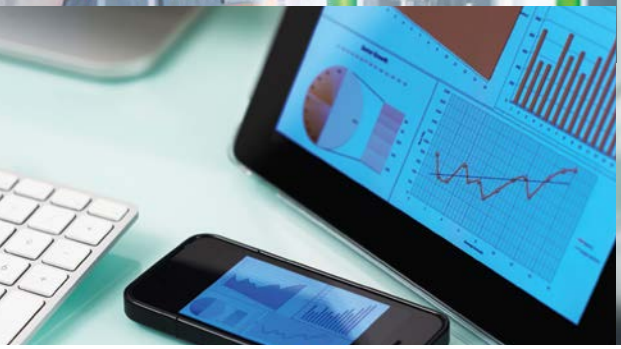
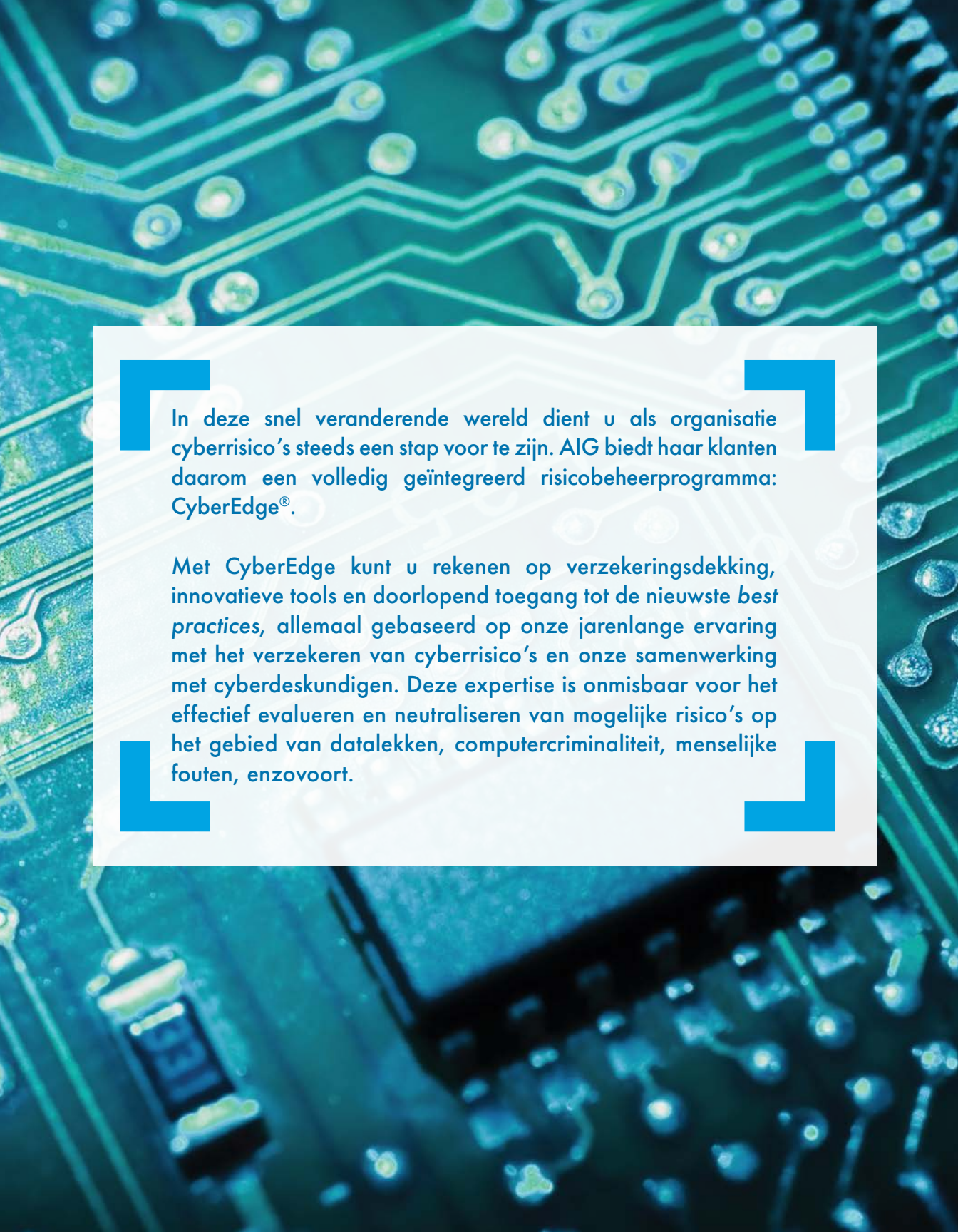


