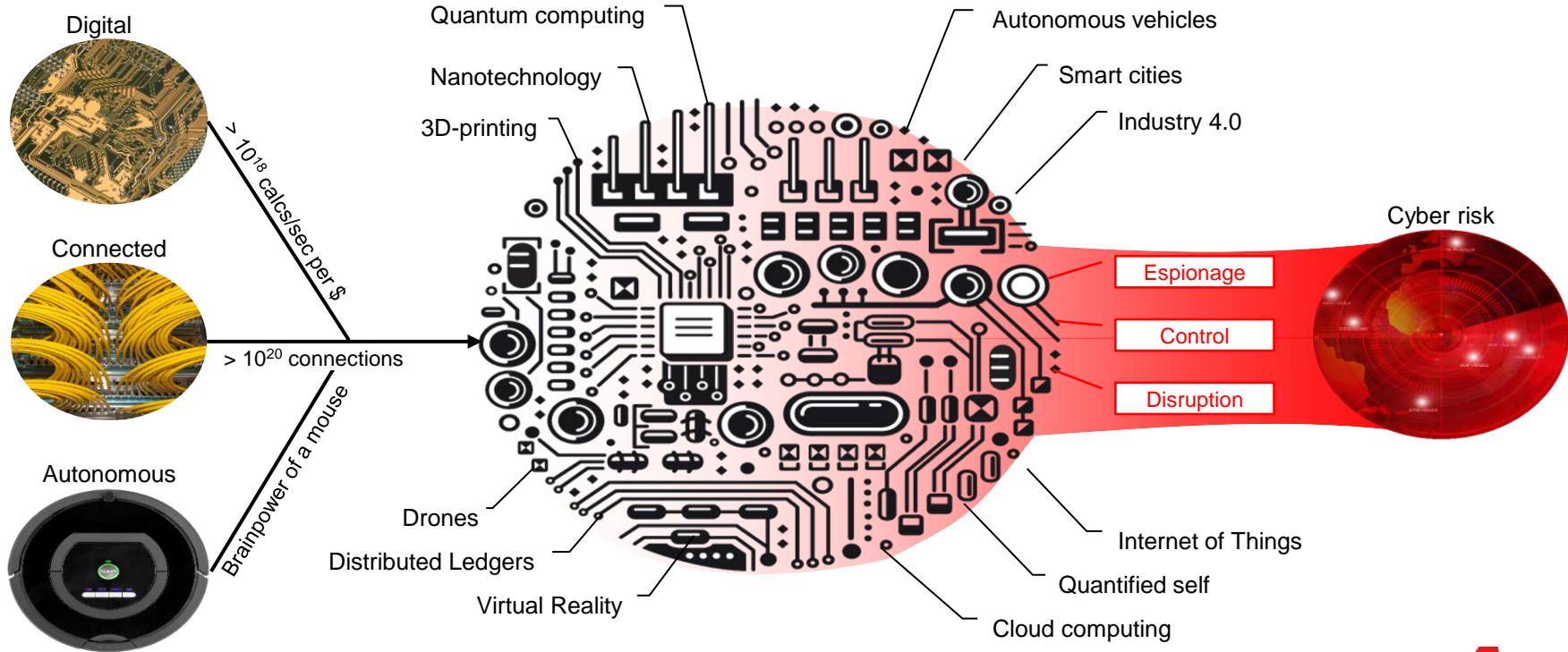




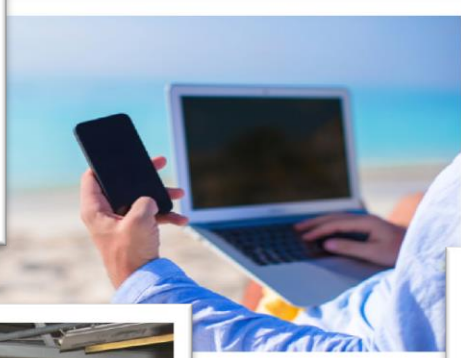
Cyber Risk Management

Nieuwjaarsbijeenkomst PvIB
Utrecht – 18 January, 2018

Our society is becoming increasingly connected – giving rise to increasing cyber risk



Growing need for Cyber Risk Management



Painful consequences of lacking Cyber Risk Management

TalkTalk fined £400,000 for theft of customer details

5 October 2016 | Business

f t v e Share



France's Renault hit in worldwide 'ransomware' cyber attack

Tweet submit



About the ICO / News and events / News and blogs /

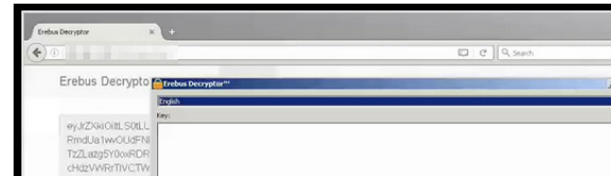
Private health firm fined £200,000 after IVF patients' confidential conversations revealed online

South Korean Hosting Firm Pays \$1 Million Ransom

Erebus Ransomware Gang Hits Pay Dirt After Encrypting Outdated Linux Servers

Mathew J. Schwartz (@euroinfosec) · June 20, 2017 · 0 Comments

Twitter Facebook LinkedIn Credit Eligible



**CYBER
RISK**

**= MORE THAN
CYBER CRIME**



About the EU General Data Protection Regulation (GDPR)

The EU has introduced strict new measures to protect its citizens by enforcing rules for any organization globally handling the personal data of EU individuals.

