen geldt. Deze complexiteit treft ook verzekeraars. Velen noemen ransomware een belangrijke factor die de verliesratio's van hun cyberverzekeringen beïnvloedt. 62% van de verzekeraars noemt toegangscontrole als een cruciaal onderwerp. Het is van cruciaal belang om concrete risicobeperkende maatregelen te laten zien, anders kunnen bedrijven onderworpen worden aan torenhoge cyberpremies. Onderneem stappen om de kwetsbaarheid van uw organisatie te verkleinen en de impact van gegevensdiefstal te minimaliseren. Behoud alleen gekwalificeerde cyberbeveiligingsprofessionals om kwetsbaarheden te identificeren, plannen voor bedrijfscontinuïteit op te stellen en te helpen bij het reageren op incidenten.

> De meeste organisaties focussen zich niet op de juiste maatregelen om ransomware-aanvallen te voorkomen en erop te reageren.

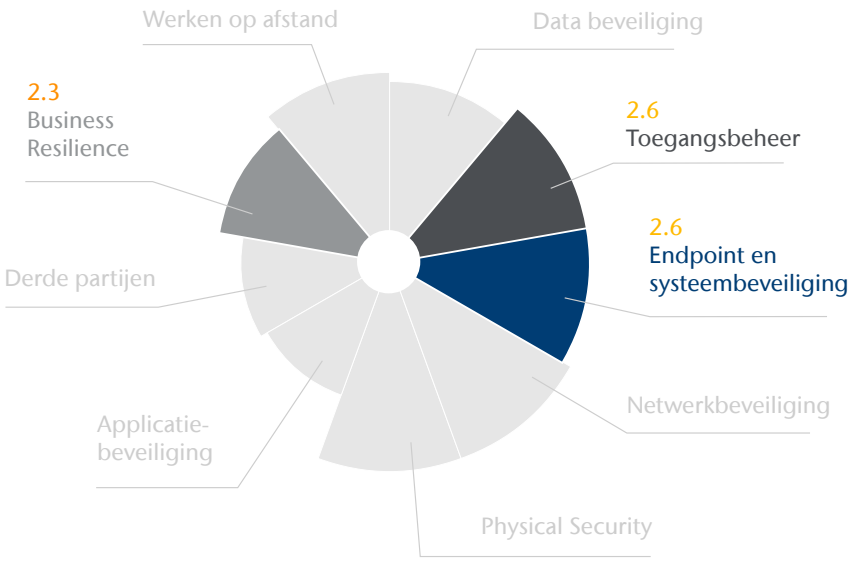
> Velen blijven gevaarlijk dicht hangen bij het begin of zelfs het allereerste stadium van risicovolwassenheid.

23 juli 2020,
Multinationaal technologiebedrijf, wereldwijde storing.
Losgeld betaald: 10 miljoen dollar.

27 juli 2020,
Business Travel Management bedrijf, 30.000 computers onbruikbaar gemaakt en vertrouwelijke zakelijke bestanden gestolen.
Losgeld betaald: 4,5 miljoen dollar.

31 december 2020,
Multinationale vermogensbeheerder, Ongeautoriseerde toegang, vervolgens 5 GB aan data versleuteld en gekopieerd.
Losgeld betaald: 2,3 miljoen dollar.

Belangrijkste risico's die voortkomen uit ransomware



CyQu score

Initieel
1 - 1.9

Basis
2 - 2.5

Beheerd
2.6 - 3.4

Geavanceerd
3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is een cyberrisicobeoordeling die de risicovolwassenheid beoordeelt op negen kritieke domeinen. Deze domeinen zijn onderverdeeld in 35 kritieke controlegebieden.

Toegangsbeheer

CyQu wereldwijd gemiddelde | 2.6 (Beheerd)

Verleent geautoriseerde gebruikers het recht om een service te gebruiken en blokkeert de toegang voor niet-geautoriseerde gebruikers.
Zie pagina 35 voor beschrijving van de score.

44% van de organisaties geeft aan adequate toegangsbeheersmaatregelen te hebben, terwijl verzekeraars deze maatregel als cruciaal beschouwen.

Deze maatregelingen houden in:

- Tweefactorauthenticatie
- Wachtwoord configuratie
- Toegangbeheer

Endpoint en systeembeveiliging

CyQu wereldwijd gemiddelde | 2.6 (Beheerd)

Levering en beheer van infrastructuurdiensten, systeembewaking, endpoint security, configuratiebeheer, opslagbeheer en infrastructuuractiviteiten. Zie pagina 35 voor beschrijving van de score.

49% van de organisaties geeft aan over voldoende endpoint- en systeembeveiliging te beschikken.

Bedrijfsweerbaarheid

CyQu wereldwijd gemiddelde | 2.3 (Basis)

Verleent geautoriseerde gebruikers het recht om een service te gebruiken en blokkeert de toegang voor niet-geautoriseerde gebruikers.
Zie pagina 35 voor beschrijving van de score.

Ransomware veroorzaakt een bedrijfsonderbrekings- en balansrisico, maar slechts 31% van de organisaties geeft aan over de adequate maatregelen voor bedrijfsweerbaarheid te beschikken.

Deze maatregelingen houden in:

- Bedrijfscontinuïteit, herstellen van een calamiteit / ramp / noodgeval
- Incident Response
- Back-up

Organisaties die niet goed omgaan met cyberrisico's, moeten een strategie overwegen voor bedrijfscontinuïteit waarin analyse, planning, testen en beheer worden meegenomen. Het is van cruciaal belang dat er een bedrijfscontinuïteitsplan opgesteld wordt, dat expliciet ingaat op cyberrisicoscenario's die zowel aandacht besteden aan de interne technologie als de services van derden.

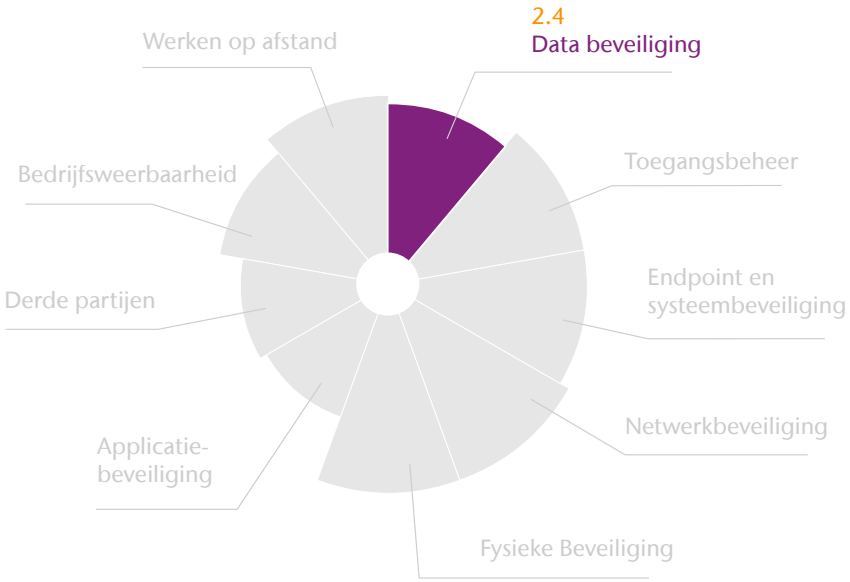
Perfectioneer de basis: regelgeving

Organisaties worstelden in 2020 met de vraag of, wanneer en hoe ze moesten investeren om compliant te zijn. Acties varieerden enorm tussen sectoren en inkomenssegmenten.

