



Thursday, April 21, 2016  
QuizXpress Studio 3.3.4.4  
C:\Users\Turien\Desktop\Quiz lac Zuid.qx



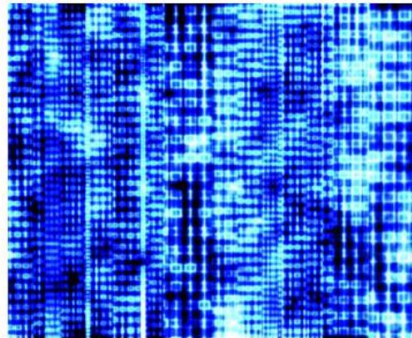
KENNISMAKEN **MET ONS**



TURIEN & CO. ASSURADEUREN

BJÖRN JALVING

# CYBER?!



## DE MARKT

### CYBER INSURANCE IN PREMIEVOLUME

▪ 2012	\$ 850 Miljoen
▪ 2013	\$ 1,3 Miljard
▪ 2014	\$ 2,0 Miljard
▪ 2015 (mei)	\$ 2,5 Miljard



# DE MARKT

## CYBER VERZEKERING IN NEDERLAND



**Bjorn Jalving**

Volmachtmanager & Business developer at Turien & Co. Assuradeuren

Leuk artikel van [mr. Yasin Chalabi](#) van onze business partner Hiscox! Ook bij [Turien & Co Assuradeuren](#) merken wij veel meer vraag sinds november / december. Op 10 mei organiseren wij daarom voor de vierde keer een Turien & College over... [show more](#)



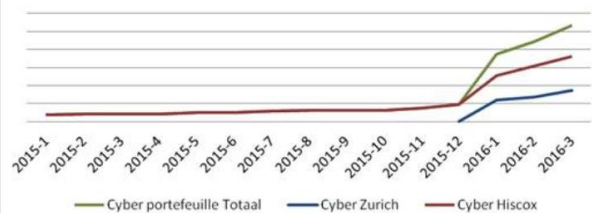
"Vraag naar #cyberverszekering stijgt explosief, aldus #Hiscox

[vvponline.nl](#) • De belangstelling onder het Nederlandse bedrijfsleven voor cyber- en dataverzekeringen neemt explosi...

[Like](#) • [Comment](#) • [Share](#) • 14

Aanbieders in de markt:  
AIG, CNA, Chubb, Hiscox,  
Liberty en Zurich

**Cyberverzekering bij Turien**



# DE SPELREGELS

## De Quiz

- Minimaal twintig seconden per vraag
- Snel geantwoord? Meer Punten!

### Puntenverdeling

- Goed geantwoord: 10 tot 30 punten
- Fout antwoord: 5 punten aftrek
- Niet geantwoord: 10 punten aftrek



### Oefenvraag 1.

In de zakelijke risicoanalyse breng ik de internetafhankelijkheid van een bedrijf in kaart

<b>A</b>	<b>B</b>
Ja ✓	Nee



### Oefenvraag 2.

In de zakelijke risicoanalyse breng ik in kaart over wat voor soort gegevens (data) een bedrijf beschikt.

<b>A</b>	<b>B</b>
Ja ✓	Nee





### Oefenvraag 3.

Onze relaties zijn geïnformeerd over de Meldplicht Datalekken

- A** Ja per (e-mail)nieuwsbrief ✓
- B** Ja op een andere manier
- C** Nee

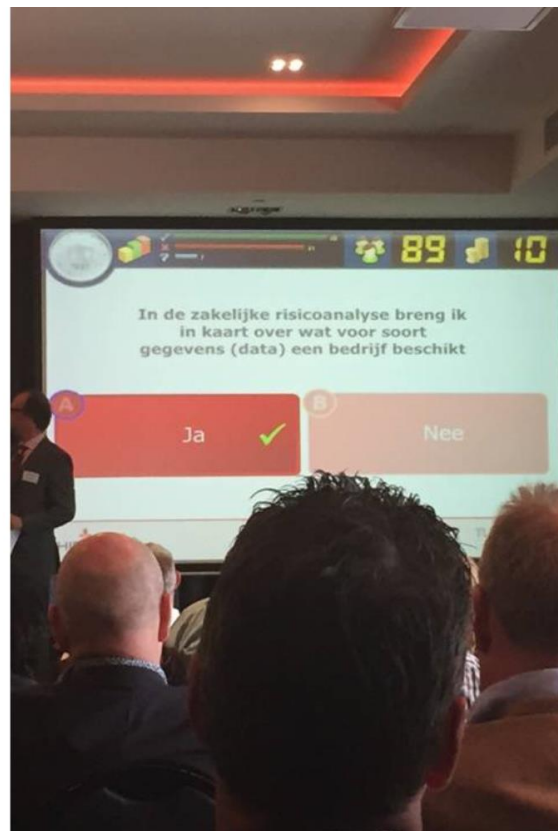
HISCOX

TURIEN & CO  
ASSURADEUREN

## CYBERADVIES 2015/2016

### ANTWOORDEN IN 2015

- 51% van de adviseurs gaf in juni 2015 aan de internetafhankelijk van een bedrijf mee te nemen in de zakelijke risicoanalyse
- 45% van de adviseurs gaf in 2015 aan in kaart te brengen over wat voor soort gegevens (data) een bedrijf beschikt
- Turien & Masterclass cyberrisico's. Dinsdag 9 en donderdag 11 juni 2015. Aantal adviseurs 145.



