Cyber Risk Management

ICT Accountancy jaarcongres 1 november 2017

Aon Global Risk Consulting | Cyber Risk Practice
Sjaak Schouteren, Cyber Risk Practice Leader
Wessel Exterkate, Consultant

AON
Empower Results®

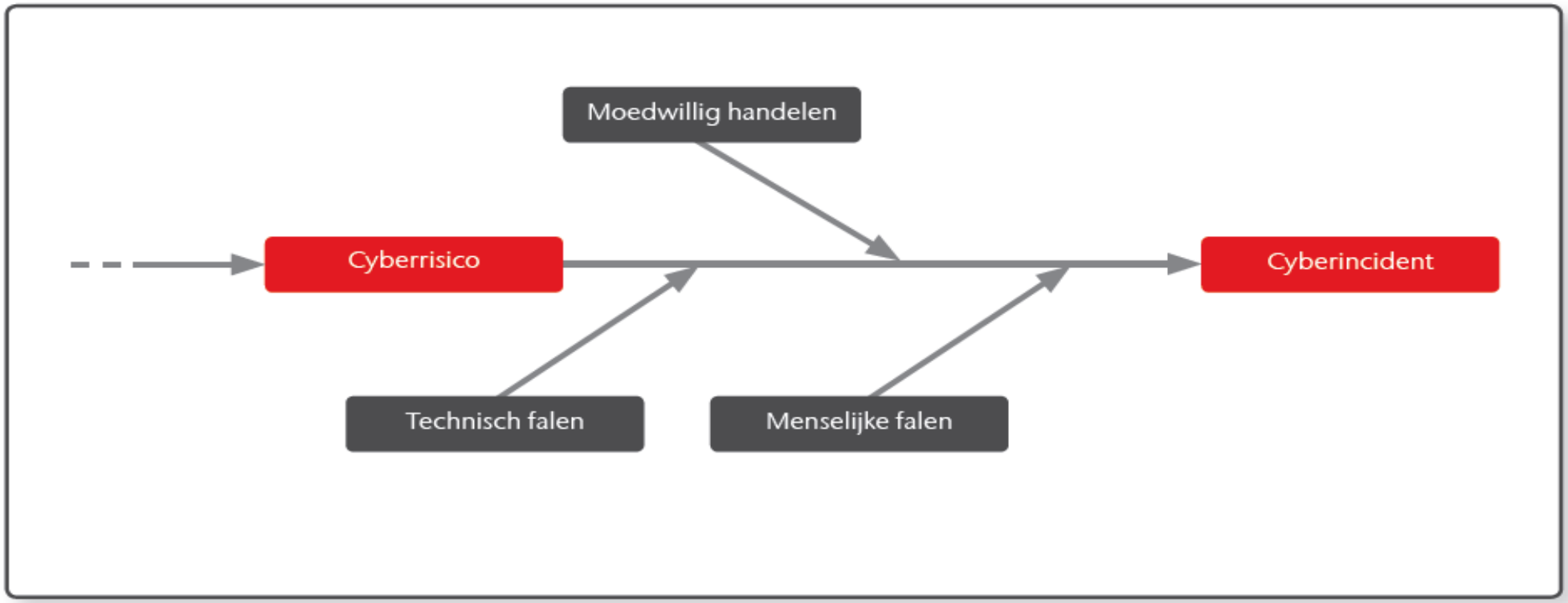
Aon's Cyber Risk Practice: integrale benadering van uw digitale en privacy risico's

Aon's Cyber Risk Practice

- Terugdringen van cyberrisico's.
- Ervaren adviseurs
- Lead Auditors ISO 27001
- Certified Information Privacy Professionals (CIPP/EU)
- Certified Data Projection Officer

- Inzichtelijk maken, beheersen als ook verzekeren van digitale en datarisico's.
- Geïntegreerde benadering van risicomanagement en organisatieadvies.