Key actions that organisations need to consider:

Understand where and how they use and store European personal data

Review their existing security controls

Assess their third parties' personal data security standards





Be prepared to report personal data breaches within 72 hours

Adhere to new duties for data processors & data subjects



Failure to comply may result in enforcement action, including fines of up to 20 million Euros or 4% of your organization's annual worldwide revenue.

Cyber risk management – drivers of change

 <p>Legislation</p>	<ul style="list-style-type: none">• Increased data regulations (e.g. GDPR)• Duty to notify data breaches (for GDPR within 72 hours)• Fines (for GDPR up to 4% of global turnover)• Red-teaming as a mandatory controls testing exercise (e.g. TIBER)• Regulations in the making (regulators are concerned with systemic risk, no easy stuff!)
 <p>Awareness</p>	<ul style="list-style-type: none">• Awareness increases due to large global cyber incidents (e.g. due to WannaCry and Not-Petya)• Also due to increasing number of breaches (everyone knows someone that got hacked (and that actually knew))• Ranking of cyber risk in ERM expected to move from 14th to 8th position by next year (2018)• In most organizations, however awareness is growing too slowly due to lacking ownership of cyber risk!
 <p>Breach Numbers</p>	<ul style="list-style-type: none">• Number of breaches up 36% (!) since 2011• Notification requirements likely to increase numbers (under reporting is demonstrably common)
 <p>Costs</p>	<ul style="list-style-type: none">• Cost of data breach in Europe 35% lower than in US (in part due to lagging risk levels and regulations)• Cost of cybersecurity as well as breaches will increase as result of increasing attacker sophistication• Also, demand for cybersecurity exceeding supply, implying cyber security controls remain expensive• Return on investment of installing proper cyber risk management (on ERM level) is steadily increasing