De snelle veranderingen die door COVID-19 geforceerd werden, hebben de reeds bestaande verschillen in compliance vergroot en nieuwe gecreëerd. Een fictief, maar realistisch voorbeeld zou een gezondheidszorgorganisatie kunnen zijn, die snel geneeskunde op afstand heeft gelanceerd om levens te redden en daarmee enkele elementen van de algemene verordening gegevensbescherming (AVG) heeft weggewuifd. Of misschien een detailhandelaar die mogelijk een dozijn contracten met derden heeft ondertekend om snel de online zichtbaarheid op te schalen, en daarmee heeft afgezien van due diligence op het gebied van cyberveiligheid. Dit is hét moment om misstappen uit het verleden op te lossen en de basis te perfectioneren om toekomstig succes te garanderen. Met ingang van 2021 is een grote verandering gaande. Aangespoord door de hack bij SolarWinds heeft de Amerikaanse president Joe Biden voorgesteld om 9 miljard dollar beschikbaar te stellen om het werk van de Cyber Security and Information Security Agency (CISA) van het land te versterken. Sectie 230 van de Amerikaanse Communications Decency Act zal waarschijnlijk worden herzien aangezien individuen aan beide kanten van het politieke spectrum duidelijk willen maken dat technologiebedrijven verantwoordelijk zijn. Bovendien moet het voldoen aan de algemene verordening gegevensbescherming (AVG) en een centrale plaats innemen in elk cyberbeveiligingsplan. Privacywet en -regelgeving, zoals de AVG, zullen blijven verschijnen. In mei 2020 zagen we de Thaise Personal Data Protection Act (PDPA) van kracht worden. Zo werd ook de Amerikaanse California Privacy Rights Act (CPRA) eind 2020 tot wet gemaakt, waarmee de oorspronkelijke California Consumer Privacy Act (CCPA) uitgebreid en gewijzigd werd om de meest restrictieve gegevensbeschermingswet in de VS te worden. Naarmate de digitale evolutie en de geneeskunde steeds meer samenkomen, zullen er meer wettelijke eisen aan de gezondheidszorg worden gesteld. De nieuwe EU Medical Device Regulation (MDR) is verplicht en eist van fabrikanten om rekening te houden met de beginselen van risicobeheer, informatiebeveiliging en bescherming tegen ongeautoriseerde toegang. Het is op zijn minst gecompliceerd te noemen en organisaties die de risico's van regelgeving verkennen, moeten zich daarvan bewust zijn. Naleving is niet hetzelfde als beveiliging; de standaarden bepalen alleen de basis. De beste beveiligingsmaatregelen vereisen op maat gemaakte oplossingen op basis van specifieke zakelijke behoeften en activiteiten en kunnen verder gaan dan geldende normen.

> Als het gaat om de omgang met huidige en aanstaande uitdagingen op het gebied van wet- en regelgeving, moeten organisaties de basis nog perfectioneren.

Belangrijke risico's die voortkomen uit verschillen in compliance



CyQu score

Initieel
1 - 1.9

Basis
2 - 2.5

Beheerd
2.6 - 3.4

Geavanceerd
3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu) is een cyberrisicobeoordeling die de risicovolwassenheid beoordeelt op negen kritieke domeinen. Deze domeinen zijn onderverdeeld in 35 kritieke controlegebieden.

Data beveiliging

CyQu wereldwijd gemiddelde | 2.4 (Basis)

Beheert veiligheidsmaatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te beschermen.

Zie pagina 35 voor beschrijving van de score.

Minder dan twee op de vijf organisaties (36%) geeft aan dat ze voldoende voorbereid zijn op gegevensbescherming.

Deze maatregelingen houden in:

- Dataclassificatie
- Awareness en training
- Databeveiliging
- Bestuur
- Risico beheersing

Het gat dichten

Er zijn ook organisaties die niet beschikken over adequate risicomanagementbenaderingen voor dataprivacy en regelgeving. Deze organisaties moeten overwegen om de risico's rondom regelgeving voor dataprivacy en cyberveiligheid te integreren in het framework voor ondernemingsrisicobeheer. Ook is het nuttig om een kampioen op directieniveau te benoemen, bijvoorbeeld een CIO, CISO of GC, die cyberveiligheidskwesties kan sponsoren en promoten bij het bestuur.

Hoe presteert uw sector?

Inzicht in de sector **Bouw**

Bouworganisaties leveren projecten volgens een strakke planning en zijn daarom een belangrijk doelwit voor ransomware-aanvallen die het werk kunnen ontwrichten. Ook is er het risico van diefstal van intellectueel eigendom, bijvoorbeeld van gevoelige blauwdrukken, net als een mogelijke inbreuk op AI-aangedreven autonome voertuigen. Hoewel de bouwsector in het verleden de schijnwerpers van cyberrisico's heeft weten te kunnen vermijden, nemen de kwetsbaarheden toe.

Hoe presteert de bouwsector

2.2 (Basis)

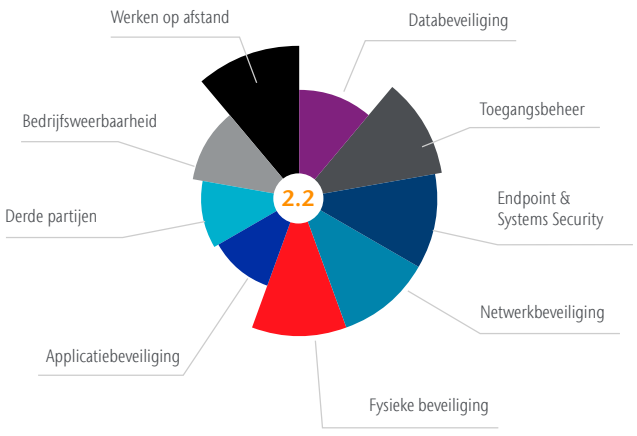
De gemiddelde CyQu-beoordeling voor bouworganisaties wereldwijd is 2.2 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische Risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd.

Risicomanagementpraktijken en -technologieën zijn niet organisatiebreed in gebruik.

Onderzoek de meest relevante cyberrisico's voor bouwbedrijven, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	2.4	2.7	↓
Applicatiebeveiliging	1.6	1.9	↓
Op afstand werken	2.6	2.5	↑
Derde partijen			
Fysieke beveiliging	2.4	2.7	↓
Derde partijen	1.7	2.0	↓
Ransomware			
Toegangsbeheer	2.5	2.6	↓
Endpoint en systeembeveiliging	2.4	2.6	↓
Bedrijfsweerbaarheid	1.9	2.3	↓
Wet en regelgeving			
Data beveiliging	1.9	2.4	↓

CyQu Score

Initieel 1 - 1.9

Basis 2 - 2.5

Beheerd 2.6 - 3.4

Gevorderd 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij bouwbedrijven.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Meer dan de helft (57%) van de organisaties voert geen enkele vorm van penetratietesten uit. Dit is geen verrassing, gezien het heersende idee binnen de bouw dat cyberrisico geen kritiek risico is voor deze sector. Naarmate de sector zich digitaal verder ontwikkelt, zullen cyberrisico's ook beter zichtbaar worden en is het belangrijk dat de juiste maatregelen dan aanwezig zijn.

Ken je partners : **Het risico van derden**

Bouwbedrijven staan er slecht voor als het gaat om het managen van het beveiligingsrisico van derden: slechts 6% zegt adequate maatregelen getroffen te hebben.

Door de opkomst van Industrial Internet of Things (IoT) in bouwomgevingen en de digitale transformatie van bouwactiviteiten, zijn de veiligheidsrisico's van derden meer en meer een dreiging gaan vormen in deze sector, die van oudsher al minder digitaal geavanceerd is.