- Nadruk op (financiële) impact van cyberrisico's

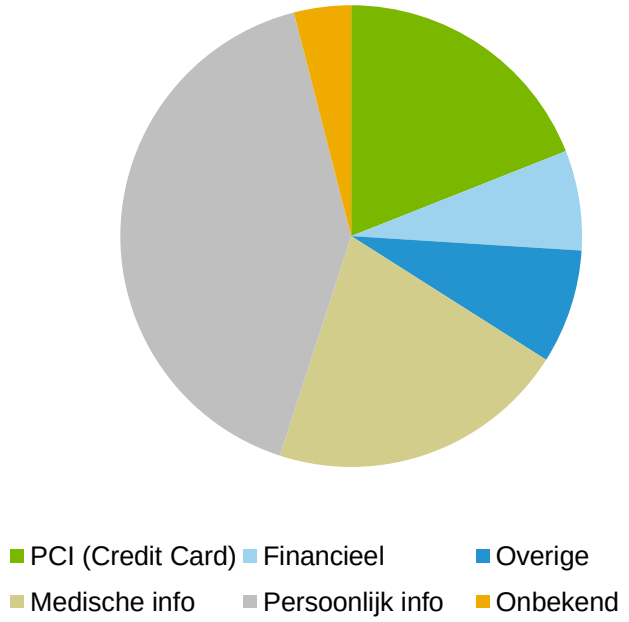

Moedwillig handelen
Cyberrisico
Cyberincident
Technisch falen
Menselijke falen


SYSTEM FAILURE

Claims inzichten, Key Take-aways

Overzicht soorten schades (%)

Overzicht soorten data (%)




CYBER RISK MANAGEMENT
= MEER DAN IT SECURITY
- 100% VOORKOMEN IS EEN ILLUSIE -

Wat is uw schade door continuïteitsverlies?

BRICKS!

Ongeveer EUR 600 miljoen schade als gevolg van grote branden

(Bron: verbond van Verzekeraars)

