Whitepaper

Cyberrisico's onder controle?
Risicomanagement in het digitale tijdperk

Wat zijn de digitale risico's die in uw organisatie om aandacht vragen? Fraude, hacken, lekken of manipuleren van informatie, bedrijfsspionage, informatiediefstal of falende ICT-systemen? Voor welke uitdaging u ook staat, een goede voorbereiding is het minste dat u kunt doen. En moet. Want zowel de financiële gevolgen, als bijvoorbeeld de dreigende reputatieschade kunnen de bedrijfscontinuïteit ernstig onder druk zetten.

Aon heeft een speciale taskforce ingesteld: de taskforce cyberrisico's. Door een samenhangende aanpak te ontwikkelen van analyseren, beheersen én bestrijden ondersteunen we organisaties en bedrijven bij de risico's die zij lopen. Laat u daarom in deze whitepaper informeren over de impact en oorzaken van digitale risico's, over hoe u risico's voor uw eigen organisatie identificeert en hoe u de gevolgen van een incident kunt beperken.

Inhoud:

Juni 2012

1 Inleiding

Het digitale tijdperk heeft tal van voordelen en zorgt voor innovaties en kansen. Voor organisaties en bedrijven levert dit veel gemak op, zeker ook in de dienstverlening aan burgers en klanten. Tegelijkertijd brengt digitalisering uit het oogpunt van bedrijfscontinuïteit nieuwe risico's met zich mee. Van een computerstoring die het treinverkeer ontregelt, hackers die vertrouwelijke klantgegevens in handen krijgen tot herhaaldelijke problemen met internetbankieren. TNO concludeerde op basis van recent onderzoek (april 2012) dat cybercrime de Nederlandse samenleving jaarlijks ten minste tien miljard euro kost. Driekwart hiervan komt voor rekening van het bedrijfsleven.

De gevolgen van digitale inbraken en technische problemen zijn zeer omvangrijk. Het gaat niet alleen om de financiële gevolgen. Cyberrisico's stellen ook de veiligheid, reputatie en zelfs de continuïteit van organisaties op de proef. Ook de diverse voorbeelden die onlangs het nieuws haalden, maken dit duidelijk (zie kader).