# En dan nu om de punten!



## 4. Welk cyberincident komt er in het bedrijfsleven het meeste voor?

- |                        |                            |                        |
|------------------------|----------------------------|------------------------|
| <b>A</b><br>Phishing ✓ | <b>B</b><br>Cyber-spionage | <b>C</b><br>Cryptoware |
| <b>D</b><br>DDOS       | <b>E</b><br>Hacking        | <b>F</b><br>Defacement |

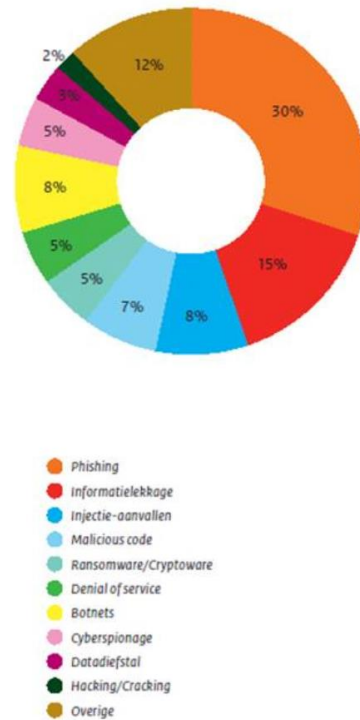


# CYBER INCIDENTEN

## IN NEDERLAND

- Cijfers van het Nationaal Cyber Security Centrum (NCSC)
- Cijfers over april 2014 tot en met april 2015
- Phishing komt met afstand het meeste voor
- Sectoren die vaak onder vuur liggen zijn overheid, financiële instellingen en de zorg.

Figuur 20 Type incidenten waarbij een private partij betrokken was



## 5. Wat is geen digitaal risico?

<b>A</b> Cryptoware	<b>B</b> Pharming	<b>C</b> Camfecting
<b>D</b> Social engineering	<b>E</b> Chesapeake	<b>F</b> Ransomware



# CYBERRISICO'S

## NADER OMSCHREVEN

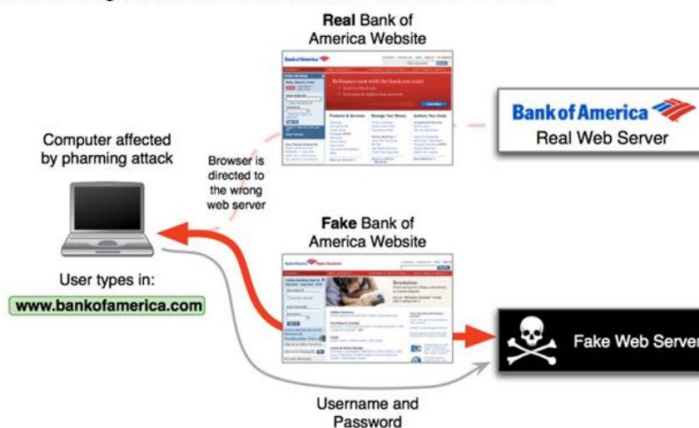
- **Cryptoware:** Het ongewild versleutelen van de bestanden op een computer. Waarbij er geld gevraagd wordt voor de sleutel
- **Pharming:** Een oplichtingstechniek die het slachtoffer misleidt door hun internetverkeer hem of haar met een bepaalde website ongemerkt om te leiden naar een andere website.
- **Camfecting:** Inbreken in een webcam of beveiligingscamera
- **Social engineering:** Een hack uitvoeren met als startpunt een menselijke fout.
- **Chesapeake:** een stad in de Verenigde Staten
- **Ransomware:** Het ongewild versleutelen van een computer. Waarbij er geld gevraagd wordt voor de sleutel.



# CYBERRISICO'S

## PHARMING NADER OMSCHREVEN

- Een oplichtingstechniek die het slachtoffer misleidt door hun internetverkeer hem of haar met een bepaalde website ongemerkt om te leiden naar een andere website.



# CYBERRISICO'S

## RANSOMWARE NADER OMSCHREVEN

- Het ongewild versleutelen van de bestanden op een computer. Waarbij er geld gevraagd wordt voor de sleutel



# CYBERRISICO'S

## CRYPTOWARE NADER OMSCHREVEN

- Het ongewild versleutelen van de bestanden op een computer. Waarbij er geld gevraagd wordt voor de sleutel



# CYBERRISICO'S

## IN HET MKB

- Gehackte telefooncentrale
- Politievirus / Locky ransomware
- DDOS
- Kwijtraken laptop of USB stick
- Datadiefstal
- Naar schatting wordt ongeveer 1 op de 3 MKB'ers slachtoffer van een of andere vorm van cybercrime
- MKB'ers vormen een aantrekkelijke prooi voor cybercriminelen omdat er meer bij hen te halen valt dan bij de gemiddelde consument, maar de meeste ondernemers hun cybersecurity niet beter hebben geregeld dan de gemiddelde consumenten.



