

Global Information Security Survey 2005

- Toelichting op enkele opvallende onderzoeksresultaten -

Drijfveren voor informatiebeveiliging

‘Voldoen aan wet- en regelgeving’ blijkt dit jaar de grootste drijfveer te zijn voor informatiebeveiliging, in plaats van computervirussen en –wormen. Dit geldt voor de Nederlandse respondenten in hogere mate (79%) dan voor de wereldwijde respondenten (61%).

Op zich is het natuurlijk geen verrassing dat organisaties als gevolg van toenemende wet- en regelgeving, zoals de Sarbanes Oxley Act en de Code Tabaksblat, meer aandacht hebben gekregen voor informatiebeveiliging. Maar zelfs bedrijven die niet aan deze specifieke wetten en regels hoeven te voldoen, geven aan dat zij qua informatiebeveiliging aan de gestelde eisen willen voldoen.

Top 3 drijfveren voor informatiebeveiliging:

Afgelopen jaar	Internationaal	Nederland
	1. Wet- en regelgeving (61%)	1. Wet- en regelgeving (79%)
	2. Computervirussen en –wormen (53%)	2. Beveiligingsbeleid eigen organisatie (51%)
	3. Bedrijfsdoelstellingen (49%)	3. Computervirussen en –wormen (39%) en bedrijfsdoelstellingen (39%)
Komende jaar	Internationaal	Nederland
	1. Wet- en regelgeving (60%)	1. Wet- en regelgeving (71%)
	2. Bedrijfsdoelstellingen (55%)	2. Bedrijfsdoelstellingen (56%)
	3. Computervirussen en –wormen (31%)	3. Beveiligingsbeleid eigen organisatie (53%)

Risicobeheersing leveranciers

Vorig jaar zagen we al dat veel bedrijven processen hebben uitbesteed, maar de beveiliging van hun zakenpartners vaak niet (laten) controleren. Dit jaar geeft 25% van de Nederlandse respondenten aan dat de vendor/partner gecertificeerd is en 19% geeft aan dat door een onafhankelijke partij is vastgesteld of de vendor/partner voldoet aan erkende standaarden. De meerderheid stelt niet zelf vast dat de beveiliging van hun zakenpartners in orde is.

Toepassing internationale standaarden

Veel Nederlandse organisaties kiezen voor internationale standaarden en modellen zoals de Code voor Informatiebeveiliging (ISO 17799), CobIT en ITIL. Maar liefst 44% van de Nederlandse respondenten maakt bijvoorbeeld gebruik van de Code voor Informatiebeveiliging, wereldwijd is dit 26%. Deze standaarden hebben zich in de praktijk bewezen en door toepassing van deze standaarden laat je als organisatie zien dat je op serieuze wijze omgaat met zaken als informatiebeveiliging en het beheer van je IT-organisatie.

Nieuwe technologieën, nieuwe risico's

Bedrijven spreken duidelijk hun zorg uit over de beveiligingsrisico's die populaire technologieën zoals mobile computing, removable media (zoals USB sticks) en draadloze netwerken met zich meebrengen. Ruim driekwart van de organisaties zegt hiervoor in het komende half jaar maatregelen te gaan treffen.

Top 3 technologische toepassingen met significante beveiligingsrisico's in Nederland

Technologie	Aandachtspunt binnen nu en zes maanden
1. Mobile computing (58%)	80%
2. Removable media (47%)	84%
3. Wireless networks (44%)	78%

Informatiebeveiliging en *enterprise risk management*

Tweederde van de respondenten geeft aan formeel een security officer te hebben aangesteld, in Nederland geldt dit zelfs voor 72%. Toch geeft meer dan een kwart van hen aan dat deze functie geen deel uitmaakt van het overkoepelende risicomanagement proces .

