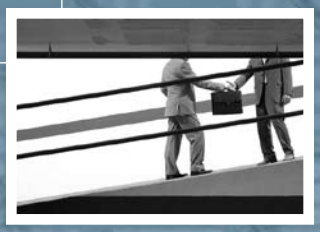
McAfee

# Onbeveiligde Economieën: Vitale Informatie Beveiligen

Het eerste wereldwijde onderzoek naar de kwetsbaarheden van 's werelds intellectuele eigendommen en gevoelige informatie.



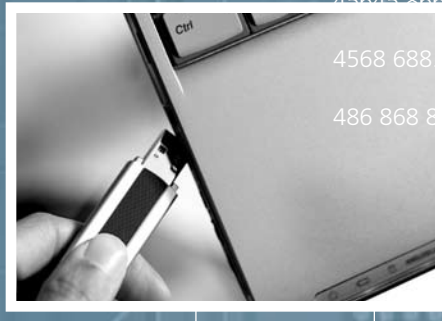
454868.45 5 48

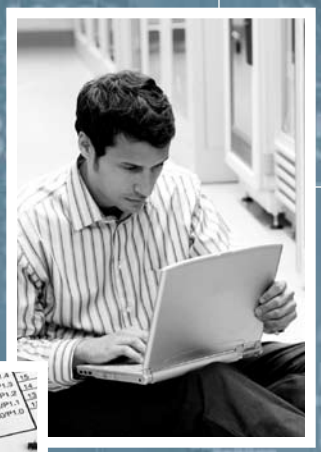
89 8 488.5545 6896

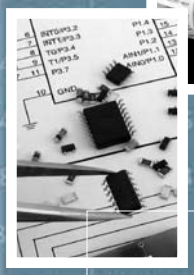
45645 866 665

4568 688 54 58

486 868 8





454868.45 5 48 4528782

89 8 488.5545 6896

44 822.656

4568 45 4582 688.54 58

486 86484 8 8

# INHOUD



**Bijdragen**


Nick Akerman
Dr. Ross Anderson, PhD
Dr. Ashish Arora, PhD
Augusto Paes de Barros
Renato Opice Blum
Lynn Robert Carter
Lilian Edwards
Gail F. Farnsley
Dr. Marco Gercke
Karthik Kannan
Sivarama Krishnan
Heejo Lee
Tom Longstaff, PhD
Jacquelyn Rees
Dr. Timothy J. Shimeall, PhD
Eugene H. Spafford
Professor Yoshiyasu Takefuji, PhD
Professor Katsuya Uchida, PhD
Michael Versace
Dr. Sun Yuqing, PhD

# Voorwoord

Nu we een van de ernstigste recessies van de laatste decennia beleven, is het beveiligen van de cruciale informatie als bedrijfseigendom, zoals intellectuele eigendommen en gevoelige gegevens, nog nooit zo belangrijk en tegelijk zo problematisch geweest. Eén beveiligingsincident of gegevensverlies kan onherstelbare financiële schade toebrengen aan de reputatie van een bedrijf, de aandelenkoers en het klantvertrouwen. Het is een risico dat bedrijven zich in het huidige klimaat niet kunnen veroorloven.

Hoe groot is het gevaar dat bedrijven intellectuele eigendommen en gevoelige gegevens verliezen die de basis voor hun succes vormen? Welke landen ontwikkelen zich onmiskenbaar als dreigingsbron voor vitale informatie? En hoe kon de economie nieuwe dreigingen in het leven roepen?

McAfee besloot deze vragen grondig te onderzoeken en ging in allerlei landen te rade bij hooggeplaatste IT-besluitvormers van 1000 grote ondernemingen en tientallen beveiligings- en bedrijfsdeskundigen van topinstituten. De bevindingen waren opmerkelijk. McAfee is van mening dat de onderzoeksresultaten niet te licht mogen worden opgevat.

De ondervraagde bedrijven schatten dat ze in 2008 gemiddeld 4,6 miljoen dollar aan intellectuele eigendommen hebben verloren. Volgens 42 procent van de respondenten vormen ontslagen werknemers in het huidige economische klimaat de grootste dreiging voor intellectuele eigendommen en andere gevoelige gegevens.

Intellectuele eigendommen en gevoelige gegevens zijn een sterk ruilmiddel geworden voor in financiële problemen verkerende of ontslagen werknemers. Cybercriminelen zien deze vitale informatie ook als hoogwaardig product en bedenken steeds sluwere manieren om via werknemers in bedrijven te infiltreren. Tot slot ontwikkelen China, Rusland en Pakistan zich als onmiskenbare dreigingsbronnen voor vitale bedrijfsgegevens.

McAfee stelt zich ten doel bedrijven en overheden te helpen bij het beschermen van hun vitale informatie. Wij weten dat technologie alleen niet het antwoord is. Wij hebben daarom onlangs, als onderdeel van McAfee's initiatief om cybercriminaliteit te bestrijden, een wereldwijde cybercriminaliteitsraad opgericht, bestaande uit bedrijfsleiders en CIO's. Het is de bedoeling dat deze raad aangeeft wat McAfee moet doen om organisaties beter tegen deze meervoudige dreigingen te beschermen.

Dit rapport is voor mij een tijdige wake-upcall dat bedrijven hun houding ten opzichte van intellectuele eigendommen en andere gevoelige informatie moeten aanpassen.

Dave DeWalt
President & CEO
McAfee, Inc.

# Inleiding

De economische recessie legt een zware druk op bedrijven over de hele wereld en de onzekerheid wordt nog verergerd door de grote risico's die het gevolg zijn van gegevenslekkage, gegevensverlies en aanvallen van buitenaf. Deze risico's zijn in het afgelopen jaar aanzienlijk toegenomen.

Welke invloed heeft de huidige economische recessie op het vermogen van organisaties om vitale informatie, zoals intellectuele eigendommen, te beschermen? Welke landen vormen de grootste bedreiging voor de economische stabiliteit in andere landen? Met welke middelen richten cybercriminelen zich op ondernemingen in allerlei landen? Hoe kan de beveiliging van digitale bezittingen het komend jaar een wereldwijd economisch herstel bevorderen of belemmeren?

McAfee heeft, in samenwerking met deskundigen op het gebied van gegevensbeveiliging en intellectuele eigendommen, geprobeerd een antwoord op deze vragen te geven. In opdracht van McAfee hebben de professors Karthik Kannan, Jacquelyn Rees en Eugene H. Spafford van de universiteit van Purdue en het CERIAS (Center for Education and Research in Information Assurance and Security) samen met experts uit de hele wereld een diepgaand onderzoek uitgevoerd.

Internationaal onderzoeksbureau Vanson Bourne heeft meer dan 1000 hooggeplaatste IT-besluitvormers in de VS, het VK, Japan, China, India, Brazilië en het Midden-Oosten ondervraagd en aan de hand van de resultaten het tot nu toe meest uitvoerige onderzoek naar dit onderwerp samengesteld.

Het resultaat *"Onbeveiligde economieën: vitale informatie beveiligen"* geeft aan in welke mate de economische recessie de beveiliging van vitale informatie zal beïnvloeden, terwijl CIO's proberen cruciale informatie in verschillende continenten en bedrijven veilig te stellen. Informatie wordt steeds meer als een soort internationale valuta gezien en cybercriminelen richten hun aanvallen steeds vaker op bedrijven. Dreigingsbronnen veranderen en er komen nieuwe landen bij die als mogelijke bedreiging voor de veiligheid van gegevens worden gezien.

Het rapport wordt afgesloten met een aantal aanbevolen procedures voor de beveiliging van waardevolle digitale bezittingen, niet alleen om te overleven, maar ook om te groeien, ondanks deze moeilijke tijden.

## Vier belangrijke bevindingen

1: Uit het onderzoek blijkt dat vitale digitale informatie, zoals intellectuele eigendommen en gevoelige klantgegevens, steeds vaker tussen bedrijven en continenten heen en weer wordt gezonden waardoor de kans op verlies van deze informatie aanzienlijk toeneemt. Een gemiddeld bedrijf heeft 12 miljoen dollar aan gevoelige informatie in het buitenland. In 2008 verloren bedrijven gemiddeld 4,6 miljoen dollar aan intellectuele eigendommen.

2: De wereldwijde economische crisis veroorzaakt grote risico's voor de informatiebeveiliging. Bedrijven zien zich genoodzaakt hun uitgaven te verlagen en personeel te ontslaan, met als gevolg gaten in de verdediging en meer kansen voor cybercriminelen. Ontslagen werknemers vormen volgens 42 procent van de respondenten de grootste dreiging die rechtstreeks aan de economische recessie kan worden toegeschreven.

3: Bepaalde landen ontwikkelen zich onmiskenbaar als dreigingsbron voor gevoelige gegevens, met name voor intellectuele eigendommen. Geopolitieke denkbeelden hebben invloed op het feitelijke gegevensbeleid. China, Pakistan en Rusland worden om verschillende juridische, culturele en economische redenen als probleemgebieden aangewezen.

4: Cyberdieven zijn de fase van het hacken en stelen van creditcardgegevens en aanmeldingsgegevens voorbij. Intellectuele eigendommen vormen een nieuw doel. Waarom zoveel tijd en geld aan onderzoek en ontwikkeling besteden als je deze ook gewoon kunt stelen?

# BELANGRIJKE BEVINDING 1:

## kostbare gegevens worden verplaatst en vervolgens verloren

Uit het onderzoek blijkt dat vitale digitale informatie, zoals intellectuele eigendommen en gevoelige klantgegevens, steeds vaker tussen bedrijven en continenten heen en weer wordt gezonden. Het onderzoek geeft tevens aan dat er tijdens dit proces veel informatie verloren raakt.

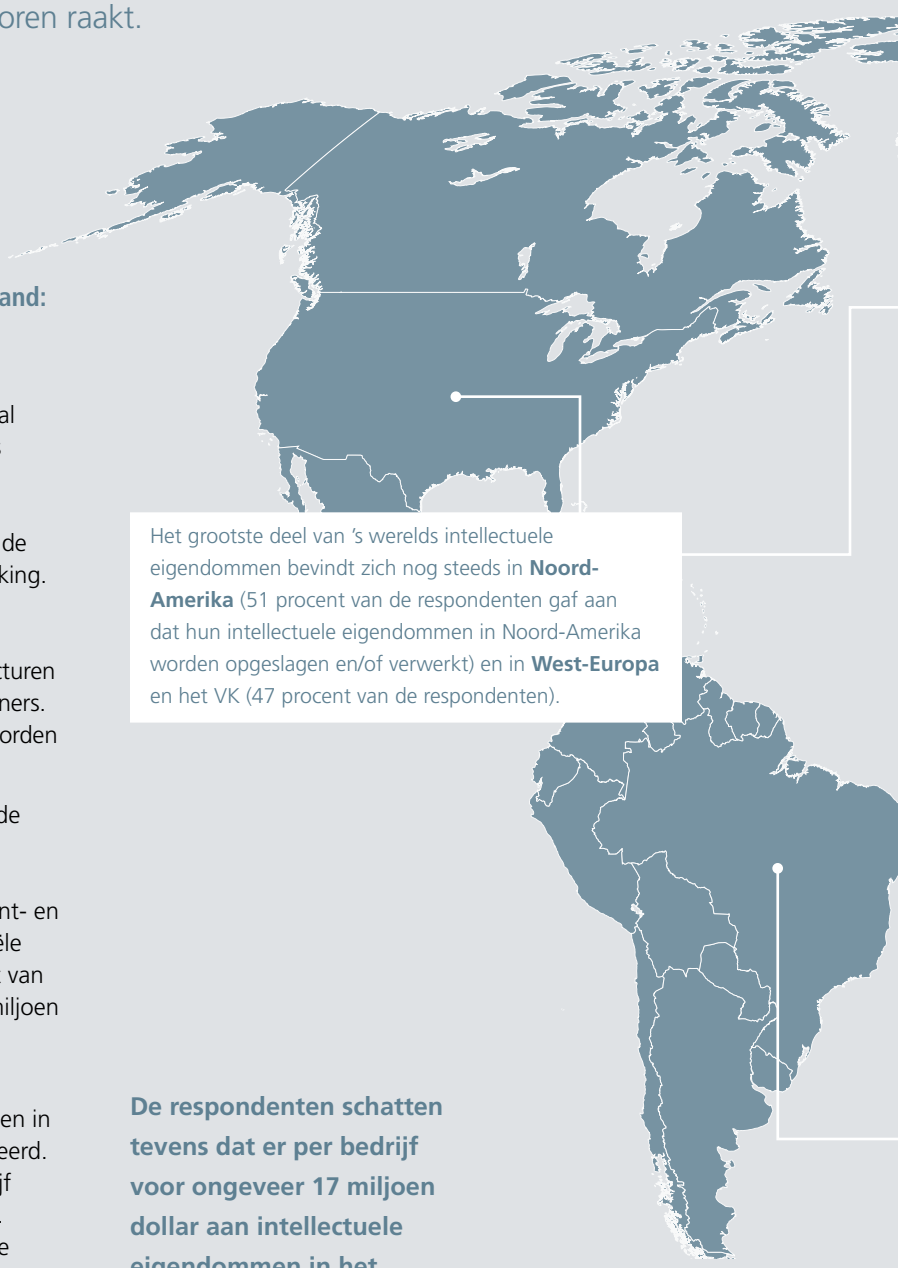
### Het groeiende bedrijfsrisico voor intellectuele eigendommen

#### De verspreiding van vitale informatie in het buitenland: een gemiddeld bedrijf heeft 12 miljoen dollar aan gevoelige informatie in het buitenland

Volgens Michael Versace, senior adviseur bij FSTC (Financial Services Technology Consortium), is de operationele grens van organisaties (die hij de "vertrouwensgrens" noemt) aanzienlijk verlegd. Veel bedrijven hebben tegenwoordig dochterondernemingen en buitenlandse vestigingen over de hele wereld en een toenemende behoefte aan samenwerking. Deze omstandigheden leiden tot het verdwijnen van de traditionele operationele grens. Informatiebezittingen zijn onderworpen aan verschillende rechtsgebieden, infrastructuren en culturen, met inbegrip van die van leveranciers en partners. Hierdoor kunnen intellectuele eigendommen moeilijker worden vergrendeld om de veiligheid ervan te waarborgen.

Het onderzoek bevestigt deze bewering. De ondervraagde wereldwijde bedrijven geven aan dat hun gevoelige informatie in het buitenland een waarde van gemiddeld 12 miljoen dollar vertegenwoordigt. Denk hierbij aan klant- en creditcardgegevens, intellectuele eigendommen, financiële gegevens en juridische documenten. Het bedrag varieert van 8,2 miljoen dollar voor een Japans bedrijf tot wel 15,2 miljoen dollar voor een bedrijf in het VK.

De respondenten schatten tevens dat er per bedrijf voor ongeveer 17 miljoen dollar aan intellectuele eigendommen in het buitenland wordt opgeslagen, geraadpleegd en beheerd. Dit bedrag varieert van 1,4 miljoen dollar voor een bedrijf in Brazilië tot 61 miljoen dollar voor een bedrijf in China. Dit zijn weliswaar ruwe en waarschijnlijk betrekkelijk lage schattingen, maar hieruit blijkt duidelijk dat een aanzienlijke hoeveelheid intellectuele eigendommen buiten het eigen land is opgeslagen en mogelijk risico loopt als gevolg van juridische, culturele en politieke verschillen.

