Artikel Cyberrisico's
Tekst Mr.drs. Pieter Steenwijk
Beeld 123RF®

De cyberrevolutie is onverbiddelijk en voltrekt zich in hoog tempo. Dit artikel zet de relevantie van cyberrisico's en een handzame aanpak voor de beheersing ervan uiteen.

Stairway to digital heaven

De digitale revolutie voltrekt zich in hoog tempo. Naar verwachting zullen er in 2020 meer dan 20 miljard laptops, mobiele telefoons en tablets met elkaar verbonden zijn tot een gigantisch wereldwijd netwerk. Spoedig zullen we voortdurend en overal verbonden zijn met internet. De virtuele ruimte die ontstaat uit de complexe interactie van mensen, technologie, software, en dienstverlening over het internet wordt steeds vaker cyberspace genoemd.[1]

Onbeperkte kansen

Nederland is een koploper in het gebruik van mobiele apparaten, internetaankopen en het benutten van online-diensten.[2] De cybersamenleving biedt onbeperkte kansen, nieuwe manieren van communiceren, leren, werken, gamen en carrièremogelijkheden. Bedrijven kunnen hun productiviteit, concurrentievermogen en zichtbaarheid vergroten door op een verstandige manier gebruik te maken van cyberkansen. Daar tegenover staan grote risico's zoals cyberpesten, grooming (online sexueel misbruik van minderjarigen), online diefstal en bedrog, het doorspelen van vertrouwelijke informatie door corrupte agenten en het faciliteren van van terrorisme en witwassen.

Vrijwel alle grote bedrijven hebben de afgelopen jaren te maken gehad met online aanvallen, virussen, datalekken en digitale afpersing. De kosten van deze inbreuken op de digitale integriteit namen de afgelopen jaren fors toe en bedragen in Nederland jaarlijks ongeveer 10 miljard euro.[3] Dit verklaart ook waarom cyber risk het grootste auditrisico voor internal auditors is geworden.[4]

Effectief beheersen is strategische noodzaak

De cyberrevolutie valt niet te stoppen. Organisaties zullen steeds meer afhankelijk worden van online dienstverlening en hun netwerken zullen steeds verder integreren. Het effectief beheersen van de digitale kansen en risico's is daarmee een strategische noodzaak geworden. Stakeholders verwachten dat bedrijven passende maatregelen nemen om hun online activiteiten te beschermen en digitale bedreigingen serieus nemen. Er staat ook veel op het spel bij digitaal mismanagement: reputatieverlies, het missen van kansen in de markt, complianceproblemen met overheden en toezichthouders, verlies van data en intellectueel eigendom en tenslotte verslechtering van de relaties met stakeholders.

Het Institute of Risk Management (IRM) definieert cyber risk als: 'Any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems'.[5] Het IRM onderscheidt vijf verschillende dreigingsactoren die de motor vormen achter cyberrisico's:

1. *activisten* (ook wel hacktivisten genoemd) die vooral ideologisch of politiek zijn gemotiveerd;
2. *cybercriminelen* die organisaties en bedrijven aanvallen om er financieel beter van te worden;
3. *vijandige spionnen* ('hostile spies') die worden aangestuurd door buitenlandse regeringen;
4. *insiders,* eigen medewerkers die bewust of onbewust om verschillende redenen fouten maken of bewust schade aanrichten;
5. *slechte IT-systemen* die door ontwerpfouten, verouderde software, onvoldoende support etc. de organisatie kwetsbaar maken voor dreigingsactoren.[6]

In de traditionele benadering werd het beheersen van cyberrisico's beschouwd als een technisch vraagstuk dat thuishoort bij de IT-afdeling. Deze benadering is inmiddels achterhaald. Volgens de gangbare opvatting kunnen cyberrisico's het best worden beheerst binnen het raamwerk van de organisatiebrede enterprise risk (ERM) raamwerk.[7]

Onzekerheid voor organisaties

Zo op het oog heeft cyber risk management (CRM) ook veel gemeen met andere vormen van riskmanagement op het gebied van IT, data security en privacy. Maar CRM onderscheidt zich van andere risicodisciplines door een aantal specifieke kenmerken. In de eerste plaats verandert de technologie voortdurend en in hoog tempo. Dit heeft grote impact op de strategie en de doelstellingen van organisaties. De dynamiek van de technologische ontwikkelingen creëert veel onzekerheid voor organisaties. Wanneer is het verstandig om een nieuwe technologie over te nemen, welke kansen biedt het en welke risico's zijn eraan verbonden? Daarnaast zijn er risico's met zeer grote impact op de organisatie, waarvan het zo goed als onmogelijk is om ze tijdig te voorzien dan wel een zinvolle inschatting van de kans van optreden te kunnen maken.[8] Deze 'black-swan'risico's kunnen gemakkelijk over het hoofd worden gezien of worden gebagatelliseerd als gevolg van misplaatst vertrouwen in de eigen beheersingsmaatregelen.
Ten slotte heeft de digitale revolutie ervoor gezorgd dat de grens tussen privé en werk allengs aan het vervagen is. Medewerkers werken steeds meer met hun eigen tablets en mobiele telefoons, of gebruiken de zakelijke IT-voorzieningen ook voor persoonlijke doeleinden (filmpje downloaden, chatten, et cetera). Het voordeel voor de organisatie is dat medewerkers flexibeler kunnen worden ingezet, buiten werktijd bereikbaar zijn en op een natuurlijke wijze vertrouwd raken met nieuwe technologie. De keerzijde is dat al dat gechat en het gebruik van eigen apparatuur ook veiligheidsrisico's met zich mee kan brengen.