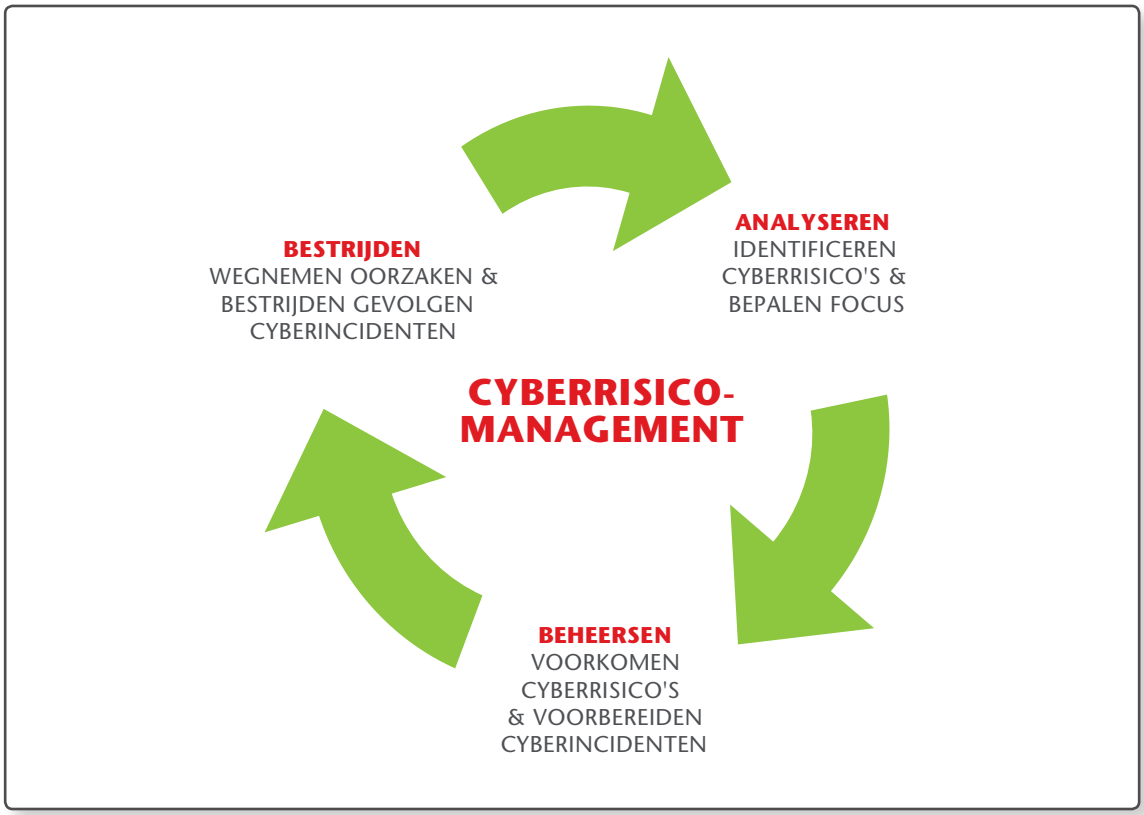
Digitale incidenten in het nieuws

1. Het netwerk van één van de grootste aanbieders van mobiele telefonie valt dagenlang uit door een brand. Miljoenen Nederlandse klanten ondervinden hinder van de storing.
2. Beveiligingscertificaten voor websites, geleverd door een commerciële certificaatautoriteit, worden door hackers vervalst en doorverkocht. De overheid is de belangrijkste afnemer en kan de veiligheid van veel websites niet langer garanderen. Het vertrouwen in het bedrijf wordt opgezegd en deze gaat failliet.
3. Een financiële instelling heeft herhaaldelijk problemen met internetbankieren. Klanten ervaren hinder en webwinkels lopen omzet mis.
4. Het treinverkeer in de randstad is urenlang ernstig ontregeld door een computerstoring.
5. Een ziekenhuis kampt gedurende een dag met een computerstoring. Het ziekenhuis moet operaties uitstellen, alle afspraken annuleren en ambulances moeten uitwijken naar nabijgelegen ziekenhuizen.
6. Een telecombedrijf krijgt te maken met een hack van de systemen. Hierdoor kan het bedrijf de veiligheid van het mailverkeer en daarmee de privacy van de klant niet garanderen. Het bedrijf besluit tijdelijk twee miljoen e-mailaccounts af te sluiten.
7. Een hacker schakelt de beveiliging van een server van een reclamebureau uit en bemachtigt de gegevens van 62.000 klanten.

Is uw organisatie voldoende voorbereid op cyberrisico's? Waarschijnlijk staat ook u niet dagelijks stil bij de risico's en mogelijke gevolgen. Dat is logisch, want pas sinds een paar jaar worden deze bedreigingen zichtbaarder. Die ontwikkeling noodzaakt organisaties tot een nieuwe kijk op risicomanagement. De vraagstelling van deze whitepaper is dan ook:

Hoe zijn cyberrisico's in te schatten en te beheersen? En hoe zijn incidenten waar mogelijk te bestrijden?

Aon heeft hiervoor een samenhangende benadering ontwikkeld; cyberrisicomanagement. Cyberrisicomanagement bestaat uit de volgende onderdelen: analyseren, beheersen en bestrijden. Het schema op de volgende pagina laat zien dat het hierbij gaat om een continu proces.



Deze whitepaper gaat met name in op de volgende onderwerpen:

- Overzicht cyberrisico's: inschatting, oorzaken en impact
- Analyseren en beheersen van risico's: hoe zijn cyberrisico's aan te pakken? En welke oplossingen biedt de huidige verzekeringsmarkt?
- Bestrijden van cyberincidenten: wat zijn de kenmerken van een cyberincident? En hoe zijn cyber-incidenten te managen?

In het laatste deel van deze whitepaper vindt u praktische adviezen gebaseerd op de drie onderdelen van cyberrisicomanagement.

Taskforce cyberrisico's

De whitepaper is samengesteld door Aon's taskforce cyberrisico's. Deze taskforce ontwikkelt oplossingen om organisaties te ondersteunen bij het analyseren, beheersen en bestrijden van hun digitale risico's.

2 Cyberrisico's: inschatting, oorzaken en impact

De cyberrisico's nemen toe. Welke uitdagingen stellen deze nieuwe risico's uw organisatie? Voor een duidelijke beantwoording van die vraag is het belangrijk om op drie gebieden nader in te gaan:

- Hoe schatten risicoadviseurs en -experts cyberrisico's in?
- Wat zijn de oorzaken van cyberrisico's?
- Wat is de impact van de risico's?

Hoe schat Aon cyberrisico's in?

Twee onderzoeken van Aon maken duidelijk dat experts cyberrisico's inschatten als één van de belangrijkste bedreigingen voor organisaties. In de Aon Global Risk Management Survey en de Security Management Survey staan cyberrisico's in 2011 zelfs voor het eerst in de top tien van meest genoemde risico's.

Aon Global Risk Management Survey 2011

Veranderingen in wet- en regelgeving, reputatie- en merkschade, onderbreking van het productieproces en falende technologie/systeemfalen zijn belangrijke bedreigingen, die allemaal een relatie hebben met cyberrisico's. Dit blijkt uit de Aon Global Risk Management Survey 2011, een tweejaarlijks onderzoek van Aon onder 960 ondernemers en managers uit 58 landen. Falende technologie en systeemuitval – cyberrisico's – behoren voor het eerst bij de meest genoemde risico's.

De top tien risico's van de Aon Global Risk Management Survey 2011

(tussen haakjes positie in 2009)

1.	(1)	Verzwakking economie
2.	(2)	Veranderingen in wet- en regelgeving
3.	(4)	Toenemende concurrentie
4.	(6)	Reputatie- en merkschade
5.	(3)	Onderbreking van het productieproces
6.	(-)	Gebrekkige innovatie/ aansluiting bij klantbehoefte
7.	(10)	Onvermogen om toptalent aan te trekken en vast te houden
8.	(5)	Prijsrisico grondstoffen
9.	(-)	Falende technologie/systeemfalen
10.	(7)	Risico van cashflow en liquiditeit

Security Management Survey 2011

Eind 2011 deed Aon in samenwerking met het vaktijdschrift Security Management van Kluwer voor de tweede keer onderzoek onder security managers in Nederland. In het Security Management Survey 2011 maakten de ondervraagde security managers net als in 2010 duidelijk welke risico's de meeste aandacht krijgen. De top tien security-risico's 2011 is een volstrekt andere dan in 2010. De nieuwe, vooral digitale risico's zoals informatiediefstal, het lekken of manipuleren van informatie en cybercrime (vooral hacking) zijn in 2011 volgens de ondervraagden opkomende, urgente risico's.