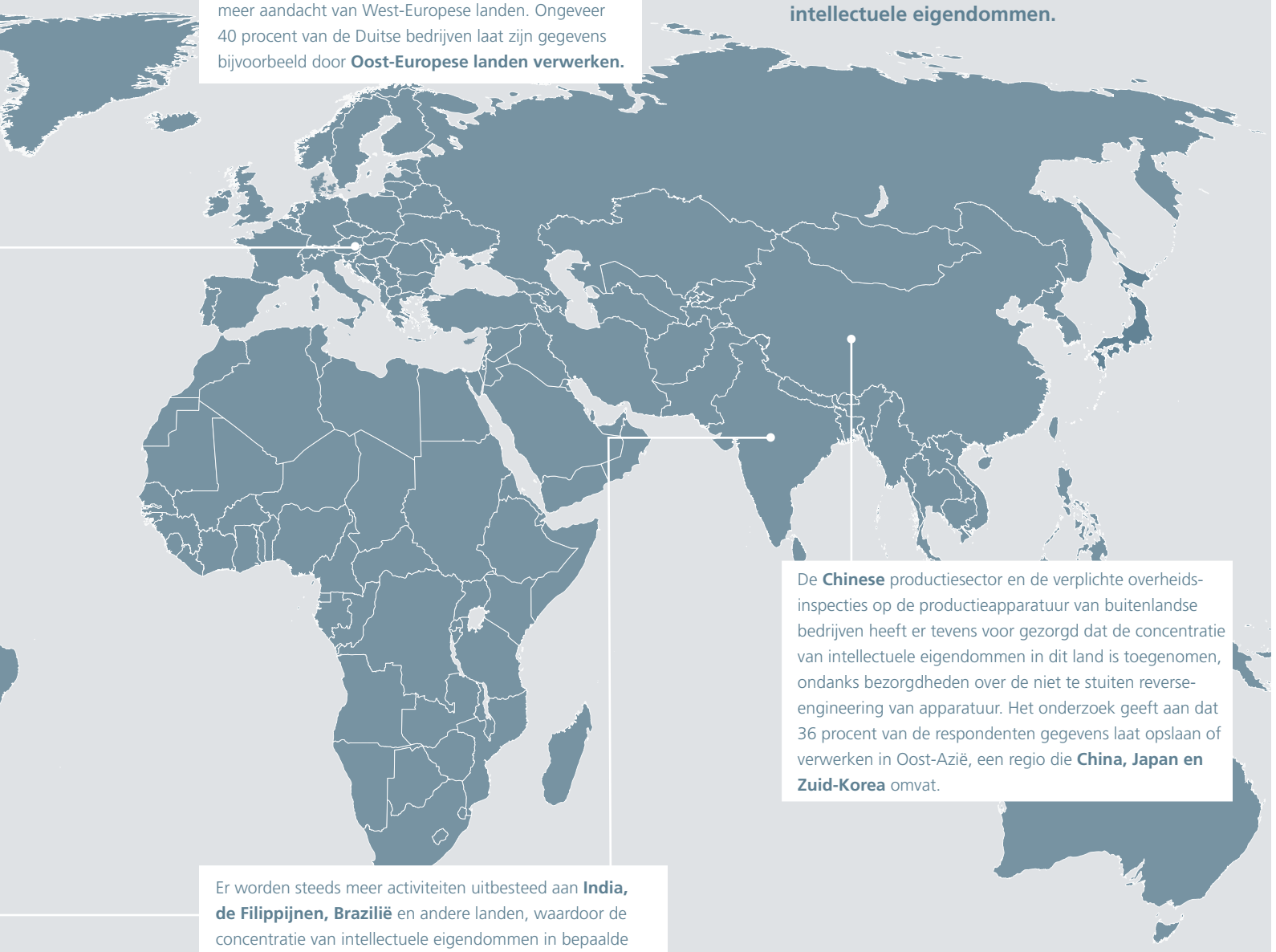


Het grootste deel van 's werelds intellectuele eigendommen bevindt zich nog steeds in **Noord-Amerika** (51 procent van de respondenten gaf aan dat hun intellectuele eigendommen in Noord-Amerika worden opgeslagen en/of verwerkt) en in **West-Europa** en het VK (47 procent van de respondenten).

**De respondenten schatten tevens dat er per bedrijf voor ongeveer 17 miljoen dollar aan intellectuele eigendommen in het buitenland wordt opgeslagen, geraadpleegd en beheerd.**

**Het is moeilijk schattingen te maken over de totale waarde aan wereldwijde intellectuele eigendommen die in het buitenland zijn opgeslagen. Van de meer dan 500 ondervraagde bedrijven gaven 197 bedrijven echter een gezamenlijk bedrag op van 3,4 miljard dollar voor in het buitenland opgeslagen intellectuele eigendommen.**

**De dienstverlenende mogelijkheden van Oost-Europese landen** met een sterke technische achtergrond (zoals Roemenië) krijgen ook steeds meer aandacht van West-Europese landen. Ongeveer 40 procent van de Duitse bedrijven laat zijn gegevens bijvoorbeeld door **Oost-Europese landen verwerken.**



De **Chinese** productiesector en de verplichte overheids-inspecties op de productieapparatuur van buitenlandse bedrijven heeft er tevens voor gezorgd dat de concentratie van intellectuele eigendommen in dit land is toegenomen, ondanks bezorgdheden over de niet te stuiten reverse-engineering van apparatuur. Het onderzoek geeft aan dat 36 procent van de respondenten gegevens laat opslaan of verwerken in Oost-Azië, een regio die **China, Japan en Zuid-Korea** omvat.

Er worden steeds meer activiteiten uitbesteed aan **India, de Filippijnen, Brazilië** en andere landen, waardoor de concentratie van intellectuele eigendommen in bepaalde gebieden aanzienlijk afneemt. Uit het onderzoek blijkt dat 22 procent van de respondenten zijn intellectuele eigendommen laat opslaan en/of verwerken in **Zuid-Centraal-Azië** (inclusief India en Pakistan) en dat 19 procent zijn intellectuele eigendommen laat opslaan en/of verwerken in **Zuid- of Midden-Amerika.**

## Waarom bedrijven vitale informatie naar het buitenland verplaatsen

Er zijn een aantal factoren die ertoe leiden dat bedrijven vitale informatie in het buitenland opslaan. De lagere kosten zijn volgens 26 procent van de respondenten een belangrijke factor. Arbeid is in veel buitenlandse locaties immers goedkoper dan in de VS en Canada, West-Europa, Japan en Australië. Andere drijfveren voor het opslaan of verwerken van gevoelige informatie buiten het eigen land zijn de efficiëntie van de toeleveringspartners (33 procent), gevolgd door een grotere deskundigheid (30 procent) en een betere veiligheid (29 procent).

De mogelijkheid om vitale informatie veilig op te slaan is een belangrijke factor volgens respondenten in verschillende landen, waaronder Brazilië, Japan en met name China. Meer dan 60 procent van de Chinese respondenten gaf "een veiliger opslag elders" als reden op voor het opslaan of verwerken van gevoelige gegevens buiten het eigen land.

## Aandacht voor beveiliging van vitale informatie varieert

Aangezien bedrijven veel vitale informatie naar het buitenland verplaatsen, is de veiligheid van deze gegevens in het huidige economische klimaat belangrijker dan ooit. De onderzoeksresultaten wijzen er echter op dat veiligheid niet altijd de hoogste prioriteit heeft.

**Het onderzoek geeft aan dat bedrijven in ontwikkelingslanden beter gemotiveerd zijn en meer geld besteden aan de beveiliging van vitale informatie dan hun Westerse collega's.**

Respondenten in landen als Brazilië, China en India besteden meer geld aan beveiliging (als percentage van hun totale IT-budget) dan de ontwikkelde landen. Respondenten in ontwikkelde landen, zoals Duitsland, Japan, de VS en het VK, geven in verhouding minder geld uit aan de beveiliging van hun vitale informatie. Uit het onderzoek blijkt dat 35 procent van de Indiase, 33 procent van de Chinese en 27 procent van de Braziliaanse bedrijven minstens een vijfde deel van hun IT-budget aan beveiliging besteden. In Duitsland geldt dat voor 20 procent, in Amerika voor 19 procent, in Japan voor 10 procent en in het VK voor slechts 4 procent van de bedrijven. In het VK wordt het laagste bedrag aan beveiliging uitgegeven (als percentage van het IT-budget). Het onderzoek bracht aan het licht dat 44 procent van de respondenten in het VK slechts 0 tot 5 procent van hun IT-budget aan beveiliging besteden.

Bij het vergelijken van de drijfveren voor investeringen in informatiebeveiliging kwam een opvallend verschil naar voren. Het blijkt dat besluitvormers in veel landen, met name ontwikkelde landen, reactief in plaats van proactief optreden. Regelnaleving is de belangrijkste drijfveer in Dubai, Duitsland, Japan, het VK en de VS. Uit het onderzoek blijkt echter dat 74 procent van de Chinese respondenten en 68 procent van de Indiase respondenten beslissingen nemen op basis van het winnen en/of behouden van een concurrentievoordeel ten aanzien van het aantrekken van klanten of opdrachtgevers.

De maatschappelijke bescherming (de rechtshandhaving en andere acties) ten aanzien van informatiebezittingen is zwakker in India en China dan in de ontwikkelde landen, maar dat geldt niet voor de organisatorische inzet op bedrijfsniveau. Een manager van een Indiaas IT-uitbestedingsbedrijf gaf aan (zelfs nog vóór de recente Mumbai-aanvallen) dat zijn bedrijf over een goed gedefinieerd bedrijfscontinuïteitsplan beschikt en dat er elk half jaar oefeningen worden gehouden, waarbij soms zelfs wordt gedaan alsof een van de locaties door een terroristische aanval is uitgeschakeld.

## Het onderzoek naar beveiligingsincidenten met intellectuele eigendommen varieert

In bepaalde landen wordt bovendien door een klein aantal bedrijven geen onderzoek gedaan naar beveiligingsincidenten. Dit zou betekenen dat diefstal van intellectuele eigendommen in bepaalde landen niet wordt gemeld.

Van de Chinese bedrijven gaf 28 procent aan dat ze geen onderzoek uitvoeren naar beveiligingsincidenten vanwege de kosten en 35 procent doet dit niet om slechte publiciteit te voorkomen. Tevens blijkt dat de kosten ook voor 23 procent van de Duitse en Japanse bedrijven en 19 procent van de Indiase bedrijven een reden is om niet op incidenten te reageren.

Interessant in dit opzicht is dat respectievelijk 24 procent en 22 procent van de bedrijven in Dubai en India beveiligingsincidenten niet onderzoeken vanwege het gebrek aan "medewerking". Deze weerstand kan zich voordoen op bedrijfs-, lokaal, nationaal of internationaal niveau. Hieruit blijkt dat noch alle bedrijven, noch alle bureaus hun volledige medewerking verlenen aan het oplossen van deze problemen.

### Tijdens een economische recessie bezuinigen bedrijven op de beveiliging van intellectuele eigendommen

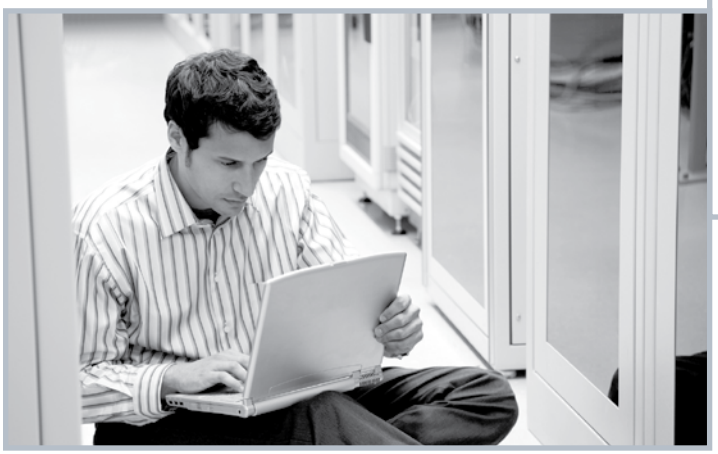
Het aantal dreigingen neemt hand over hand toe, maar in de landen waarin de meeste intellectuele eigendommen zijn opgeslagen, blijven de investeringen voor het beschermen van intellectuele eigendommen op hetzelfde niveau. Het blijkt zelfs dat een alarmerend percentage van de respondenten minder aan de beveiliging van hun vitale informatie wil besteden vanwege de aanhoudende financiële crisis, variërend van 14 procent in China en Dubai tot 31 procent in Brazilië.

Het grootste probleem is volgens deskundigen dat veel bedrijven beveiliging als een kostenpost blijven zien en er tijdens een recessie vaak op kostenposten wordt bezuinigd. Dit levert georganiseerde cybercriminelen een groeiend aantal eenvoudige doelwitten op, terwijl de criminelen zelf hun aanvallen steeds verder verfijnen.

## EEN HOGE PRIJS

### In 2008 verloren bedrijven gemiddeld 4,6 miljoen dollar aan intellectuele eigendommen

Volgens de respondenten bedroeg het verlies aan intellectuele eigendommen als gevolg van beveiligingslekken gemiddeld 4,6 miljoen dollar per bedrijf. Dit varieerde van slechts 375.000 dollar in het VK tot wel 7,2 miljoen dollar in China. De financiële dienstverlening leed het afgelopen jaar het hoogste verlies met 5,3 miljoen dollar per bedrijf, gevolgd door productontwikkeling en productie met 4,6 miljoen dollar per bedrijf. Bij de respondenten bedroeg het totale verlies van intellectuele eigendommen in de afgelopen 12 maanden 559 miljoen dollar (verliezen als gevolg van piraterij niet meegerekend).



Volgens de respondenten is een bedrijf gemiddeld bijna 600.000 dollar kwijt voor het afhandelen van elk beveiligingslek dat betrekking heeft op het verlies van vitale informatie, zoals intellectuele eigendommen. Dit bedrag zal naar verwachting hoger worden naarmate de wereldwijde recessie langer duurt. Let erop dat deze 600.000 dollar alleen betrekking heeft op de kosten voor het herstel achteraf (bijvoorbeeld juridische kosten, kennisgevingen aan slachtoffers), niet op de kosten voor preventie en detectie.

Uit het onderzoek blijkt dat respondenten zich meer zorgen maken over de reputatieschade dan over de financiële gevolgen die een lek of verlies van vitale informatie met zich meebrengt. De helft van de respondenten gaf aan dat ze zich in het geval van gegevensverlies meer zorgen maakten over de reputatieschade dan over de economische (33 procent) en juridische (16 procent) gevolgen.

**PRAKTIJKVOORBEELD:** Tele Atlas North America levert digitale kaarten en andere informatie voor navigatiesystemen en locatiegebaseerde diensten. Willis North America, zorg-verzekeringsbeheerder van Tele Atlas North America, meldde op 9 juni 2008 dat back-uptapes met werknemersgegevens van Tele Atlas North America tijdens het verzenden naar de opslagfaciliteit waren "verloren". Het is niet bekend of de tapes versleuteld waren, maar waarschijnlijk was dit niet het geval.

De tapes bevatten gevoelige persoonsgegevens van Tele Atlas North America-werknemers en hun medeverzekerden, onder andere namen, adressen, geboortedatums en burgerservice-nummers. Hoeveel records er op de verloren tapes stonden is niet bekend, maar Tele Atlas North America had op dat moment ongeveer 1700 werknemers in dienst.