**CYBER RISK
MANAGEMENT**

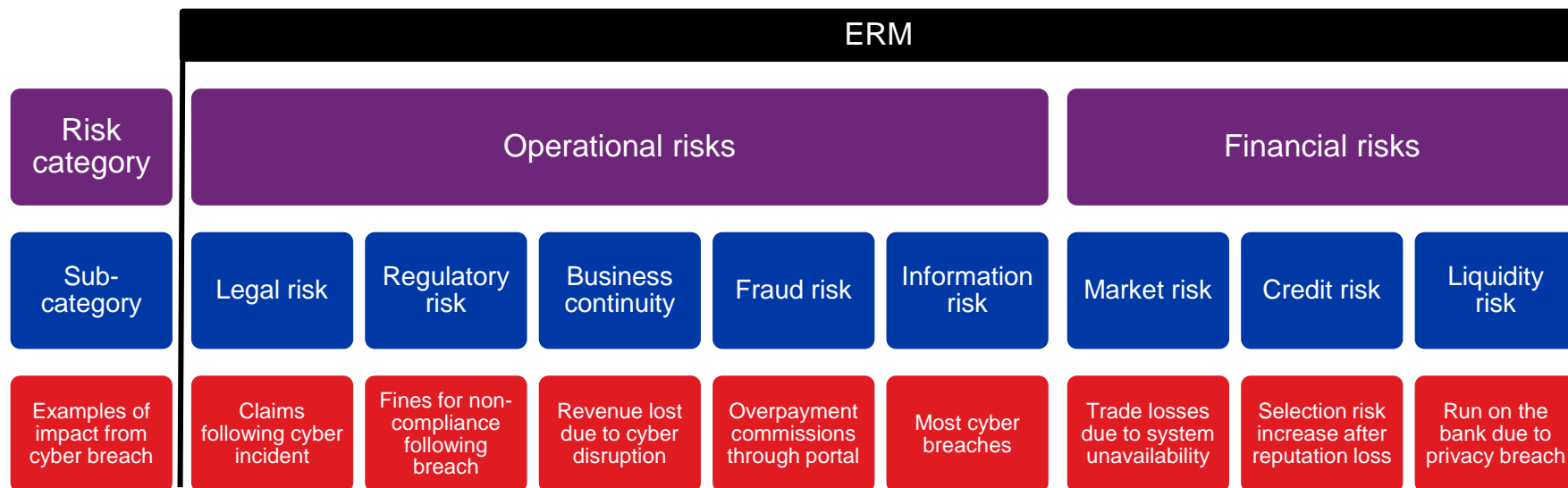
**= MORE THAN
IT SECURITY**

- 100% safety is an illusion

Cyber risk is not a new risk type, but a new enabler of existing risk

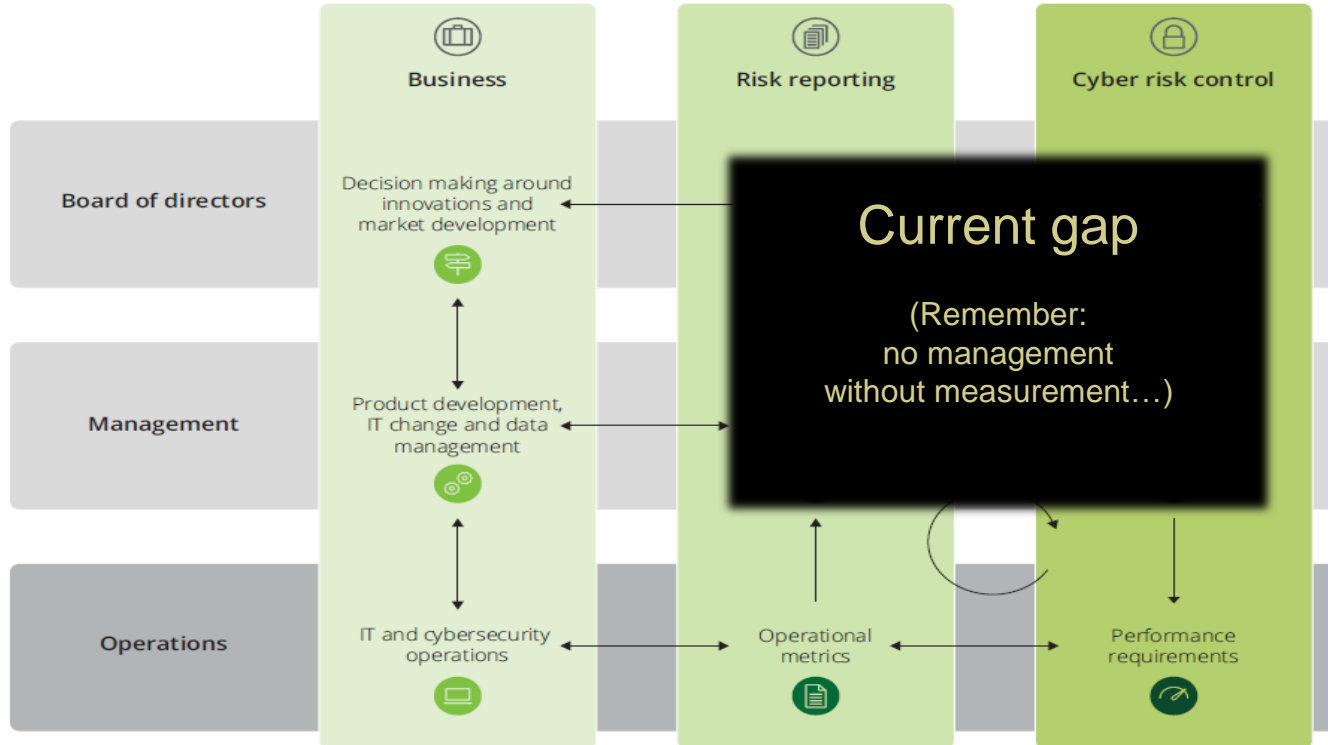
- Initially, cyber risk has been typically regarded as part of Operational Risk or IT risk (it is not!)
- IT is becoming integrated in all business operations, leading to an all pervasive cyber domain
- Consequently, the cyber domain is becoming a pathway almost any know risk

How should we deal with these complex interdependencies?



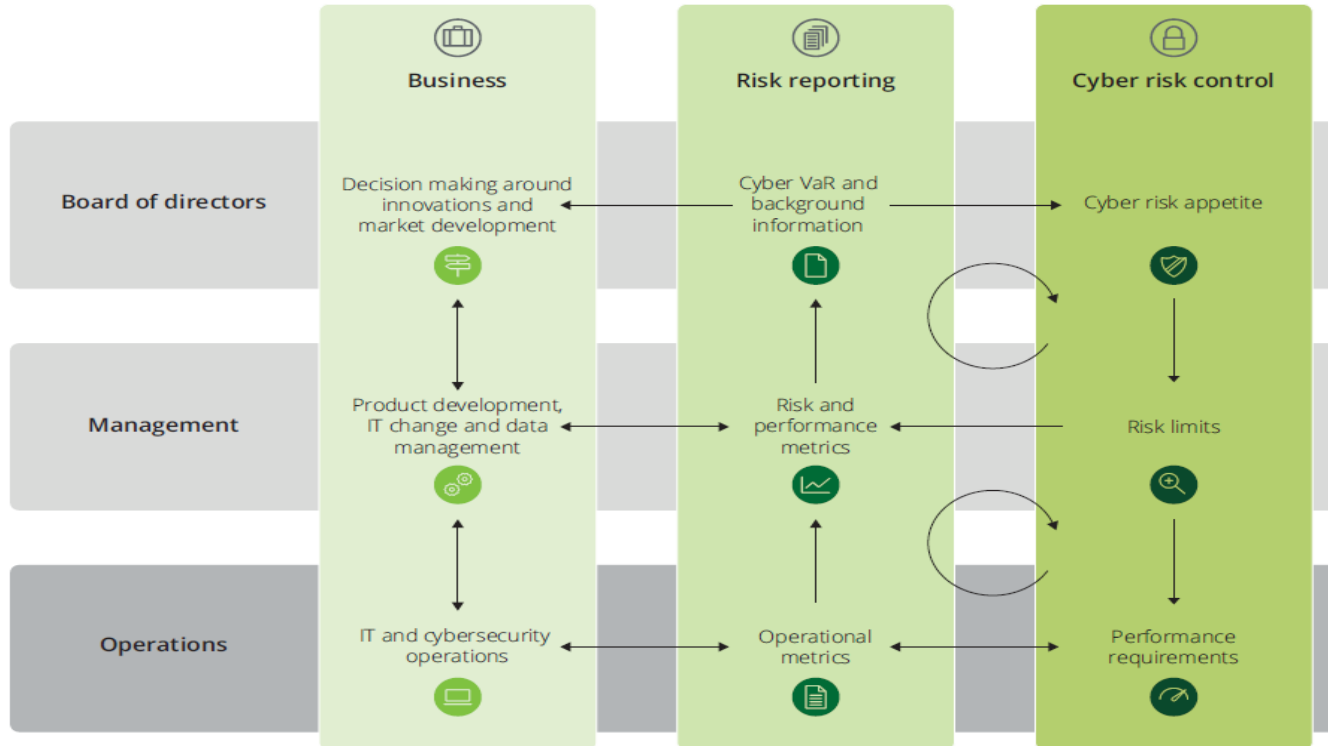
Cyber risk management is an emerging need for organizations

- Many organizations lack board-level risk reporting, good governance and risk management processes
- For most firms, the current state of cyber risk management is not in control...