DIGITALE RISICO'S…

Ongeveer EUR 10 miljard schade als gevolg van Cyberincidenten

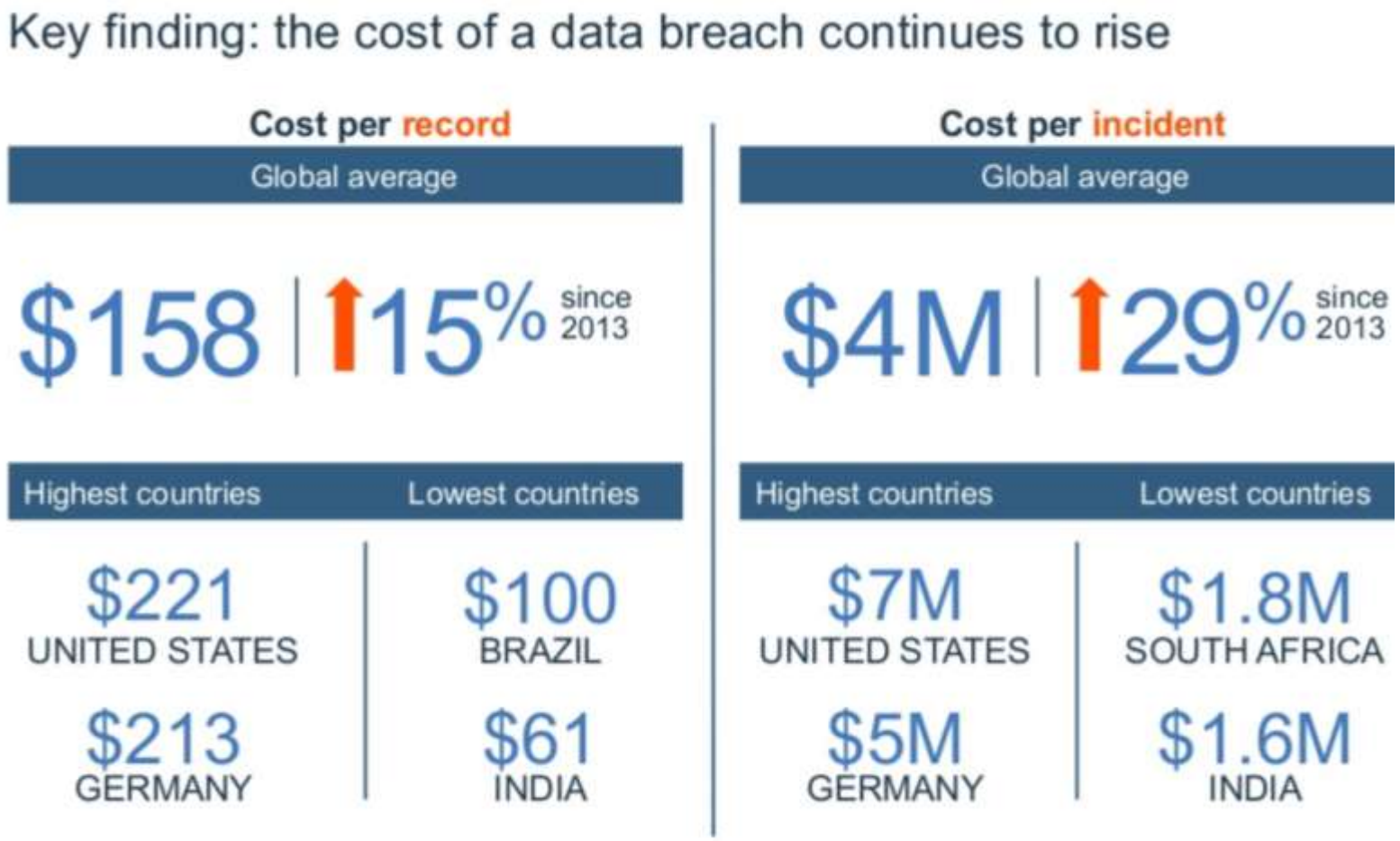
(Bron: Deloitte Cyber Value at Risk in the Netherlands)

56% van de bedrijven heeft geen encryptie of geen beleid inzake encryptie van gevoelige of kritieke data

(Bron: Aon Cyber Risk Diagnostic Tool Nederland)