Tele Atlas North America en Willis North America zijn beide gevestigd in de Verenigde Staten, maar de tapes waren onderweg naar een opslagfaciliteit in de buurt van Mumbai, India. Het is niet duidelijk of de tapes zijn gevonden of dat de gegevens op de tapes illegaal worden gebruikt. Maar gezien de waarde van de gegevens is de kans groot dat de informatie in verkeerde handen zal vallen.

## BELANGRIJKE BEVINDING 2:

## de huidige economische recessie is een perfecte voedingsbodem voor beveiligingslekken

De wereldwijde economische crisis veroorzaakt grote risico's voor de informatiebeveiliging. Bedrijven zien zich genoodzaakt hun uitgaven te verlagen en personeel te ontslaan, met als gevolg gaten in de verdediging en meer kansen voor cybercriminelen.

De respondenten maken zich duidelijk zorgen over de financiële crisis en de gevolgen voor de beveiliging van cruciale informatie, zoals intellectuele eigendommen en gevoelige informatie. Volgens 39 procent van de respondenten is deze informatie in het huidige economische klimaat kwetsbaarder geworden.

**Gegevensdiefstallen door insiders hebben vaak grotere financiële gevolgen, vanwege het hogere niveau van gegevenstoegang. Daarnaast oefent de huidige economische neergang zijn invloed uit op de investeringen in de IT-beveiliging, wat een nog groter financieel risico voor bedrijven kan opleveren.**

Het onderzoek toont aan dat beveiligingsproblemen tijdens economisch zware tijden om verschillende redenen erger worden. Dreigingen van binnenuit blijven nog steeds een probleem. Daar komt nog bij dat als gevolg van massale ontslagen een percentage van voorheen loyale werknemers belangstelling voor criminele activiteiten zal opvatten. Als gevolg van deze economische feiten kunnen steeds meer in financiële problemen verkerende, ontslagen werknemers in de verleiding komen hun toegang tot bedrijfsgegevens te gebruiken om vitale informatie te stelen. Wie weet immers beter waar de goederen zich bevinden en hoe er toegang tot de goederen kan worden verkregen dan mensen die een binding met de organisatie hebben?

Dergelijke voorspellingen worden ondersteund door de ondervraagde bedrijven: 68 procent noemt "dreigingen van binnenuit" als de grootste bedreiging voor vitale informatie. Dit is *hoger* dan de dreigingen die worden veroorzaakt door het patchen van kwetsbaarheden (51 procent), cyberterrorisme (38 procent) en industriële spionage (36 procent).

De grootste dreiging die rechtstreeks aan de economische recessie kan worden toegeschreven bestaat volgens 42 procent van de respondenten uit ontslagen werknemers, gevolgd door gegevensdieven van buitenaf (39 procent). Bovendien maakt 36 procent zich zorgen over de beveiligingsdreiging die uitgaat van werknemers met financiële problemen. Duitse respondenten maakten zich zeer grote zorgen over ontslagen (70 procent), net als Braziliaanse respondenten (59 procent) en Amerikaanse respondenten (46 procent).

"Dreigingen van binnenuit zijn moeilijk te bestrijden" zegt Tim Shimeall, analist bij de groep CERT/NetSA (CERT Network Situational Awareness) van de Carnegie Mellon-universiteit. "Werknemers en andere insiders, zoals contractanten, consultants, leveranciers en verkopers, kunnen tegenwoordig steeds makkelijker informatie stelen, omdat ze steeds meer toegang tot gegevens krijgen en bovendien gebruik kunnen maken van zeer geavanceerde technologieën".

Gegevensdiefstallen door insiders hebben vaak grotere financiële gevolgen, vanwege het hogere niveau van gegevenstoegang. Daarnaast oefent de huidige economische neergang zijn invloed uit op de investeringen in de IT-beveiliging, wat een nog groter financieel risico voor bedrijven kan opleveren.

## Financieel gewin of concurrentievoordeel: vitale informatie wordt een gewild ruilmiddel voor werknemers

Nu de economische druk ook voor particulieren voelbaarder wordt, kunnen werknemers of ex-werknemers een steeds grotere dreiging vormen. Deze groep kan grote problemen veroorzaken omdat ze toegang tot specifieke informatie

**De grootste dreiging die rechtstreeks aan de economische recessie kan worden toegeschreven bestaat volgens 42 procent van de respondenten uit ontslagen werknemers, gevolgd door gegevensdieven van buitenaf (39 procent).**

Als gevolg van het verhoogde risico van binnenuit zijn sommige bedrijven ertoe overgegaan de USB-poorten en cd-romstations op de computers van werknemers te vergrendelen.

hebben en de "beloning" soms heel hoog is. Insiders die gegevens stelen doen dat in sommige gevallen om er financieel beter van te worden, maar voor anderen is het een manier om hun kans op werk bij de concurrentie te verhogen. Het concurrentievoordeel kan zich nog verder uitbreiden als medewerkers die ontslag vrezen gaan zoeken naar een "baan achter de hand" bij concurrerende bedrijven en een potentiële nieuwe werkgever met bestaande kennis (en zelfs gegevens) van hun vorige werkgever over de streep proberen te trekken. Met de verkregen inzichten kunnen ze ook hun eigen bedrijf beginnen. "Als gevolg van de huidige economische situatie lopen bedrijven het risico dat ontslagen werknemers zelf een bedrijf beginnen met behulp van gestolen informatie", aldus Renato Opice Blum (een Braziliaans advocaat en professor).

Steeds weer blijkt dat de dreiging van binnenuit voortdurend groter wordt, zowel voor als tijdens de huidige economische wereldcrisis.

## Bedrijven moeten krachtige maatregelen treffen om informatie te vergrendelen

Als gevolg van het verhoogde risico van binnenuit zijn sommige bedrijven ertoe overgegaan de USB-poorten en cd-romstations op de computers van werknemers te vergrendelen. Deze techniek wordt overal ter wereld gebruikt en is met name populair bij IT-bedrijven in India. Andere extreme maatregelen zijn: werknemers verplichten hun manager een kopie van alle uitgaande e-mail te sturen en afdrukwachtrijen controleren op potentiële lekken.

Dergelijke drastische maatregelen hebben vaak negatieve gevolgen voor de productiviteit en kunnen meer kosten dan het gebruik van geschikte beveiligingsoplossingen en het voorschrijven en handhaven van de juiste beleidsregels.

**PRAKTIJKVOORBEELD:** in juni 2006 zou een werknemer van Acme Tele Power Private Limited, een in India gevestigd bedrijf, het softwarecomponent van Acme's gepatenteerde product, PIU (Power Interface Unit), naar Acme's concurrent Lambda Eastern Telecom hebben gelekt. Al snel na dit incident verliet de werknemer Acme en ging bij Lambda werken, volgens de geruchten tegen een veel hoger salaris. Acme beweert dat Lambda zijn product, BTS Shelter, heeft ontwikkeld op basis van de gestolen onderzoeks- en ontwikkelingsgegevens (R&D).

Acme voert aan dat Lambda zijn product alleen via illegaal gebruik van Acme's intellectuele eigendommen in zo'n korte tijd kon maken. De politie voerde een onderzoek uit en arresteerde uiteindelijk de verdachte werknemer, hoewel deze later op borgtocht werd vrijgelaten. De rol van Lambda in het incident blijft onduidelijk. Acme verplaatst later zijn R&D-activiteiten (ter waarde van 10 miljoen dollar) naar Australië, in de hoop daar een bedrijfsvriendelijker klimaat voor de beveiliging van intellectuele eigendommen te vinden.

**PRAKTIJKVOORBEELD:** in augustus 2008 arresteerden FBI-agenten Rene Rebollo, uit Pasadena, in de Amerikaanse staat Californië. Rebollo, voormalig senior financieel-analist bij Countrywide Financial, werd beschuldigd van het downloaden van twee miljoen klantrecords naar een geheugenstick en het verkopen van de gegevens aan identiteitsdieven.

Rebollo werkte als senior financieel-analist bij Full Spectrum Lending, de afdeling voor subprime-leningen van Countrywide. Hij zou naar verluidt circa 20.000 klantrecords hebben gedownload. Hij downloadde de records op zondagavonden via een kantoorcomputer die, in tegenstelling tot de andere computers, niet van beveiligingsfuncties was voorzien. Vervolgens verkocht hij de records als potentiële hypotheekklanten voor 400 tot 500 dollar per batch aan vertegenwoordigers van andere bedrijven. Zijn compagnon, Wahid Siddiqi, trad hierbij als wederverkoper van de gegevens op.

Het schijnt dat de gegevens werden gebruikt om nieuwe hypotheekhandel voor andere bedrijven te genereren en er dus geen sprake was van rechtstreekse identiteitsdiefstal. De werkelijke omvang van deze diefstal is echter nog steeds niet bekend. Volgens de Amerikaanse minister van Justitie lijkt het erop dat Rebollo de records voor ongeveer tweeënhalve dollarcent per stuk verkocht, veel minder dan hun waarde bij een legitieme gegevenshandelaar en zelfs veel minder dan ze op de zwarte markt zouden opbrengen.

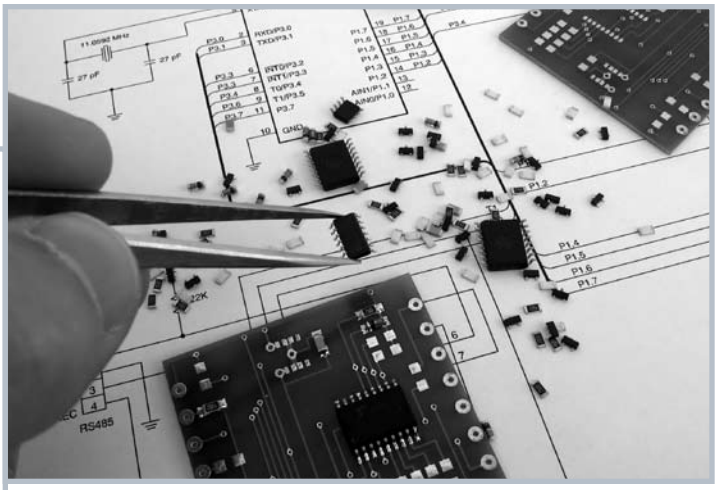
De zaak Rebollo is rechtstreeks toe te schrijven aan de ondergang van de subprime-hypotheeksector. Er zullen ongetwijfeld nog meer zaken volgen als gewetenloze en in financiële problemen verkerende werknemers (en ex-werknemers) hun financiële situatie proberen te verbeteren ten koste van de klant.


**PRAKTIJKVOORBEELD:** in juni 2008 zou een voormalige werknemer van Intel Corporation voor 1 miljard dollar aan vertrouwelijke documenten over intellectuele eigendommen hebben gedownload voordat hij het bedrijf verliet en bij AMD (een concurrent) ging werken.

De FBI vond meer dan 100 pagina's gevoelige documenten en 19 CAD-tekeningen van toekomstige processorchips in het huis van de verdachte. Het Amerikaanse ministerie van Justitie en de FBI werden ingeschakeld nadat een andere werknemer van Intel Corporation had ontdekt dat de verdachte bij AMD was gaan werken nog voordat zijn dienstbetrekking met Intel was afgelopen, en dat er tijdens die periode gevoelige informatie was geraadpleegd.

De voormalige werknemer werd in september 2008 schuldig bevonden aan vijf aanklachten met betrekking tot het stelen van handelsgeheimen en elektronische fraude. De beklaagde kan maximaal 90 jaar gevangenisstraf krijgen als hij op alle punten wordt veroordeeld.

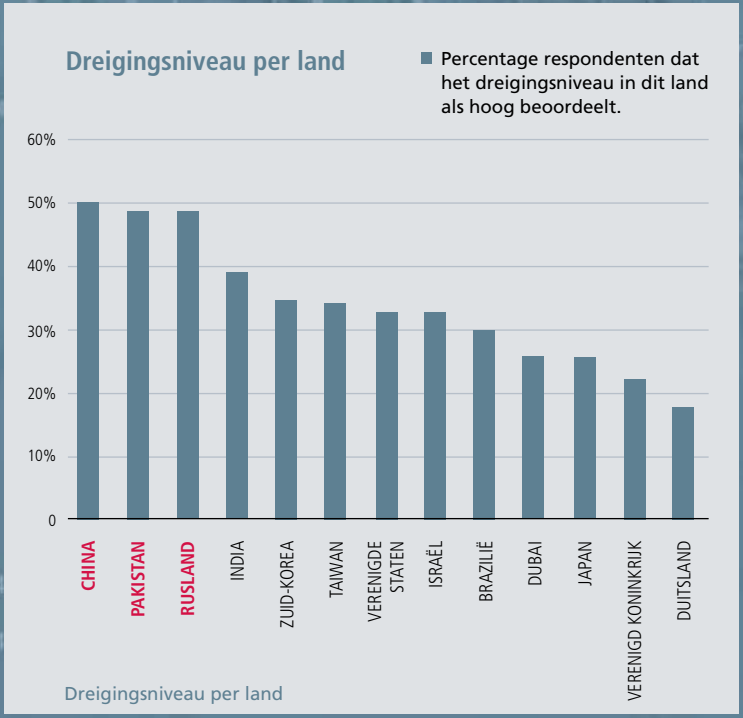
AMD maakte geen gebruik van de informatie, maar een ander bedrijf had mogelijk minder scrupules gehad.



# BELANGRIJKE BEVINDING 3:

## geopolitieke denkbeelden werken door in het informatiebeveiligingsbeleid

Bepaalde landen ontwikkelen zich onmiskenbaar als dreigingsbron voor gevoelige gegevens, met name voor intellectuele eigendommen. Uit het rapport blijkt dat geopolitieke denkbeelden invloed hebben op het gegevensbeleid. China, Pakistan en Rusland worden om verschillende juridische, culturele en economische redenen als probleemgebieden aangewezen.



## China, Rusland en Pakistan vormen de grootste dreigingen voor vitale informatie

Drie landen kwamen als grootste dreiging uit de bus. Niet onmogelijk is dat bepaalde andere denkbeelden over beveiliging hierbij een belangrijke rol hebben gespeeld. China, Pakistan en Rusland werden aangewezen als de landen waarin de beveiliging van digitale bezittingen het slechtst is geregeld.

Pakistan, China en Rusland (in die volgorde) worden ook beschouwd als landen met een slechte reputatie ten aanzien van het oplossen of onderzoeken van beveiligingsincidenten. Respondenten noemden als hoofdredenen de corrupte rechtshandhaving en rechtssystemen alsmede de slechte vaardigheden van de autoriteiten.

- **De denkbeelden van de respondenten zijn mogelijk geworteld in zowel historische conflicten als hedendaagse economische, culturele en politieke verschillen.** De reacties kunnen vaak worden teruggevoerd naar de spanningen die er van oudsher heersen tussen China en Japan, India en Pakistan, de VS en Rusland, het VK en Rusland, en de meer actuele conflicten tussen China en Taiwan en China en de VS. Professor Takefuji van de universiteit van Keio en adviseur van de Japanse National Security Association zegt hierover het volgende: "In Japan is gegevenslekkage door werknemers de grootste dreiging".