Daarom moeten bouworganisaties ervoor zorgen dat beveiligings-beoordelingen toegepast worden tijdens de selectie van derde partijen. Daarnaast moeten cyberverzekerings-bepalingen en -vereisten opgenomen worden in contracten met derden, om de beveiliging vanuit leveranciers te waarborgen.

Focus op maatregelen: **ransomware**

59% van de organisaties beschikt niet over een geformaliseerd bedrijfscontinuïteitsplan, daarnaast geeft 69% van de respondenten aan geen formeel incidentresponsproces te hebben. Naarmate de sector een meer digitale omgeving gaat gebruiken, zal de kans op serieuze verstoringen waarschijnlijk ook toenemen.

Perfectioneer de basis: **wet- en regelgeving**

Bouwbedrijven zijn erg achtergebleven in het toepassen van goede gegevensbeveiliging en regelgevend beheer. Slechts 14% van de organisaties zegt voldoende maatregelen te hebben getroffen voor het beheer van wet- en regelgeving op het gebied van privacy en cyberveiligheid.

Als bouwprojecten meer gebruik gaan maken van data-analyse, web-connected operationele technologieën (OT) en automatisering, zullen regelgeving met betrekking tot dataprivacy en incidentmeldingen ook een steeds belangrijkere rol aannemen in hun risicoprofiel. Bouworganisaties moeten meer voorop lopen door gebruik te maken van betere bestuurs- en gegevens-beschermings-maatregelen.

Inzicht in de sector **Energie, voorzieningen en natuurlijke hulpbronnen**

De rol van energievoorziening en de financiële invloed ervan in een kritieke infrastructuur, maakt de sector een uitnodigend doelwit voor buitenlandse staten, economische spionage en hacktivisten. Digitale evolutie, afhankelijkheid van derden en de opkomst van slimme IoT-apparaten en slimme netwerken, maken van de energiesector een aantrekkelijk doelwit.

Hoe presteert de energie, voorzieningen en natuurlijke hulpbronnen sector?

2.4 (Basis)

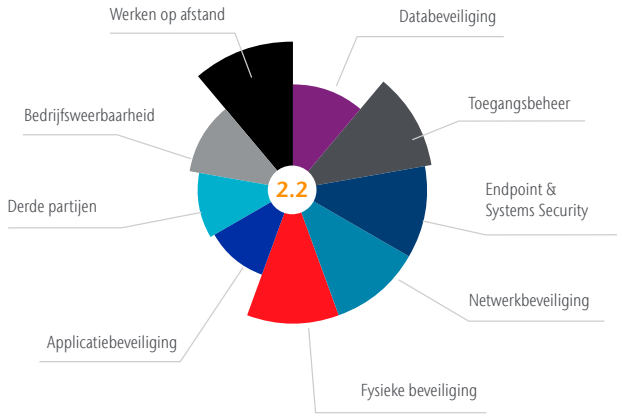
De gemiddelde CyQu-beoordeling voor energie-, voorzieningen en natuurlijke hulpbronnen wereldwijd is 2.4 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische Risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd.

Risicomanagementpraktijken en -technologieën zijn niet organisatiebreed in gebruik.

Onderzoek de meest relevante cyberrisico's voor energie-, voorzieningen en natuurlijke hulpbronnen, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	2.4	2.7	↓
Applicatiebeveiliging	1.6	1.9	↓
Op afstand werken	2.6	2.5	↑
Derde partijen			
Fysieke beveiliging	2.4	2.7	↓
Derde partijen	1.7	2.0	↓
Ransomware			
Toegangsbeheer	2.5	2.6	↓
Endpoint en systeembeveiliging	2.4	2.6	↓
Bedrijfsweerbaarheid	1.9	2.3	↓
Wet en regelgeving			
Data beveiliging	1.9	2.4	↓

CyQu Score

- Initieel 1 - 1.9
- Basis 2 - 2.5
- Beheerd 2.6 - 3.4
- Gevorderd 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij energie-, voorzieningen en natuurlijke hulpbronnen.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Er zijn grote verschillen tussen organisaties binnen deze sector. Hoewel de meerderheid boven de wereldwijde benchmark ligt, voert 24% geen enkele vorm van penetratietests uit. 27% daarentegen, past de beste methodes toe en maakt regelmatig gebruik van penetratietestteams om maatregelen te testen.

Ken je partners : **Het risico van derden**

Deze sector lijkt over goede basiscontracten voor derden te beschikken. Hierbij wordt gebruik gemaakt van minimale verzekeringseisen en vooraf bepaalde service level agreements (SLA) voor de cyberveiligheid. Slechts 2% van de organisaties verplicht ook daadwerkelijk maatregelen voor alle contracten/ derde partijen. Dit laat zien hoe belangrijk het is om gebruik te maken van robuuste assessments en gelaagde maatregelen.

Focus op maatregelen: **ransomware**

Deze sector ziet een verhoogd aantal incidenten rond gegevensdiefstal, spionage en factureringsfraude. Daarom is het ook niet verrassend dat 21% van de organisaties aanzienlijk hoger scoort dan het wereldwijde sectorgemiddelde als het gaat om incidentrespons (IR). 41% geeft echter aan een ad-hocaanpak te hanteren.

Perfectioneer de basis: **wet- en regelgeving**

Voor veel organisaties is het inbedden van cyberrisicomanagement in bredere risicomanagementkaders een uitdaging. 61% geeft dan ook aan niet over de juiste governance-, risicomanagement- of gegevensbeschermingsmaatregelen te beschikken.
Ook samenwerkingen met andere toezichthoudende risicobeheerfuncties, zoals audit, Enterprise Risk Management (ERM) en juridische zaken blijven achter. Dit heeft invloed op het vermogen van een organisatie om te anticiperen op toekomstige privacyregels.

Inzicht in de sector **Financiële instellingen**

Onder constant toezicht van toezichthouders en privacywetten, zijn financiële instellingen experts geworden als het gaat om het omgaan met cyberrisico's. Vanwege de verschuiving naar het op afstand werken moeten veel organisaties echter hard werken om onverwachte kwetsbaarheden te beheersen en mitigeren.

Hoe presteren de financiële instellingen?

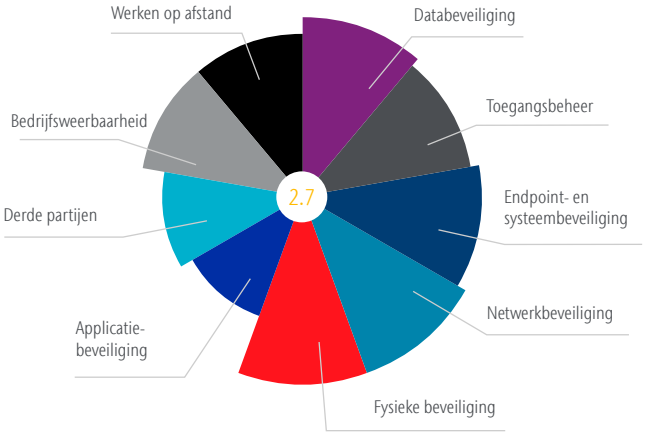
2.7 (Beheerd)

De gemiddelde CyQu-beoordeling voor financiële instellingen wereldwijd is 2.7 / 4 (beheerd).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cyberbeveiligingsmaatregelen op een beheerd niveau ligt. Risicobeheerpraktijken en -technologieën worden in het grootste deel van de organisatie uitgevoerd en vastgesteld. De organisatie past haar cyberbeveiligingspraktijken aan op basis van best practices en voorspellende indicatoren in het grootste deel van de organisatie. Beleid, processen en procedures worden gedefinieerd, geïmplementeerd zoals bedoeld en herzien. Er zijn consistente methoden om effectief te reageren op veranderingen in risico's in gebruik.