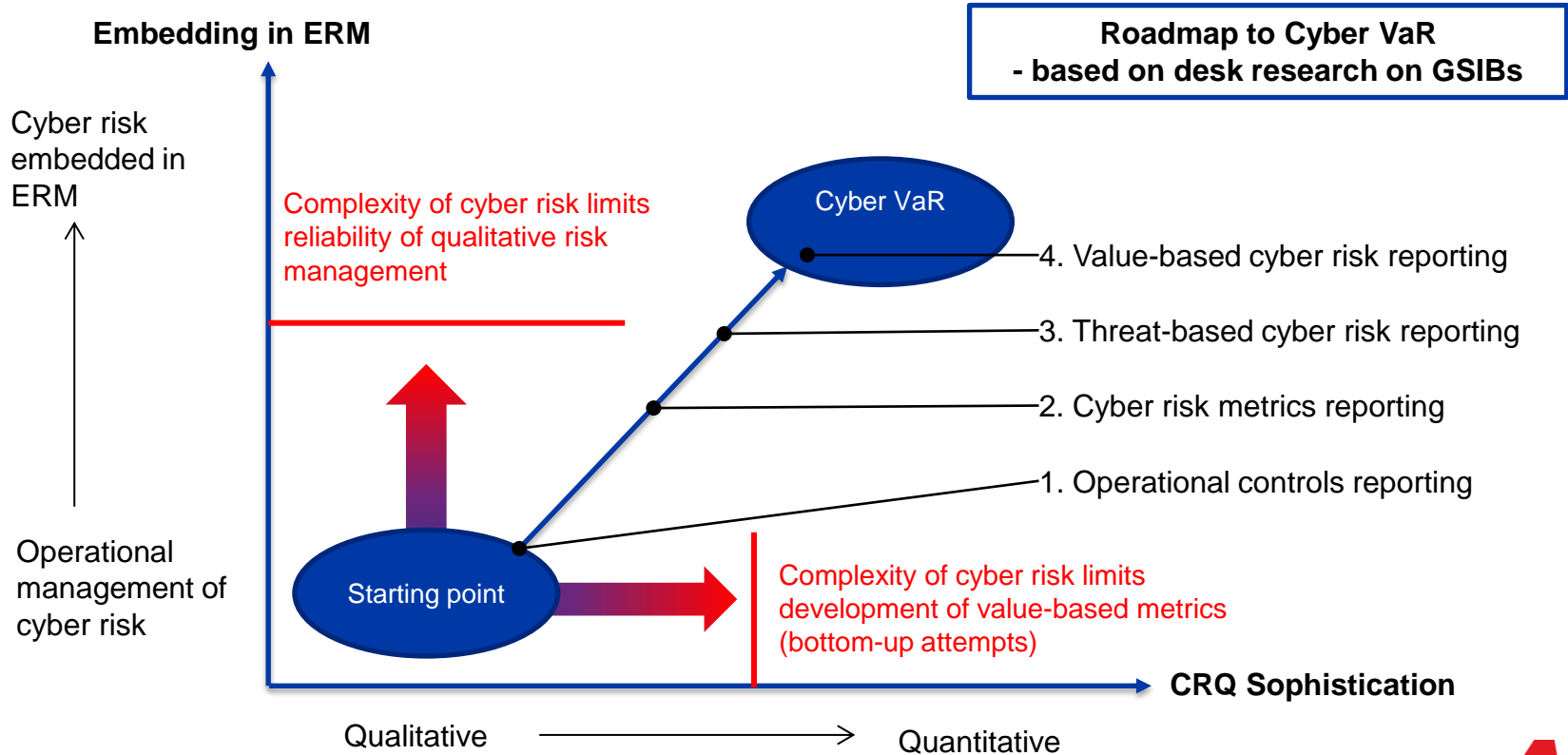


Cyber risk management is an emerging need for organizations

- Balancing cyber risk and reward, requires implementing cyber risk reporting cycles and business alignment
- Given the magnitude of cyber risk quantitative, i.e. economic metrics are required