## 6. Datalek: voor welke sector zijn de kosten met € 287 per record het hoogste bij een inbreuk op data?

<b>A</b> Zakelijke en professionele dienstverlening	<b>B</b> Transport	<b>C</b> Gezondheidszorg ✓
<b>D</b> Detailhandel	<b>E</b> Financiële dienstverlening	<b>F</b> Media en entertainment

## 7. Datalek: welke sector is het vaakst doelwit van een inbreuk op data?

<b>A</b> Zakelijke en professionele dienstverlening ✓	<b>B</b> Transport	<b>C</b> Gezondheidszorg
<b>D</b> Detailhandel	<b>E</b> Financiële dienstverlening	<b>F</b> Media en entertainment

### CYBER EN DATA RISKS

#### DE WERELD OM ONS HEEN

Welke gegevens zijn blootgesteld aan risico's?

- Persoonsgegevens
- Beschermde (gezondheid/zorg) gegevens
- Betaalkaart gegevens

Waarom worden persoonsgegevens gestolen?

Persoonsgegevens zijn simpelweg **veel geld waard**. Criminelen kunnen gestolen persoonsgegevens en vertrouwelijke informatie eenvoudig te gelde maken, bijvoorbeeld door fraude te plegen of door vertrouwelijke informatie te koop aan te bieden.

Ter bescherming van persoonsgegevens zijn **strengere regels opgelegd** aan het bedrijfsleven; bedrijven die een fout maken of gehackt worden, moeten de kosten van de inbreuk betalen.





# CYBER EN DATA RISKS

## DE FEITEN

- Kwaadwillenden tasten systemen voortdurend af op zoek naar zwakheden in de beveiliging die toegang hebben tot waardevolle vertrouwelijke informatie en persoonsgegevens. Veel bedrijven denken dat het met inbreuken op de privacy en gegevens wel los zal lopen, maar dat is een misvatting, zoals blijkt uit de volgende drie feiten:
- Feit 1: nog nooit waren omvang en kosten van inbreuken zo hoog
- Feit 2: elke sector en elk bedrijf, van groot tot klein, loopt risico
- Feit 3: geen enkele organisatie is immuun voor interne en externe bedreigingen



## CYBER EN DATA RISKS

### FEIT 1: Nog nooit was de omvang en waren de kosten van inbreuken zo hoog als nu

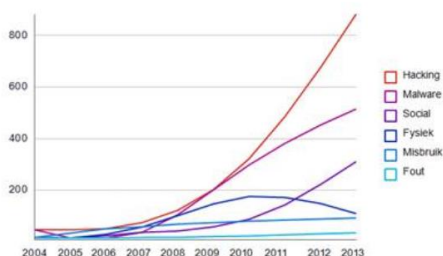
Inbreuken op gegevens worden steeds groter en het aantal getroffen records per gegevensinbreuk neemt toe.

**2,144,583,675** records gingen verloren door inbreuken in 2014<sup>1</sup>

**37%** meer inbreuken ten opzichte van 2013<sup>1</sup>

#### TYPEN INBREUKEN DOOR DE JAREN HEEN

Hacking is de meest voorkomende oorzaak van gegevensverlies en het aantal hackingincidenten neemt snel toe.<sup>2</sup>

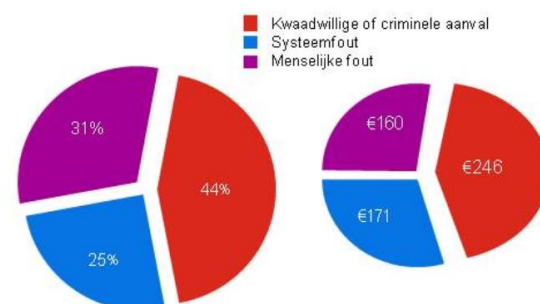


<sup>1</sup>Source: Information Security Incident Response Team (ISIRT) at the University of Cambridge, 2014.  
<sup>2</sup>Source: Information Security Incident Response Team (ISIRT) at the University of Cambridge, 2014.  
<sup>3</sup>Source: Information Security Incident Response Team (ISIRT) at the University of Cambridge, 2014.