CyberEdge®

Geïntegreerde oplossingen voor cyberrisicobeheer

AIG®



In deze snel veranderende wereld dient u als organisatie cyberrisico's steeds een stap voor te zijn. AIG biedt haar klanten daarom een volledig geïntegreerd risicobeheerprogramma: CyberEdge®.

Met CyberEdge kunt u rekenen op verzekeringsdekking, innovatieve tools en doorlopend toegang tot de nieuwste *best practices*, allemaal gebaseerd op onze jarenlange ervaring met het verzekeren van cyberrisico's en onze samenwerking met cyberdeskundigen. Deze expertise is onmisbaar voor het effectief evalueren en neutraliseren van mogelijke risico's op het gebied van datalekken, computercriminaliteit, menselijke fouten, enzovoort.

CyberEdge Risicobeheeroplossing

Wij bieden onze verzekerden actieve ondersteuning bij alle mogelijke aspecten van cyberrisico's: van innovatieve schadepreventie-tools – waarmee u uw werknemers kunt opleiden om cyberrisico's te herkennen en mogelijke datalekken kunt voorkomen – tot begeleiding door ons CyberEdge Breach Resolution Team wanneer zich daadwerkelijk een lek voordoet.

Risicoadvisering en -preventie	Verzekeringsdekking	Breach Resolution Team
Opleiding en kennis	Schadeclaims van derden ten gevolge van een beveiligings- of datalek	Continue begeleiding:
Training en compliance	Door u gemaakte kosten voor het verhelpen van een lek	Juridische en forensische diensten
Mondiale risico-updates en evaluaties	Inkomstenderving en operationele kosten ten gevolge van een beveiligings- of datalek	Callcenter voor meldingen, krediet- en identiteitsbewaking
Blokkeringsdiensten	Dreigen met het naar buiten brengen van vertrouwelijke informatie of systeemaanvallen door afpersers	Crisis communicatie deskundigen
Deskundig advies en overleg	Online smaad en inbreuken op het auteursrecht en handelsmerk	Meer dan 15 jaar ervaring met cyber-gerelateerde schades

Risicoadvisering en -preventie

De bescherming die CyberEdge biedt, vormt een waardevolle aanvulling op de 'eerste verdedigingslinie' van een bedrijf tegen cyberrisico's: zijn eigen IT-systeem. Cyberrisico's blijven zich ontwikkelen. Toch zijn onze verzekerden altijd goed voorbereid, omdat wij ontwikkelingen in de sector op de voet volgen. Onze preventieve tools geven onze klanten de kennis, training, veiligheidsmaatregelen en hulplijnen die zij nodig hebben om risico's steeds een stap voor te zijn.

CyberEdge app voor iPhone®, iPad®, en Android™

Met de CyberEdge app hebben gebruikers continu toegang tot de nieuwste datalek-updates, nieuwsberichten, opinies en risicoanalyses. De app combineert een strak design met uiteenlopende internationale functies, en is niets minder dan een wereldprimeur. Beschikbaar voor iPhone, iPad en Android.

De CyberEdge app biedt onder andere de volgende functies:

- Datalek-risicokaart, die een overzicht geeft van lekken over de hele wereld. De kaart geeft ook informatie over eventuele wettelijke meldingsplichten in het land waar de cyberlek zich heeft voorgedaan.
- Claims Scenario's, met voorbeelden uit de praktijk van cyberincidenten die door CyberEdge worden gedekt.
- Kostencalculator, die het bedrijf – door zijn bedrijfsgegevens in te vullen – kan gebruiken om een schatting te maken van de potentiële kosten van een datalek.
- Het grootste deel van de app content wordt aangeboden in het Engels, Frans en Spaans.

Dark Net Intelligence *mogelijk gemaakt door K2 Intelligence*

Cybercriminaliteit wordt steeds makkelijker en winstgevender voor criminelen, vooral nu dat organisaties steeds meer activiteiten ontplooien in een digitale, onderling verbonden wereld.