De top tien security risico's van Security Management Survey 2011

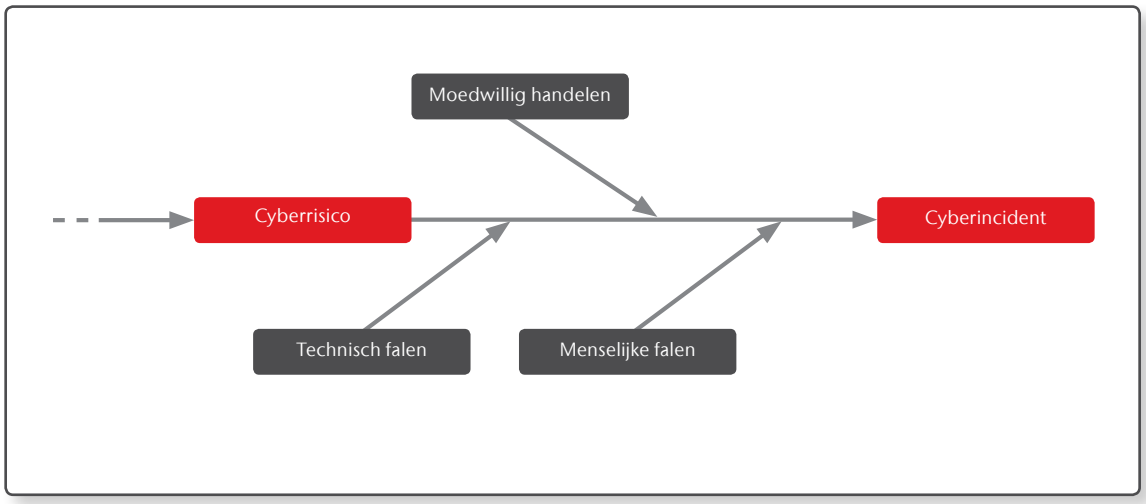
(tussen haakjes positie in 2010)

1. (1) Diefstal
2. (-) Informatiediefstal
3. (4) Agressie
4. (6) Vandalisme
5. (5) Fraude
6. (7) Lekken of manipuleren van informatie
7. (9) Cybercrime
8. (-) Bedrijfsspionage
9. (-) Bewust toebrengen imagoschade
10. (-) Bewuste negatieve continuïteitsbeïnvloeding

Wat zijn oorzaken van cyberrisico's?

De drie belangrijkste oorzaken van cyberrisico's op een rij:

1. Moedwillig handelen: risico's die te maken hebben met cybercriminaliteit. Denk aan het verspreiden van kwaadaardige software, identiteitsfraude en hacking.
2. Technisch falen: risico's als gevolg van falende systemen zoals ICT-storingen of uitval.
3. Menselijk falen: onder deze categorie vallen risico's door het niet goed beheren of beveiligen van de ICT-infrastructuur. Denk aan het kwijtraken of onbetrouwbaar raken van informatie, het te laat of niet adequaat updaten van software of systemen.



Wat is de impact van cyberrisico's?

De schade van een digitaal incident beperkt zich meestal niet tot één onderdeel van de organisatie. Hoewel de aanleiding vaak van technische aard is, werken de gevolgen door op tal van andere terreinen, zoals:

- Reputatie: een zorgvuldig opgebouwde reputatie kan in één klap op losse schroeven komen te staan.
- Continuïteit: er treedt verstoring op van kernprocessen waardoor de operatie vertraging oploopt of zelfs volledig stagneert.
- Veiligheid: de veiligheid van systemen en informatie valt niet langer te garanderen.
- Betrouwbaarheid: onder invloed van één casus is de kans aanzienlijk dat de betrouwbaarheid van de gehele informatievoorziening en dienstverlening van een organisatie in het geding komt.
- Kwaliteit: processen, systemen en dienstverlening leiden tot potentieel kwaliteitsverlies.
- Privacy: de privacy van medewerkers, klanten of leveranciers wordt mogelijk bedreigd.
- Financiële positie: directe kosten die voortvloeien uit een cyberincident en/of indirecte kosten verbonden met herstel en preventieve maatregelen kunnen de financiële positie van een organisatie negatief beïnvloeden.
- Stakeholders: belanghebbenden ervaren de gevolgen van cyberrisico's.
- Compliance: normen, standaarden, regel- en wetgeving worden mogelijk geschonden.