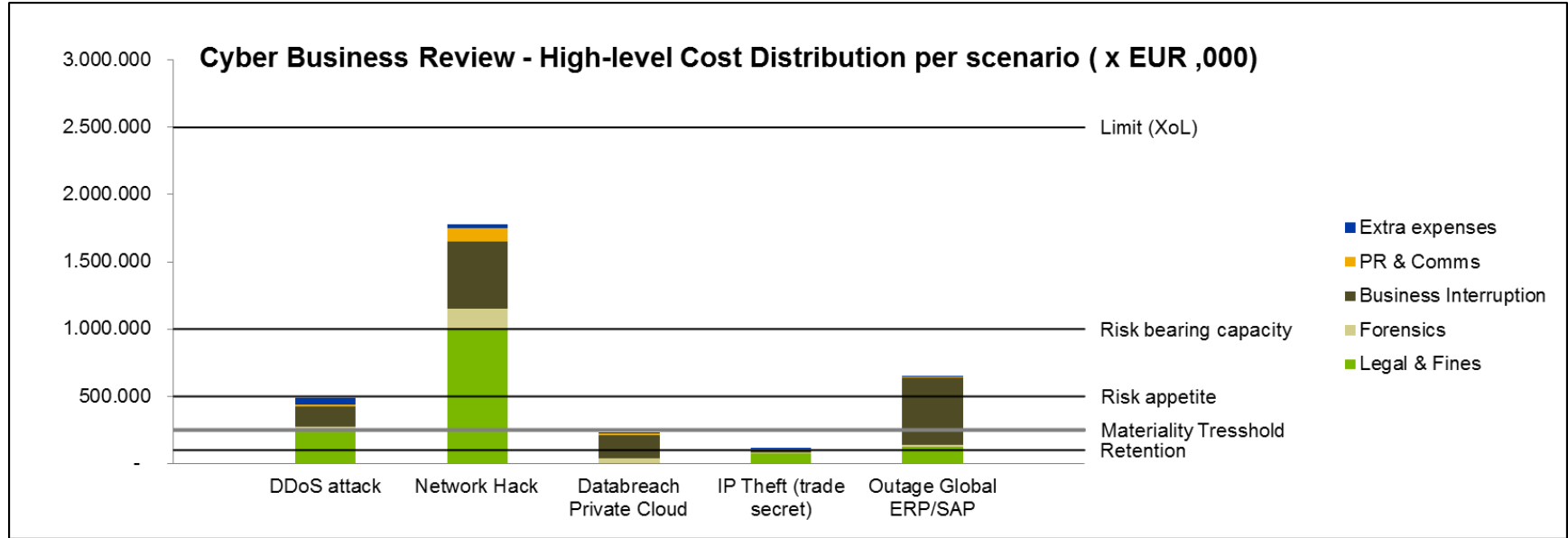
Cyber risk management requires balancing governance with quantification



Cyber Solutions Group: Aon's integrated approach



Cyber Exposure Analyzed



Cyber risk and insurance

No coverage
 Limited coverage
 Coverage

	Property	General Liability	Crime/Bond	K&R	Professional indemnity	D&O	Cyber
1st Party Privacy/Network Risks							
Physical damage to data only	Limited coverage	No coverage	Limited coverage	No coverage	No coverage	No coverage	Coverage
Virus/hacker damage to data only	Limited coverage	No coverage	Limited coverage	No coverage	No coverage	No coverage	Coverage
Denial of service attack	Limited coverage	No coverage	No coverage	No coverage	No coverage	No coverage	Coverage
B.I. loss from security event	Limited coverage	No coverage	No coverage	No coverage	No coverage	No coverage	Coverage
Extortion or threat	No coverage	No coverage	No coverage	Limited coverage	No coverage	No coverage	Coverage
Employee sabotage of data only	Limited coverage	No coverage	Limited coverage	No coverage	No coverage	No coverage	Coverage
3rd Party Privacy/Network Risks							
Theft/ disclosure of private info.	No coverage	Limited coverage	Limited coverage	No coverage	Limited coverage	No coverage	Coverage
Confidential corporate info. Breach	No coverage	Limited coverage	Limited coverage	No coverage	Limited coverage	No coverage	Coverage
Technology E&O	No coverage	Limited coverage	No coverage	No coverage	No coverage	No coverage	Limited coverage
Media liability (electronic content)	No coverage	Limited coverage	No coverage	No coverage	No coverage	No coverage	Coverage
Privacy breach expense/notificaton	No coverage	No coverage	No coverage	No coverage	Limited coverage	No coverage	Coverage
Damage to third party's data only	No coverage	Limited coverage	No coverage	No coverage	No coverage	No coverage	Coverage
Regulatory privacy defense/fines	No coverage	No coverage	No coverage	No coverage	Limited coverage	Limited coverage	Coverage
Virus/malicious code transmission	No coverage	Limited coverage	No coverage	No coverage	Limited coverage	No coverage	Coverage

Key features of cyber insurance

Liability Sections

*Defense Costs + Damages
+ Regulator Fines*

- ✓ Failure of Network Security
- ✓ Failure to Protect/
Wrongful Disclosure
of Information
- ✓ Privacy or Security
related regulator
investigation
- ✓ Wrongful Collection
of Information
(some policies)
- ✓ Media content
infringement/
defamatory content

First Party Sections

Insured's Loss

- ✓ Network-related BI
- ✓ Extra Expense
- ✓ System Failure BI /
Dependent BI
(some policies)
- ✓ Intangible Asset
damage
- ✓ Reputation
Damage (some
policies)