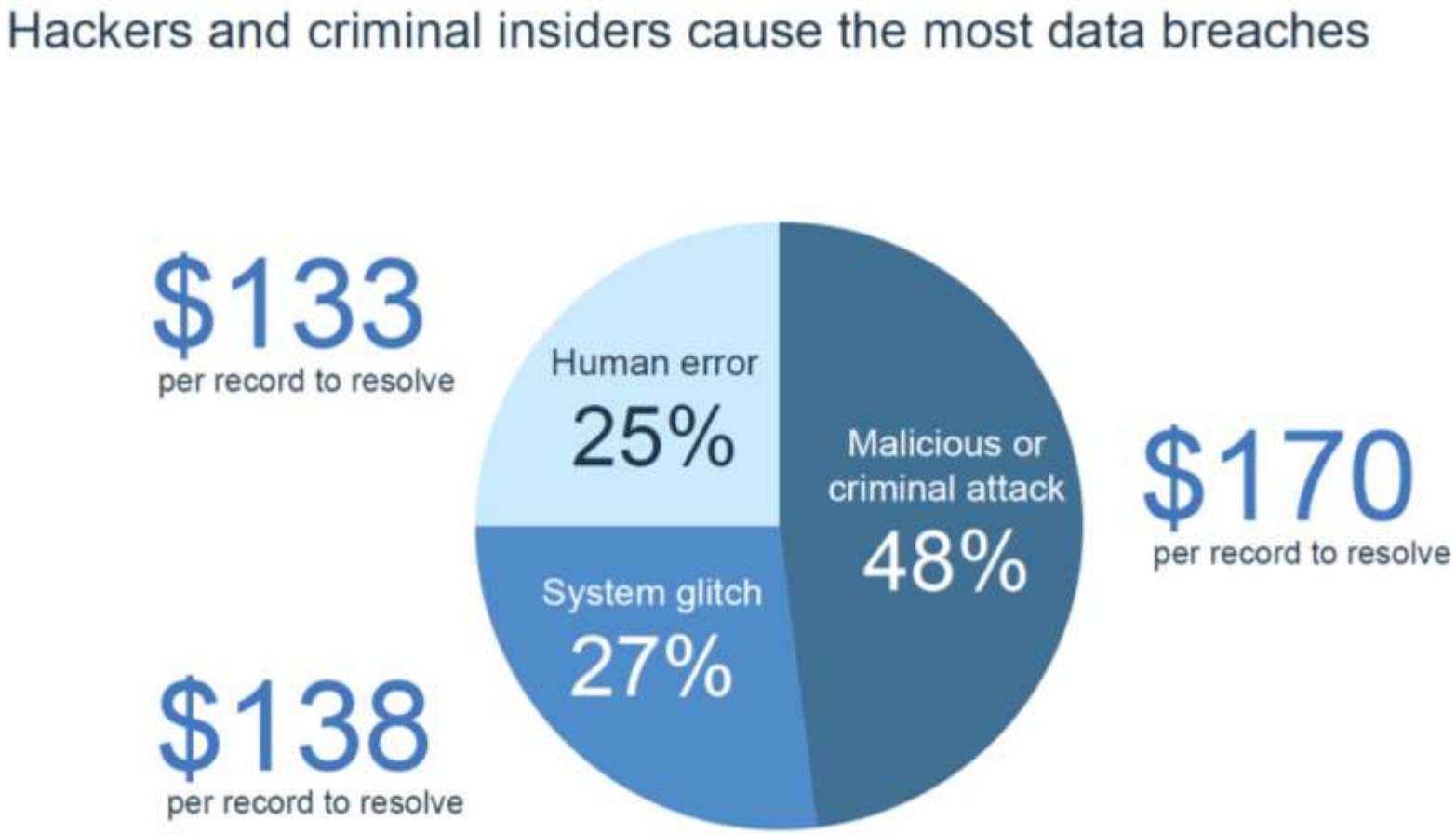
…VOORTDUREND IN FLUX

Financiële impact neemt toe…



Bron: Ponemon 2016 Global Cost of a Data Breach Study

Financiële impact neemt toe…



Bron: Ponemon 2016 Global Cost of a Data Breach Study

AON
Empower Results®

…terwijl de financiële gevolgen nog niet goed zijn afgedekt

Insurance mapping

AANSPRAKELIJKHEIDSRISICO'S (THIRD PARTY)	BRAND	ELEKTRONICA	AANSPRAKELIJKHEID	D&O *	BEROEPSAANSPRAKELIJKHEID	CRIME	CYBER
Ongeautoriseerde toegang op netwerk of systeem	☒	☒	☒	☒	☑	☒	☑
Aansprakelijkheid verlies van persoonsgegevens	☒	☒	☒	☒	☑	☒	☑
Externe kosten ter beperking en voorkoming van (gevolg)schade	☑	☒	☒	☒	☑	☒	☑
Reputatieschade	☒	☒	☒	☒	☑	☒	☑
Verlies van bedrijfsinformatie	☒	☒	☒	☒	☑	☒	☑
Blokkering toegang door frauduleuze handelingen	☒	☒	☒	☒	☑	☒	☑
EIGEN SCHADE (FIRST PARTY)							
Bedrijfsstilstand als gevolg van een cyberevent (verlies netto/bruto winst)	☒	☒	☒	☒	☒	☒	☑
Bedrijfsstilstand als gevolg van een programmeerfout	☒	☒	☒	☒	☒	☒	☒
Eigen kosten als gevolg van een programmeerfout	☒	☒	☒	☒	☒	☒	☒
Schade door misbruik van een programmeerfout	☒	☒	☒	☒	☒	☑	☑
Externe kosten ter beperking en voorkoming van (gevolg)schade	☒	☒	☒	☒	☒	☑	☑
Eigen kosten ter beperking en voorkoming van (gevolg)schade	☑	☒	☑	☒	☒	☑	☑