Bovendien zijn de uitgaven bij de afwikkeling van een gegevensinbreuk schrikbarend hoog, ongeacht de omvang van het bedrijf. Hieruit voortvloeiende kostenposten zijn opsporing/forensisch, escalatie, kennisgeving, herstel en inkomsten- en imago-verlies.<sup>3</sup>

€ — gemiddelde kosten na gegevensinbreuk in 2014: €3,4 miljoen  
 — gemiddelde kosten door derving in 2014: €1,4 miljoen  
 — gemiddeld aantal records dat verloren is gegaan per inbreuk in 2014: 21.158  
 — gemiddelde kosten per record in 2014: €182

#### MEEST VOORKOMENDE TYPEN INBREUKEN EN DAARMEE SAMENHANGENDE KOSTEN PER RECORD



## CYBER EN DATA RISKS

### FEIT 2: Elke sector en elk bedrijf, van groot tot klein, loopt risico

Enkele sectoren springen eruit als opvallende doelwitten die bijna de helft (49%) van alle inbreuken in 2014 te verduren kregen. De kosten per record waarop inbreuk is gemaakt, zijn in bepaalde sectoren hoger dan in andere.

SECTOR	2014 %	KOSTEN PER RECORD <sup>1</sup>	SECTOR	2014 %	KOSTEN PER RECORD <sup>2</sup>
 Zakelijke & Professionele dienstverlening	17%	€ 203	 Juridische dienstverlening	7%	Nvt
 Detailhandel	14%	€ 114	 High-Tech & IT	7%	€ 164
 Financiële dienstverlening	10%	€ 214	 Gezondheidszorg	6%	€ 287
 Media & Entertainment	8%	€ 166	 Transport	5%	€ 260
 Bouw & Techniek	8%	Nvt	 Luchtvaart & Defensie	3%	Nvt
 Overheid & Internationale organisaties	7%	€ 156	 Overige	8%	Nvt

**60%** van de kleine en middelgrote ondernemingen sluit na zes maanden de poorten als gevolg van de schade door een inbreuk

Helaas zijn de meeste kleine organisaties niet in staat om de kosten voor de afwikkeling van een gegevensinbreuk te dragen.<sup>3</sup>

**22%** kans op een inbreuk op 10.000 records of minder gedurende een periode van twee jaar

Organisaties van alle soorten en maten kunnen getroffen worden. Vooral kleine en middelgrote ondernemingen zijn kwetsbaar omdat de meeste niet over de middelen beschikken om een deugdelijk cyberbeveiligingssysteem op te tuigen.<sup>4</sup>

Source: The Eye B-Trends 2015 Report  
<sup>1</sup> Pioneiron Inc. N/A; 2014 Cost of Data Breach Study  
<sup>2</sup> Source: Clockwork, Gary. "Expensive Data Breach Solutions Address Small Businesses' Issue Prepared for Data Breach." Expert Business Information Services, November 2013.  
<sup>3</sup> Source: Pioneiron Inc. N/A; 2014 Cost of Data Breach Study

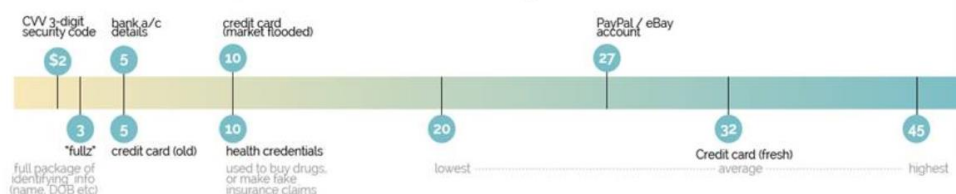
## CYBER EN DATA RISKS

### OORZAAK EN GEVOLG

1. Schadelijke of criminele aanvallen veroorzaken 44% van de inbreuken
2. Nalatigheid 31% van de inbreuken zijn te wijten aan de nalatigheid van personeel.
3. Falen van het IT-systeem – 25% van de inbreuken worden hierdoor veroorzaakt.



### How Much is Your Hacked Data Worth? Black market \$ prices





# CYBER EN DATA RISKS

WAT ZIJN DE BELANGRIJKSTE  
RISICO'S?

First Party-risico's

- Kosten van digitaal forensisch onderzoek. De kosten kunnen sterk uiteenlopen, afhankelijk van hoe groot of ingrijpend de inbreuk is.
- Melden en inlichten van gedupeerden. Kosten lopen uiteen van € 1,25 tot € 5,- p.p.
- Kosten voor PR en crisismanagement.
- Ransomware, betaling voor cyberafpersing
- Kosten voor herstel van ICT-systemen
- Bedrijfsschade (BI)



## 8. Wat is de PCI Data Security Standaard?

A

Dit is de Privacy, Compliance & International trade Data Security Standaard.

B

Dit is de Patiënten Compliance en Informatieuitwisselings Data Security Standaard.

C

Dit is de Payment Card Industry Data Security Standaard. ✓

D

Dit is de Private Computer & Informatie Data Security Standaard.