Onderzoek de meest relevante cyberrisico's voor financiële instellingen, wijs ze toe aan de belangrijkste beveiligings-maatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	3.0	2.7	↑
Applicatiebeveiliging	2.2	1.9	↑
Op afstand werken	2.7	2.5	↑
Derde partijen			
Fysieke beveiliging	3.0	2.7	↑
Derde partijen	2.4	2.0	↑
Ransomware			
Toegangsbeheer	2.8	2.6	↑
Endpoint en systeembeveiliging	2.9	2.6	↑
Bedrijfsweerbaarheid	2.7	2.3	↑
Wet en regelgeving			
Data beveiliging	2.9	2.4	↑

CyQu Score

- Initieel 1 - 1.9
- Basis 2 - 2.5
- Beheerd 2.6 - 3.4
- Gevorderd 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij energie-, voorzieningen en natuurlijke hulpbronnen.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

De meerderheid (62%) van de financiële instellingen heeft goed ontwikkelde netwerkomgevingen. Dit houdt in dat er, ondanks de grote hoeveelheden legacy applicaties, een sterke architectuur en verdedigingsmechanismen zijn om inbreuken tegen te gaan. Ook de netwerkbeveiliging is goed verzorgd, 60% voert namelijk regelmatig netwerkpenetratietests uit.

Ken je partners : **Het risico van derden**

Ongeveer 2 op de 5 financiële instellingen beschikt niet over een goed due diligenceproces voor derden. Met het oog op de recente spraakmakende gebeurtenissen bij derde partijen, is het juist voor financiële diensten cruciaal om dit op orde te hebben.

Focus op maatregelen: **ransomware**

Bijna de helft van alle organisaties (45%) voert scans uit om kwetsbaarheden te identificeren. Bijna een derde (27%) heeft geen tweefactorauthenticatie ingevoerd voor logins die van buiten het bedrijfsnetwerk (door bijv. thuiswerken) gedaan worden.

Perfectioneer de basis: **wet- en regelgeving**

Gelukkig versleutelt een groot aantal organisaties automatisch data-at-rest en in-transit. 18% heeft echter nog geen goed schema voor dataclassificatie geïmplementeerd. Dit benadrukt maar weer de uitdaging waarmee organisaties, die over veel data beschikken, worden geconfronteerd wanneer zij een sterke datamanagement-benadering willen implementeren.

Inzicht in de sector **Levenswetenschappen**

Onder constant toezicht van toezichthouders en privacywetten, zijn financiële instellingen experts geworden als het gaat om het omgaan met cyberrisico's. Vanwege de verschuiving naar het op afstand werken moeten veel organisaties echter hard werken om onverwachte kwetsbaarheden te beheersen en mitigeren.

Hoe presteren de levenswetenschappen sector?

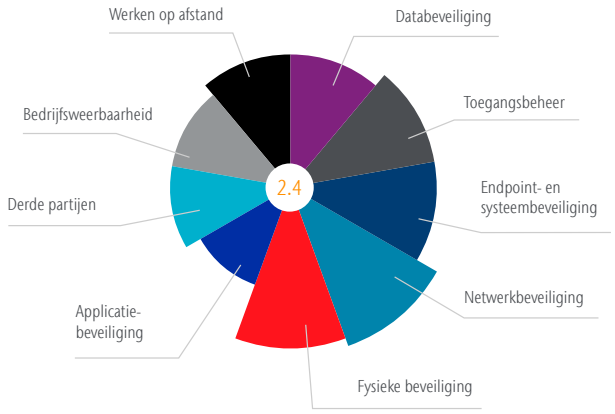
2.4 (Basis)

De gemiddelde CyQu-beoordeling voor organisaties in de levenswetenschappen sector is wereldwijd 2.4 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd. Risicomanagementpraktijken en -technologieën zijn niet in gebruik.

Onderzoek de meest relevante cyberrisico's voor levenswetenschappenorganisaties, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	2.9	2.7	↑
Applicatiebeveiliging	1.9	1.9	→
Op afstand werken	2.4	2.5	↓
Derde partijen			
Fysieke beveiliging	2.8	2.7	↑
Derde partijen	2.2	2.0	↑
Ransomware			
Toegangsbeheer	2.6	2.6	→
Endpoint en systeembeveiliging	2.6	2.6	→
Bedrijfsweerbaarheid	2.2	2.3	↓
Wet en regelgeving			
Data beveiliging	2.4	2.4	→

CyQu Score	
Initieel	1 - 1.9
Basis	2 - 2.5
Beheerd	2.6 - 3.4
Gevorderd	3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij levenswetenschappenorganisaties.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Een aanval op de Operational technology (OT) omgeving is voor de meeste levenswetenschappenorganisaties een worstcase scenario. Toch geeft slechts 36% van de organisaties aan ook echt regelmatig penetratietesten uit te laten voeren, door zowel interne als externe partijen. Nog schrikbarender is dat 17% zelfs geen enkele vorm van penetratietesten uitvoert. Gespecialiseerde penetratietesters zijn nodig om grote kwetsbaarheden te identificeren.

Ken je partners : **Het risico van derden**

Slechts 13% van de organisaties beschikt over adequate due diligence procedures voor derde partijen. Hiermee kunnen de risico's op het gebied van vertrouwelijke gegevens, toeleveringsketen-systemen en kritieke Operational Technology (OT)-infrastructuur gemitigeerd en opgespoord worden. Het ontbreken hiervan zorgt ervoor dat bewakingssystemen voor geneesmiddelen, distributiesystemen en operationele productieprocessen blootgesteld worden aan cyberaanvallen via inbraak bij een derde partij.

Focus op maatregelen: **ransomware**

87% van de organisaties in de sector passen sterke maatregelen toe. Dit laat zien dat wachtwoordbeheer zeer serieus wordt genomen. Slechts 17% implementeert echter sterke multi-factorauthenticatie (MFA) in hun IT-netwerken. Dit betekent dat ecompromitteerde-wachtwoorden nog steeds kunnen leiden tot het in gevaar brengen van gevoelige gegevens of toegang voor hackers.

Perfectioneer de basis: **wet- en regelgeving**

Gezien de sterk gereguleerde omgeving, is dit onderwerp voor de levenswetenschappen bekend terrein. Toch is de sector nog niet genoeg ontwikkeld en is dataclassificatie nog steeds een uitdaging. Dit is zorgwekkend. Gegevens zijn in deze sector namelijk van groot belang, net als de bescherming van waardevol intellectueel eigendom. Maar liefst 37% van de organisaties geeft aan niet over een adequate aanpak te beschikken om cyberveiligheid en privacyregelgeving te beheren.

Inzicht in de sector **Productie**

Productiebedrijven hebben niet dezelfde achtergrond als data-intensieve sectoren, zoals financiële instellingen. Tegenwoordig zien productiebedrijven een versnelling in het tempo van technologische veranderingen zoals bij de digitale wereldwijde toeleveringsketen, verbonden apparaten zoals Human Machine Interfaces (HMI), Industrial Control Systems (ICS) en het Industrial Internet of Things (IOT).

Hoe presteert de productie sector?