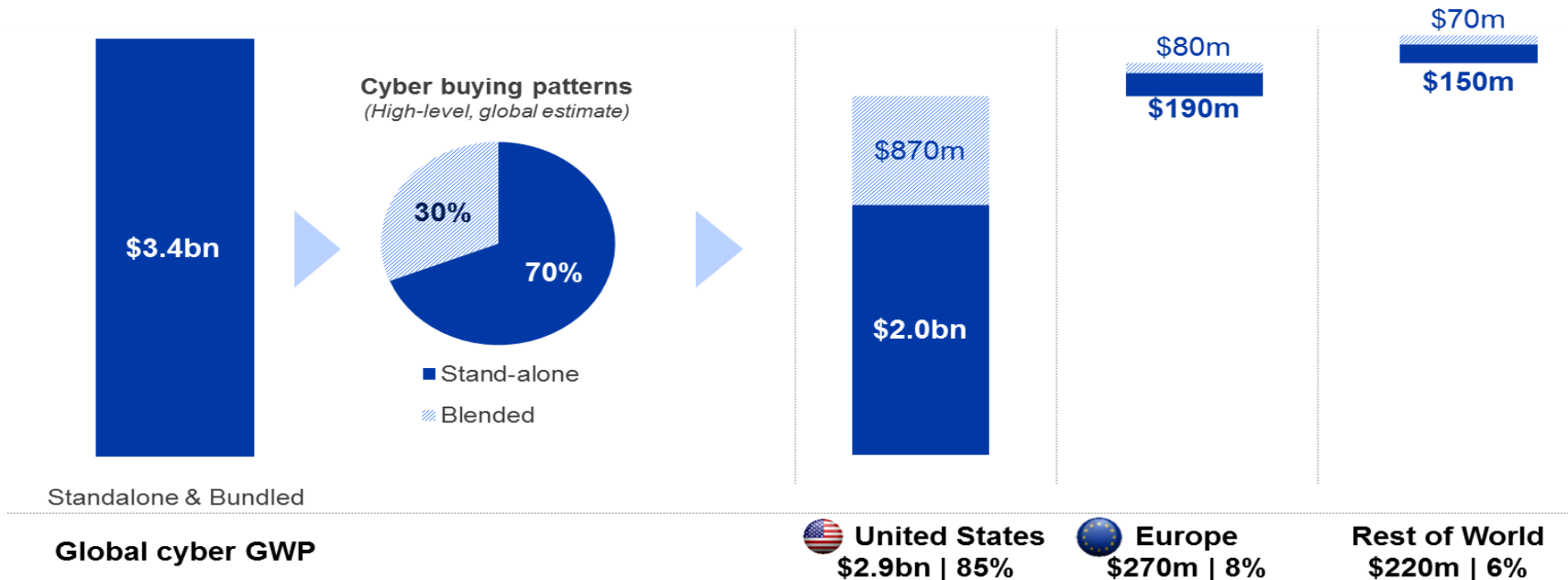
Expense/Service Sections

Expenses Paid to Vendors

- ✓ Crisis Management
- ✓ Breach-related
Legal Advice
- ✓ Forensics
- ✓ Breach Notification
- ✓ Call Center
- ✓ Credit Monitoring,
Identity
Monitoring, ID
Theft Insurance
- ✓ Cyber Extortion
Payments

The global cyber market is estimated to be worth c.\$3.4bn in premium

- 70% - c. \$2.3bn relates to standalone cyber products
- 85% of the business originates from the US



Source: Aon Inpoint analysis, Swiss Re Sigma, Aon GRIP data, Aon cyber whitepaper, Aon practitioner insights, PWC, Allianz, Advisen



Over the last decade, the US market has shown high growth levels

US standalone cyber GWP (figures where available)

- +32% year on year growth between 2011-2016
- Growth driven by several factors:



Legislation

Data breach legislation enacted in 48 states between 2002-2017



Awareness

Cyber ranked as their 5th most important risk in 2015 vs. 18th in 2011



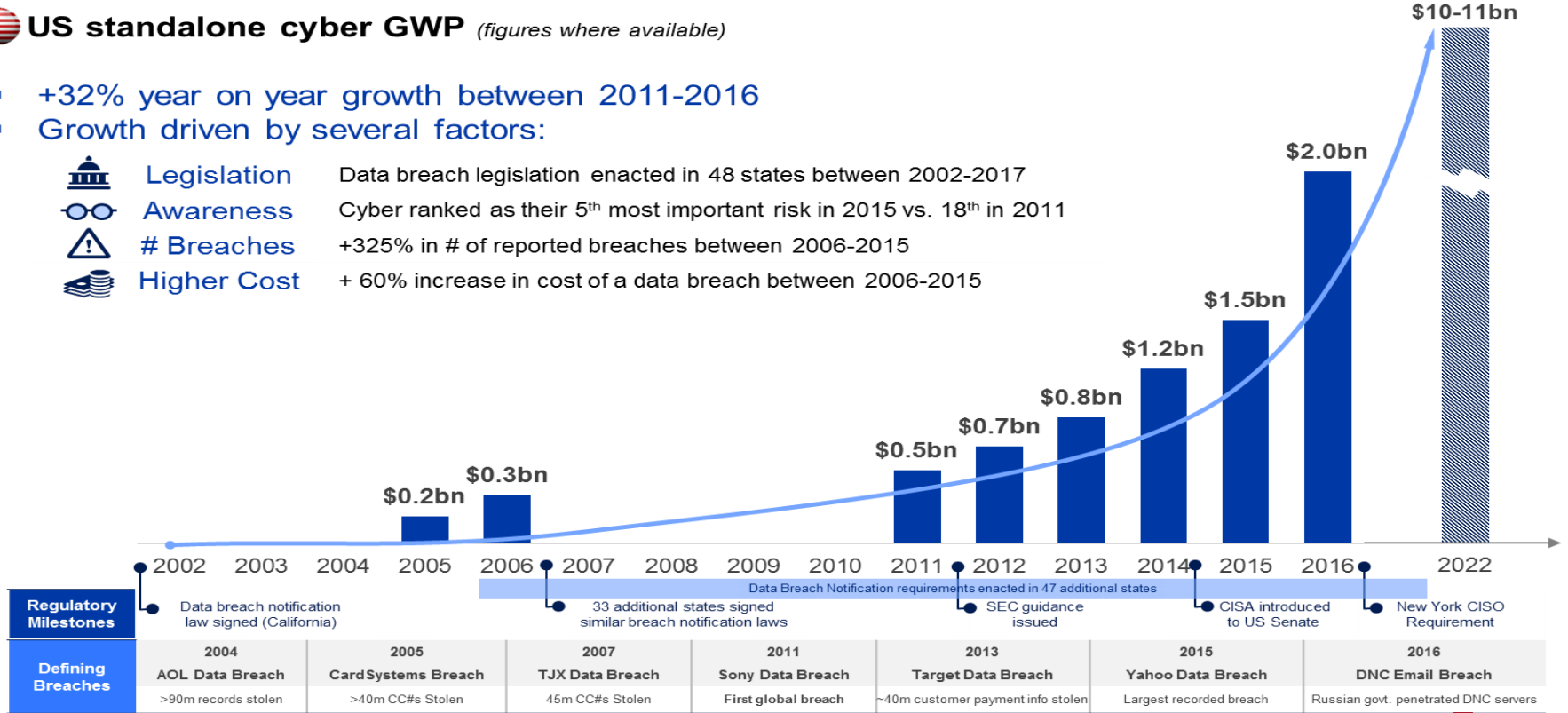
Breaches

+325% in # of reported breaches between 2006-2015



Higher Cost

+ 60% increase in cost of a data breach between 2006-2015



Source: Betterley Report, Advisen, PropertyCasualty360, Business Insider, Marsh, Aon, datalossdb.org, Identity Theft Resource Center, NCSL, Ponemon Institute, Aon Global Risk Survey, Aon Inpoint analysis

Notes: 1. Aon Global Risk Survey
2. Identity Theft Resource Centre/ Breach Level Index
3. The Ponemon Institute

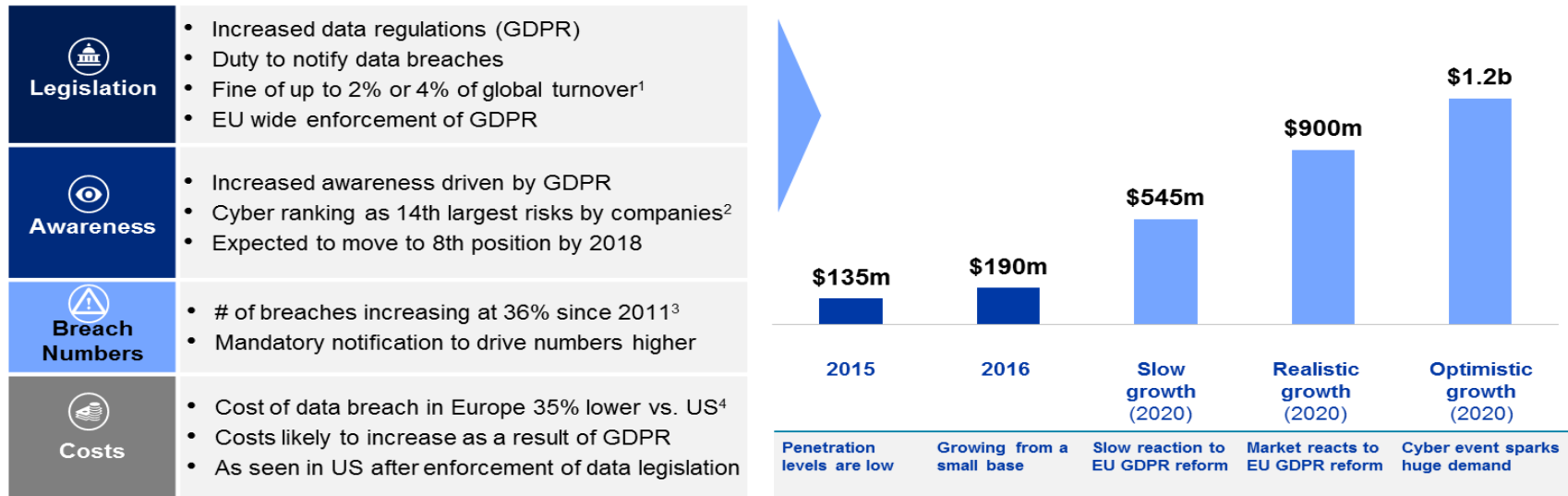




The EU standalone cyber market is estimated to be worth c.\$190m and could grow to c.\$900m by 2020 as a result of GDPR's impact on buyer awareness and demand

EU standalone cyber GWP

- +40% GWP growth between 2015-2016
- Expected to see accelerated growth due to stricter regulations and increased awareness



Source: The European Union, Breach Level Index, IBM, Ponemon Institute, Aon Global Risk Survey, Aon Inpoint analysis