K2 Intelligence biedt CyberEdge-verzekerden de mogelijkheid om tegen een speciaal tarief op de hoogte te blijven van wat er op dit moment over hun organisatie wordt gezegd op de markten en fora van criminele hackers, ook wel bekend als het 'dark net'. Het dark net vormt een uitvalsbasis en schuilplaats voor 's werelds meest geraffineerde cybercriminelen, van waaruit zij hun aanvallen opzetten.

Met behulp van web-crawlers en een geavanceerde menselijke inlichtingendienst kamt K2 Intelligence het dark net uit voor relevante data. Dergelijk maatwerk is van onschatbare waarde voor organisaties die:

- Een proactieve strategie volgen bij het ontwikkelen en verfijnen van hun beheerprogramma voor cyberrisico's en zich ervan verzekeren dat de relevante bestuurlijke normen en protocollen worden aangehouden.
- Zich bezighouden met fusies en overnames. Organisaties die betrokken zijn bij een overname of fusie kunnen de deskundigen en inlichtingen van K2 Intelligence gebruiken voor een due diligence op het gebied van cyberbeveiliging.

Infrastructuur-kwetsbaarheidsscan *mogelijk gemaakt door IBM*

CyberEdge-klanten die hiervoor in aanmerking komen, kunnen IBM een kwetsbaarheidsscan laten uitvoeren op hun infrastructuur. IBM scant op afstand externe infrastructuren van deze klanten die gekoppeld zijn aan het internet. Dit helpt om kwetsbaarheden op te sporen die mogelijk door een hacker via het internet kunnen worden benut. Daarnaast biedt deze infrastructuur-kwetsbaarheidsscan:

- Opsporing en prioritering van verborgen risico's in een extern verbonden netwerk-infrastructuur.
- Gedetailleerd inzicht in het kwetsbaarheidsniveau van het bedrijf, zodat de klant zijn beveiligingspositie effectiever kan bewaken, begrijpen en rapporteren.
- Prioritering van zwakke punten zodat klanten hun algemene risicoprofiel kunnen verbeteren.
- Unieke rapportagemogelijkheden, waardoor het makkelijker wordt om zwakke punten op te sporen en te verhelpen.

BitSight Veiligheidsratings

BitSight produceert veiligheidsratings die organisaties kunnen gebruiken bij het meten en bewaken van hun eigen netwerk en de netwerken van hun dienstverleners. Deze ratings worden discreet gegenereerd op basis van een continue meting van extern toegankelijke data. Veiligheidsratings zijn gebaseerd op de volgende gegevens:

- Waargenomen veiligheidsincidenten en sporen van succesvolle cyberaanvallen. Dit houdt ook in communicatie met botnets, spam, malware en andere interacties.
- Kwalitatieve kenmerken voor diligence-programma's, of aanwijzingen dat het bedrijf gerichte stappen heeft ondernomen om een aanval te voorkomen. Dit omvat ook een grondige analyse van de beveiligingsconfiguratie.

CyberEdge-verzekerden die hiervoor in aanmerking komen ontvangen een BitSight Veiligheidsratingrapport. Dit rapport doet verslag van een meting van het beveiligingsniveau van hun organisatie. Daarnaast komen polishouders in aanmerking voor speciale kortingen op de producten en diensten van BitSight. Verzekerden kunnen ervoor kiezen om dagelijkse ratings te ontvangen als onderdeel van hun integrale beheerprogramma voor cyberrisico's. Deze updates geven hen actueel inzicht in mogelijke cyberrisico's in alle hoeken van hun digitale netwerk.

Statusbeoordeling van Cyberveiligheidsprogramma *mogelijk gemaakt door RSA*

Verzekerden kunnen eenmalig gebruik maken van zes maanden gratis toegang tot RSA's Governance, Risk & Compliance (GRC) programma om vast te stellen aan welke cyberrisico's hun organisatie is blootgesteld. Deze evaluatie is gebaseerd op het meest vooraanstaande platform in de sector: RSA Archer GRC.