2.2 (Basis)

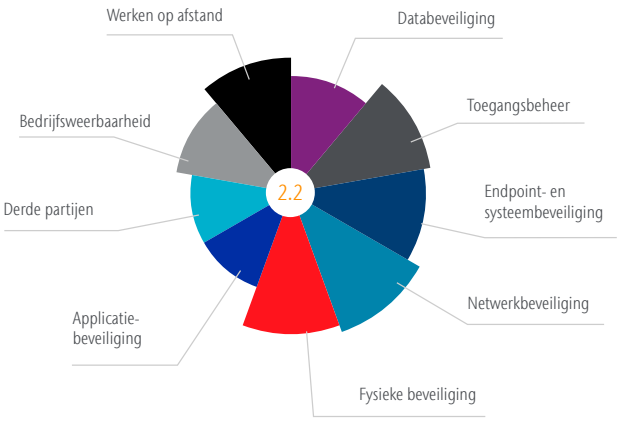
De gemiddelde CyQu-beoordeling voor productiebedrijven wereldwijd is 2.2 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische Risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd.

Risicomanagementpraktijken en -technologieën zijn niet organisatiebreed in gebruik.

Onderzoek de meest relevante cyberrisico's voor productie bedrijven, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde
snelle digitale evolutie		
Netwerkbeveiliging	2.6	2.7 ↓
Applicatiebeveiliging	1.8	1.9 ↓
Op afstand werken	2.4	2.5 ↓
Derde partijen		
Fysieke beveiliging	2.5	2.7 ↓
Derde partijen	1.8	2.0 ↓
Ransomware		
Toegangsbeheer	2.5	2.6 ↓
Endpoint en systeembeveiliging	2.4	2.6 ↓
Bedrijfsweerbaarheid	2.1	2.3 ↓
Wet en regelgeving		
Data beveiliging	2.1	2.4 ↓

CyQu Score

- Initieel: 1 - 1.9
- Basis: 2 - 2.5
- Beheerd: 2.6 - 3.4
- Gevorderd: 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij productie bedrijven.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Het is wellicht niet verrassend dat klanten in de productiesector een sterke focus hebben op maatregelen tegen omgevingsinvloeden. Zo heeft 37% van alle organisaties een N + 1 configuratie (parallelle redundantie) voor belangrijke systemen, brandbestrijding en continue stroomvoorziening (Uninterruptible Power Supply (UPS)).

Ken je partners : **Het risico van derden**

Fabrikanten worden afhankelijker van een groot aantal derde partijen, die hun waardeketen ondersteunen. Toch blijft meer dan de helft (57%) van de organisaties ad-hoc implementaties uitvoeren, zonder dat zij een consistent due diligenceplan hebben geformaliseerd. Het meest zorgwekkende is misschien wel dat 17% helemaal geen due diligence procedure voor derden heeft.

Focus op maatregelen: **ransomware**

Van de fabrikanten implementeert 60% geen tweefactorauthenticatie (2FA) wat een cruciale extra beveiligingslaag is. Zonder authenticatie en encryptie, heeft 46% van de organisaties moeite met logging en het monitoren van endpoints, waardoor de controle op industriële controlesystemen (ICS) en kritische operationele netwerken slecht is.

Het meest verrassende is dat fabrikanten nog steeds achterlopen met de responsmogelijkheden voor incidenten en nog niet klaar zijn om bedrijfscontinuïteit te garanderen.

Perfectioneer de basis: **wet- en regelgeving**

Van de fabrikanten heeft 46% geen beveiligingsoplossing die een consistente en herhaalbare dataclassificatie ondersteunt. Dit is ook van invloed op hun vermogen om aanvullende gegevensbeschermings-maatregelen in te zetten.

Inzicht in de sector **Zakelijke dienstverlening**

In vergelijking met vele andere sectoren heeft de zakelijke dienstverlening de COVID-19-pandemie relatief goed doorstaan. Dit komt deels door de aanhoudende vraag naar de diensten, maar ook door het feit dat werknemers redelijk gemakkelijk kunnen overschakelen naar het thuiswerken. Dit betekent niet dat cyberrisico's hier niet relevant zijn. De industrie is een doelwit voor ransomware-aanvallen en organisaties geven aan dat ze cyberrisico's niet verder beheren dan het basisniveau.

Hoe presteert de zakelijke dienstverlening sector?

2.5 (Basis)

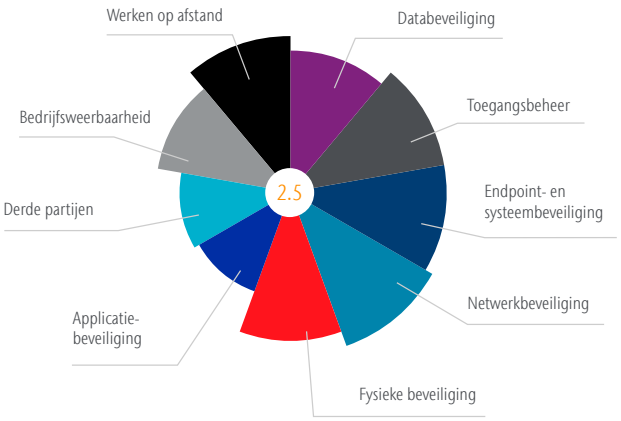
De gemiddelde CyQu-beoordeling voor zakelijke dienstverleners wereldwijd is 2,5 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische Risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd.

Risicomanagementpraktijken en -technologieën zijn niet organisatiebreed in gebruik.

Onderzoek de meest relevante cyberrisico's voor zakelijke dienstverleners, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	2.8	2.7	↑
Applicatiebeveiliging	1.9	1.9	→
Op afstand werken	2.7	2.5	↑
Derde partijen			
Fysieke beveiliging	2.6	2.7	↓
Derde partijen	2.0	2.0	→
Ransomware			
Toegangsbeheer	2.7	2.6	↑
Endpoint en systeembeveiliging	2.7	2.6	↑
Bedrijfsweerbaarheid	2.4	2.3	↑
Wet en regelgeving			
Data beveiliging	2.5	2.4	↑

CyQu Score

- Initieel: 1 - 1.9
- Basis: 2 - 2.5
- Beheerd: 2.6 - 3.4
- Gevorderd: 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij zakelijke dienstverleners

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Het beheren van kwetsbaarheden van apparaten die zich buiten de organisaties bevinden, blijkt een grote uitdaging te zijn voor deze sector. 17% van de organisaties geeft aan hiervoor geen formele aanpak of processen te hanteren. Verontrustend is dat slechts 4% er vertrouwen in heeft dat zij over sterke en consistente maatregelen beschikken.

Ken je partners : **Het risico van derden**

Het managen van derden blijft een grote uitdaging. 50% van de organisaties heeft een risicovolwassenheids-score van 1. Helemaal zorgwekkend is het gebrek aan aandacht voor due diligence van externe leveranciers. 58% van de organisaties geeft aan hiervoor geen formeel proces te hebben. Aangezien professionele dienstverleners vanwege de data die ze bezitten vaak het doelwit zijn, moet dit probleem beter worden aangepakt.

Focus op maatregelen: **ransomware**

Er is een grote kloof tussen organisaties als het gaat om de beveiliging van ransomware. 30% beschikt over een goed monitoringsproces. Zij maken gebruik van geavanceerde tools voor endpointdetectie en -respons (EDR) en gedragsanalyses. 39% van de organisaties daarentegen, doet vrijwel niet aan monitoring. Zonder te beschikken over effectieve logbestanden is het voor deze organisaties vrijwel onmogelijk om te weten of klantgegevens mogelijk aangetast zijn door een aanval.