- **Chinese en Japanse respondenten zijn argwanend ten aanzien van de informatiedreigingen in elkaars land.** De respondenten moesten bijvoorbeeld aangeven welk land het hoogste dreigingsniveau had. Hierbij koos 47 procent van de Chinese respondenten de VS, gevolgd door Taiwan (41 procent). Japanse respondenten kozen China (57 procent) gevolgd door Rusland (44 procent). Indiase respondenten kozen massaal voor Pakistan (61 procent) als het land met het hoogste dreigingsniveau. In de VS wonende respondenten kozen China (62 procent) gevolgd door Rusland (59 procent). In het VK wonende respondenten kozen Rusland (74 procent) gevolgd door Pakistan (68 procent) en China (66 procent).

**China, Pakistan en Rusland werden aangewezen als de landen waarin de beveiliging van digitale bezittingen het slechtst is geregeld.**

- **Chinese respondenten (42 procent) wezen de beveiliging van persoonsgegevens in het Japanse rechtssysteem aan als de primaire dreigingsbron voor gevoelige gegevens, terwijl Japanse respondenten (30 procent) de beveiliging van intellectuele eigendommen in het Chinese rechtssysteem als de primaire dreigingsbron aanwezen.** Japanse respondenten vonden dat China onvoldoende voorbereid is om zich te verdedigen tegen dreigingen (69 procent), waarbij de cultuur van het land werd aangewezen als de primaire reden voor deze slechte voorbereiding (38 procent).

- **Amerikaanse bedrijven vinden de dreigingen in China, en in mindere mate India, zorgelijk, maar Indiase en Chinese respondenten beoordelen de dreigingen in elkaars landen lager.** Indiase respondenten beschouwen China bijvoorbeeld als een lagere dreiging voor gevoelige gegevens dan Pakistan (38 procent versus 61 procent) en Chinese respondenten beschouwen India en Japan als een lagere dreiging (beide 38 procent) dan de VS (47 procent) en Taiwan (41 procent). Chinese respondenten gaven aan dat ze India voornamelijk vermijden vanwege zorgen over intellectuele eigendommen (24 procent), terwijl veel minder Indiase respondenten (11 procent) in dat opzicht afwijzend tegenover China staan.

Bijna alle landen schatten het risico in andere landen hoger in dan in hun eigen land. De voornaamste uitzonderingen hierop zijn Japan en de VS. Zowel Japanse als Amerikaanse bedrijven zijn van mening dat het risico in hun land hoger is

dan in de rest van de wereld wordt gedacht. Japan ziet zichzelf als een hoger risico (15 procent) dan de rest van de wereld (12 procent). De VS beschouwt zichzelf als een hoger risico (21 procent) dan de rest van de wereld (18 procent).

### Bedrijven mijden landen als gevolg van bezorgdheden over de beveiliging

Wantrouwen leidt ertoe dat sommige bedrijven zonder meer weigeren hun producten te produceren in of hun intellectuele eigendommen te verplaatsen naar landen die zij als een dreiging beschouwen. Een groot aantal respondenten gaf aan dat ze geen informatie wilden laten verwerken in bepaalde landen, met name Pakistan, China en Rusland, omdat ze zich zorgen maakten over hun intellectuele eigendommen en/of de bescherming van persoonsgegevens.

Landen waarmee bedrijven geen zaken willen doen vanwege bezorgdheden over de informatiebeveiliging

**Uit het onderzoek blijkt dat 26 procent van de respondenten het opslaan en/of verwerken van gegevens in China doelbewust vermijdt.**

### China

Uit het onderzoek blijkt dat 26 procent van de respondenten het opslaan en/of verwerken van gegevens in China doelbewust vermijdt.

Het ontbreken van privacy en de slechte beveiliging van intellectuele eigendommen zijn volgens de respondenten de primaire redenen waarom China zo'n grote dreiging voor gevoelige gegevens vormt.

Net als bij veel andere opkomende economieën is de groei van China vele malen groter dan het vermogen om wetgeving op te stellen en te handhaven. Misschien nog belangrijker is de culturele houding ten aanzien van het beveiligen van digitale privacy en gevoelige gegevens. De procedure voor beveiligingscertificering in China (China Compulsory Certification) is bijvoorbeeld ontmaskerd als een van de technieken waarmee de Chinese regering zich intellectuele eigendommen toe-eigent. De certificering schrijft voor dat bedrijven die elektronische onderdelen in China willen verkopen, tekeningen, schema's en het voltooide product moeten indienen bij de Chinese overheidsinstantie die toezicht houdt op de certificering.

"China is een groot ontwikkelingsland" zegt Shimeall van de Carnegie Mellon-universiteit. "Het land is rijk aan mensen maar niet rijk aan hulpbronnen. De Chinezen zijn erg gebrand op het ontwikkelen van de economie. De goedkoopste manier (niet per se de ethische manier) is industriële spionage. Dit probleem speelt ook bij andere ontwikkelingslanden, zoals India en Brazilië. Professor Heejo Lee van de universiteit van Korea in Seoul ontdekte dat verschillende recente aanvallen op Zuid-Koreaanse bedrijven werden uitgevoerd door in China gevestigde hackerbendes.

**PRAKTIJKVOORBEELD:** de trend om de productie uit te besteden is goed gedocumenteerd en gebaseerd op de optimalisatiebeginselen van de leveringsketen: kosten, flexibiliteit en snelheid. In de afgelopen decennia hebben de grote productielanden, zoals Mexico, China en Zuidoost-Azië, een enorme groei doorgemaakt en zijn de traditionele productiebanen in bijvoorbeeld de VS en West-Europa fors gedaald. Maar als bedrijven er niet op kunnen rekenen dat hun kerngegevens (de intellectuele eigendommen) goed beschermd zijn, kunnen zelfs deze sterke wereldwijde economische krachten het onderspit delven.

Een aantal jaar geleden vestigde een bekende contractfabrikant een productie-centrum voor medische apparatuur in Singapore. Deze locatie werd gekozen om een aantal belangrijke redenen: de sterke logistiek, de toegang tot relatief betaalbaar talent en de krachtige juridische en culturele infrastructuur ten aanzien van gegevensbeveiliging. De klanten van deze fabrikant hadden hun wensen duidelijk kenbaar gemaakt: ze wilden de laagste totale kosten, maar ze wilden niet het risico lopen hun intellectuele eigendommen te verliezen door de belangrijkste onderdelen van hun apparaten in China te laten maken. De dozen en basisproducten worden daarom in China gemaakt, maar de technologie en assemblage blijven in Singapore, waarbij de aanzienlijk hogere kosten voor lief worden genomen.

– Voormalig leidinggevende van een bekende internationale contractfabrikant

Professor Katsuya Uchida is werkzaam bij het Japanse Institute of Information Security en is tevens assistent-CIO van de stad Yokohama. Uchida wees erop dat het Institute of Information Security in 2006 een onafhankelijk onderzoek heeft uitgevoerd, waaruit bleek dat ongeveer 64 procent van de respondenten China de schuld gaf van de diefstal van hun intellectuele eigendommen.

## Pakistan: een cyberdreiging? Mythe of realiteit?

Uit de onderzoeksresultaten blijkt dat Pakistan niet wordt gezien als vertrouwd land om zaken mee te doen. Van de respondenten geeft 27 procent aan het opslaan en/of verwerken van gegevens in Pakistan doelbewust te vermijden.

De uitbestedingssector van Pakistan is veel minder ontwikkeld dan die van het buurland India. Pakistan wordt echter gezien als toevluchtsoord voor hackers of cyberfraudeurs, net als de voormalige sovjetrepublieken, Oost-Europa en Nigeria.

Pakistan wordt ervan verdacht leden van de Taliban en Al-Qaeda te herbergen. Dit vermoeden heeft mogelijk bijgedragen aan het denkbeeld van de respondenten dat het land een groot risico vormt voor de integriteit van cruciale gegevens en niet geschikt is voor het uitbesteden van gevoelige informatie en intellectuele eigendommen.

"Pakistan is minder geïsoleerd dan Iran en heeft zeer goede universiteiten die vol zitten met intelligente studenten" aldus Lynn Robert Carter, associate teaching professor aan de Carnegie Mellon-universiteit in Qatar. "Het extreem fundamentalisme is echter nog niet verdwenen en er is een hoog werkloosheidscijfer, zelfs onder hoogopgeleiden. Deze combinatie leidt tot grote en minder grote dreigingen voor de informatiebeveiliging".

## De cybermaffia van Rusland

Uit het onderzoek blijkt dat 19 procent van de respondenten het opslaan en/of verwerken van gegevens in Rusland doelbewust vermijdt.

Volgens Tim Shimeall van de Carnegie Mellon-universiteit vormt de maffia de grootste dreiging in Rusland. "De Russische maffia beschikt over onuitputtelijke middelen en heeft bewezen meedogenloos te zijn. Men zegt dat de maffia eigenaar is van 8 procent van 's werelds bodemschatten. Met dergelijke middelen kan de maffia een eigen communicatie-infrastructuur opbouwen. Het bieden van bescherming tegen aanvallen van een dergelijke rijke criminele organisatie is daarom allesbehalve eenvoudig. De maffia richt zich voornamelijk op bankrekeningnummers, bankoverboekingen, enzovoort" aldus Shimeall.

Pakistan, China en Rusland (in die volgorde) worden ook beschouwd als landen met een slechte reputatie ten aanzien van het oplossen of onderzoeken van beveiligingsincidenten. Respondenten noemden als hoofdredenen de corrupte rechtshandhaving en rechtssystemen alsmede de slechte vaardigheden van de autoriteiten.

**PRAKTIJKVOORBEELD:** een Indiase softwareontwikkelaar die de code van een klant wou verbeteren, plaatste een gedeelte van de code op internet om input van de ontwikkelaarsgemeenschap te ontvangen, zonder zich te realiseren dat hij hiermee inbreuk maakte op de vertrouwelijkheid van het intellectuele eigendom van de klant. De inspanningen van de ontwikkelaar om de code te verbeteren waren oprecht, maar het eindresultaat had voor de klant zeer nadelig kunnen zijn.

**Volgens 18 procent van de Indiase respondenten is er wel regelgeving ter bescherming van informatiebezittingen maar wordt deze niet gehandhaafd.**

## India

De reputatie van India als minder geschikte plaats voor het opslaan en/of verwerken van gegevens is mogelijk het gevolg van de alarmerende krantenkoppen toen het land steeds meer uitbestedingsactiviteiten voor andere landen ging uitvoeren. Veel bedrijven hebben zich ongetwijfeld door deze krantenkoppen nerveus laten maken.

Met dergelijke krantenkoppen is het geen wonder dat sommige bedrijven ervoor hebben gekozen geen zaken te doen in India: een Canadees bedrijf voor mobiele weegapparatuur ging niet in op het aanbod van een Indiaas bedrijf om het product in India te produceren en op de markt te brengen, voornamelijk omdat het Canadese bedrijf zich zorgen maakte over zijn intellectuele eigendommen.

## Verschillende culturele houdingen

De cultuur beïnvloedt de waarde die wordt gehecht aan intellectuele eigendommen. Het is heel goed mogelijk dat derde- en tweedewereldlanden de intellectuele eigendommen van anderen geen beveiliging waard achten als het hun helpt hun economische omstandigheden te verbeteren. Tussen bedrijven kunnen zich ook verschillen voordoen met betrekking tot het beveiligen van verschillende typen intellectuele eigendommen.

Professor Heejo Lee van de universiteit van Korea wees op een aantal gegevenslekken en privacy-inbreuken bij Auction en andere grote Koreaanse bedrijven. Hij zei dat deze incidenten in de Koreaanse cultuur als intellectuele eigendoms-problemen worden gedefinieerd. Veel in Amerika gevestigde bedrijven zullen deze gegevens weliswaar als gevoelig classificeren, maar niet altijd als intellectuele eigendommen beschouwen.

"Cultuur is een belangrijk probleem" aldus Sivarama Krishnan, een in India gevestigde partner van PricewaterhouseCoopers. Hij wijst erop dat mensen in India en Amerika verschillende ideeën over privacy hebben. In India worden salarissen bijvoorbeeld openlijk besproken onder collega's, maar in de VS is dat niet gebruikelijk. Indiase bedrijven die zaken doen met Amerikaanse bedrijven en in contact komen met hun gegevens, moeten alert zijn op dit soort kwesties en werknemers, leveranciers, contractanten en zelfs klanten hierin trainen en begeleiden.

**PRAKTIJKVOORBEELD MET EEN ANDERE WENDING:** sommige bedrijven stellen zichzelf bewust bloot aan dreigingen. In de zware industrie zijn onderzoek en ontwikkeling van groot belang om nieuwe producten in een zeer concurrerende markt te kunnen introduceren. Maar door de stagnerende groei in de VS en West-Europa zagen veel bedrijven in de zware industrie zich gedwongen opkomende markten, zoals India en China, in overweging te nemen. Cummins, Inc. opende zelfs een onderzoeks- en ontwikkelingscentrum in Wuhan, China. Hoewel Cummins enige controle over zijn intellectuele eigendommen kan verliezen door zich op deze markten te begeven, vertrouwt het bedrijf erop dat zijn reputatie en zijn vermogen om sneller vernieuwingen uit te voeren dan een pas beginnend bedrijf meer gewicht in de schaal zullen leggen. Tot op heden hebben ze daarin gelijk gekregen.

**PRAKTIJKVOORBEELD:** India was voorpaginanieuws toen een Britse krant een undercoveroperatie uitvoerde onder medewerkers van een Indiaas callcenter en contactgegevens van Britse burgers in handen wist te krijgen. Dit incident maakte de callcentermedewerkers beter bewust van Westerse ideeën over privacy die afwijken van die van India.

## Gebrekkige handhaving

Veel regionale respondenten beschouwen de beleidshandhaving ook als een probleem. Volgens 18 procent van de Indiase respondenten is er wel regelgeving ter bescherming van informatiebezittingen maar wordt deze niet gehandhaafd.

De respondenten waren van mening dat Brazilië en Pakistan het slechtst op dreigingen zijn voorbereid. Renato Opice Blum zegt hierover: "Het voornaamste probleem is dat de rechtshandhaving en rechtssystemen in Brazilië onvoldoende zijn voorbereid op het afhandelen van informatiedreigingen. De Braziliaanse wetten zijn niet specifiek op informatiecriminaliteit gericht en bedrijven moeten het daarom doen met wetten die zijn bedoeld voor traditionele misdaden die meer van fysieke dan virtuele aard zijn. Dit houdt onder meer in dat de bewijslast veel hoger is. Het slachtoffer moet bijvoorbeeld niet alleen bewijzen dat de aanvaller een particulier netwerk is binnengedrongen, maar ook dat de aanvaller schade heeft veroorzaakt. Bewijzen dat er gegevens zijn verloren is in de digitale context veel moeilijker en daardoor ligt de bewijslast hoger".

"Het VK en de EU hebben strengere wetten, maar de Amerikaanse wetten zijn beter doordacht" zegt professor Lilian Edwards van de universiteit van Southampton. "In het VK moet de wet bijvoorbeeld worden gehandhaafd door een onafhankelijke commissie. De commissie bezit echter weinig geldmiddelen en heeft weinig handhavingsmogelijkheden. In de VS zijn de wetten (bijvoorbeeld de HIPAA en de financiële verslagleggingswetten) echter specifiek op het probleem gericht".

Interessant is dat Indiase en Chinese bedrijven zich zorgen lijken te maken over de strenge Amerikaanse wetten en dat Indiase bedrijven zich met name zorgen maken over de strenge privacywetten in het VK, maar niet over vergelijkbare wetten in Duitsland.