Juridische risico's

Aan cyberrisico's kleven ook juridische risico's. Aan het vastleggen, bewaren en omgaan met privacy-gevoelige gegevens zijn verantwoordelijkheden en verplichtingen verbonden. De Europese Commissie heeft recent nieuwe en strengere privacywetgeving aangekondigd. Hierin is de controle op privacyschending aangescherpt. Bedrijven moeten de ontdekking van een datalek binnen 24 uur melden bij de nationale toezichthouder. Bij overtreding kunnen organisaties geldboetes verwachten tot 2 procent van de jaaromzet. Deze ontwikkelingen illustreren de impact die cyberrisico's mogelijk inhouden voor privacy en compliance.

EU Privacyverordening (concept 25 januari 2012), in het kort:

- Binnen de EU komt één set privacyregels.
- De verordening is van toepassing als de hoofdvestiging van het bedrijf zich in de EU bevindt, of als een niet EU-bedrijf producten of diensten levert aan EU-burgers.
- Bevoegd wordt de nationale toezichthouder in de EU-lidstaat, waar het bedrijf zijn hoofdvestiging heeft ('one-stopshop').
- Bedrijven zullen meer verantwoording en rekenschap moeten afleggen over de verwerking van persoonsgegevens.
- De informatieplicht wordt aangescherpt.
- Wanneer voor de verwerking toestemming vereist is, moet deze uitdrukkelijk worden verkregen.
- Betrokkenen krijgen meer rechten.
- Er komen speciale verplichtingen voor het verwerken van gegevens van kinderen.
- Datalekken moeten binnen 24 uur worden gemeld.
- Bij overtreding kunnen boetes worden opgelegd tot maximaal 2% van de wereldwijde jaaromzet van een onderneming.

Bron: Van Doorne Advocaten, 'Bedrijfsleven moet zich voorbereiden op strengere EU privacyregels', februari 2012.

Conclusies

- Cyberrisico's vormen in toenemende mate een zorg voor het bedrijfsleven en de overheid.
- De oorzaken van cyberrisico's zijn divers en complex.
- Gevolgen van cyberrisico's vormen een bedreiging voor de continuïteit en het imago van organisaties.
- Wet- en regelgeving dwingt tot actie.

3 Analyseren en beheersen van cyberrisico's

"Onze nieuwe omgeving wordt de komende jaren gedefinieerd door een toenemende hoeveelheid informatie. Het evolutionaire dan wel competitieve voordeel zal liggen bij degenen die zich hieraan het beste kunnen aanpassen." Dit waren de woorden van Thornton May, Futurist & Executive Director bij IT Leadership Academy. Hij sprak ze uit tijdens de Chief Information Officers Day in november 2011.

Blijkbaar is de vraag hoe organisaties zich het beste kunnen aanpassen aan de overheersende betekenis van informatie. Dat is gemakkelijker gezegd dan gedaan. Veel bedrijven die (te) weinig rekening hielden met cyberrisico's en schade leden, kunnen hier over meepraten. In dit deel van de whitepaper gaan we in op de vraag hoe u risico's effectief en efficiënt kunt beheersen, op een manier waarbij risicomanagement en informatiebeveiliging elkaar versterken. Vooral de afhankelijkheid van informatie vormt in de praktijk een groot risico voor organisaties.

Risico's identificeren

Risico's zijn op een gestructureerde manier te identificeren, met behulp van drie klassieke aandachtsgebieden: vertrouwelijkheid, integriteit en beschikbaarheid.

1. Vertrouwelijkheid

Hierin staat de vraag centraal: welke informatie moet opvraagbaar zijn voor degene die op basis van functie

en/of verantwoordelijkheden ook daadwerkelijk die informatie nodig heeft? Denk aan notulen van het directieoverleg, prijsstrategieën en persoons- en personeelsinformatie. Deze informatie kent (al dan niet wettelijk bepaald) een ander vertrouwelijkheidsniveau dan bijvoorbeeld informatie in het orderbestand of de documentatie over de inventaris van een organisatie.

2. Betrouwbaarheid

De focus binnen dit gebied ligt op de correctheid van de informatie van de organisatie. Is de opgeslagen informatie juist? Is de informatie gaandeweg bewust of onbewust gewijzigd en op welke wijze? Als bijvoorbeeld de financiële gegevens van een organisatie niet correct zijn en als er op basis van deze informatie bedrijfsstrategische beslissingen worden genomen, kan dit verstrekkende gevolgen hebben voor de onderneming.

3. Beschikbaarheid

Organisatieprocessen zijn steeds afhankelijker van continu beschikbare en bijgewerkte informatie. De vraag is: is de correcte informatie beschikbaar op het juiste moment? Een voorbeeld is de klantenservice van een organisatie. Het is van groot belang dat deze afdeling snel toegang heeft tot alle actuele klantinformatie. Nog een voorbeeld is de productie. Organisaties die produceren zijn wat betreft productieplanning en logistieke afhandeling vaak afhankelijk van een directe koppeling met de order- en verkoopinformatie.

Door per aandachtsgebied de specifieke risico's te benoemen die voor uw organisatie spelen, zet u een belangrijke eerste stap. Het resultaat is een bedrijfsspecifieke lijst van alle informatierisico's. Deze lijst is aan te vullen met beheersmaatregelen per risico die binnen de onderneming al aanwezig zijn.