Perfectioneer de basis: **wet- en regelgeving**

Risicomanagement en gegevensbeheer blijven zwakke punten voor professionele dienstverleners. 36% beschikte niet over echte gegevensbeheers-processen en 45% gaf aan geen geformaliseerde methode te hebben voor het risicobeheer van gegevensbeveiliging. Het is van belang dat bedrijven op de hoogte zijn van de financiële gevolgen van een datalek binnen het bedrijf.

Inzicht in de sector **Retail**

‘Alles online’ was het thema voor 2020 en retailers blijven een vraag zien naar digitale klantervaringen. In een sector die al vol was van cyberrisico’s en onder toezicht staat van toezichthouders, moeten detailhandelaars nu ook de gaten - als gevolg van snelle technologische innovaties - identificeren en dichten, en gevoelige klantgegevens zorgvuldig blijven beschermen.

Hoe presteert de de retailsector

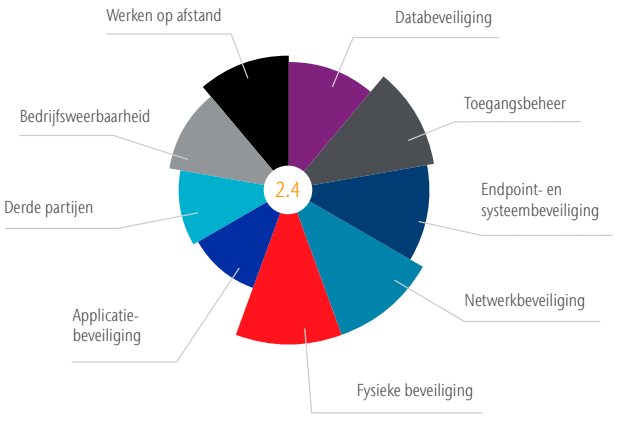
2.4 (Basis)

De gemiddelde CyQu-beoordeling voor retailorganisaties wereldwijd is 2.4 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische Risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico’s worden op een ad-hoc en soms reactieve manier beheerd. Risicomanagementpraktijken en -technologieën zijn niet organisatiebreed in gebruik.

Onderzoek de meest relevante cyberrisico’s voor retail organisaties, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico’s te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	2.7	2.7	→
Applicatiebeveiliging	1.9	1.9	→
Op afstand werken	2.4	2.5	↓
Derde partijen			
Fysieke beveiliging	2.7	2.7	→
Derde partijen	2.0	2.0	→
Ransomware			
Toegangsbeheer	2.6	2.6	→
Endpoint en systeembeveiliging	2.5	2.6	↓
Bedrijfsweerbaarheid	2.2	2.3	↓
Wet en regelgeving			
Data beveiliging	2.3	2.4	↓

CyQu Score

Initieel 1 - 1.9

Basis 2 - 2.5

Beheerd 2.6 - 3.4

Gevorderd 3.5 - 4

*Aon’s Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico’s. CyQu evalueert cyberrisico’s over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij retail organisaties.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Er bestaat een aanzienlijk verschil in de mate van risicovolwassenheid tussen organisaties in deze sector. 36% van de retailers geeft aan extreem kwetsbaar te zijn voor netwerkoverbelasting en Denial of Service-aanvallen (DDoS). Daarentegen zegt 20% van de retailers een vergevorderde risicovolwassenheid te hebben. Dit betekent dat ze over de mogelijkheid beschikken om veilig op te schalen wanneer vanuit de consument de vraag naar digitale kanalen blijft stijgen.

Ken je partners : **Het risico van derden**

Meer dan de helft (58%) van de retail organisaties beschikt over onvoldoende beveiligingsmaat-regelen voor derden. Dit benadrukt het belang om het selectie- en implementatieproces voor samenwerken met derde partijen te verbeteren.

Winkeliers blinken uit in het beveiligen van fysieke toegang tot gebouwen, winkels en kantoren. Het testen van dergelijke beveiligings-maatregelen is daarentegen erg zwak. Fysieke penetratietesten werden door 71% van de organisaties niet op een uniforme manier uitgevoerd. Het is absoluut noodzakelijk dat deze maatregelen regelmatig worden getest om de beveiligingsmaatregels robuust te houden.

Focus op maatregelen: **ransomware**

Gezien de recente toename in ransomware aanvallen, is het nog belangrijker geworden voor organisaties om over weerbaarheidsmaat-regelen te beschikken. Dit is vooral relevant in de detailhandel, waarbij de verkoop- en distributieprocessen steeds meer online plaatsvinden. Helaas heeft slechts 24% van de retailorganisaties voldoende maatregelen genomen om de bedrijfscontinuïteit te beschermen voor de toenemende dreiging van ransomware-aanvallen en te kunnen herstellen in het geval van nood. Detailhandels worden steeds afhankelijker van direct beschikbare e-commerce- en distributiesystemen. Juist daarom is het van belang dat deze organisaties de slechte staat van hun bedrijfsweer-baarheid aanpakken.

Perfectioneer de basis: **wet- en regelgeving**

40% van de organisaties heeft een risicovolwassenheids-score van minder dan 2. Dit laat zien dat er duidelijk verbetering nodig is om ervoor te zorgen dat retailers beter in staat zijn gegevens te beheren en te beveiligen. 30% van de organisaties blinkt echter uit in dit domein (met een risicovolwassenheids-score van hoger dan 3). Dit laat zien dat de sector steeds dichterbij het juiste niveau begint te komen.

Inzicht in de sector **Technologie, media en telecommunicatie**

Technologie-, media- en telecommunicatiebedrijven (TMT) ondersteunen alle andere sectoren en de vraag naar hun producten en diensten is groter dan ooit. Van software voor digitale handtekeningen tot de implementatie van een 5G-infrastructuur en IoT, de industrie is fundamenteel voor de toekomst. Dit vergroot het accent op cyberveiligheid, zeker ook gezien belangrijke recente gebeurtenissen die kwetsbaarheden in wereldwijde besturingssystemen en toeleveringsketens blootleggen.

Hoe presteert de technologie, media en telecommunicatie sector?

2.5 (Basis)

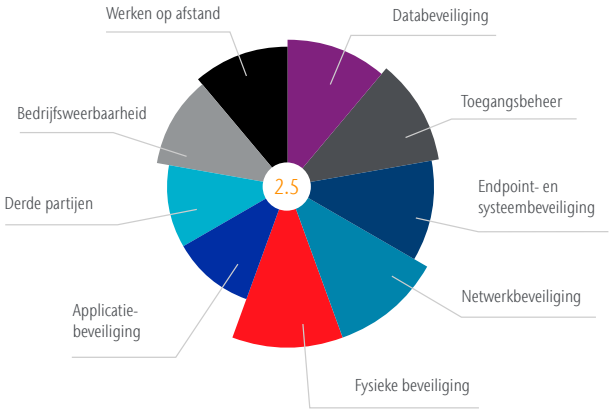
De gemiddelde CyQu-beoordeling voor retailorganisaties wereldwijd is 2.4 / 4 (basis).

Wat betekent dit?

Deze beoordeling geeft aan dat de volwassenheid van cybersecurity zich op een basisniveau bevindt. Organisatorische Risicomanagementpraktijken en -technologie voor cyberveiligheid zijn niet geformaliseerd, en risico's worden op een ad-hoc en soms reactieve manier beheerd.

Risicomanagementpraktijken en -technologieën zijn niet organisatiebreed in gebruik.

Onderzoek de meest relevante cyberrisico's voor technologie-, media- en telecommunicatieorganisaties, wijs ze toe aan de belangrijkste beveiligingsmaatregelen en bepaal welke acties uw organisatie kan nemen om de risico's te mitigeren.