## Vietnam en de Filippijnen gunstig beoordeeld (op dit moment)

Uit het onderzoek blijkt dat de landen in het Verre Oosten, zoals Vietnam en de Filippijnen, in het bedrijfsleven als gunstig worden beoordeeld. Een partner van Accenture (met een vestiging in de Filippijnen) wees erop dat de salarissen van IT-medewerkers in India met minstens 10 procent zijn gegroeid, maar dat Accenture in deze andere landen een goed evenwicht heeft gevonden tussen technologische knowhow en kosten.

Een leidinggevende in de halfgeleiderindustrie die zijn aarzelingen uitsprak over China, wees er tevens op dat de intellectuele eigendomswetten in Vietnam en de Filippijnen weliswaar niet streng zijn, maar dat de problemen op dit gebied minder ernstig zijn dan in China. Met veel aandacht van overheidswege hebben deze landen een groot potentieel om als bestemmingsgebied voor intellectuele eigendommen in aanmerking te komen.

Vooraanstaand informatiebeveiligingsexpert professor Eugene Spafford van de universiteit van Purdue verwacht dat deze voordelen van korte duur zullen zijn. Spafford denkt dat wanneer de hoeveelheid intellectuele eigendommen in deze regio's toeneemt, de criminelen zich ook op deze landen zullen richten.

# BELANGRIJKE BEVINDING 4:

## intellectuele eigendommen zijn een nieuwe valuta voor cybercriminelen

"Criminelen stalen vroeger geld om rijk te worden, maar nu hebben ze ontdekt dat ze rijk kunnen worden door bedrijfsinformatie te stelen".

– Ambtenaar van het Amerikaanse ministerie van Financiën

De activiteiten van cyberdieven bestaan niet alleen meer uit het hacken en stelen van creditcard- en aanmeldingsgegevens. Intellectuele eigendommen zijn het nieuwe doel. *Waarom zoveel tijd en geld aan onderzoek en ontwikkeling besteden als je deze ook gewoon kunt stelen?*

Creditcardfraude en identiteitsdiefstal bevinden zich nu in de "melkkoe"[1]-fase van de criminele strategie. Met andere woorden, het is een bron van inkomsten die niet veel ruimte voor groei meer biedt. Criminelen richten hun aandacht daarom op de nieuwe sterren in hun portfolio. En intellectuele eigendommen zijn als favoriet uit de bus gekomen.

[1] Zie de BCG-matrix (Boston Consulting Group) over productlevenscycli op www.bcg.com.

Cybercriminelen beseffen steeds beter hoe waardevol bedrijfsinformatie kan zijn en ze zullen zich daarom ook steeds meer op bekende kwetsbaarheden richten. Over het algemeen kan worden gesteld dat de aard en het raffinement van de aanvallen toeneemt. Dit komt overeen met de bevinding dat het patchen van kwetsbaarheden de tweede grootste zorg van respondenten is.

Aanvallen van gegevensdieven wordt door 39 procent van de respondenten als dreiging genoemd. Japanse respondenten maakten zich het meeste zorgen over de dreiging van gegevensdiefstal van buitenaf (70 procent), net als de Chinese respondenten (56 procent).

Veel bedrijven stellen zich ondanks deze bezorgdheden bloot aan uitbuiting en aanvallen omdat ze niet op de hoogte zijn van de waarde en locatie van hun intellectuele eigendommen. Sommige van die eigendommen zijn opgeslagen in Microsoft Word-bestanden, Adobe Acrobat pdf-documenten, Microsoft PowerPoint-presentaties en andere media-indelingen. Volgens Ashish Arora van de Duke-universiteit kunnen hackers en anderen steeds makkelijker aanvallen op intellectuele eigendommen uitvoeren omdat gegevens steeds vaker worden geclassificeerd en op servers worden opgeslagen.

"We merken een stijging van inbraken in bedrijfsnetwerken met als doel het verkrijgen van interne bedrijfsgegevens. Georganiseerde criminelen, waaronder maffia-achtige organisaties, gaan zich steeds meer bezighouden met cybercriminaliteit. Hieruit blijkt dat de beloning voor het stelen van immateriële bezittingen vrij hoog is", zegt Tom Longstaff, voormalig vice-directeur bij CERT en tegenwoordig werkzaam in het Applied Physics Laboratory van de Johns Hopkins-universiteit.

### Cybercriminelen investeren in onderzoek en ontwikkeling en zetten testcentra op

De hulpmiddelen die cybercriminelen ter beschikking staan, worden ook steeds verfijnder. Volgens 54 procent van de respondenten vormt de veranderende aard van de dreigingen een groot probleem. Professor Ross Anderson van de universiteit van Cambridge merkt op dat malwareschrijvers nu de beschikking hebben over R&D- en testafdelingen.

**Aanvallen van gegevensdieven wordt door 39 procent van de respondenten als dreiging genoemd. Japanse respondenten maakten zich het meeste zorgen over de dreiging van gegevensdiefstal van buitenaf (70 procent), net als de Chinese respondenten (56 procent).**

**PRAKTIJKVOORBEELD:** Industriële spionage in Zuid-Korea [2]

Vier Koreaanse staatsburgers zijn door de Koreaanse justitie aangeklaagd omdat ze hadden geprobeerd draadloze en breedband internettechnologie naar de Verenigde Staten te lekken. Het gaat om drie voormalige werknemers en een huidige onderzoeker van POSDATA Co. Ltd., een afdeling voor computerservices van Korea's belangrijkste staalproducent POSCO Co. Voor de drie voormalige werknemers (die momenteel een permanente verblijfsvergunning in Amerika hebben) is een uitleveringsprocedure naar Korea in gang gezet.

WiBro (een afkorting van wireless broadband) is een draadloze internetbreedband-technologie die is ontwikkeld door Koreaanse telecommunicatiebedrijven. Met WiBro kunnen gegevens sneller worden overgedragen dan met de bestaande mobiele technologieën. De commerciële WiBro-service, die in juni 2006 in Korea van start ging, verhoogt de gegevensoverdrachtsnelheid tussen mobiele apparaten, zoals mobiele telefoons. Een in Amerika gevestigd bedrijf was van plan de door de vier Koreanen aangeboden informatie te kopen en had reeds enige gegevens verkregen die door de aanklagers als "niet-kerninformatie" is aangemerkt. De vier waren van plan de informatie aan het Amerikaanse bedrijf te verkopen voor 180 miljoen won (193 miljoen dollar). Bovendien wilden ze 30 belangrijke onderzoekers bij POSDATA weglokken voor banen bij het Amerikaanse bedrijf. POSDATA besteedde 90 miljoen won aan het ontwikkelen van de technologie.

[2] "Four Indicted for Attempt to Leak WiBro Technology"
(Vier aangeklaagd voor poging tot lekken WiBro-technology) *The Korean Herald,* 21 mei 2007.

**PRAKTIJKVOORBEELD:** Industriële spionage in Singapore [3]

SMC Marine Services, Pte., Ltd., is een in Singapore gevestigde transportonderneming die met behulp van sleepboten en andere vaartuigen kolen, gips, zand en andere bulkgoederen vervoert tussen Indonesië, Vietnam, Thailand en de Filippijnen. Het bedrijf heeft voormalig systeemengineer Thangavelu Boopathiraja beschuldigd van het heimelijk instellen van wachtwoorden in een systeem dat hij voor het bedrijf had ontwikkeld. Boopathiraja ontwikkelde een realtime controlesysteem voor vaartuigen dat informatie over brandstofverbruik en andere belangrijke cijfers vanaf de schepen naar het hoofdkantoor van het bedrijf in Singapore moest sturen. Het systeem omvatte hardware die aan boord van de schepen moest worden geïnstalleerd, en waarvoor codes moesten worden gebruikt. Met behulp van de software die is gebruikt om de codes te schrijven kunnen ook wachtwoordbeveiligingsfuncties in het systeem worden opgenomen, hoewel deze functie niet standaard is geïnstalleerd. Boopathiraja verliet SMC al gauw nadat hij aan het systeem had gewerkt en startte een concurrerend bedrijf dat een vergelijkbaar controlesysteem voor schepen verkoopt. De advocaten van SMC beweren dat werknemers het systeem nu niet kunnen controleren, wijzigen of upgraden. Boopathiraja kan zowel strafrechtelijke als civielrechtelijke sancties krijgen opgelegd.

[3] "Firm Takes Systems Engineer to Court; Former Employee is Accused of Setting Passwords that Access Program He Created"
(Bedrijf sleept systeemengineer voor de rechter; voormalig werknemer beschuldigd van instellen van wachtwoorden voor zijn programma)
*The Straights Times (Singapore)* 14 juni 2008.

**PRAKTIJKVOORBEELD:** softwarebedrijf Oracle heeft op 22 maart 2007 zijn aartsrivaal aangeklaagd voor industriële spionage.
In november 2006 kwam Oracle zware downloadactiviteiten op het spoor op websites die zijn bedoeld voor klanten die producten gebruiken van afdelingen van PeopleSoft en J.D. Edwards (door Oracle opgericht na overname van beide bedrijven). Deze site met beperkte toegangsrechten, bevatte details over patches, instructies en softwareupdates. Volgens de rechtszaak die werd ingediend bij het Federal District Court in de Amerikaanse staat Californië, werd het grootste deel van deze downloads uitgevoerd vanaf een IP-adres bij TomorrowNow, een dochteronderneming van SAP. TomorrowNow verkocht technische ondersteuning voor producten van PeopleSoft, J.D. Edwards en Siebel, die alle door Oracle zijn overgenomen. Volgens Oracle meldden werknemers van SAP zich aan bij de website van Oracle door zich voor te doen als klanten met vervallen of binnenkort te vervallen rechten, onder andere van bedrijven als Honeywell International, Merck en Metro Machine Corp. Aan de hand van het logboekbestand van de website stelt Oracle dat er naar schatting meer dan 10.000 keer op onrechtmatige wijze software- en ondersteuningsmateriaal voor diverse producten is gedownload. Oracle is van mening dat SAP zich met dit vermoedelijk gestolen materiaal informatie heeft toegeëigend waarmee het bedrijf niet alleen zijn software heeft verbeterd maar ook probeert klanten van Oracle over te halen producten van SAP te gebruiken.

In veel bedrijven praten IT-medewerkers niet met bedrijfsjuristen over dit onderwerp en niemand beseft de belangen die de andere partij in dit verband heeft.

Malware (zoals MPack) wordt regelmatig door de ontwikkelaars bijgewerkt. De updates hebben betrekking op kwetsbaarheden die moeten worden uitgebuit, vergelijkbaar met systeembeveiligingsproducten die updates ontvangen over kwetsbaarheden die moeten worden verholpen.

Bedrijven reageren slechts langzaam op deze nieuwe complexiteit. Nick Akerman woont in New York en werkt als advocaat bij de firma Dorsey & Whitney. Akerman, die is gespecialiseerd in computermisbruik en –fraude, zegt hierover: "Bedrijven hebben geen geïntegreerde oplossing voor het probleem. Het personeelsbeleid, de informatiebeveiliging en de nalevingsprogramma's worden vaak als afzonderlijk eenheden behandeld. In veel bedrijven praten IT-medewerkers niet met bedrijfsjuristen over dit onderwerp en niemand beseft de belangen die de andere partij in dit verband heeft".

## Leidinggevenden slachtoffer van phishingaanvallen

Cybercriminelen richten zich op leidinggevenden met behulp van geavanceerde technieken, zoals phishing. Phishing heeft zich ontwikkeld van valse e-mails vol spelfouten tot zeer geavanceerde en gerichte "speerphishing'-aanvallen. Zelfs hooggeschoolde beveiligingsprofessionals hebben soms moeite om onderscheid te maken tussen een phishing-e-mail en een legitieme e-mail. Deze aanvallen kunnen verrassend effectief zijn. Speerphishing-aanvallen zijn een zwak punt in de beveiligingsprogramma's van veel organisaties omdat drukbezette leidinggevenden vaak wat minder oplettend zijn en onbedoeld gebruiker-id's en wachtwoorden weggeven, zelfs in zeer slecht in elkaar gezette aanvallen, laat staan geavanceerde aanvallen.

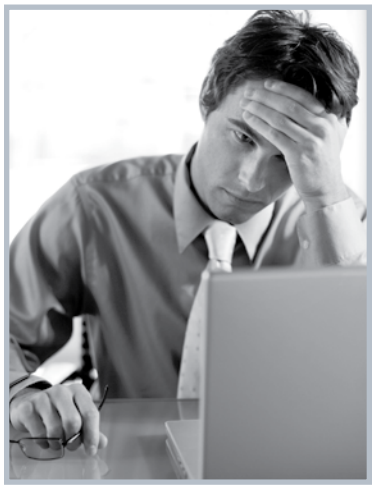
## Industriële cyberspionage in de lift

Deskundigen zijn het erover eens dat indien een onderneming tegen minimale kosten (vergeleken met de concurrentie) de hand kan leggen op onderzoek en ontwikkeling en een vergelijkbaar product tegen veel lagere kosten kan produceren, het bedrijf volgens de algemene economische basisbeginselen succes zal hebben op de markt. De beloningen voor industriële spionage zijn daarom hoog, met name op de zeer gewilde ontwikkelingsmarkten, waar de merkreputatie van "oude economie"-bedrijven mogelijk nog niet goed is gevestigd.

Als bedrijven in gevestigde economieën miljoenen, of zelfs miljarden dollars in onderzoek en ontwikkeling investeren, is de heersende verwachting dat de investerende partijen de vruchten van het eventuele succes op de markt mogen plukken.

Maar niet alle culturen omarmen deze filosofie. Dit geldt met name voor opkomende economieën, zoals China en Brazilië. Het is daarom geen wonder dat industriële spionage als de vierde meest serieuze dreiging door de respondenten wordt aangewezen.

**Bedrijven reageren slechts langzaam op deze nieuwe complexiteit.**



**Cybercriminelen richten zich op leidinggevenden met behulp van geavanceerde technieken, zoals phishing.**

# Toekomstige dreigingen en problemen voor ’s werelds vitale informatie

**Toekomstige dreigingen**

Na het analyseren van de huidige opkomende dreigingen voor vitale informatie, zoals intellectuele eigendommen, zijn McAfee en deskundigen van het CERIAS (Center for Education and Research in Information Assurance and Security) in de Verenigde Staten tot de overtuiging gekomen dat cruciale informatie kwetsbaarder zal worden door de volgende drie trends.

## Groeiende dreigingen van binnenuit

Faillissementen, massale ontslagen, krimpende markten en slechte economische vooruitzichten zullen ertoe leiden dat steeds meer in financiële problemen verkerende werknemers en ex-werknemers waardevolle bedrijfsinformatie gaan stelen, zowel voor financieel gewin als om hun kans op werk te verbeteren.

Hoewel het totale aantal aanvallen door insiders altijd lager is geweest dan het aantal aanvallen van buitenaf, zijn de gemiddelde verliezen in de meeste gevallen groter.

Combineer dit gegeven met bedrijven die zeer snel reageren en daardoor mogelijk geen sterke procedures hebben voor het vergrendelen van accounts, geen regelmatige interne controles uitvoeren en geen andere maatregelen nemen om aanvallen te voorkomen, en het is duidelijk dat bedrijven grote risico's nemen.

Bedrijven krijgen bovendien te maken met toenemende fusie- en overnameactiviteiten, en zolang de systemen van de samengevoegde bedrijven nog niet zijn geïntegreerd, lopen deze bedrijven een groter risico.