Kosten ter vervanging van de tankpassen na een cyberincident	☒	☒	☒	☒	☒	☒	☑
Kosten voor kennisgeving van inbreuk op gegevens	☒	☒	☒	☒	☒	☒	☑
Financiële schade door diefstal gegevens	☒	☒	☒	☒	☒	☑	☑
Boetes t.g.v. overtreding wetgeving (civiele boete's)	☒	☒	☒	☒	☒	☒	☑
Crisis management, Bereddingskosten	☒	☒	☒	☒	☒	☑	☑
Kosten Forensisch onderzoek, PR, advertenties	☒	☒	☒	☒	☒	☑	☑
Vervanging van hardware/software	☒	☑	☒	☒	☒	☒	☒
Juridische kosten; terugvorderen frauduleuze of cyber gerelateerde schade	☒	☒	☒	☒	☒	☑	☑

☑ Dekking
☑ Dekking mogelijk
☒ Geen dekking

Empower Results®


100% VOORKOMEN
IS EEN ILLUSIE
FOCUS DUS
(OOK) OP IMPACT

Kans? **Impact, impact, impact!**

Weet u wat uw essentiële digitale productiefactoren en -belangen zijn?


DIGITALE
ASSETS
HARDWARE
SOFTWARE
DATA
LEVERANCIERS

DIGITALE ASSETS: DATA, SOFTWARE & HARDWARE

SYSTEMEN

WEBSITE

APPLICATIES

OPSLAG

BEREIKBAARHEID

PRIVACY

INTERNET

INTRANET

PROCESBESTURING

PERSONEELSDATA

COMMUNICATIEMIDDELEN

LEVERANCIERS

KLANTGEGEVENS

FINANCIELE GEGEVENS

Empower Results®

Cyberrisico's: anatomie

AON
Empower Results®

Wat is uw risicobereidheid?

WAT KOST EEN UUR DOWNTIME?

WAT KOST DATAVERLIES?

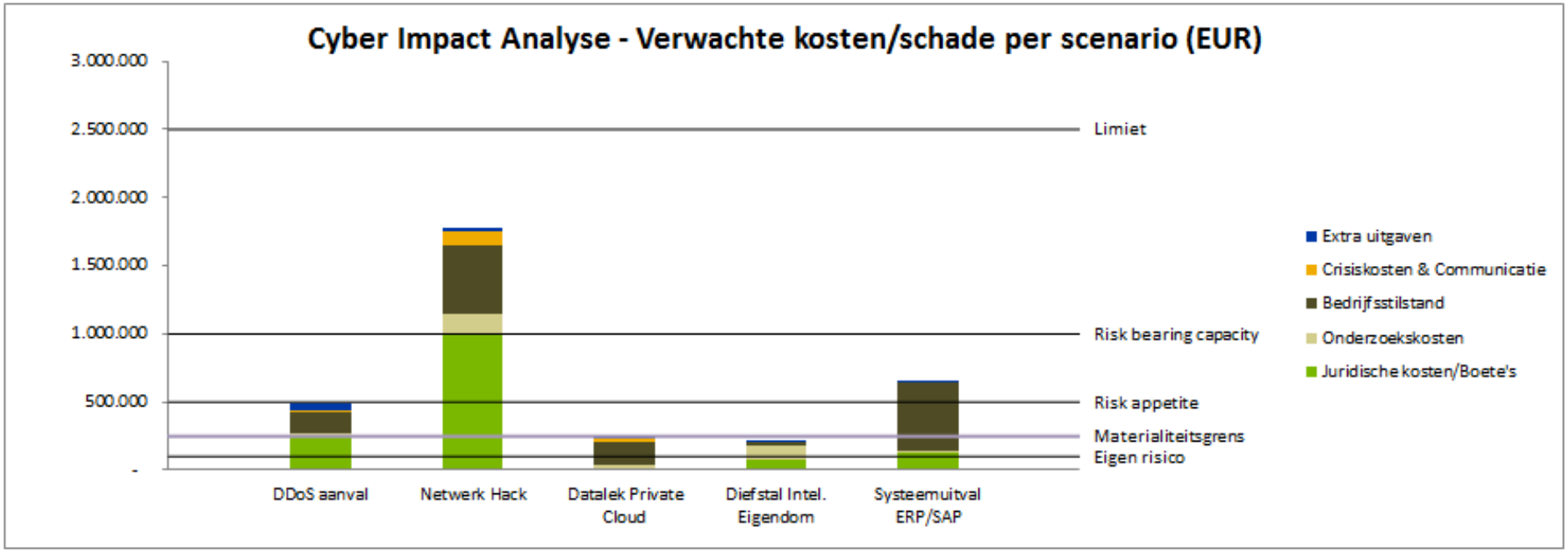
WELKE SCHADE *KAN* UW ORGANISATIE INCASSEREN?