Beveiligingsdomeinen	Sector gemiddelde	Wereldwijd gemiddelde	
snelle digitale evolutie			
Netwerkbeveiliging	2.8	2.7	↑
Applicatiebeveiliging	2.2	1.9	↑
Op afstand werken	2.5	2.5	→
Derde partijen			
Fysieke beveiliging	2.8	2.7	↑
Derde partijen	2.2	2.0	↑
Ransomware			
Toegangsbeheer	2.7	2.6	↑
Endpoint en systeembeveiliging	2.6	2.6	→
Bedrijfsweerbaarheid	2.4	2.3	↑
Wet en regelgeving			
Data beveiliging	2.6	2.4	↑

CyQu Score

- Initieel 1 - 1.9
- Basis 2 - 2.5
- Beheerd 2.6 - 3.4
- Gevorderd 3.5 - 4

*Aon's Cyber Quotient Evaluation (CyQu). is een online self-assessment platform voor cyberrisico's. CyQu evalueert cyberrisico's over negen beveiligingsdomeinen en 35 kritieke controlegebieden.

Dit rapport is gebaseerd op eigen gegevens uit Aon's Cyber Quotient (CyQu), en deskundig inzicht vanuit verschillende sectoren. Het rapport focust op vier belangrijke risicothema's die prominent aanwezig zijn bij retail organisaties.

Nieuwe dreigingen verkennen: **snelle digitale evolutie**

Verrassend is dat 22% van de organisaties geen gebruik maakt van penetratietesten, in wat voor vorm dan ook, om hun bedrijfsomgeving te testen. Gezien de immateriële aard van technologie, media, en telecommunicatie activa, wordt het creëren van een veerkrachtige infrastructuur steeds belangrijker

Ken je partners : **Het risico van derden**

Het risicobeheer van derden bracht een aanzienlijke splitsing in de sector aan het licht, waarbij 28% van de organisaties aangaf dat cyberbeveiliging niet specifiek wordt meegenomen bij het sluiten van contracten met derden. 20% geeft aan dat cyberbeveiliging juist een cruciaal onderdeel is van alle contracten, waarbij expliciete vereisten en minimumnormen in de contractformulering ingebouwd zijn.

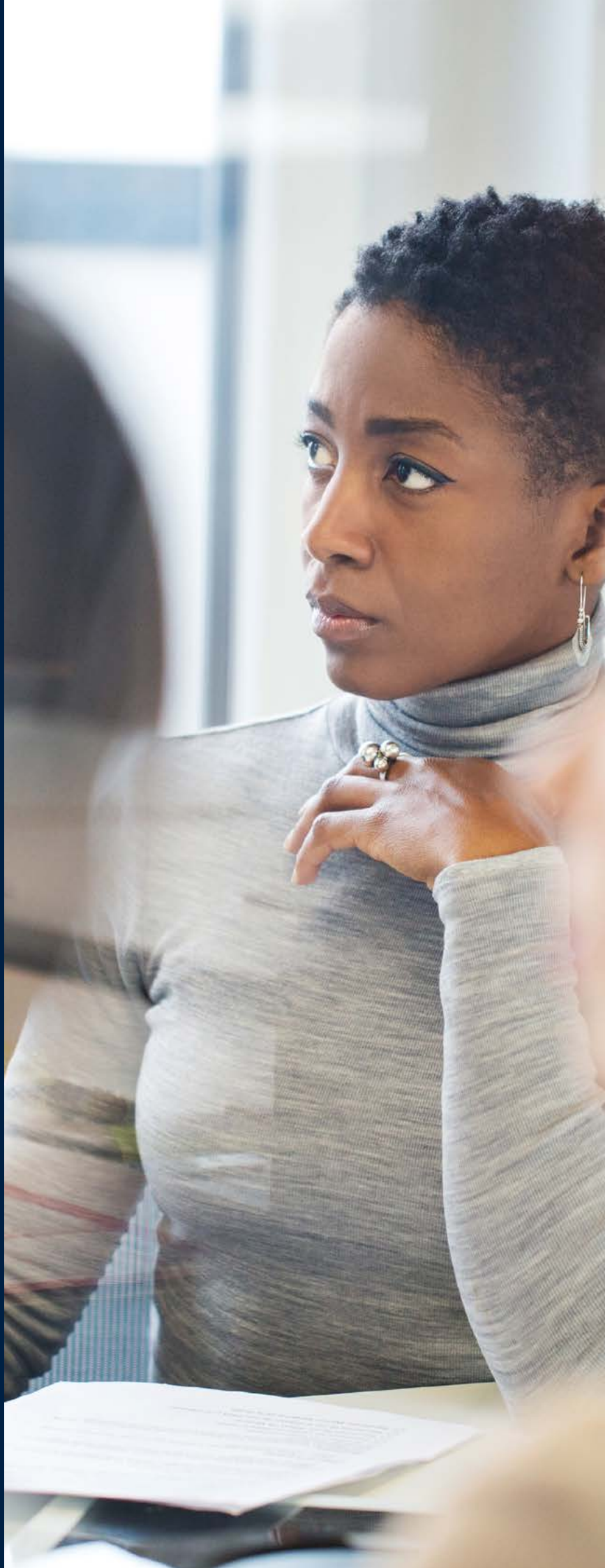
Focus op maatregelen: **ransomware**

Bij endpoint-beveiliging zien we verschillende reacties. 37% van de organisaties beschikt over zeer basale maatregelen, terwijl daar tegenover 31% juist de beste methodes toepast. Ook blijkt dat 34% van de organisaties endpoints niet monitoren op verdachte activiteiten en dit is een uitdaging die aangepakt moet worden.

Perfectioneer de basis: **wet- en regelgeving**

Het trainen van gebruikersbewustzijn is een grote focus geweest in deze sector. 46% van de organisaties geeft aan een robuust proces te gebruiken, inclusief beveiligingstraining, regelmatige phishing tests en herhaling hiervan. 22% van de organisaties had echter moeite om een goede en consistente benadering van dataclassificatie te implementeren. Dit betekent dat gevoelige gegevens mogelijk niet geïdentificeerd zijn en niet het juiste beschermingsniveau krijgen.

Conclusie



De kansen

Voorspellingen over de toekomst van cyberrisico's zijn er in overvloed. In plaats van te focussen op de vraag 'wat is de volgende stap?', heeft dit rapport zich tot nu toe gericht op de vraag 'wat speelt er nu?' Wat moeten organisaties vandaag doen om zich op risico's te concentreren? Gebaseerd op praktisch inzicht en harde gegevens hebben we antwoord gezocht op de vragen: 'wat zijn op dit moment de meest relevante cyberrisico's?' en 'hoe voorbereid zijn organisaties binnen verschillende sectoren en regio's om deze risico's te beheren?'

Dan komen we nu toe aan de kansen. Gewapend met kennis hebben organisaties het vermogen om methodisch de juiste vragen te stellen, om cyberrisico's als bedrijfsrisico aan te pakken, om een grondige beoordeling van cybervolwassenheid uit te voeren en de huidige gaten te dichten.

Organisaties hebben ook de kans om klaar te zijn voor morgen en te kijken naar de toekomst en het veranderende cyberrisicolandschap. Dagelijks duiken nieuwe risico's op en is waakzaamheid essentieel.

De focus op het heden houden: betere beslissingen nemen

De gegevens uit de Cyber Quotient Evaluation (CyQu) laten ons zien dat organisaties, van verschillende omzetgroottes en in verschillende sectoren en regio's, onder het basisniveau presteren als het gaat om het beheren van cyberrisico's. Dus, hoe kunnen organisaties zich beter voorbereiden en beschermen?