Michael Versace, senior adviseur bij Financial Services Technology Consortium, zegt: "Als twee bedrijven fuseren of als twee zaken van hetzelfde bedrijf worden geconsolideerd, moet er allereerst een gemeenschappelijk of gedeeld beleid voor informatiegovernance worden opgesteld en geïmplementeerd. Als gevolg van de grote media-aandacht voor veel financiële instellingen en de wereldwijde economische recessie, staan criminelen en anderen al klaar om misbruik te maken van een mogelijk gebrek aan focus op risicobeheer en een slecht ontworpen en/of geïmplementeerd beleid voor informatiegovernance en beveiliging".

## Meer geavanceerde en gerichte aanvallen van cybercriminelen

Criminelen smeden steeds complexere plannen om misbruik te maken van werknemers, nieuwe technologieën en kwetsbaarheden in software.

Aanvallers stellen in toenemende mate gedetailleerde en geavanceerde profielen van leidinggevenden en andere doelwitten samen om de speerphishing-aanvallen naar het spreekwoordelijke "volgende niveau" te tillen.

Blogs, persberichten, tijdschrift- en kranten-artikelen, databases met bedrijfsinformatie en sociale netwerksites worden door aanvallers uitgekamd om gegevens van het openbare en privéleven van leidinggevenden te verzamelen. Met deze informatie kan toegang worden verkregen tot gebruiker-id's, wachtwoorden, gegevens van financiële en systeemaccounts en andere gevoelige bedrijfsgegevens (ook wel "open source-informatie" genoemd).

Web 2.0-technologieën en "cloud computing" geven mensen de gelegenheid om samen te werken, te delen en bestaande componenten te gebruiken om nieuwe toepassingen te bouwen. Hiermee wordt niet alleen een zeer vernieuwende omgeving gecreëerd, maar ook een "achterdeur" via welke cybercriminelen gevoelige gegevens kunnen stelen.

## "Hot zones" voor geo-informatie

Nu de economieën van China en Rusland zwakker worden, staan deze landen nog meer onder druk om zich intellectuele eigendommen toe te eigenen als middel om de economische groei in stand te houden. De georganiseerde misdaad in Rusland en door de overheid gesponsorde groepen in Rusland en China zijn continu op zoek naar nieuwe en winstgevende doelen. Pakistan blijft in eerste instantie de grootste dreiging, met aanvallers die gemotiveerd zijn door ideologie in plaats van economisch gewin.

## Aanbevelingen van deskundigen

In een wereld waarin handelsbarrières worden geslecht, maar het strafrecht, het privaatrecht en de rechtshandhaving nog steeds geografische beperkingen kennen, en cybercriminaliteit steeds geraffineerder wordt, is er behoefte aan een gecombineerde benadering die bedrijven helpt hun vitale informatie te beveiligen.

Bedrijven moeten de bescherming van vitale informatie anders aanpakken en hun houding ten opzichte van hun vitale "informatie-bezittingen" veranderen.

### DESKUNDIGEN RADEN DE VOLGENDE STAPPEN AAN

#### Een internationaal geaccepteerd protocol voor het afhandelen van zakelijke internetbeveiligingsincidenten

Verschillende landen hebben niet alleen verschillende wetten en verschillende standpunten ten aanzien van het handhaven van bestaande wetten, maar criminelen en slachtoffers bevinden zich vaak ook nog eens in verschillende rechtsgebieden, zodat de pleger van de misdaad aanzienlijke schade kan veroorzaken zonder zelfs maar fysiek het pand van het slachtoffer te betreden.

Het detecteren van misdaden die betrekking hebben op gevoelige gegevens en intellectuele eigendommen kan moeilijk zijn in bepaalde omstandigheden. Maar de identificatie en uitlevering van de dader, alsmede een geslaagde gerechtelijke procedure zijn vaak in praktisch opzicht niet uitvoerbaar.

Deskundigen zijn van mening dat het verdrag van de Raad van Europa inzake cybercriminaliteit een grote bijdrage zal leveren aan het oplossen van sommige van deze problemen, maar dat de bepalingen nog steeds te flexibel worden geïnterpreteerd en geïmplementeerd. Bovendien hebben de meeste landen het verdrag nog niet geratificeerd, waardoor de totale effectiviteit van dergelijke inspanningen beperkt blijft.

**Criminelen smeden steeds complexere plannen om misbruik te maken van werknemers, nieuwe technologieën en kwetsbaarheden in software.**

Dr. Marco Gercke, docent recht op het gebied van cybercriminaliteit aan de universiteit van Keulen (Duitsland) is van mening dat de landen het verdrag van de Raad van Europa inzake cybercriminaliteit moeten ratificeren en de bepalingen volledig moeten aanvaarden.

Hij merkt tevens op dat Oost-Europa in veel opzichten beter is voorbereid op het handhaven van de bepalingen van het verdrag dan de West-Europese landen. Veel Oost-Europese landen, zoals Bulgarije en Roemenië hebben het verdrag ondertekend en geratificeerd, terwijl Duitsland en het VK het verdrag wel hebben ondertekend maar niet geratificeerd. De VS heeft het verdrag zowel ondertekend als geratificeerd met ingang van 1 januari 2007. Canada, Japan en Zuid-Afrika hebben het verdrag wel ondertekend, maar niet geratificeerd. Rusland heeft geweigerd het verdrag te ondertekenen en geeft als reden op dat er verschil van mening is over bepalingen inzake de grensoverschrijdende toegang tot gegevensverwerkende netwerken.

Dr. Gercke wijst er tevens op dat het verdrag moet worden bijgewerkt om zowel uitdrukking te geven aan de toenemende complexiteit aan de zijde van cybercriminelen als de doorgaande vernieuwingen in de technologie zelf.

**PRAKTIJKVOORBEELD:** in oktober 2007 brak de Oekraïner Oleksandr Dorozhko in op de systemen van Thomson Financial, een Amerikaanse uitgeverij van bedrijfsinformatie. De inbraak werd uitgevoerd vanaf een computer in Oekraïne. Dorozhko las naar verluidt een rapport met negatief nieuws over IMS Health (een bedrijf dat genoteerd is aan de NYSE), dat niet voor onmiddellijke publicatie was bestemd. In het rapport werd de verwachting uitgesproken dat de aandelenkoers van IMS Health zou dalen zodra het negatieve nieuws bekend werd gemaakt. Dorozhko kon van dit nieuws profiteren door onmiddellijk putopties op IMS Health te verkopen, met als resultaat een winst van 300.000 dollar (een putoptie is een optiecontract dat de houder het recht geeft een bepaalde hoeveelheid aandelen op een bepaalde datum tegen een vooraf bepaalde prijs te verkopen). De SEC (Securities Exchange Commission) probeerde de opbrengst te bevriezen maar in een tegenaanklacht van Dorozhko oordeelde de rechter dat hacken geen overtreding van de voorkenniswet is. Dorozhko mocht de opbrengst dus houden. De partijen waren het er wel over eens dat Dorozhko de wet overtrad door in te breken op het netwerk. Volgens de New York Times hoeft er echter weinig medewerking van de plaatselijke autoriteiten te worden verwacht en is de kans vrij klein dat Dorozhko door Oekraïne wordt uitgeleverd om zich voor de Amerikaanse rechter te verantwoorden.

Sivarama Krishnan van PricewaterhouseCoopers is voorstander van een andere benadering, namelijk een internationaal geaccepteerde reeks protocollen voor het definiëren van acceptabele en onacceptabele activiteiten, procedures voor onderzoek en aanhouding van verdachten en richtlijnen voor vonnissen. Een dergelijke gestroomlijnde benadering leidt tot een veel grotere doeltreffendheid in de vervolging van internationale cybermisdaadzaken.

Krishnan wijst op de IATA-protocollen (International Air Travel Association) voor aankomende en vertrekkende vliegtuigen als mogelijk model voor dergelijke protocollen. De IATA-protocollen worden gevolgd ongeacht de nationaliteit van de luchtvaartmaatschappij, de primaire taal die door de bemanning wordt gesproken en het land waarin het vliegtuig aankomt en vertrekt.

### Bedrijven moeten zich anders opstellen ten opzichte van de beveiliging van hun informatiebezittingen

Deskundigen, zoals Michael Versace, senior adviseur bij FSTC (Financial Services Technology Consortium), zeggen dat bedrijven hun standpunt ten opzichte van de waardering en beveiliging van vitale informatie moeten aanpassen.

Versace zegt dat bedrijven hun beleidsvisie op informatiegovernance en beveiliging moeten uitbreiden tot voorbij de bedrijfsgrenzen. Ook moeten ze strategisch nadenken over de waarde van informatiebezittingen in samenwerkende ondernemingen, de gerelateerde risico- en risicoverminderingstechnieken en de juiste methoden voor risicobeheer en -bewaking als onderdeel van de dagelijkse bedrijfsactiviteiten.

Tom Longstaff, voorheen vice-directeur bij CERT en momenteel werkzaam aan de Johns Hopkins-universiteit, zegt het volgende: "Van oudsher hebben bedrijven beveiligingsmaatregelen ontwikkeld op basis van de intrinsieke waarde van informatie. Aangezien het erg moeilijk is om de waarde van informatiebezittingen te bepalen, leidt een dergelijke benadering tot inherente problemen. De beveiliging van deze bezittingen kan beter worden gebaseerd op de kosten die een bedrijf kwijt is aan het genereren van de betreffende informatie. Sommige banken zijn al gestart met het invoeren van een dergelijk systeem".

"Het geschatte verlies aan intellectuele eigendommen is aanzienlijk minder dan de werkelijke verloren waarde. Het zal nog wel enige jaren duren voordat bedrijven beseffen hoe groot dergelijke verliezen zijn", aldus Longstaff.

Veel bedrijven staan onder een enorme tijdsdruk om het aantal werknemers terug te brengen en het mes te zetten in andere uitgaven. Het blijft echter van groot belang om zorgvuldig met het menselijk element om te gaan.

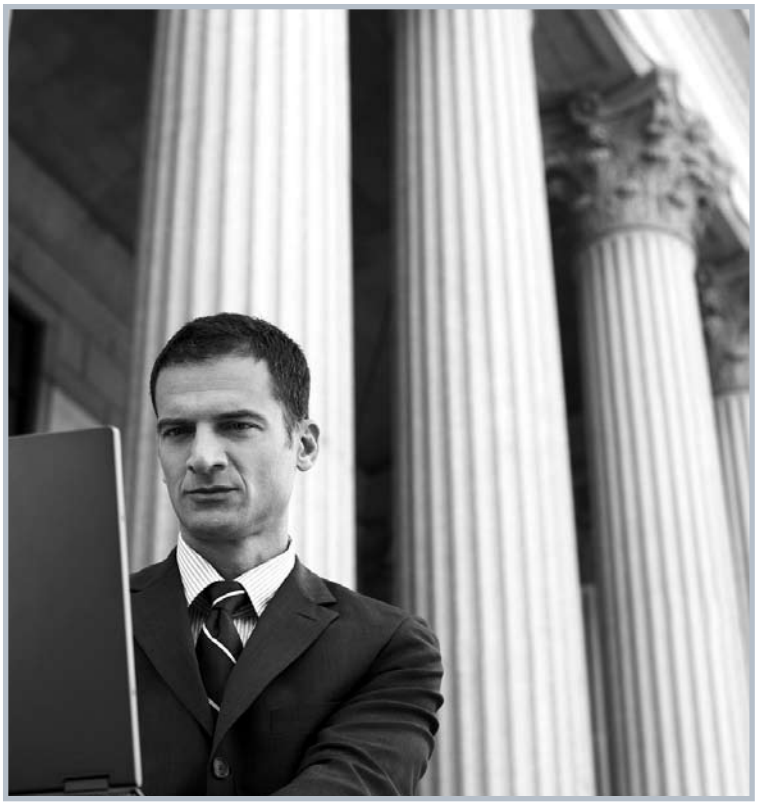
Een andere deskundige, Ashish Arora, professor aan de Duke-universiteit en gespecialiseerd in intellectuele eigendommen, geeft uitleg over de moeilijkheden die zich voordoen bij het bepalen van de waarde van informatiebezittingen (zoals intellectuele eigendommen): "We hebben maateenheden, zoals kosten per vierkante meter, waarmee we de waarde van een huis in een bepaalde buurt kunnen bepalen. Er is echter geen vergelijkbare maateenheid om de waarde van patenten en andere intellectuele eigendommen te bepalen. Het is moeilijk om voor die bezittingen de juiste risicoverminderende maatregelen op te stellen en de beveiliging van deze bezittingen kan daarom grote hiaten vertonen".

**CSO's van de toonaangevende softwarebedrijven in India, te weten Satyam, Wipro, Infosys, Tata, Cognizant en HCL (gezamenlijk ook wel SWITCH genaamd) zijn gaan samenwerken om de algemene problemen met betrekking tot het beveiligen van vitale informatie het hoofd te bieden. Ze komen elk half jaar bij elkaar om overleg te voeren over klantproblemen die betrekking hebben op dreigingen, en om te bepalen welke veranderingen er moeten worden uitgevoerd.**

### Bedrijven moeten werknemers beter scholen en personeelszaken en IT beter op elkaar afstemmen

Veel bedrijven staan onder een enorme tijdsdruk om het aantal werknemers terug te brengen en het mes te zetten in andere uitgaven. Het blijft echter van groot belang om zorgvuldig met het menselijk element om te gaan. Ontslagprocedures moeten zorgvuldig worden opgesteld en het gedrag van werknemers moet nauwkeurig worden gecontroleerd. Daarnaast moeten bedrijven gebruik maken van educatieve hulpmiddelen (bijvoorbeeld effectieve training) en technologische controles om hun systemen te bewaken en tegen ongewenst gedrag te beschermen.

Werknemers op alle niveaus van het bedrijf moeten worden getraind (en de training moet regelmatig worden herhaald) in de gevaren van phishing en andere social engineering-aanvallen. Bedrijven moeten beleidsregels opstellen en werknemers wijzen op de gevaren van blogs, sociale netwerksites en andere plaatsen waar informatie voor iedereen toegankelijk is. Daarnaast moeten bedrijven een partnerrelatie met leveranciers aangaan met als doel het ontwikkelen van geavanceerdere software en traceringsprogramma's om de validiteit van alle elektronische communicatie te waarborgen.



"Een bedrijf kan gegevens beveiligen en risico's verminderen door rekening te houden met informatiebeveiliging op de volgende zeven zakelijke gebieden: bedrijfsregels; indiensttredingsprocedures om de regels toe te lichten en te voorkomen dat gegevens van concurrenten de werkplek binnendringen; overeenkomsten met bestuurders, werknemers en derden waarin het gegevensbeleid wordt bevestigd; het complianceprogramma van het bedrijf; het gebruik van technologie voor het handhaven van de regels en het detecteren van gegevenslekken; ontslagprocedures en protocollen voor het reageren op een aanval", aldus Nick Akerman.

### Gegevensverlies in een recessie

Het is altijd, maar in het bijzonder tijdens een recessie, van groot belang zorgvuldig om te gaan met intellectuele eigendommen en waardevolle gegevens van klanten en burgers of andere bedrijfsinformatie. Veel bedrijven zijn van mening dat dit veel geld kost, maar als er zich een gegevenslek voordoet (van welke omvang dan ook) zijn de kosten alleen maar hoger. En een incident doet zich meestal voor op een tijdstip waarop een bedrijf zich geen extra kosten kan veroorloven. Hieronder staan enkele aanbevolen maatregelen voor deze bijzonder woelige tijden.