Hoog op de corporate agenda

Door de combinatie van snelle technologische, stijgende kosten van cybercrime en de bescherming tegen langetermijnreputatieschade staat cyberrisicomanagement hoog op de corporate agenda. Na compliance is kwetsbaarheid voor cyberaanvallen het belangrijkste zorgpunt voor raden van bestuur in de financiële sector.[9] Veel organisaties, overheden en toezichthouders worstelen echter met de vraag op welke manier de risico's en de kansen op een evenwichtige wijze kunnen worden

NIST CYBER SECURITY FRAMEWORK

Identify	Protect	Detect	Respond	Recover
Asset management	Access control	Anomalies & events	Response planning	Recovery planning
Business environment	Awareness & training	Security continuous monitoring	Communications	Improvements
Governance	Data security	Detection processes	Analysis	Communications
Risk management	Info protection process & procedures		Mitigation	
Risk management strategy	Maintenance		Improvement	
	Protective technology			

Figuur 1. NIST cyber security framework

afgewogen. In Nederland ontbreekt het bij de meerderheid van de bedrijven aan een solide, overkoepelende cyberrisicostrategie en is de board onzeker over de effectiviteit van de investeringen in technologische beheersmaatregelen. Ook in de publicatie *Cybersecuritybeeld Nederland* wordt met zorg geconstateerd dat het gat tussen cyberdreiging en weerbaarheid is gegroeid en de digitale kwetsbaarheid ondanks alle inspanningen over de gehele linie is toegenomen.

Top-7 verstandige algemene randvoorwaarden

Bedrijven bevinden zich tussen de Scylla en Charibdes van de online revolutie. Wie niet bereid is om alle technologie overboord te gooien, moet op zoek naar een passende vorm van cyberrisicomanagement. Naast de standaardsystemen zijn er talrijke tools, checklisten, stappenplannen, technische systemen, handige vragenlijsten, quick reference cards en specifieke diensten van advieskantoren beschikbaar. Uit dit aanbod kan een Top-7 van verstandige algemene randvoorwaarden voor effectief cyberrisicomanagement worden afgeleid.

1. Bepaal de cyber risk en opportunity appetite van de organisatie en communiceer het daaruit voortvloeiende risicoprofiel op maat met in- en externe stakeholders.
2. Maak een lijst met de bedrijfsmiddelen die de grootste toegevoegde waarde voor online activiteiten hebben en hun kwetsbaarheid voor cyberdreigingen.
3. Identificeer en implementeer basale beheersmaatregelen. Dit voorkomt tot 85% van alle cyberaanvallen.
4. Investeer zowel in preventieve beheersing maar ook in robuuste incident response procedures (IRP) om reputatieschade te voorkomen.
5. Ken de oorzaken en kwetsbaarheden van cyberrisico's en identificeer de kosten-opbrengsteneffecten van beheersingsmaatregelen.
6. Besteed voldoende aandacht aan de menselijke aspecten, zoals de risicopercepties van in- en externe stakeholders. De effectiviteit van technische controls (firewalls, encryptie, et cetera) wordt medebepaald door acceptatie en het bewustzijn van gebruikers.
7. Beheers cyberrisico's vanuit het overkoepelende risk management en niet stand-alone.

ERM of stand-alone?

Schade door cyberrisico kan gemakkelijk uitwaaieren buiten de directe operationele en financiële impact. Een geslaagde hackoperatie kan uiteindelijk de reputatie van een bedrijf voor jaren aantasten, klanten wegjagen en een wezenlijk gevaar voor de continuiteit teweegbrengen. Juist omdat cyberrisico's gemakkelijk kunnen cascaderen naar andere enterprise-riskcategorieën is het effectiever en goedkoper om ze te beheersen als onderdeel van het brede enterprise riskmanagement. De belangrijkste risicostandaarden hebben cyber in hun algemene riskfocus opgenomen. Zowel COSO, COBIT als IRM hebben leidraden en algemene adviezen gepubliceerd die

organisaties kunnen helpen om het management van cyberrisico's op een lijn te brengen met de eigen standaard. ISO Standaard 27032-IEC-2012 bevat een aantal uitgangspunten en richtlijnen voor het beheersen van cyberrisico's. In tegenstelling tot ISO 27001-IEC voor information security management (ISMS) leidt invoering van de cyber securitystandaard niet tot certificering. ISO 27001 (met een uitgebreide catalogus van controlmaatregelen) en ISO-IEC 27032 (met een specifieke lijst van bedrijfsmiddelen met focus op cyber risk en incident response) in combinatie met de algemene van 27005 is een bewerkelijke, maar interessante optie.