Hieronder vindt u een blauwdruk die bedrijven helpt betere beslissingen te nemen door de juiste vragen te stellen.

Assessment

- Wat is de staat van onze beveiliging en maatregels, in het bijzonder waar deze van toepassing zijn op de digitale evolutie, risico's van derden, ransomware en risico's met betrekking tot wet- en regelgeving?
- Wat zijn de belangrijkste middelen die we moeten beschermen?
- Wat zijn de meest waarschijnlijke dreigingen?
- Hoe houden we zakelijke behoeften in evenwicht met cyberrisico's?

Kwantificering

- Kennen we het soort en de impact van onze potentiële verliezen? Weten we dit ook voor ransomware, verder dan het risico van data-encryptie?
- Begrijpen we de belangrijkste wet- en regelgeving, de eisen hiervan en de kosten van het niet naleven?
- Hoe nemen we beslissingen over investeringen in beveiliging?
- Kunnen we de effectiviteit van ons huidige risicobeheer en onze verzekering meten in termen van totale risicokosten (TCoR)?

Verzekering

- Begrijpen we de dreigingen en de impact hiervan?
- Hebben we een effectieve strategie om verliezen te beperken?
- Moeten we een deel van ons risico overdragen naar de verzekeringsmarkt of moeten we alternatieve strategieën voor risico-overdracht overwegen?

Incident response readiness

- Hebben we een geschikt en bruikbaar incidentresponsplan? Zo ja, is het responsteam getraind en klaar om te reageren?
- Beschikken we over de juiste beveiligings- en forensische tools, processen en procedures?
- Hebben we onze cyberbeveiligingstechnologie goed geconfigureerd?
- Kunnen we snel en effectief reageren op een incident?

Een blik op de horizon: **klaar zijn voor morgen**

Experts vanuit Aon's Cyber Solutions noemden vijf belangrijke risico's die in de nabije toekomst van cruciaal belang zijn. Het is essentieel om bekend te worden met deze risico's.

- **Kunstmatige intelligentie.** Machine learning groeit in een enorm tempo en is een onvermijdelijk onderdeel van de manier waarop organisaties zaken zullen doen. Op een gegeven moment maakt kunstmatige intelligentie keuzes voor ons en elke keuze die aangevallen of beïnvloed kan worden, vormt een aanzienlijk risico.
- **Alternatieve betalingen**. Overal waar een betaling plaatsvindt, bestaat een cyberrisico. De digitaal evoluerende wereld heeft dringend behoefte aan alternatieve manieren van betalingen en nieuwe manieren om rijkdom te vergaderen en op te slaan. Bedrijven zullen partijen tegenkomen die geen gebruik meer maken van banken. En business-to-consumer-bedrijfsmodellen zullen uiteindelijk niets meer te maken hebben met traditionele valuta.
- **Pensioenregelingen.** Pensioenregelingen bevatten een schat aan gegevens en zijn tevens een toegangspoort tot enorme sommen geld. Organisaties moeten weten wie toegang heeft tot pensioengegevens van medewerkers en wie de fiduciaire verantwoordelijkheid heeft bij de aanbieder. Omdat pensioenplannen steeds vaker online en vanaf mobiele apparaten bekeken worden, worden deze gegevens ook steeds gevoeliger voor inbreuken.
- **Toeleveringsketen voor technologie.** Elk jaar komen er nieuwe dreigingen bij geïntroduceerd via technologieleveranciers. Omdat steeds meer gevoelige gegevens en intellectuele eigendommen worden uitgewisseld via software van derden, moeten organisaties waakzamer worden bij het beoordelen van kwetsbaarheden en blootstelling aan cyberrisico's.
- **Het Dark Web.** Gevoed door de groei van cryptocurrency, het gebruik van browsertechnologie zoals TOR en de toenemende verfijning van ransomwaregroepen, worden criminele markten sterker. Het dark web is hun werkplek en zij blijven daarvanuit aanwezig. Organisaties moeten niet proberen om zonder gids of kaart door deze ruimte te navigeren. Blijf te allen tijde waakzaam.

Bronnen

1 2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and insurance challenges," Aon, https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

2 The Cyber Loop: Managing cyber risk requires a circular strategy," Aon, 2019, https://www.aon.com/cyber-solutions/thinking/the-cyber-loop-managing-cyber-risk-requires-a-circular-strategy/.

3 This Year in Ransomware Payments (2020 Edition)," December 2020. https://heimdalsecurity.com/blog/ransomware-payouts-of-2020/.

4 2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and insurance challenges," Aon, https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

5 Cyber Security Ventures," https://www.thesslstore.com/blog/ransomware-statistics/ https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/.

6 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware Ransomware Marketplace Report, Q4 2020, https://www.coveware.com/blog.

7 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," Coveware Ransomware Marketplace Report, Q4 2020, https://www.coveware.com/blog.

8 2021 Errors and Omissions and Cyber Insurance Snapshot: A focused view of 2021 risk and insurance challenges," Aon, https://www.aon.com/cyber-solutions/thinking/aons-errors-omission-cyber-insurance-snapshot-a-focused-view-of-2021-risk-insurance-challenges/.

CyQu risicovolwassenheidsscore

Initieel | 1–1.9

Cyberrisicobeheer op organisatorisch niveau wordt niet of nauwelijks toegepast. Als de organisatie risico's identificeert en aanpakt, gebeurt dit alleen binnen silo's; onderdelen en acties binnen het risicobeheerproces zijn beperkt in scope en worden ad hoc geïmplementeerd.

Basis | 2–2.5

Cyberisicobeheer, zowel technisch als organisatorisch, zijn niet geformaliseerd en worden niet organisatiebreed opgepakt. Risico's worden ad hoc en soms reactief beheerd.

Beheerd | 2.6–3.4

Cyberrisicobeheer, zowel technisch als organisatorisch, zijn voor het overgrote deel geformaliseerd en worden ook toegepast. De organisatie past het beheer van cyberbeveiliging aan op basis van best practices en voorspellende indicatoren in het grootste deel van het bedrijf. Beleid, processen en procedures worden gedefinieerd, geïmplementeerd en beoordeeld. Er zijn consistente methoden om effectief te reageren op verandering van de risico's.

Gevorderd | 3.5–4

Cyberrisicobeheer, zowel technisch als organisatorisch, is volledig geformaliseerd en wordt ook organisatiebreed toegepast. Cyberrisicobeheer wordt regelmatig en volgens vaste procedures bijgewerkt. Het beheer van organisatorische cyberbeveiliging wordt regelmatig bijgewerkt op basis van de toepassing van risicobeheerprocessen op veranderingen in bedrijfs- / missievereisten en een veranderend dreigings- en technologielandschap. Er bestaat een proces van voortdurende verbetering met behulp van geavanceerde cyberbeveiligings-technologieën en -procedures.

Vragen

aon.com/cyber-solutions

Over Aon

Aon plc (NYSE:AON) is een toonaangevende wereldwijde dienstverlener op het gebied van risk, retirement en health. Aon analyseert de personele risico's en bedrijfsrisico's, geeft passend risicoadvies, zorgt voor de (financiële) oplossing en staat klanten bij als een incident de bedrijfscontinuïteit bedreigt. Zo helpen wij klanten succesvol te ondernemen. Aon heeft in Nederland 15 locaties met 2.500 medewerkers en wereldwijd meer dan 50.000 medewerkers in ruim 120 landen.

www.aon.nl

20.007-03-cyber-risk-report-2021-22