In hoeverre is de informatiebeveiligingsfunctie geïntegreerd met uw overkoepelende risicomanagement

(Niveau 1 = niet geïntegreerd, niveau 5 = volledig geïntegreerd)

Niveau 5	13%
Niveau 4	22%
Niveau 3	30%
Niveau 2	27%
Niveau 1	7%

Verantwoording informatiebeveiliging

Bij 40% van de wereldwijde respondenten vindt zelden of nooit overleg plaats tussen degenen die verantwoordelijk zijn voor informatiebeveiliging en de topdirectie of de audit commissie. Dit geldt ook voor 37% van de Nederlandse respondenten.

In Nederland vindt het meeste overleg plaats met de IT-afdeling. 78% van de Nederlandse respondenten geeft aan dat hiermee minstens iedere maand overleg plaatsvindt. Het minst vaak vindt overleg plaats met Juridische afdelingen: wereldwijd geeft 44% van de respondenten aan hier zelden of nooit overleg mee te hebben, in Nederland gaat dit om 50% van de respondenten.

Percentage Nederlandse respondenten dat aangeeft zelden tot nooit overleg te voeren met:

Board of Directors / Audit Committee	37%
Internal Audit	16%
Compliance	36%
Legal	50%

Belemmerende factoren op strategisch niveau

Wereldwijd geeft meer dan de helft van de respondenten aan dat er te weinig ervaren en goed opgeleid personeel beschikbaar is voor aandacht voor informatiebeveiliging op strategisch niveau. In Nederland wordt daarnaast het gebrek aan een beheersraamwerk door veel respondenten genoemd als belangrijk obstakel (48%).

Training en awareness programma's

Wereldwijd heeft 48% van de respondenten formele procedures voor training en awareness programma's (Nederland: 27%). De meerderheid van de Nederlandse respondenten heeft hier informele procedures voor (54%).

Minder dan de helft van de deelnemende organisaties geeft voorlichting aan de algemene gebruikersgroepen over de impact van mogelijke beveiligingsincidenten op de organisatie. Ook wordt weinig voorlichting gegeven over de voorschriften en procedures die in acht moeten worden genomen in het geval zich daadwerkelijk een incident voordoet, alhoewel daar in Nederland duidelijk meer aandacht aan wordt besteed.

Onderwerpen die voor de verschillende doelgroepen aan bod komen in training en awareness programma's:

	Hoger management	Algemene gebruikersgroepen
Impact van security issues op de organisatie	Wereldwijd: 67 % Nederland: 76%	Wereldwijd: 46% Nederland: 42%
Richtlijnen en procedures	Wereldwijd: 64% Nederland: 43%	Wereldwijd: 85% Nederland: 77%
Hoe te handelen in geval van incidenten	Wereldwijd: 32% Nederland: 43%	Wereldwijd: 41% Nederland: 53%

Over de Global Information Security Survey

Ernst & Young Technology & Security Risk Solutions (in Nederland EDP Audit genoemd) doet al sinds 1993 onderzoek naar de stand van zaken op het gebied van informatiebeveiliging. Aan de 2005 editie van het onderzoek Global Information Security Survey hebben wereldwijd meer dan 1.300 organisaties uit 55 landen meegedaan. In Nederland hebben 95 organisaties uit verschillende sectoren aan het onderzoek meegewerkt. Het volledige onderzoeksrapport kunt u downloaden via www.ey.nl (publicaties).

Over Ernst & Young EDP Audit

Ernst & Young EDP Audit is een gespecialiseerde adviesgroep van Ernst & Young Accountants. Internationaal wordt de groep TSRS (Technology and Security Risk Services) genoemd. In deze onafhankelijke adviesgroep werken edp-auditors met verschillende achtergronden (informaticadeskundigen, technische specialisten en accountants) met elkaar samen om cliënten te helpen met het optimaliseren van de kwaliteit, veiligheid en betrouwbaarheid van hun ICT en het minimaliseren en beheersen van de risico's.

Meer informatie:

Ernst & Young EDP Audit, Monique Otten, tel.(030) 259 26 01, edp-audit@nl.ey.com.