# CYBER EN DATA RISKS

## WAT ZIJN DE BELANGRIJKSTE RISICO'S?

### Third Party-risico's

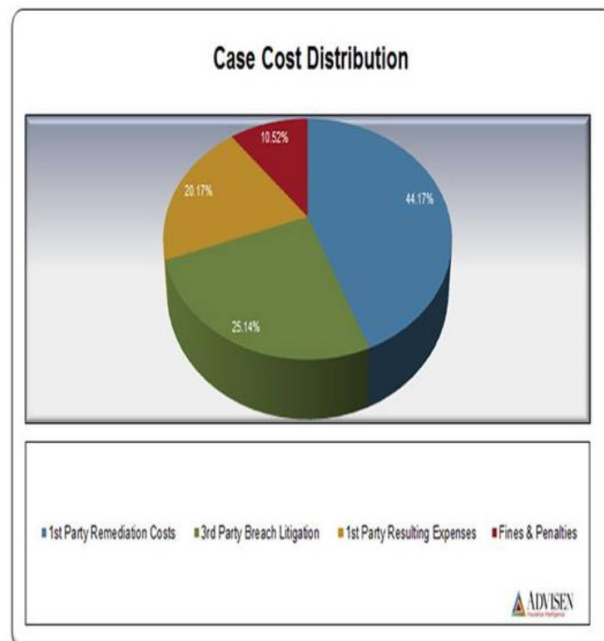
- Kosten voor nieuwe betaalkaart
- Kosten van fraude met betaalkaart
- PCI boetes
- Boetes van de AP
- Rechtzaken
- Lichamelijk, psychische en emotionele schade door verloren of openbaar gemaakte gegevens
- Overdracht of verspreiding van computervirus/-worm of schadelijke software als gevolg van onachtzaamheid



# CYBER EN DATA RISKS

## OORZAAK EN GEVOLG

1. Kosten van herstel (1st party)
2. Aansprakelijkheid (3rd party)
3. Overige kosten (1st party)
4. Geldboetes en dwangsommen



## 9. Waar moeten organisaties sinds 1 januari 2016 een Datalek melden?

- A** Onafhankelijke Post en Telecommunicatie autoriteit (OPTA)
- B** Autoriteit Persoonsgegevens (AP) ✓
- C** College bescherming Persoonsgegevens (CBP)
- D** Autoriteit Consument en Markt
- E** Informatie Beheer Groep (IBG)
- F** Kamer van Koophandel (KvK)

## 10. Veel organisaties besteden de verwerking van (persoons)gegevens uit aan een 'Bewerker'. Wat voor gevolgen heeft dit voor de Meldplicht Datalekken?

- A** Door de werkzaamheden uit te besteden is de organisatie niet langer verantwoordelijk.
- B** Dit hangt af van wie de "fout" heeft gemaakt. Indien dit bij de Bewerker heeft plaatsgevonden is de organisatie niet verantwoordelijk.
- C** De organisatie blijft volledig zelf verantwoordelijk. ✓



**11. Een datalek moet vaak bij de Autoriteit Persoonsgegevens gemeld worden. Wanneer dienen ook de betrokkenen over een datalek geïnformeerd te worden?**

**A**

Altijd indien de Autoriteit Persoonsgegevens geïnformeerd moeten worden

**B**

Indien de data niet versleuteld waren (cryptografie) en andere technische beschermingsmaatregelen van de data niet gewerkt hebben

**C**

Indien de data niet versleuteld waren en andere technische beschermingsmaatregelen van de data niet gewerkt hebben en de inbreuk waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer ✓

**D**

Indien de data niet versleuteld waren en andere technische beschermingsmaatregelen van de data niet gewerkt hebben en indien de gestolen data online is gepubliceerd



## CYBER EN DATA RISKS

### MELDPLICHT DATALEKKEN

- Implementatie 1-1-2016
- Voor commerciële instellingen en (semi-) overheid
- Binnen 48 uur melden bij falen van technische en organisatorische beveiliging met kans op verlies of onrechtmatige verwerking van persoonsgegevens
- Aard en vermoedelijke omvang van het datalek
- Inspanningen om de schade te herstellen
- Raadgevingen aan publiek en klanten
- Boete van bijvoorbeeld maximaal € 820.000



# CYBER EN DATA RISKS

## JURIDISCHE CHECK BEWERKERSOVEREENKOMST

- Wanneer gaat de bewerker de verantwoordelijke informeren?
  - Welke informatie verstrekt de bewerker?
  - Krijgt de verantwoordelijke updates over de ontwikkelingen?
  - Wie draait voor welke kosten op?
- 
- Gratis juridische check van de bewerkerovereenkomst ter waarde van € 1.200 door ICTRecht voor alle verzekerden.