Prioriteren van risico's

Zijn de cyberrisico's voor uw organisatie waar mogelijk inzichtelijk gemaakt? Dan is de volgende stap om prioriteiten aan te brengen. Want niet elk risico heeft evenveel impact op de bedrijfsvoering. Van belang is dat alle disciplines binnen de onderneming bij het prioriteren vertegenwoordigd zijn. Beoordeel de risico's met de hoogste prioriteit – die dus de meeste impact zullen hebben – op mogelijke oorzaken en gevolgen. En ga na of bestaande beheersmaatregelen hierop voldoende inspelen. Stel vervolgens vast welke acties nodig zijn om de risico's beter te beheersen.

Beheersen van risico's via Business Continuity Management

Business Continuity Management kan een effectief middel zijn om cyberrisico's te beheersen en de impact zoveel mogelijk te beperken. In deze managementsystematiek is alles erop gericht de continuïteit van uw bedrijfsvoering in stand te houden. Ook als zich een incident voordoet. Gebrek aan personeel, onvoldoende toegang tot (productie)middelen, verlies van vitale data en uitval van de ICT-infrastructuur zijn belangrijke aandachtspunten voor wie op deze manier de digitale risico's wil beperken. Met name verlies van vitale data en uitval van de ICT-infrastructuur zijn voor deze whitepaper relevant.

Cybercontinuïteitsmanagement in drie stappen:

Stap 1 Voer een Business Impact Analyse uit: wat zijn de effecten van cyberrisico's op de kernprocessen van uw organisatie?

Stap 2 Stel een Business Continuity Plan op: welke maatregelen kunt u nemen om continuïteitsverlies te voorkomen? Hoe kunt u de gevolgen van uitval bestrijden?

Stap 3 Test en train uw medewerkers: weten uw medewerkers wat ze moeten doen als er sprake is van continuïteitsrisico's?

Conclusies:

- Breng de cyberrisico's in kaart en baseer hierop een plan van aanpak.
- Focus op bestrijding van risico's die voor uw organisatie ontoelaatbaar zijn.

4 Beheersen van risico's door verzekeren

Hoe goed uw organisatie de cyberrisico's ook inzichtelijk en beheersbaar heeft gemaakt, van 100 procent veiligheid kan nooit sprake zijn. Dat geldt zeker in een wereld waarin de digitale ontwikkelingen zo snel gaan. Er blijft altijd een risico bestaan dat zich een incident voordoet met een grote impact op uw organisatie. U kunt dit risico voor eigen rekening nemen. Andere organisaties kiezen ervoor dit te verzekeren. De markt biedt hiervoor verschillende mogelijkheden en verzekeringsvormen.

Een specifieke cyberverzekering afsluiten

Diverse verzekeraars bieden cyberverzekeringen aan. Wel is het acceptatieproces op dit moment nog vrij ingewikkeld. Zo moeten organisaties die zich willen verzekeren veel informatie aanleveren over de beveiligingsmaatregelen tegen cybercrime en over de interne processen. Een cyberverzekering is daardoor vooral geschikt voor organisaties, die zich voldoende hebben beschermd tegen cyberrisico's. Ook sluit de dekking van dit type verzekering niet altijd aan op de specifieke wensen van een organisatie.

De belangrijkste risico's inpassen in bestaande verzekeringen

De bestaande verzekeringen bieden in veel gevallen een basis om de gevolgen van cyberrisico's te beheersen. Een nadeel van de huidige verzekeringsoplossingen is dat er vaak geen volledige dekking bestaat. Hieronder vindt u een lijst van soorten verzekeringen die (delen van) cyberrisico's verzekeren.

Fraudeverzekeringen

Fraudeverzekeringen hebben als voornaamste doel een organisatie te beschermen tegen de schade als gevolg van interne fraude. Bijvoorbeeld door een medewerker of fraude door een derde partij. Uit onze ervaring blijkt dat de meeste financiële instellingen, zoals banken en verzekeraars, een dergelijke fraudedekking wel hebben geregeld. Dit is in andere sectoren veel minder het geval.

De toenemende dreiging van computerfraude is een goede aanleiding om binnen uw organisatie een fraudedekking te overwegen. Ga vooraf na of een standaard fraudeverzekering mogelijke beperkingen heeft. Het spreekt voor zich dat een zo ruim mogelijke omschrijving van computerfraude of manipulatie wenselijk is. En dat er een duidelijk beeld is van de mogelijke gevolgen die de verzekering moet compenseren, zoals dataverlies of compensatie voor een bedrijfsstilstand. Verzekeraars zijn meestal bereid om een fraudeverzekering op maat voor u te regelen.

(Beroeps)aansprakelijkheidsverzekeringen

Cyberrisico's kunnen ook impact hebben op de productie en uw dienstverlening. Dit raakt de aansprakelijkheid van uw onderneming. Een algemene aansprakelijkheidsverzekering (AVB) of beroepsaansprakelijkheidsverzekering (BAV) kan dan bescherming bieden. Deze verzekeringen dekken de schade aan derden.

Daarnaast krijgen organisaties steeds vaker te maken met strenge regelgeving op het gebied van veiligheid. Dit gaat vaak gepaard met hoge kosten om de veiligheid te waarborgen. Klanten, en ook de overheid, moeten steeds uitvoeriger en sneller geïnformeerd worden over incidenten ('duty to notify') op straffe van hoge boetes.