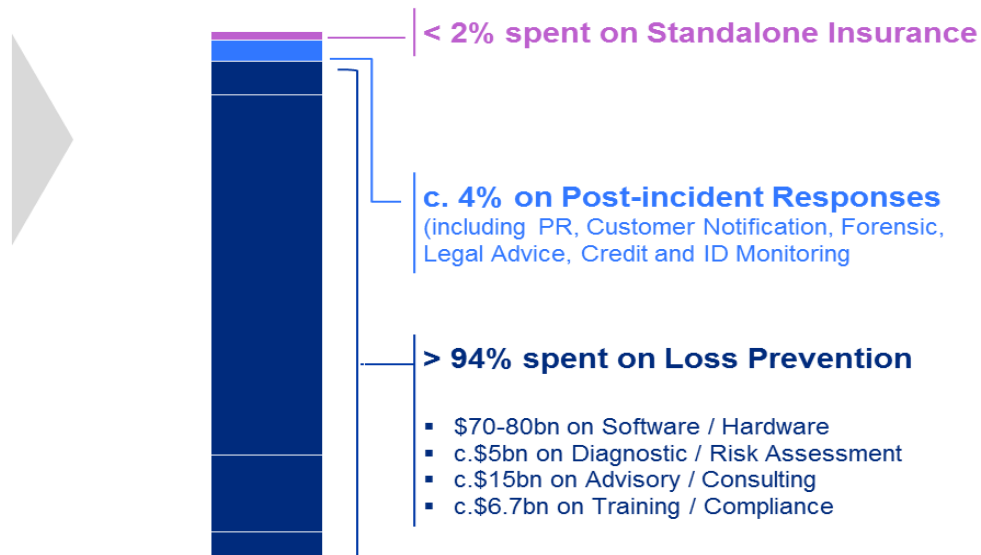
Notes: 1. Depending on activity | 2. Aon Global Risk Survey | 3. The Breach Level Index | 4. IBM

Insurance only represents a small fraction of companies' spend on cyber security

We estimated the total 2015 cyber security market to be worth **c.\$100bn**

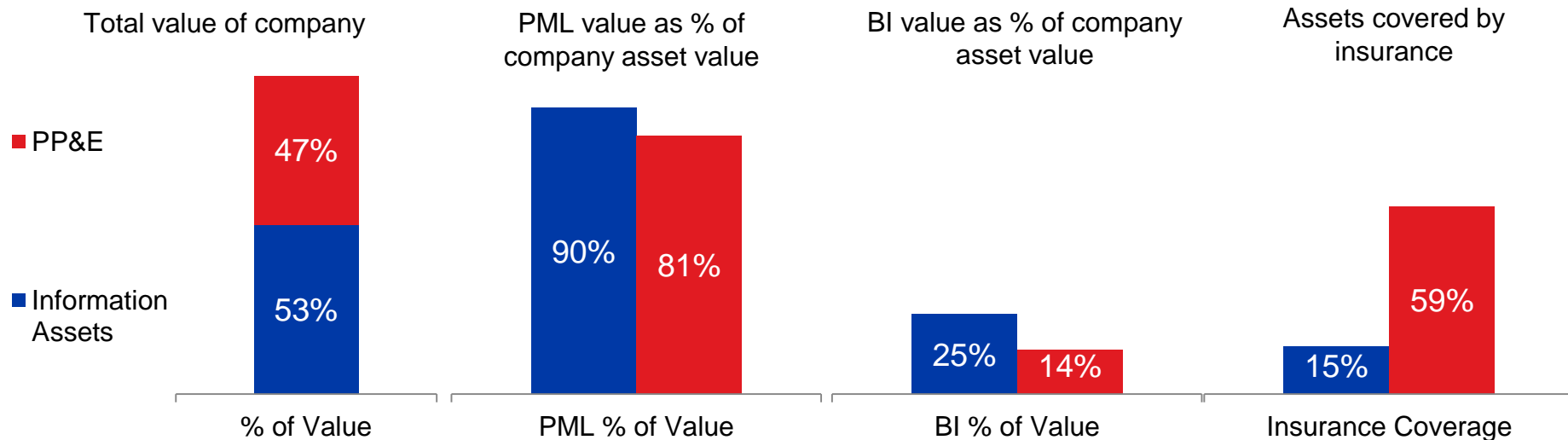
- The majority of cyber spend is on loss prevention solutions
- Despite strong growth over the last few years, Insurance only accounts for c.2%

**2015
Global cyber security
spend**



2017 Aon Sponsored Ponemon Institute Global Cyber Risk Transfer Study

Information Asset vs. PP&E Risk Summary



Probable Maximum Loss (PML): A property loss control term referring to the maximum loss expected at a given location in the event of a fire at that location, expressed in dollars or as a percentage of total values.

Key Takeaways from Study

- Information asset values have eclipsed PP&E asset values and is expected to continue growing
- Companies face greater risk to their enterprise due to information asset risk exposure than ever before
- Information assets are underinsured against theft or destruction based on the value, probable maximum loss (PML), and likelihood of an incident

Making your firm Cyber Resilient

- Take a holistic approach and create a solution that fits your business
- Impact of under-insurance for information assets is real; mitigate and transfer when possible

Link to full [2017 Global Cyber Risk Transfer Comparison Report](#)

Questions?

Maarten van Wieren

Managing Director – Aon Cyber Solutions Group

Rotterdam, The Netherlands

+31682019225

maarten.van.wieren@aon.nl

Disclaimer

© Aon plc or its affiliates ("Aon"). All rights reserved.

NOTE: Aon does not provide or express an opinion or recommendation regarding any company or matter mentioned herein. The recipient understands that Aon has endeavoured to include information known to it which it believes to be relevant to the recipient. The recipient further understands that neither Aon nor its employees shall make any representation or warranty as to the accuracy or completeness of this information. Aon shall not have any liability to the recipient or any other party resulting from the use of this information by the recipient or such other party.

May not be reproduced in any way or disseminated to any other party without the prior written consent of Aon.

Aon has endeavoured to ensure that this report is free of any virus or any other thing that would affect the recipient's computer system. However, Aon cannot guarantee the security status of this report and shall not have any liability to the recipient or any other party resulting from access to or use of the report.