## 12. Wat is in de regel niet gedekt op een cyber verzekering?

- A** De aansprakelijkheid als gevolg van de diefstal van niet-elektronische gegevens (fysieke mappen of dossiers)
- B** De aansprakelijkheid bij het uitbesteden van werkzaamheden
- C** De boete op grond van de Meldplicht Datalekken
- D** Diefstal van geld van de rekening 

# HUIDIGE VERZEKERINGSPAKKET

## Standaard

- Aansprakelijkheidsverzekeringen bedrijven
- Inventaris- goederenverzekering
- Opstalverzekering
- Bedrijfsschadeverzekering

## Minder gebruikelijk

- Beroepsaansprakelijkheidsverzekering
- Fraudeverzekering
- Bestuurdersaansprakelijkheidsverzekering
- Technische varia verzekering

## DEKKING BESTAANDE PAKKETTEN

### CONCLUSIE:

Verbond van verzekeraars (2013): "Mind the gap"

Geen enkele traditionele verzekering biedt dus uitgebreide dekking in geval van cyberincidenten. Daarom heeft een cyberriskverzekering in veel gevallen toegevoegde waarde. Analyseer de bestaande verzekeringen op mogelijke overlap, maar: *mind the gap*





# CYBER EN DATA RISKS



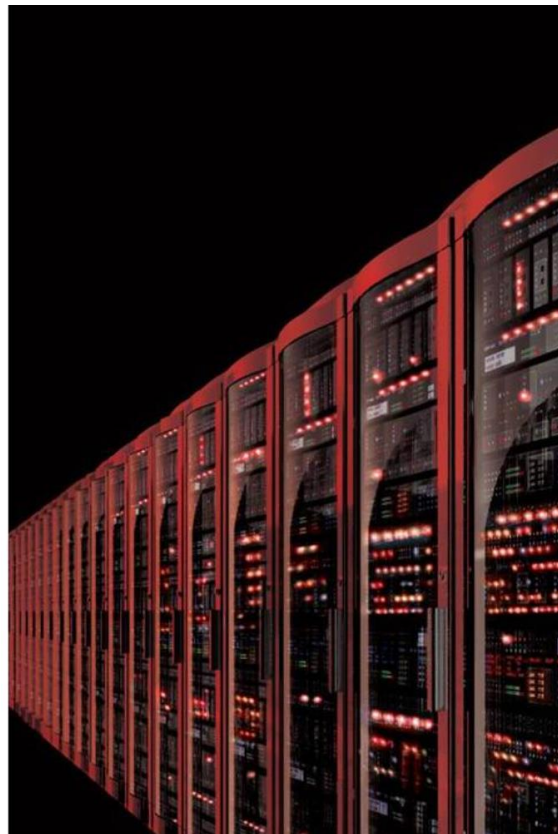
AANSPRAKELIJKHEID  
(third party)

EIGEN SCHADE  
(first party)

## CYBER EN DATA RISKS

### AANSPRAKELIJKHEID (third party)

- **Privacy aansprakelijkheid**  
De gevolgen van gestolen privacygevoelige gegevens
  - Kosten van onderzoek
  - Claims van individuele personen
  - Schending geheimhoudingsplicht
  - Boetes opgelegd door autoriteiten / toezichthouders, of andere verplichte vergoedingen
- **Cyber aansprakelijkheid**  
Schade die ontstaat als een website of e-mail onbedoeld een auteursrecht schendt, laster verspreidt of een virus bevat.



# CYBER EN DATA RISKS

EIGEN SCHADE (first party)

- **Data inbreuk**
  - Forensisch ICT onderzoek
  - Kosten externe deskundigen melden inbreuk (juridisch, communicatie betrokkenen, meldplicht, callcenter etc.)
  - Kosten kredietbewaking betrokkenen
  - Kosten crisismanagement en PR
- **Cyber business interruption**  
Omzetderving veroorzaakt door een hack
- **Hacker schade**  
Kosten herstel website, intranet, netwerk, computersysteem, programma's of data
- **Cyber afpersing**  
Kosten en vergoedingen van onderzoek, assistentie en eventueel betaald losgeld
- **Verlies van geld op rekening en hacking van telefooncentrale**

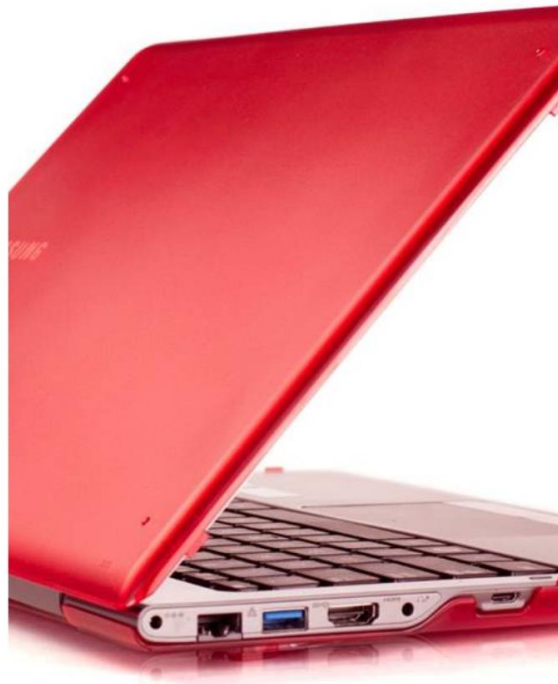


# CYBER EN DATA RISKS

PRAKTIJKVOORBEELDEN

## Adviesbureaus

Bij een bureau voor personeelsadviesing raakt iemand een **laptop kwijt**. Namen, adressen en BSN-nummers van honderden contractmedewerkers waren er in opgeslagen. Ongeacht of de informatie ooit wordt verspreid, moet het bureau de getroffen werknemers inlichten en fraudecontrole aanbieden.