- De statusbeoordeling gebruikt het NIST Cybersecurity Framework om te bepalen tot op welke hoogte het cyberveiligheidsprogramma van de organisatie is uitgewerkt en op welke punten cruciale functies nog verder kunnen worden verbeterd.
- Wanneer de beoordeling is afgerond heeft de organisatie inzicht in de eventuele gaten tussen haar huidige en haar ideale risicopositie.
- Daarnaast krijgen verzekerden toegang tot RSA's Advanced Cyber Defense (ACD) programma, dat hen operationele deskundigheid biedt bij het dichten van deze gaten en het beschermen van kritieke bedrijfsmiddelen.

Proactieve Blokkering *mogelijk gemaakt door RiskAnalytics*

Klanten die hiervoor in aanmerking komen, krijgen toegang tot de nieuwste informatie en technologie op het gebied van cyberrisico's. Deze dienst isoleert en blokkeert IP-adressen die momenteel door criminelen worden gebruikt. Voordat cybercriminelen een netwerk aanvallen, doen zij eerst verkennend onderzoek om te bepalen welke IP-adressen goede doelwitten zijn. Als dergelijke communicaties worden geblokkeerd, kunnen criminelen niet meer bij het netwerk komen en kunnen zij niet vaststellen welke IP-adressen geschikt zijn. Wanneer deze verkenningsfase mislukt is er een veel kleiner risico op verdere inbreuken door de criminelen.

Blokkering kan een organisatie ook beschermen tegen aanvallen van binnenuit. Wanneer een van de computers in een netwerk met malware is besmet, kan blokkering ervoor zorgen dat het netwerk niet kan communiceren met de controleservers van de crimineel. Hierdoor is de malware effectief onschadelijk gemaakt. Deze proactieve blokkering gebeurt in *real time*, op volledige verbindingssnelheid. Het is schaalbaar naar behoefte en kan bescherming bieden voor al uw activiteiten – van een enkele locatie tot een wereldwijde onderneming.

Portfolioanalyse *mogelijk gemaakt door Axio Global*

Als CyberEdge-polishouder kunnen onze klanten een beroep doen op Axio Global (Axio) om een samenhangend beeld te krijgen van hun verschillende cyberrisico's, en om hun technologische en operationele beheermiddelen effectief te combineren met hun dekking. Axio's methode richt zich op alle mogelijke cyberschades – van het stelen van gegevens tot aansprakelijkheid, van eigendomsschade tot milieuschade en van lichamelijk letsel tot bedrijfsonderbrekingen. CyberEdge-polishouders ontvangen korting op de onderstaande diensten van Axio:

- Een eendaagse schadescenario-workshop, waarin een schatting wordt gemaakt van de financiële gevolgen van verschillende schadescenario's voor de informatietechnologie- en beheerssystemen van de deelnemer. Deze scenario's zijn aangepast aan de specifieke behoeften van de klant en ingedeeld in een classificatie die kan worden gebruikt om de verzekeringsdekking te testen onder verschillende omstandigheden.
- Analyse van het volledig portfolio aan schade- en aansprakelijkheidsverzekeringen om te bepalen hoe deze een complex cyberincident zouden opvangen. In combinatie met de schadescenario-workshop, kan deze analyse worden gebruikt om de verzekeringsportfolio van de klant te testen tegen een aantal realistische scenario's.
- Zelfevaluatie door de klant van zijn cyberveiligheidsprogramma op basis van het Cybersecurity Capability Maturity Model (C2M2), een aanbevolen toepassing van het NIST Cybersecurity Framework. Deze zelfevaluatie resulteert in een rapport dat scores geeft op specifieke onderdelen, als ook een samenvatting van de resultaten van de evaluatie. C2M2 is ontworpen door een van de oprichters van Axio, die al jaren organisaties helpt om de inhoud van het model correct te interpreteren zodat zij hun cyberveiligheidsprogramma zo effectief en efficiënt mogelijk kunnen evalueren.