De afgesloten dekking van een aansprakelijkheidsverzekering biedt niet altijd bescherming in geval van een technologisch falen. Daarin verschillen de verzekeraars onderling nogal. Sommige sluiten dergelijke risico's uit. Andere verzekeraars zijn bereid om dergelijke uitsluitingen te beperken of hebben zelfs geen uitsluitingen. De huidige polissen omvatten meestal dekking voor onder meer netwerkveiligheids-aansprakelijkheid, privéaansprakelijkheid, privacy-notificatiekosten en wettelijke boetes.

Bestuurdersaansprakelijkheid

Voor zover bekend zijn er in Nederland nog geen bestuurders aansprakelijk gesteld voor cyberrisico's. Deze situaties zijn wel denkbaar. Bijvoorbeeld als blijkt dat er vanuit het bestuur van een onderneming onvoldoende maatregelen zijn getroffen, of als er aan beveiliging onvoldoende aandacht is geschonken. Een aansprakelijkheidsverzekering voor bestuurders biedt dekking voor aanspraken die privé gesteld worden tegen hen. Hierbij gaat het om fouten die gemaakt zijn bij het besturen van een onderneming. Enkele verzekeraars bieden de mogelijkheid de dekking uit te breiden met crisismanagement. Cyberrisico's zijn niet uitgesloten, maar vanwege het (vooralsnog) ontbreken van schadeclaims is niet duidelijk hoe verzekeraars in de praktijk zullen reageren.

Gebouwen, inventaris en goederen

Een brand- en/of elektronicaverzekering dekt schade aan gebouwen, inventaris en goederen. Maar wat als er schade ontstaat aan data en software? Vooral het financiële belang van beschikbare data is groot. Van dit risico zijn steeds meer organisaties zich bewust. Om deze data te verzekeren is een geoptimaliseerde dekking noodzakelijk. Hiervoor bestaan aanvullende verzekeringsoplossingen waarmee de gangbare brand- en/of elektronicaverzekering is uit te breiden.

Conclusies

- Er zijn uiteenlopende verzekeringen op de markt om de financiële gevolgen van digitale risico's te beperken.
- Welke verzekeringsvorm het beste aansluit bij een organisatie hangt sterk samen met de vraag voor welke specifieke risico's dekking nodig is.
- Nieuwe cyberverzekeringen zijn in ontwikkeling, maar sluiten nog niet altijd volledig aan op de behoeften.

5 Bestrijden van digitale incidenten

Naast een grote verscheidenheid aan digitale incidenten zijn er ook negatieve bijverschijnselen in alle soorten en maten. Van problemen om klant- en contractuele verplichtingen na te komen tot negatieve publiciteit in gedrukte en online (sociale) media. Een belangrijk kenmerk van dit soort incidenten is dat wat als een ICT-vraagstuk begint al snel de gehele organisatie beïnvloedt. De vraag wat een cyberincident voor een organisatie betekent, wordt hier beantwoord.

Wat kenmerkt een cyberincident?

Ondanks de grote diversiteit aan ongewenste cyberincidenten, bestaat er een aantal opvallende kenmerken. Aon spreekt in dit verband over de zes 'O's':

1. Onzichtbaar

Een cyberincident blijft vaak (lang) onzichtbaar, in tegenstelling tot bijvoorbeeld een bedrijfsongeval. Dit maakt het lastig om een crisissituatie onmiddellijk te herkennen. Hierdoor wordt de urgentie ervan, onterecht, minder gevoeld. Dit geldt ook voor het inschatten en overzien van de gevolgen van een cyberincident.

2. Omvangrijk

De ervaring leert dat de effecten van een cyberincident omvangrijk zijn. En juist door de aanzienlijke afhankelijkheid van ICT en data, zijn de gevolgen van een cyberincident snel op grote schaal merkbaar. Daarbij vergroten (sociale) media meestal de omvang van een incident.

3. Onduidelijk

Een cyberincident heeft doorgaans een 'modern technologisch karakter'. In de praktijk blijkt dan ook dat het voor niet-techneuten moeilijk is een dergelijk incident te overzien, laat staan te begrijpen of op te lossen.

4. Opzettelijk

Moedwillig handelen door criminelen is bij een cyberincident nooit uit te sluiten.

5. Onbegrensd

Cyberincidenten zijn per definitie grensoverschrijdend. De effecten blijven vrijwel nooit beperkt tot één afdeling of onderdeel van de organisatie. Vanwege de toenemende afhankelijkheid van systemen ervaren ook andere organisaties al snel de effecten van een cyberincident. Bovendien zijn deze effecten letterlijk onbegrensd: wat als een lokaal issue begint, heeft al snel internationale gevolgen.

6. Onzeker

Elk incident kenmerkt zich door onzekerheid. De eerste vijf 'O's' maken dit nog het beste duidelijk. Ondanks de hoge mate van onzekerheid vergt een cyberincident snel en adequaat handelen van de betrokkenen.