- Stel duidelijke contracten met specifieke beveiligingsvereisten voor outsourcebedrijven op.
- Handhaaf deze vereisten.
- Stel u op de hoogte van de wetten van het land en probeer te achterhalen of het land deze wetten ten uitvoer kan brengen als er zich een gegevenslek voordoet.
- Investeer in de juiste oplossingen om gegevens te beschermen, maar investeer ook in de werknemers. Zorg dat er voldoende werknemers in dienst blijven die weten waar de gegevens zich bevinden, hoe deze zijn beschermd en hoe er moet worden gereageerd als er zich een incident voordoet.
- Bescherm uw accounts tijdens ontslagen om er zeker van te zijn dat geen personen toegang hebben die niet op de actuele loonlijst staan.
- Verhoog de training en bewustwording van werknemers.
- Handhaaf het beleid jegens werknemers, zodat ze het belang van veilige bedrijfsactiviteiten beter begrijpen.

**Werknemers op alle niveaus van het bedrijf moeten worden getraind (en de training moet regelmatig worden herhaald) in de gevaren van phishing en andere social engineering-aanvallen.**

# Conclusie

Eén beveiligingsincident of verlies van vitale bedrijfsinformatie (zoals intellectuele eigendommen) kan onmiddellijke gevolgen hebben voor de winst, de aandelenkoers en het klantvertrouwen. In de huidige economische recessie zal de vraag naar illegaal verkregen intellectuele eigendommen of andere gevoelige informatie alleen maar toenemen nu cybercriminelen zoeken naar manieren om hun winst te verhogen en bedrijven proberen alle mogelijke onderzoeks- en ontwikkelingskosten te schrappen en de marktintroductietijd van goederen en diensten te versnellen.

Vitale informatie wordt kwetsbaarder nu technologieën steeds verder worden ontwikkeld en informatie zich verspreidt over netwerken van niet-beveiligde economieën. De onderlinge verbondenheid van de wereldeconomieën, in combinatie met de groeiende economische onzekerheid en de verschillende manieren waarop cybercriminaliteit wordt aangepakt, zullen grote problemen opleveren voor degenen die verantwoordelijk zijn voor het handhaven van de vertrouwelijkheid, integriteit en beschikbaarheid van vitale informatie, zoals intellectuele eigendommen.

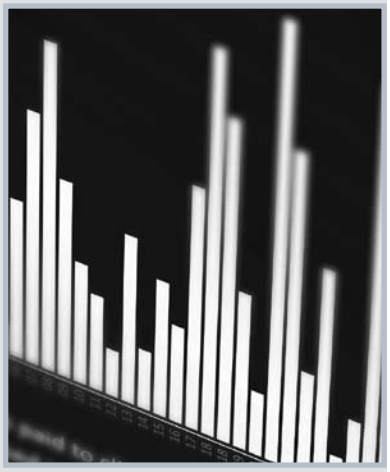
Professor Spafford van de universiteit van Purdue zegt hierover het volgende: "Informatiebeveiliging is veranderd van eenvoudig 'voorkomen dat er slechte dingen gebeuren' tot een essentieel bedrijfsonderdeel. Leidinggevenden op C-niveau moeten inspelen op deze verandering. Onder andere door internetbeveiliging als cruciaal bedrijfsmiddel te zien in plaats van slechts een kostenpost waarop zonder merkbare gevolgen voor de eindresultaten kan worden bezuinigd. Niet alle gevolgen zijn direct en rechtstreeks merkbaar. In sommige gevallen kan een bedrijf met een verlaagde internetbeveiliging zonder voorafgaande waarschuwing in één keer volledig worden geruïneerd".

"Cyberbeveiliging speelt meerdere rollen in een bedrijf en alle rollen zijn belangrijk om een organisatie gezond te houden, aldus professor Spafford.

- **Ten eerste** moet internetbeveiliging zorgen voor een positieve controle over de middelen waaraan het bedrijf zijn concurrentievoordeel ontleent: intellectuele eigendommen, klantgegevens, trends, toekomstverwachtingen, financiële en werknemersrecords, enzovoort. Een slechte beveiliging brengt deze middelen in gevaar.
- **Ten tweede** moet een goede beveiliging leidinggevenden het vertrouwen geven dat de gegevens die ze onder ogen krijgen waarheidsgetrouw en nauwkeurig zijn, zodat er gezonde beslissingen kunnen worden genomen en overheids- en bedrijfsregels correct worden nageleefd.
- **Ten derde** biedt een krachtige internetbeveiliging ondersteuning aan bedrijven die nieuwe risico's nemen en nieuwe markten betreden en daarbij vertrouwen op hun vermogen om correct op veranderingen te reageren.
- **En ten vierde** is goede internetbeveiliging nodig om een reputatie op te bouwen en te behouden op het gebied van betrouwbaarheid en gezond gedrag; waarden die op hun beurt nodig zijn om klanten en partners aan te trekken en te behouden. Uit dit onderzoek komt duidelijk naar voren dat sommige klanten geen zaken willen doen met entiteiten die als slecht beveiligd worden beschouwd."

Professor Spafford gaat verder "Gezien de grote wanorde op de markten, de aanzienlijke fraude en de toenemende dreigingen als gevolg van onoplettendheid en regelingen van overheidswege, zijn bedrijven met strikte controles, een transparante administratie, een flexibele infrastructuur en een eersteklas reputatie duidelijk in het voordeel. En een krachtige internetbeveiliging is een essentieel onderdeel van al deze vier voorwaarden. Leidinggevenden die hier rekening mee houden, kunnen internetbeveiliging gebruiken als organisch element voor het voortbestaan en de groei van een bedrijf (of overheidsinstelling)".

Tot slot merkt professor Spafford nog op: "Dit onderzoek toont aan dat men overal ter wereld op de hoogte is van internetbeveiligingsincidenten en cybercriminaliteit en dat er op veel gebieden sprake is van een aanzienlijk gebrek aan vertrouwen. Onze toekomst wordt echter niet bepaald door personen die dit soort resultaten gebruiken om angst te zaaien. Integendeel, onze toekomst wordt bepaald door leiders die mogelijkheden voor positieve actie zien en die streven naar het oplossen van de problemen".



**"Dit onderzoek toont aan dat men overal ter wereld op de hoogte is van internetbeveiligingsincidenten en cybercriminaliteit en dat er op veel gebieden sprake is van een aanzienlijk gebrek aan vertrouwen , aldus professor Spafford.**

# BIJDRAGEN

## NOORD-AMERIKA

**Nick Akerman** is partner in de praktijkgroep Trial van de firma Dorsey & Whitney LLP en covoorzitter van de sectie Computer Fraud and Abuse.

Hij vertegenwoordigt cliënten bij rechtszaken, beroepszaken en arbitragezaken in heel de Verenigde Staten. Zijn specialiteiten zijn: bescherming van bedrijfsgeheimen en computergegevens, complexe commerciële juridische procedures, interne onderzoeken en witteboordencriminaliteit. Akerman is voormalig openbaar aanklager en was werkzaam als assistent-aanklager in het Southern District of New York en tijdens de Watergate-affaire als assistent van de speciale aanklager bij de Watergate Special Prosecution Force. In 1972 behaalde Akerman de titel Doctor of Laws aan de Harvard Law School. Hij mag het beroep van advocaat uitoefenen in New York en Massachusetts.

**Dr. Ashish Arora (PhD)** is professor aan de Fuqua School of Management van de Duke-universiteit.

Hij doet onderzoek naar de economische aspecten van technologie en technische veranderingen. Arora's onderzoek is onder andere gericht op technologie-intensieve bedrijfstakken, zoals software, biotechnologie en chemische producten; de ondersteunende rol van patenten en licenties voor nieuwe technologiebedrijven en de economische aspecten van informatiebeveiliging. Samen met Alfonso Gambardella en Andrea Fosfuri schreef hij in 2001 het boek *Markets for Technology: The Economics of Innovation and Corporate Strategy in 2001*. Hij was tot 2006 werkzaam als mededirecteur bij het Software Industry Center van de Carnegie Mellon-universiteit. Hij zat in diverse commissies van organisaties, zoals de National Academy of Sciences en de Association of Computing Machinery. Hij is lid van de adviescommissie Measuring Innovation in the 21st Century Economy van het Amerikaanse ministerie van Economische zaken.

**Gail F. Farnsley** is momenteel gastprofessor aan het College of Technology van de universiteit van Purdue.

Voordat ze ging werken bij de universiteit van Purdue was Farnsley werkzaam als CIO en vicepresident van de afdeling IT bij Cummins, Inc. In deze functie was ze wereldwijd verantwoordelijk voor de informatietechnologie van het bedrijf, met inbegrip van het opstellen van strategieën en normen, de ontwikkeling, implementatie en ondersteuning van toepassingen, alsmede de IT-werkzaamheden en de infrastructuur. Voorafgaand aan haar aanstelling als CIO had ze verschillende IT-functies en woonde ze tweeënhalf jaar in het VK, waar ze leiding gaf aan de IT-organisatie van de regio Europa, Midden-Oosten en Afrika, alsmede aan de wereldwijde IT-organisatie van Cummins Power Generation. Voordat Farnsly bij Cummins aan de slag ging, was ze negen jaar in dienst bij Georgia-Pacific in Atlanta (in de Amerikaanse staat Georgia), werkte ze als analist bij Emery Airfreight en begon ze haar carrière bij Public Service Indiana (nu onderdeel van Duke Energy). Farnsly begon als programmeuse en werkte zich omhoog in de IT, voornamelijk door het ontwikkelen van toepassingen en in supportorganisaties. Ze maakte slechts één uitstapje buiten de IT om leiding te geven aan een verbeteringsproject voor bedrijfsprocessen.

**Karthik Kannan** is momenteel wetenschappelijk medewerker Management Information Systems aan de Krannert School of Management van de universiteit van Purdue en tevens faculteitslid van CERIAS.

Hij heeft een master in de elektro- en computertechniek en in overheidsbeleid en -beheer, alsmede een PhD in informatiesystemen, alle behaald aan de Carnegie Mellon-universiteit. Zijn twee voornaamste onderzoeksinteressen gaan uit naar de economische aspecten van informatiebeveiliging en de prijsstelling van goederen in de informatiecontext. Hij heeft wetenschappelijk artikelen over informatiesystemen gepubliceerd in belangrijke tijdschriften, onder andere in *Management Science* en *Information Systems Research*. Zijn artikelen zijn gebruikt bij een groot aantal conferenties en workshops, waaronder de Workshop on Economics of Information Security (WEIS), de International Conference on Information Systems (ICIS), de Workshop on Information Technology and Systems (WITS) en de Workshop on Information Systems Economics (WISE).

**Tom Longstaff (PhD)** is senior adviseur wetenschap en technologie bij de vakgroep Applied Information Science van het Applied Physics Laboratory (APL), Johns Hopkins-universiteit.

Longstaff trad in 2007 in dienst bij APL om in opdracht van de Amerikaanse overheid te werken aan een brede verscheidenheid van informatiegerichte activiteitenprojecten. Deze projecten hadden betrekking op informatiezekerheid, inlichtingenwerk en wereldwijde informatienetwerken. Voordat hij bij APL ging werken was Longstaff plaatsvervangend directeur technologie voor de CERT, bij het Software Engineering Institute van de Carnegie Mellon-universiteit. In de 15 jaar bij CERT heeft Longstaff een bijdrage geleverd aan het opzetten van veel van de projecten en centra op basis waarvan CERT een internationaal erkende netwerkbeveiligingsorganisatie kon worden. Longstaff moest onder andere het Amerikaanse ministerie van Binnenlandse Veiligheid en andere instellingen helpen om aan de hand van respons- en kwetsbaarheidsgegevens een onderzoeks- en activiteitenprogramma op te zetten en aan te sturen, dat werd gebruikt voor het analyseren en voorspellen van netwerkbeveiligings- en cyberterrorisme-incidenten. De wetenschappelijke publicaties van Longstaff bestrijken onderwerpen als malware-analyse, informatiebehoud, dreigingen van binnenuit, inbraakdetectie en het samenstellen van inbrekersprofielen. Hij speelt nog steeds een actieve rol in de gemeenschap voor informatiezekerheid en geeft organisaties regelmatig advies over de toekomst van netwerkdreigingen en informatiezekerheid. Longstaff is faculteitslid van de Johns Hopkins-universiteit en fellow van het International Information Integrity Institute.

**Jacquelyn Rees** is momenteel universitair hoofddocent Management Information Systems aan de Krannert Graduate School of Management van de universiteit van Purdue.

205 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656
546 78952 565.369 21 4477787 4651

Ze behaalde in 1998 haar PhD in besliskunde en informatica aan het Warrington College of Business van de universiteit van Florida. Haar onderzoeksinteressen gaan onder andere uit naar risicobeheer in informatiebeveiliging, privacy en evolutionaire berekeningen. Ze heeft artikelen gepubliceerd in tijdschriften als *Communications of the ACM*, *Decision Sciences, Decision Support Systems*, *European Journal of Operational Research*, *INFORMS Journal on Computing*, *Information Technology and Management*, *International Journal of Electronic Commerce* en de *Journal of Organizational Computing and Electronic Commerce*.

**Dr. Timothy J. Shimeall (PhD)** is senior lid van de technische afdeling bij het Networked Systems Survivability Program van het Software Engineering Institute (SEI).

Het CERT Coordination Center maakt ook deel uit van dit programma en voor zijn werkzaamheden maakt Shimeall veel gebruik van gegevens van het Center. Shimeall houdt toezicht op en werkt mee aan de ontwikkeling van analysemethoden op het gebied van beveiliging en behoud van netwerksystemen. Zijn werk omvat het ontwikkelen van methoden voor het identificeren van trends in beveiligingsincidenten en in de ontwikkeling van software die door computer- en netwerkinbrekers wordt gebruikt. De nadruk ligt op incidenten die invloed hebben op verdedigingsystemen en kwaadaardige software die ondanks algemene verdedigingsmiddelen toch effectief is.

**Eugene H. Spafford** wordt algemeen erkend als een van de belangrijkste leiders op het gebied van informatiebeveiliging. Spaf, zoals hij door zijn vrienden en collega's wordt genoemd, is al meer dan 25 jaar betrokken bij onderzoek, onderwijs en praktijk op het gebied van IT-beveiliging en IT-betrouwbaarheid. Hij is hoogleraar Informatica aan de universiteit van Purdue in de Verenigde Staten en is oprichter en algemeen directeur van CERIAS. Spafford is fellow van de ACM, de IEEE, de AAAS en de (ISC)$^2$. Zie http://bio.spaf.us voor meer informatie.

**Michael Versace** is momenteel Senior Advisor bij het Financial Services Technology Consortium (FSTC).

Zijn prestaties omvatten de ontwikkeling en introductie van FEDNET (het Amerikaanse backbone-netwerk voor het betalingsverkeer), de invoering van internet- en chipkaartbetalingsmogelijkheden, de implementatie van gedistribueerde cryptografische systemen in ATM- en POS-netwerken en het ontwerp van algemene programma's voor technologierisico's. Hij was voorzitter en vicevoorzitter van de technische commissie voor de beveiliging van financiële systemen bij de International Standards Organization (ISO), hoofd van de Amerikaanse vertegenwoordiging bij de ISO, bestuursvoorzitter van X9, Inc. en programmamanager bij het Financial Services Technology Consortium. Hij heeft meegewerkt aan de ontwikkeling van een groot aantal technische normen voor cryptografie, risicobeheer en informatiebeveiligingsbeleid.