Verzekeringsdekking

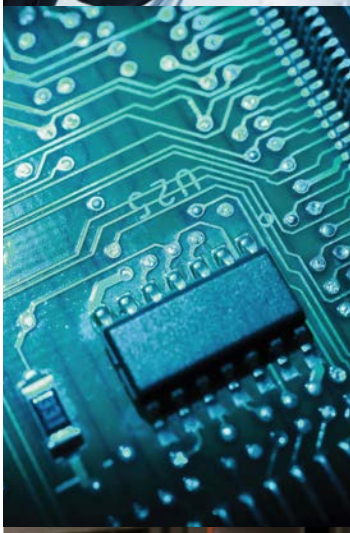
CyberEdge biedt bedrijven dekking voor de onderstaande gevolgen van cybercriminaliteit:

- Schadeclaims door derden ten gevolge van een lek in de netwerkbeveiliging van de verzekerde partij of het ongewenst openbaar maken van gegevens. De dekking strekt zich ook uit tot de kosten die gemoeid zijn met interventies door toezichthouders in verband met een beveiligingslek of het niet-tijdig melden van een beveiligings- of privacylek.
- De directe kosten van de verzekerde ten gevolge van een beveiligings- of privacylek. Het gaat hier onder andere om de kosten voor de melding van het incident, public relations en andere activiteiten die de organisatie moet ondernemen om de negatieve effecten goed te beheren en te minimaliseren. De verzekering biedt ook dekking voor de kosten van forensische onderzoeken, juridisch advies en identiteitsbewaking voor alle slachtoffers van de lek.
- Bedrijfsonderbrekingen ten gevolge van een lek in de netwerkbeveiliging, waarbij zowel gederfde inkomsten als operationele uitgaven worden vergoed. De verzekerde krijgt ook hulp bij het beperken van klantenverlies en reputatieschade, en er zijn ook uitbreidingen beschikbaar voor schades veroorzaakt door systeemfouten, *cloud computing* en externe leveranciers.
- Situaties waarbij een externe partij dreigt het computernetwerk van een bedrijf te verstoren of vertrouwelijke informatie vrij te geven in een poging geld of andere waardevolle zaken af te persen. De dekking strekt zich onder andere uit tot betalingen die worden gedaan om een dergelijke dreiging te neutraliseren en de kosten van een onderzoek naar de herkomst van de dreiging.
- Kosten die verband houden met de aansprakelijkheid van een bedrijf voor *content* die via zijn website wordt verspreid. De verzekering biedt dekking voor een groot aantal media-gerelateerde risico's, waaronder inbreuk op het auteursrecht, inbreuk op het handelsmerk, smaad en privacyschending.

Breach Resolution Team

Het CyberEdge Breach Resolution Team staat verzekerden bij vanaf het moment dat er een netwerklek wordt vermoed. Ons team combineert lokale aanwezigheid met wereldwijde ondersteuning en expertise. Hierdoor kunnen onze specialisten een incident effectief beheren terwijl het zich ontvouwt en kunnen zij snel reageren op klantvragen.

Wanneer een lek wordt vermoed, krijgt de verzekerde via het CyberEdge Breach Resolution Team toegang tot meer dan 15 jaar ervaring in het afhandelen van cyber-specifieke claims.



- Claims-experts zijn bevoegd om snel de noodzakelijke beslissingen te nemen en klanten die met een lek worden geconfronteerd effectief te ondersteunen.
- Wij brachten de allereerste cyberaansprakelijkheidsverzekering op de markt in 1999. Sinds deze introductie hebben wij duizenden bedrijven en meer dan twintig miljoen privépersonen geholpen effectief om te gaan met een cyberaanval.
- Dankzij onze zeer uitgebreide claimsportfolio, zijn wij uitzonderlijk goed gepositioneerd om nieuwe ontwikkelingen in claims en dekkingswaarden te herkennen en erop te anticiperen.
- Gemiddeld hebben onze claims-experts meer dan zeven jaar praktijkervaring in het afhandelen van de meest ingewikkelde cyberclaims – zowel van onze verzekerden als van derden.

Ondersteund door een sterk en uitgebreid netwerk van wederverkopers, biedt onze CyberEdge Breach Resolution Team een extra ondersteuningslaag die voor een IT-afdeling van grote waarde kan zijn bij het afweren van een cyberaanval.

- KPMGs cyber-responsteam bestaat uit technische deskundigen, ervaren incidentmanagers en forensische experts.
- Daarnaast bieden wij deskundige juridische ondersteuning via onze samenwerkingen met de toonaangevende advocatenkantoren Norton Rose Fulbright en CMS Cameron McKenna.
- Tijdig reageren is van cruciaal belang bij een beveiligings- of privacylek. Met een draaiboek voor dergelijke incidenten en toegang tot externe middelen bent u in staat om efficiënt en kosteneffectief te reageren op het lek en er snel van te herstellen.