# CYBER EN DATA RISKS

## PRAKTIJKVOORBEELDEN

### Motel

Een klein motel aan zee met 10 kamers biedt haar klanten de mogelijkheid om kamers online op haar website te reserveren. De website wordt gehacked en reserveren is niet meer mogelijk.

- Kosten Inbreuk → forensisch ICT onderzoek
- Hacker schade → herstel netwerk + website + data
- Business interruption → internetinkomsten (vaste vergoeding per uur +/- retentietijd)



# CYBER EN DATA RISKS

## PRAKTIJKVOORBEELDEN

### Advocatuur

Een partner van een kantoor laat vier dossiers op de achterbank van haar auto liggen. Na inbraak in de auto krijgt zij een telefoontje dat ze de dossiers kan terugkopen voor € 20.000

- Cyber afpersing → analyse bedreiging (hoe serieus)
- Is exact bekend welke dossiers het betreffen?  
Ja → Kosten Inbreuk (communicatiekosten belanghebbenden)  
Nee → Kosten Inbreuk (kosten onderzoek)
- Eventueel Privacy (aansprakelijkheid)





# CYBER EN DATA RISKS

## CASUS

### Elektrische huishoudelijke toestellen

Een hacker beweert **200.000** email adressen en telefoonnummers van de website van een elektronica concern geplukt te hebben. Als gevolg hiervan kwam het bedrijf erachter dat de veiligheid van hun microsites (websites door hun gebruikt voor advertenties en andere acties) niet up to date was. De server van de websites was voor het laatst in 2006 bijgewerkt, dat het succes van de hacking verklaart. De hacker heeft een deel van de adressen en telefoonnummers uit de database online gezet en de rest van de gegevens verkocht aan spammers.



# CYBER EN DATA RISKS

## CASUS

### Wat zullen de kosten omvatten:

▪ Forensisch onderzoek	€ 89.000
▪ Communicatiekosten	€ 110.000
▪ Juridische kosten	€ 300.000
▪ Notificatie aan stakeholders	€ 250.000
▪ Herstelkosten	€ 175.000
▪ Claims van consumenten	€ 750.000
<b>Totaal kosten</b>	<b>€ 1.674.000</b>



## 15. Wat zijn de sprinklers op het gebied van cyber risico's?

A

De stekker uit het stopcontact trekken

B

Een virusscanner en firewall

C

Een responseplan



HISCOX

TURIEN & CO  
ASSURADEUREN

## DATA RISKS

### PREMIES

Premies	< € 1 miljoen	> € 1 < € 2.5 miljoen	> € 2.5 < € 5.0 miljoen	> € 5 miljoen < € 10 miljoen
€ 250.000,-	€ 690	-	-	-
€ 500.000,-	€ 1.100	-	-	-
€ 1.000.000,-	€ 1.450	€ 1.800	€ 2.300	€ 2.750
€ 2.000.000,-	-	€ 2.550	€ 3.150	€ 3.750

Van boven naar beneden het verzekerd bedrag. Van links naar rechts de omzet.  
Voor hogere verzekerde bedragen en omzetten ruimschoots maatwerk mogelijkheden.

HISCOX

TURIEN & CO  
ASSURADEUREN

# CYBER EN DATA RISKS

## INCIDENT ROADMAP

---

Als onderdeel van de Hiscox Cyber en Data Risk verzekering, hebben we samen met onze partners een incident roadmap opgesteld.

Het incident roadmapplan is ontwikkeld om u te ondersteunen met:

**Onmiddellijk actie ondernemen, in het geval van schade aan uw database of website als gevolg van een hack**



# CYBER EN DATA RISKS

## WAAROM HISCOX?

---

- Jarenlange ervaring op het gebied van Cyber en Data Risks verzekeringen
- First- and third party dekking
- Volledige dekking is altijd het uitgangspunt!
- Primair geen eisen rondom procedures voor gegevens- en informatiebeveiliging, back-up systemen en processen etc. bij aanvang van het contract en in de polisvoorwaarden (als voorwaarden voor dekking)
- Product speciaal voor assurantieadviseurs via Turien & Co.
- Juridische Expertise (geen uurtarief en directe ervaring in het omgaan met data inbreuken)







1.

---

-Answer :

2.

---

-Answer :

3.

---

-Answer :

4.

---

-Answer :

5.

---

-Answer :

6.