WELKE SCHADE *WIL* UW ORGANISATIE INCASSEREN?

AON
Empower Results®

Analyseren & kwantificeren van uw topscenario's: voorbeeld

ANALYSEREN EN KWANTIFICEREN VAN TOPSCENARIO'S



INZICHT IN IMPACT

Empower Results®


Bent u bekend met
de impact van
cyberrisico’s?

Ransomware

Via een fishing mail weet een hacker toegang te krijgen tot de systemen van uw organisatie en belangrijke bestanden worden versleuteld. Hierdoor valt uw bedrijf stil en kunnen klanten niet meer bediend worden.

Tevens bestaat de kans dat binnen enkele uren data wordt gelekt indien er niet wordt betaald.

Welke vragen komen er nu naar boven?

- Wie doet het gele hesje aan?
- Is er sprake van een datalek?
- Moeten we betalen (en hoe)?
- Wat zijn de gevolgen op korte termijn?
- Wat zijn de gevolgen op lange termijn?
- Hoe weet ik of ze niet in andere systemen zitten?
- Wie is aansprakelijk?
- Zijn we verzekerd?
- Hadden we dit niet moeten oefenen?!
- Etc.

AON
Empower Results®

Cyberverzekering nader bekeken

Empower Results®

Verzekeren van uw privacyrisico: Cyberdekking

- **Financiële waarborg voor vervolgkosten na eigen schade (‘first party’)**
  - Kosten voor IT-forensics / reconstructie van data
  - Kosten voor juridische ondersteuning
  - Kosten voor crisismanagement/crisiscommunicatie
  - Kosten gemoeid met continuïteitsverlies
  - Kosten als gevolg van de meldplicht en (bestuurlijke) boetes
  - Schade als gevolg van identiteitsfraude

- **Financiële waarborg bij schade voor derden (‘third party’)**
  - Aansprakelijkheidsclaims

Empower Results®

Dekkingen cyberverzekering

Dekkingen van de Aon Cyberverzekering:

Aansprakelijkheid: schadevergoeding en juridische bijstand in geval van aanspraken van derden als gevolg van verlies van persoonsgegevens en/of bedrijfsinformatie;

Crisismanagement: kosten (forensisch) onderzoek, PR, klant notificatiekosten, kredietbewaking, IT-diensten, cyberincident responsediensten;

Boetes: kosten voor onderzoek door een toezichthouder, juridische bijstand, bestuurlijke boetes.