## EMEA

**Dr. Ross Anderson (PhD)** is professor in Security Engineering aan de universiteit van Cambridge.

Hij is medeoprichter van een zeer snel groeiende nieuwe discipline: beveiligingseconomie. Veel beveiligingsproblemen kunnen worden teruggevoerd op verkeerde stimulansen in plaats van technische fouten. De toepassing van de micro-economische theorie heeft nieuw licht geworpen op veel problemen die voorheen als bijna onoplosbaar werden beschouwd. Anderson heeft tevens veel bijdragen geleverd op technisch gebied. Hij is pionier op het gebied van peer-to-peer-systemen, knoeibestendigheid van hardware, copyrightwatermerken en API-beveiliging. Anderson was tevens mede-uitvinder (met Eli Biham en Lars Knudsen) van het Serpent-algoritme, dat een finaleplaats in de Advanced Encryption Standard-wedstrijd wist te veroveren. Hij is voorzitter van de Foundation for Information Policy Research, in het VK het belangrijkste researchinstituut op het gebied van internet- en technologiebeleidsproblemen. Hij is fellow van het IET en de IMA en schreef het gezaghebbende handboek *Security Engineering—A Guide to Building Dependable Distributed Systems*.

**Lynn Robert Carter** is al meer dan negentien jaar senior onderzoeker en docent aan de Carnegie Mellon-universiteit.

Tijdens zijn twaalf jaar bij de SEI bestond zijn werk onder andere uit ondersteuningswerkzaamheden tijdens de implementatie van onsite software-technologieën bij een groot aantal militaire en commerciële klanten. Het ging hierbij om de volgende technologieën: realtime schedulability, client/server-systeemarchitecturen, objectoriëntatie, procesverbetering en organisatorische wijzigingen. Na zijn vertrek bij SEI ondersteunde hij de ontwikkeling en invoering van hbo-masterstudies Software Engineering bij CMU West, bij onze partners van de SSN School of Advanced Software Engineering te Chennai (India) en bij het International Institute for Information Technology te Hyderabad (ook in India). Momenteel helpt hij mee aan het uitstippelen van een softwareontwikkelingstraject voor bachelorstudenten binnen het afstudeer-programma Informatica van de Carnegie Mellon-universiteit in Katar en werkt hij aan de ontwikkeling van hbo-masterstudies van deze nieuwe faculteit. Zijn onderzoek is gericht op de invoering van nieuwe softwaretechnologieën en spitst zich met name toe op de verwachte ontwikkeling en beheer van kwaliteitssoftware voor hoogwaardige systemen. Carter heeft zich meer dan 11 jaar ingezet voor de accreditatie van informatica en softwareontwikkeling en is momenteel actief als ABET Commmissioner en Executive Committee Member. Voorafgaand aan zijn periode bij de Carnegie Mellon-universeit, hield Carter zich 17 jaar lang bezig met het ontwikkelen van software, het leiding geven aan teams en het leiden van onderzoeksactiviteiten bij verschillende commerciële bedrijven, onder andere: Tektronix, Motorola, GenRad en twee nieuwe bedrijven. Bij GenRad gaf hij leiding aan de leveraged buyout van de testapparatuurdivisie voor datacommunicatie en trad hij op als directeur en CEO van de spinout. In 1980 behaalde hij aan de universiteit van Colorado (in Boulder) zijn PhD in de informatica en in 1972 en 1974 behaalde hij aan de Portland State-universiteit achtereenvolgens zijn bachelor en master in wiskunde, met informatica als specialisatie.

5 5622350479 658. 7895200.02. 33695 454868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656 546 78952 565.369 21 77787 4651

54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568

4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568 44 822.656

**Lilian Edwards:** professor Internetrecht, universiteit van Sheffield, VK.

Lilian Edwards leidt aan de Sheffield-universiteit een onderzoeks- en onderwijsprogramma gericht op internetrecht en nieuwe technologieën. Haar onderzoeksinteressen gaan voornamelijk uit naar internetrecht en communicatietechnologieën (met speciale aandacht voor Europees recht en rechtsvergelijking). Haar onderzoek concentreert zich momenteel op de rol van tussenpersonen en ISP's op internet, online privacy- en gegevensbeveiliging, cybercriminaliteit en cyberbeveiliging, Web 2.0 en de wetgeving, digitale intellectuele eigendommen en e-commerce. Ze heeft als mederedacteur gewerkt aan twee edities van haar bestseller *Law and the Internet* (de derde editie wordt begin 2009 verwacht) en een derde reeks essays, genaamd *The New Legal Framework for E-Commerce in Europe.* Voor haar werk met betrekking tot online consumentenprivacy ontving Edwards in 2004 de Barbara Wellbery Memorial Prize voor de beste oplossing voor het privacyprobleem en wereldomspannende gegevensstromen. Edwards is adviseur voor BILETA, ISPA, FIPR en de Online Rights Group en werkt als consultant voor de Europese Commissie en WIPO.

**Dr. Marco Gercke** is advocaat in Duitsland. Hij doceert Rechten (cybercriminaliteit en Europees strafrecht) aan de universiteit van Keulen en is gastdocent Internationaal strafrecht aan de universiteit van Macau.

Gercke geeft regelmatig lezingen in allerlei landen en heeft meer dan 50 publicaties over het onderwerp cybercriminaliteit op zijn naam staan. Zijn voornaamste onderzoeksgebieden zijn de internationale aspecten van cybercriminaliteit (met name de problemen ten aanzien van de bestrijding van cybercriminaliteit en de juridische respons) en rechtsvergelijkende analyses inzake de implementatie van internationale normen. Zijn laatste onderzoek was gericht op de activiteiten van terroristische organisaties op internet, identiteitsdiefstal, online witwassen van geld en de juridische respons op de opkomst van encryptietechnologie. Gercke is secretaris van de afdeling Strafrecht van het Duitse Gesellschaft für Recht und Informatik, lid van de ITU High Level Expert Group en werkzaam als expert voor de Raad van Europa, de International Telecommunication Union en andere internationale organisaties.

## LATIJNS-AMERIKA

**Augusto Paes de Barros** is sinds 2000 werkzaam als informatiebeveiligingsprofessional.

Hij heeft niet alleen als consultant maar ook als beveiligingsmanager gewerkt. Momenteel werkt hij als Senior Information Security Specialist voor een van de grote Canadese banken in Toronto. Hij publiceert regelmatig opiniestukken over verschillende beveiligingsonderwerpen, met name via zijn blog, artikelen in vakbladen en presentaties op conferenties over de hele wereld. In 2006 en 2007 was hij tevens president van het Braziliaanse ISSA Chapter.

**Renato Opice Blum:** Opice Blum Advogados Associados, Brazilië

Opice Blum Advogados Associados beschikt over een jarenlange gedegen ervaring op de belangrijkste rechtsgebieden, met name in technologie, e-wetgeving, informatietechnologie en variaties daarop. Het bedrijf is, als pionier op dit terrein, tevens actief op het gebied van bemiddelingsprocedures, arbitragezaken, mondelinge ondersteuning bij rechtszaken, biowetgeving, specifieke technologische contracten, cybercriminaliteit, enzovoort. Het werkgebied omvat het hele Braziliaanse grondgebied en het bedrijf heeft tevens internationale correspondenten in de belangrijkste internationale financiële centra, zoals Miami en New York.

Als lid van diverse institutionele organisaties draagt Opice Blum Advogados Associados bij aan de ontwikkeling van de wetgeving inzake technologische ontwikkelingen. Het bedrijf heeft bijzondere prestaties op zijn naam staan, onder andere als oprichtende partner van de Braziliaanse Kamer van Elektronische Handel en als lid van de Braziliaanse Vereniging voor Computergebruik.

## AZIË-PACIFIC

**Sivarama Krishnan** is momenteel directeur bij PricewaterhouseCoopers, te Mumbai.

Krishnan heeft meer dan 15 jaar ervaring en geeft leiding aan de afdeling IT-risicobeheer en -beveiliging in het bedrijf. Hij heeft ervaring met projecten in verschillende landen, waaronder India, Koeweit, Bahrein, de Verenigde Arabische Emiraten, Oman, Sri Lanka, Bangladesh, Nederland, Singapore, het VK en de VS. Hij geeft leiding aan een team van meer dan 75 IT-professionals en is expert op het gebied van onder andere IT-beveiliging, e-governance en telecommunicatie. Krishnan heeft praktische ervaring in het ontwerpen van netwerken, het implementeren van e-governance-toepassingen en het opzetten van IS, een beheer- en beveiligingsstructuur voor grote bedrijven en overheden. Hij heeft een opleiding tot accountant genoten en is werkzaam als gastdocent bij het Institute of Chartered Accountants in India en het Indian Institute of Foreign Trade te Delhi.

**Heejo Lee** is associate professor bij de divisie Computer and Communication Engineering aan de universiteit van Korea (in Seoul).

Voordat hij zich verbond aan de universiteit van Korea, werkte hij van 2001 tot 2003 als CTO bij AhnLab, Inc. Van 2000 tot 2001 werkte hij als postdoc bij de vakgroep Computer Sciences en het beveiligingscentrum CERIAS van de universiteit van Purdue. Hij behaalde zijn bachelor, master en PhD in Computer Science and Engineering op de Pohang University of Science & Technology (in Korea). Lee werkt tevens als redacteur bij het Journal of Communications and Networks. Daarnaast is hij adviserend lid van het Korea Information Security Agency en het Korea Supreme Prosecutor's Office. Lee heeft met steun van de Koreaanse overheid gewerkt aan het samenstellen van de nationale CERT op de Filippijnen (2006) en het verstrekken van adviezen over internetbeveiliging in Oezbekistan (2007). Zie http://ccs.korea.ac.kr voor meer informatie.

8 4568 44 822.656 546 78952 565.369 21
54868.45 5 48 4528782 45 4582 688.54 58 89 8 4568

5 4528782 45 4582 688.54 58 89 8 4568 44 822.656 54868.45 5

**Yoshiyasu Takefuji (PhD)** is sinds april 1992 als professor verbonden aan de faculteit Environmental Information van de universiteit van Keio. Hij was sinds 1988 werkzaam aan de faculteit Electrical Engineering van de Case Western Reserve-universiteit.

Daarvoor gaf hij les aan de universiteit van Zuid-Florida en de universiteit van Zuid-Carolina. Hij behaalde zijn bachelor (1978), master (1980) en PhD (1983) in Electrical Engineering aan de universiteit van Keio, met als promotor professor Hideo Aiso. Zijn onderzoeksinteressen gaan uit naar neurale netwerken, beveiliging, internetgadgets en non-lineair gedrag. Hij ontving in 1989 de National Science Foundation/Research Initiation Award en in 1992 de IEEE Transactions on Neural Networks-award (voor bijzondere diensten op het gebied van neurale netwerken). Daarnaast werkt hij als adviserend NSF-lid. Van 1993 tot 1995 ontving hij de TEPCO-onderzoeksprijs en in 1995 de Takayanagi-onderzoeksprijs. Verder kreeg hij van 1993 tot 1995 de Kanagawa Academy of Science and Technology-onderzoeksprijs. Hij heeft bovendien diverse boeken gepubliceerd en is redacteur geweest bij verschillende tijdschriften. Hij heeft meer dan 100 conferentieverslagen en meer dan 120 wetenschappelijke artikelen in tijdschriften gepubliceerd. Hij staat vermeld in *Who's Who in America, Who's Who in the Midwest* en *Who's Who in Science and Engineering, Men of Achievement.* Hij was respectievelijk adviseur voor de Multimedia-universiteit in Maleisië, de PSDI (Philippines Software Development Institute) van de Filippijnse overheid, de VITTI (Vietnam Information Technology Training Institute) en de CTTISC (Computer Technology, Training and Industrial Studies Center) van Sri Lanka, Thailand en Jordanië. Hij is officieel raadgever van de regering in Hongkong.

**Professor Katsuya Uchida (PhD)** is faculteitslid van de Graduate School van het Institute of Information Security in Japan. Hij behaalde zijn PhD in Science en Engineering aan de universiteit van Chuo. Hij houdt zich bezig met de ontwikkeling en gebruikersondersteuning van COBOL-compilatieprogramma's bij een kleine handelaar in bedrijfscomputers; EDP-controles en technische ondersteuning voor het elektronisch bankiersysteem van een Amerikaanse bank in Japan; een implementatieproject voor computerverzekeringen en een onderzoek naar informatiebeveiliging bij een grote non-life verzekeringsmaatschappij in Japan. Momenteel is hij verbonden aan het Institute of Information Security, waar hij les geeft in systemen voor informatiebeveiligingsbeheer, risicobeheer en praktische beveiligingssystemen. Zijn belangrijkste onderzoeksonderwerpen zijn systemen voor informatiebeveiligingsbeheer, informatiebeveiligingspsychologie en risicobeheer. Uchida is lid van het Computer Security Institute en van de Information Processing Society van Japan. Hij is tevens assistent-CIO van de stad Yokohama.

**Dr. Sun Yuqing (PhD)** is momenteel universitair hoofddocent aan de School of Computer Science en directeur van de vakgroep Electronic Business Technology aan de universiteit van ShanDong.

Haar onderzoeksactiviteiten hebben betrekking op verschillende onderwerpen: onder andere toegangscontrolemodellen en -technologie, beveiligingsbeleid, beveiliging in webservices, werkstroombeheer en vertrouwensbeheer. Ze heeft in de afgelopen jaren meer dan twintig wetenschappelijke artikelen voor internationale conferenties en tijdschriften gepubliceerd. Daarnaast is ze hoofdonderzoeker bij diverse projecten, onder andere het project voor fundamenteel wetenschappelijk onderzoek en de Momentous Science Development Plan Program van de provincie Shandong. Ze schrijft recensies voor een groot aantal vakbladen en is lid van programmacommissies van veel internationale conferenties. Momenteel is ze lid van de programmacommissies van ICESS'09, MUE'09, CIS'08, ICPCA08, SCC08, EDOC08, ICMLC08, ICESS08, MUE08, enzovoort.

McAfee International
Gatwickstraat 25
Postbus 58326
1043 GL Amsterdam
The Netherlands

+ 31 (0)20 5863800

www.mcafee.com/nl

Neem voor vragen over PR en
andere vragen contact op met:

Sal Viveros
McAfee, Inc.
+44 (0) 1753.217492 of +1.408.346.3696
Sal_Viveros@mcafee.com

Stuart Yeardsley
Red Consultancy for McAfee, Inc.
+1.415.618.8814
stuart.yeardsley@redconsultancy.com

McAfee, Inc. is het grootste bedrijf ter wereld dat gespecialiseerd is in beveiligingstechnologie. Het hoofdkantoor is gevestigd in Santa Clara, in de Amerikaanse staat Californië. McAfee streeft voortdurend naar het oplossen van 's werelds grootste beveiligingsproblemen. Het bedrijf biedt proactieve en bewezen oplossingen en services die systemen en netwerken over de hele wereld beveiligen, zodat gebruikers veiliger op internet kunnen surfen en winkelen. McAfee kan dankzij zijn bekroond onderzoeksteam vernieuwende producten ontwikkelen die thuisgebruikers, bedrijven, de overheid en serviceproviders de mogelijkheid bieden om regelnaleving te bewijzen, gegevens te beveiligen, onderbrekingen te voorkomen, kwetsbaarheden te identificeren en hun beveiliging voortdurend te controleren en te verbeteren.

http://www.mcafee.com