---

-Answer :

**7. Oefenvraag 1. In de zakelijke risicoanalyse breng ik de internetafhankelijkheid van een bedrijf in kaart**

- 
- A. Ja  
B. Nee

**8. Oefenvraag 2. In de zakelijke risicoanalyse breng ik in kaart over wat voor soort gegevens (data) een bedrijf beschikt.**

---

A. Ja

B. Nee

**9. Oefenvraag 3. Onze relaties zijn geïnformeerd over de Meldplicht Datalekken**

---

- A. Ja per (e-mail)nieuwsbrief
- B. Ja op een andere manier
- C. Nee

**10.**

---

-Answer :

**11. En dan nu om de punten!**

---

-Answer :

**12. 4. Welk cyberincident komt er in het bedrijfsleven het meeste voor?**

---

- A. Phishing
- B. Cyber-spionage
- C. Cryptoware
- D. DDOS
- E. Hacking
- F. Defacement

**13.**

---

-Answer :

**14. 5. Wat is geen digitaal risico?**

---

- A. Cryptoware
- B. Pharming
- C. Camfecting
- D. Social engineering

E. Chetaspeaking

F. Ransomware

15.

---

-Answer :

16.

---

-Answer :

17.

---

-Answer :

18.

---

-Answer :

19.

---

-Answer :

**20. 6. Datalek: voor welke sector zijn de kosten met € 287 per record het hoogste bij een inbreuk op data?**

---

A. Zakelijke en professionele dienstverlening

B. Transport

C. Gezondheids-zorg

D. Detailhandel

E. Financiële dienstverlening

F. Media en entertainment

**21. 7. Datalek: welke sector is het vaakst doelwit van een inbreuk op data?**

- 
- A.** Zakelijke en professionele dienstverlening
  - B. Transport
  - C. Gezondheids-zorg
  - D. Detailhandel
  - E. Financiële dienstverlening
  - F. Media en entertainment

**22.**

---

-Answer :

**23.**

---

-Answer :

**24.**

---

-Answer :

**25.**

---

-Answer :

**26.**

---

-Answer :

**27.**

---

-Answer :

**28. 8. Wat is de PCI Data Security Standaard?**

---

- A. Dit is de Privacy, Compliance & International trade Data Security Standaard.
- B. Dit is de Patiënten Compliance en Informatieuitwisselings Data Security Standaard.
- C. Dit is de Payment Card Industry Data Security Standaard.
- D. Dit is de Private Computer & Informatie Data Security Standaard.

29.

---

-Answer :

30.

---

-Answer :

**31. 9. Waar moeten organisaties sinds 1 januari 2016 een Datalek melden?**

---

- A. Onafhankelijke Post en Telecommunicatie autoriteit (OPTA)
- B. Autoriteit Persoonsgegevens (AP)
- C. College bescherming Persoonsgegevens (CBP)
- D. Autoriteit Consument en Markt
- E. Informatie Beheer Groep (IBG)
- F. Kamer van Koophandel (KvK)

**32. 10. Veel organisaties besteden de verwerking van (persoons)gegevens uit aan een 'Bewerker'. Wat voor gevolgen heeft dit voor de Meldplicht Datalekken?**

---

- A. Door de werkzaamheden uit te besteden is de organisatie niet langer verantwoordelijk.
- B. Dit hangt af van wie de "fout" heeft gemaakt. Indien dit bij de Bewerker heeft plaatsgevonden is de organisatie niet verantwoordelijk.
- C. De organisatie blijft volledig zelf verantwoordelijk.

**33. 11. Een datalek moet vaak bij de Autoriteit Persoonsgegevens gemeld worden. Wanneer dienen ook de betrokkenen over een datalek geïnformeerd te worden?**

---

- A. Altijd indien de Autoriteit Persoonsgegevens geïnformeerd moeten worden
- B. Indien de data niet versleuteld waren (cryptografie) en andere technische beschermingsmaatregelen van de data niet gewerkt hebben



- C. Indien de data niet versleuteld waren en andere technische beschermingsmaatregelen van de data niet gewerkt hebben en de inbreuk waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer
- D. Indien de data niet versleuteld waren en andere technische beschermingsmaatregelen van de data niet gewerkt hebben en indien de gestolen data online is gepubliceerd

**34.**

---

-Answer :

**35.**

---

-Answer :

**36. 12. Wat is in de regel niet gedekt op een cyber verzekering?**

---

- A. De aansprakelijkheid als gevolg van de diefstal van niet-elektronische gegevens (fysieke mappen of dossiers)
- B. De aansprakelijkheid bij het uitbesteden van werkzaamheden
- C. De boete op grond van de Meldplicht Datalekken
- D. Diefstal van geld van de rekening

**37.**

---

-Answer :

**38.**

---

-Answer :

**39.**

---

-Answer :

**40.**

---

-Answer :

**41.**

---

-Answer :

**42.**

---

-Answer :

**43.**

---

-Answer :

**44.**

---

-Answer :

**45.**

---

-Answer :

**46.**

---

-Answer :

**47. 15. Wat zijn de sprinklers op het gebied van cyber risico's?**

- 
- A. De stekker uit het stopcontact trekken
  - B. Een virusscanner en firewall
  - C. Een responseplan

**48.**

---

-Answer :

**49.**

---

-Answer :

**50.**

---

-Answer :

**51. En de winnaar is...**

---

-Answer :