NIST cybersecurity framework

Voor wie liever een op cyber risk toegesneden raamwerk prefereert, is er het NIST cybersecurity framework (NIST CF) dat in 2014 ontwikkeld is om de vitale infrastructuur van de Verenigde Staten te beschermen tegen cyberdreigingen (zie *figuur 1*).

NIST bestaat uit drie onderdelen, te weten 1) de kern, 2) de implementatieniveaus, 3) profiel.

1. Kern: de kern bestaat uit de vijf functies (identificeren-beschermen-detecteren-respond-recover) waarmee de cyberrisico's worden beheerst. De functies zijn onderverdeeld in 22 activiteiten (assetmanagement, data security, response planning, et cetera) die de ruggengraat van een solide cyber riskmanagementsysteem vormen. De activiteiten kunnen worden opgedeeld in subactiviteiten. De subactiviteiten zijn weer opgedeeld in best practices, standaarden en richtlijnen gebaseerd op COBIT, ISO 2700, ISA 62443, et cetera.
2. Implementatie: implemenatie gebeurt in een iteratief proces waarin de 'isst en soll' centraal staan. Het model onderscheidt vier fasen (partieel, risk informed, repetetief en adaptief) voor het markeren van de huidige situatie en het formuleren van het ambitieniveau.
3. Profiel: waarin cyberstrategie, risk appetite en governance samenvallen en fungeert als monitorings, plannings, en communicatie-instrument.

NIST is een overzichtelijk, holistisch, technologisch onafhankelijke aanpak op basis van best practices en andere standaarden. Het volgt de ERM-benadering en is bruikbaar voor elke organisatie, ongeacht sector of omvang. Het is een flexibele, kosteneffectieve benadering die naast – en dus niet in plaats van – de bestaande risicobenadering wordt ingezet. Op de website worden best practices, casestudies, en algemene adviezen gedeeld. In de Verenigde Staten is NIST aan een indrukwekkende opmars bezig. Naar verwachting zal de helft van alle bedrijven in de Verenigde Staten op termijn de aanpak toepassen.

Conclusie

De toekomst is digitaal. De komende jaren zullen het internet of things, het gebruik van social media en de uitbreiding van oplossingen in de cloud de bestaande businessmodellen en risicopercepties ingrijpend op de proef stellen. De enige manier om digitale risico's volledig te neutraliseren is door alle online activiteiten stop te zetten. Zoals Bill Gates al een decennium geleden in Davos opmerkte; "In de 21e eeuw zullen er slechts twee typen bedrijven zijn, bedrijven die op internet zitten en bedrijven die het loodje zullen leggen". Voor riskmanagers en auditors ligt er de nobele taak om te kijken op welke wijze cyberrisicomanagement effectief kan worden ondergebracht binnen de overkoepelende benadering van de organisatie. <<

De enige manier om digitale risico's volledig te neutraliseren is door alle online activiteiten stop te zetten

Noten

1. https://www.iso.org/standard/44375.html
2. https://tweakers.net/nieuws/97212/google-nederland-heeft-hoogste-tablet-en-laptopgebruik.html
3. Deloitte, *Cyber Value at risk in the Netherlands 2017,* 2017.
4. KPMG, Top 10 Internal Audit Considerations, 2017. https://home.kpmg.com/nl/nl/home/insights/2017/01/top-10-internal-audit-considerations.html
5. Institute of Risk Management, Cyber Risk, 2014. www./.theirm.org/media88344/final_IRM_Cyber_Risk-Executive Summary_A5_low-res.pdf
6. Zie onder meer: https://www.coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf.
7. Zie onder meer: Philpott, D. en S. Ganz, *FISMA and the Risk Management Framework: The new practice of federal cyber security,* Syngress Media, 2012.
8. Zie: Taleb N.N., *The black swan: The impact of the highly improbable.* Random House, 2007.
9. Deloitte, *2016 Financial Servics Survey*, 2016.

Pieter Steenwijk is jurist en bedrijfskundige en is docent risicomanagement. Hij doet onderzoek naar witwassen en terrorismefinanciering aan de The Hague School of Applied Sciences en is promovendus aan de Universiteit van Maastricht.