Bestrijden van cyberrisico's met crisismanagement

Crisismanagement biedt uw onderneming een hulpmiddel om digitale incidenten, issues en crises snel en effectief te bestrijden. Zo wordt uw organisatie niet overrompeld door de acute dreiging, de daarmee gepaard gaande urgentie en de eerder geschetste onzekerheid. Wat namelijk kenmerkend is aan crises, is dat deze ook patronen en regelmatigheden vertonen. Sterker nog, als u een crisis benadert als een proces, vallen er duidelijk interventiemogelijkheden te identificeren. En ondanks dat het vaak lijkt alsof een crisis verlies aan regie impliceert, kunt u ook in het oog van de storm, de windrichting veranderen, deze doen afnemen óf zelfs voorblijven.

Hoewel crises qua karakter sterk kunnen variëren, zijn er basisregels en wetmatigheden die u zeker moet kennen. Het vertrouwen in organisaties en bestuurders kan door een crisis namelijk zwaar onder druk komen te staan. Vaak ligt het vergrootglas op de organisatie waardoor zelfs dagelijkse werkzaamheden niet volgens hun normale routine kunnen worden uitgevoerd. De ruimte die een organisatie krijgt - de 'license to operate' - neemt snel af. Onzekerheid, tijdgebrek en de noodzaak tot het nemen van beslissingen kenmerken de situatie. En er moet vaak worden samengewerkt met veel (en nieuwe) partijen. Crisismanagement stelt uw onderneming in staat om de noodzakelijke – veelal non-routine – reactie vooraf te stroomlijnen en voor te bereiden.

Minimumvereisten voor effectief management van cybercrises

Om u een indruk te geven van wat voor een snel reagerende en effectief opererende crisismanagement-organisatie van belang is, presenteren wij hieronder een aantal 'minimumvereisten'.

- Hoger management onderkent het belang van crisismanagement.
- Eén of enkele functionarissen zijn aangewezen voor het beheer en de (door)ontwikkeling van de crisis-managementorganisatie.
- Er is een crisismanagementorganisatie ingericht.
- Er zijn geschikte functionarissen geselecteerd als lid van de crisismanagementorganisatie.
- Er is een crisismanagementplan opgesteld, dat rekening houdt met de bijzonderheden die zich voor kunnen doen.
- Leden van de crisismanagementorganisatie worden periodiek getraind en geoefend.

Conclusies:

- Cyberincidenten kunnen veel gedaantes aannemen en zijn onvoorspelbaar. Voor een organisatie kunnen de ongewenste effecten groot zijn, naast financiële schade en imagoschade.
- Crisismanagement helpt het niveau van voorbereiding van een organisatie op digitale risico's te verhogen. Zo kunnen oorzaken en gevolgen van een cyberincident snel worden weggenomen en de normale bedrijfsvoering snel worden hersteld.

6 Praktische adviezen

Afsluitend geven we een serie praktische adviezen die eraan bijdragen cyberrisico's het hoofd te bieden. Leidend hierin zijn de drie stappen die we binnen de aanpak van cyberrisicomanagement hanteren: analyseren, beheersen en bestrijden.

Analyseren

- Maak een zorgvuldige inventarisatie van de cyberrisico's die voor uw organisatie relevant zijn ('treat & transfer') en zorg dat medewerkers zich hiervan bewust zijn.
- Richt een cyberrisicomanagementsysteem in. Of integreer cyberrisico's in uw risicomanagementactiviteiten.
- Laat de verantwoordelijkheid voor cyberrisico's niet liggen bij de afdeling ICT of security. Het betreft een organisatiebrede verantwoordelijkheid, van werkvloer tot management.

Beheersen

- Laat de verzekeringsportefeuille beoordelen op dekking tegen cyberrisico's.
- Verken het nut en de noodzaak voor het afsluiten van een fraudeverzekering met adequate dekking voor computerfraude.

- Check de bestaande (beroeps)aansprakelijkheidsverzekering op dekking van cyberrisico's.
- Houd bij verlenging van een schadeverzekering ook rekening met de waarde van de elektronische data die de onderneming beheert. Let dus niet alleen op de waarde van de hardware.
- Besef dat bestuurders en commissarissen in toenemende mate mederisicodrager zijn van cyberrisico's. Overweeg een aansprakelijkheidsverzekering voor bestuurders af te sluiten.
- Voer een business impact analyse uit om duidelijk te krijgen welke gevolgen cyberrisico's kunnen hebben voor uw organisatie.
    - Gebruik hiervoor een scenariobenadering en ga zeker niet voorbij aan het 'worst case scenario'.
    - Ken de bedrijfsprocessen die het meest gevoelig zijn voor cyberrisico's. Ken ook uw afhankelijkheden buiten de organisatie, bijvoorbeeld van derden en overheden.
    - Ontwikkel een strategie om de gevolgen van uitval, onbetrouwbaarheid of onveiligheid te beheersen. Doe dit bijvoorbeeld in de vorm van een Business Continuity Plan (BCP) gericht op cyberrisico's.