- **Digitale media**, schadevergoeding en kosten van verweer in verband met aanspraken van derden tegen u die voortvloeien uit uw multimedia-activiteiten. Bijvoorbeeld smaad en laster of plagiaat;
- **Cyber- / privacy afpersing**, waaronder ransomware;
- **Hacking telefooncentrale**, vergoeding van de belkosten.
- **Cyberdiefstal**: verlies van geld of geldwaarden en/of goederen door diefstal (let op sub limiet)

- **Netwerkonderbreking**, gederfde netto winst in verband met netwerkonderbreking.

Speciale verzekeringen voor: Scholen, Gemeenten, WoCo, Touroperators, etc.

Cyberrisicomanagement: vijf essentiële vragen

1. Wat zijn de belangrijkste digitale assets van mijn organisatie?
2. Welke specifieke risico's vormen een bedreiging voor onze digitale assets?
3. Wat zijn de meest impactvolle risico's voor onze organisatie?
4. Wat is de (financiële) schade die kan ontstaan?
5. In hoeverre zijn wij in staat om / bereid om impact te beperken?

Cyberrisicomanagement: Maak er een gezamenlijk project van!

Empower Results®

Cyberrisicomanagement:
Vijf praktische vragen aan uw hoofd juridische zaken:

1. Wat hebben wij afgesproken met onze klanten en leveranciers in geval van een cyberincident?
2. Hoe groot kan de organisatieschade zijn door ICT-uitval en/of datadiefstal?
3. Welk deel daarvan kunnen wij terugvorderen bij onze leverancier(s)? Onder welke voorwaarden?
4. Voor welk deel kunnen wij aansprakelijk worden gehouden, en wat is daarvan de verwachte omvang?
5. Welke wettelijke regelingen en contractuele bepalingen liggen hieraan ten grondslag? Voldeed onze organisatie aan haar verplichtingen en waar/hoe is dit vastgelegd?

Cyberrisicomanagement:
Vijf praktische vragen aan uw risico- en verzekeringsmanager:

1. In hoeverre voorziet ons huidige verzekeringsprogramma in de werkelijke cyberrisico's?
2. Waar zitten de gaten en in welke mate betreft dit verzekerbare risico's?
3. Zijn dit risico's die de organisatie zelf kan/wil dragen? Hoe verhouden deze zich tot de risicotoleranties en het financiële draagvermogen?
4. Hoe ziet ons ideale verzekeringsprogramma eruit, en wat zijn daarvan de kosten en voorwaarden?
5. Is risico-overdracht een zinvolle en kosteneffectieve aanvulling op onze totale set aan beheersmaatregelen?

Cyberrisicomanagement:
Vijf praktische vragen aan uw financieel bestuurder:

1. Hebben wij een actueel en volledig beeld van onze belangrijkste risico's (bijvoorbeeld risico-register)?
2. Kennen wij de bestaande beheersmaatregelen en risico-eigenaren?
3. Hoe verhoudt de verwachte en/of maximale schade door cyberrisico's zich tot onze risico-toleranties?
4. Hoe verhoudt dit risico zich tot onze financiële kernratio's en financiële draagvermogen?
5. Wat is financieel gezien de meest effectieve beheersmaatregel voor onze cyberrisico's?

Cyberrisicomanagement:
Vijf praktische vragen aan uw ICT-manager:

1. Wat zijn voor onze totale organisatie de kosten van een datalek, systeemuitval of een hack?
2. Welke gegevens zijn voor kwaadwillende interessant en waarom?
3. Waarom zijn wij goed beveiligd? En hoe zijn wij voorbereid op een incident?
4. Hebben wij passende beheersmaatregelen getroffen? Waaruit blijkt dit?
5. Wat is de verantwoordelijkheid en bevoegdheid van de interne ICT-afdeling met betrekking tot cyberincidenten?

CYBER?

VAN SECURITY

NAAR IMPACTMANAGEMENT

VAN ABSTRACTE DREIGING

NAAR EEN AFGEWOGEN AANPAK

AON
Empower Results®

Empower Results®