- Doorlopend toegang tot ons callcenter om claims te melden en voor ondersteuning.
- Één vaste locatie voor het tijdig rapporteren, bevestigen en verwerken van claims.
- Toegang tot lokale claims-experts uit de hele wereld.
- Toegang tot een panel van internationale advocaten met lokale expertise in het afhandelen van cyberclaims.

Cyberrisico's trekken zich niets aan van grenzen

Ons internationaal dienstenplatform Passport biedt onze klanten een efficiënte en naadloze oplossing om cyberrisico's altijd een stap voor te zijn. Daarnaast kunnen zij vertrouwen op de deskundigheid van onze lokale teams, die precies weten hoe die markten waar u zaken doet in elkaar steken. Het CyberEdge Breach Resolution Team biedt actieve begeleiding en ondersteuning – waar dan ook ter wereld. Onze geïntegreerde risicobeheeroplossing is letterlijk onbegrensd.

Betere, snellere en efficiëntere wereldwijde bescherming

Passport is een simpele, effectieve manier om toegang te krijgen tot uitgebreide internationale voordelen, waaronder:

- Lokaal vastgestelde dekking die in overeenstemming is met de plaatselijke wetgeving, regelgeving, taal en gebruiken.
- Toegang tot lokale acceptanten en claims-deskundigen.
- Heldere dekking die wereldwijd wordt gecoördineerd.

Een minder omslachtige aanpak van mondiale cyberrisico's

Passport maakt het voor klanten zo eenvoudig mogelijk om zich te wapenen tegen mondiale cyberrisico's.

- De klant ontvangt een offerte die het wereldwijde cyberprogramma uiteenzet. Deze bestaat uit de internationale polis en mogelijke lokale polissen indien de klant daar om heeft verzocht.
- De zaak is geregeld zodra de klant de beschreven dekking heeft geaccepteerd.
- De betreffende lokale polissen worden uitgegeven door onze lokale kantoren over de hele wereld. Deze lokale polissen houden rekening met lokale regelgeving, gebruiken in de sector en risico's.[1]

[1]Maximale uitkeringen zijn onderhevig aan capaciteitsbeheer: in bepaalde landen kunnen restricties gelden voor ofwel de totale jaarlijkse uitkering ofwel de aparte wereldwijde maximale uitkering.

Bestemmingen die zijn opgenomen in het CyberEdge Passport programma

- Australië
- Bahrein
- België
- Brazilië*
- Bulgarije
- Canada
- Chili
- Colombia
- Cyprus
- Denemarken
- Duitsland
- Ecuador
- Filippijnen
- Finland
- Frankrijk
- Griekenland
- Hongarije
- Hongkong
- Ierland
- Israël
- Italië
- Japan
- Koeweit
- Libanon
- Luxemburg
- Maleisië
- Mexico
- Nederland
- Nieuw-Zeeland
- Noorwegen
- Oeganda
- Oman
- Oostenrijk
- Panama
- Polen
- Portugal
- Puerto Rico
- Qatar
- Roemenië
- Rusland*
- Singapore
- Slowakije
- Spanje
- Taiwan
- Tsjechië
- Turkije
- Uruguay
- Verenigde Arabische Emiraten
- Verenigd Koninkrijk
- Verenigde Staten
- Zuid-Afrika
- Zuid-Korea
- Zweden
- Zwitserland

Wij voegen regelmatig nieuwe bestemmingen toe aan het Passport programma. Aarzel niet contact op te nemen met een van onze Passport-medewerkers indien u meer informatie wenst.

*Bij Brazilië en Rusland dienen klanten een aanvullende premie te betalen en een toeslag voor speciale behandelingskosten.

Wilt u meer weten over CyberEdge?

E-mail ons op CyberEdge@aig.com • Bezoek onze website: www.aig.com/CyberEdge

Download de CyberEdge app

Available on the App Store

ANDROID APP ON Google play

Volg CyberEdge

Follow@AIGinsurance

AIG Bring on tomorrow®

NLL00000325 CyberEdge Services Br Nov15