Bestrijden

- Bereid uw incident- en crisismanagement toereikend voor.
    - Besteed in een incident- of crisismanagementplan aandacht aan wat uw organisatie in het geval van een incident of crisis nodig heeft.
    - Selecteer geschikte functionarissen, garandeer hun bereikbaarheid, beschikbaarheid en vervanging.
    - Train leden van de crisismanagementorganisatie periodiek, óók op cyberrisico's.
- Focus tijdens een cyberincident op de kernactiviteiten van uw organisatie. Draag daarbij zorg voor inzicht in impact op derden (zoals afnemers en leveranciers) van het cyberincident. Pas stakeholdermanagement actief toe.
- Bestrijdt een cyberincident niet alleen vanuit technisch perspectief en met behulp van technische middelen. Werk vanuit een bedrijfsbreed perspectief en weeg technische belangen altijd af tegen bredere organisatiebelangen. De beste technische oplossing is niet noodzakelijk de beste oplossing voor uw organisatie.
- Wacht bij ICT-incidenten nooit op dé kant-en-klare oplossing. Houdt altijd rekening met een vertraagde, gedeeltelijke of tijdelijke oplossing van de technische problemen en draag zorg voor een adequate (tijdelijke) aansluiting van de kernactiviteiten hierop.
- Zorg ervoor dat het crisismanagement zoveel mogelijk 'plug and play' is uitgevoerd. Dit organiseert u door in uw keuze van crisismanagementprocessen en -middelen, onder meer, passende uitwijkvoorzieningen te treffen.

Tot slot

Problemen rondom dataveiligheid zijn aan de orde van de dag. De bescherming van data schuift dan ook snel op in de top 10 van belangrijkste bedrijfsrisico's. Cybercrime en datalekken halen regelmatig de media met soms grote financiële gevolgen en imagoschade. Actie is geboden om met innovatieve oplossingen deze nieuwe risico's beheersbaar te maken. Aon kan u hierbij met haar kennis en ervaring helpen, zodat u zich kunt concentreren op de bedrijfsvoering en op de dienstverlening aan burgers of klanten. Met een duidelijke visie en adequate aanpak brengt u de cyberrisico's onder controle.

Peter Hartman

Peter Hartman is Managing Director Innovation binnen Aon Risk Solutions. In deze rol is hij verantwoordelijk voor het ontwikkelen van nieuwe ideeën en oplossingen, die van toegevoegde waarde zijn voor onze relaties. Heeft een brede kennis van het bedrijfsleven en de verzekeringsmarkt en is nauw betrokken bij de introductie van nieuwe producten en diensten.

Mark Braam

Mark Braam is Senior Consultant binnen Aon Global Risk Consulting. Mark begeleidt bedrijven bij de implementatie en optimalisatie van de (cyber)risicomanagementprocessen. Daarbinnen is Mark altijd op zoek naar efficiency en effectiviteit van het proces, de daaruit voortvloeiende beheersmaatregelen en aansluiting met overige initiatieven. Voordat Mark in 2007 bij Aon kwam was hij Information Security Officer en Risk Manager bij Sanoma Media.

Dennis de Hoog

Dennis de Hoog is als senior adviseur werkzaam bij het COT Instituut voor Veiligheids- en Crisismanagement, an Aon company. Dennis adviseert sinds 2004 een grote verscheidenheid aan opdrachtgevers in het bedrijfsleven over risicomanagementvraagstukken en -oplossingen. Dennis is gespecialiseerd in crisis-, security- en continuïteitsmanagement.

Bart Claessens

Bart Claessens is sinds 2007 werkzaam bij Aon. Hij is momenteel broking director binnen het departement Financial Institutions Benelux en werkt vanuit de Aon-kantoren in Rotterdam en Brussel. In deze functie bemiddelt hij onder meer aansprakelijkheids- en fraudeverzekeringen voor internationale banken, verzekeraars en pensioenfondsen.

Contact

Voor meer informatie over de inhoud van deze whitepaper en de oplossingen die Aon kan bieden, kunt u contact opnemen met:

Peter Hartman T **020 430 5051**
E **peter.hartman@aon.nl**

www.aon.nl

Over Aon en COT

Aon Nederland, toonaangevend adviseur in risicomanagement, employee benefits en verzekeringen, draagt bij aan het realiseren van de ambities van zijn cliënten. In Nederland heeft Aon 10 vestigingen met 1.900 medewerkers. Het bedrijf maakt deel uit van Aon plc in Londen, Verenigd Koninkrijk. Het wereldwijde Aon-netwerk omvat circa 600 kantoren in meer dan 120 landen en telt ruim 61.000 medewerkers. Hiermee is Aon een van de grotere financiële dienstverleners ter wereld. Aon plc is gespecialiseerd in financiële en verzekeringsdienstverlening en staat genoteerd aan de effectenbeurs van New York (NYSE). Aon is hoofdsponsor van Manchester United, lees hierover op www.aon.com/manchesterunited. Meer informatie over Aon: www.aon.nl.

Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismanagement. Ons werkterrein strekt zich uit van vraagstukken over security ambities en de vormgeving van lokaal veiligheidsbeleid tot de voorbereiding op crisissituaties. Met onze kennis en kunde helpen we opdrachtgevers in complexe situaties waarbij grote risico's worden gelopen, strategische belangen op het spel staan en vaak vele stakeholders zijn betrokken. Advies, onderzoek, en training en oefening vormen de basis van onze dienstverlening. Het COT opereert vanuit Den Haag en is een volledige dochteronderneming van Aon Nederland. Meer informatie: www.cot.nl

7152-V4-Cyber-WP

COT | Instituut voor Veiligheids- en Crisismanagement

AON