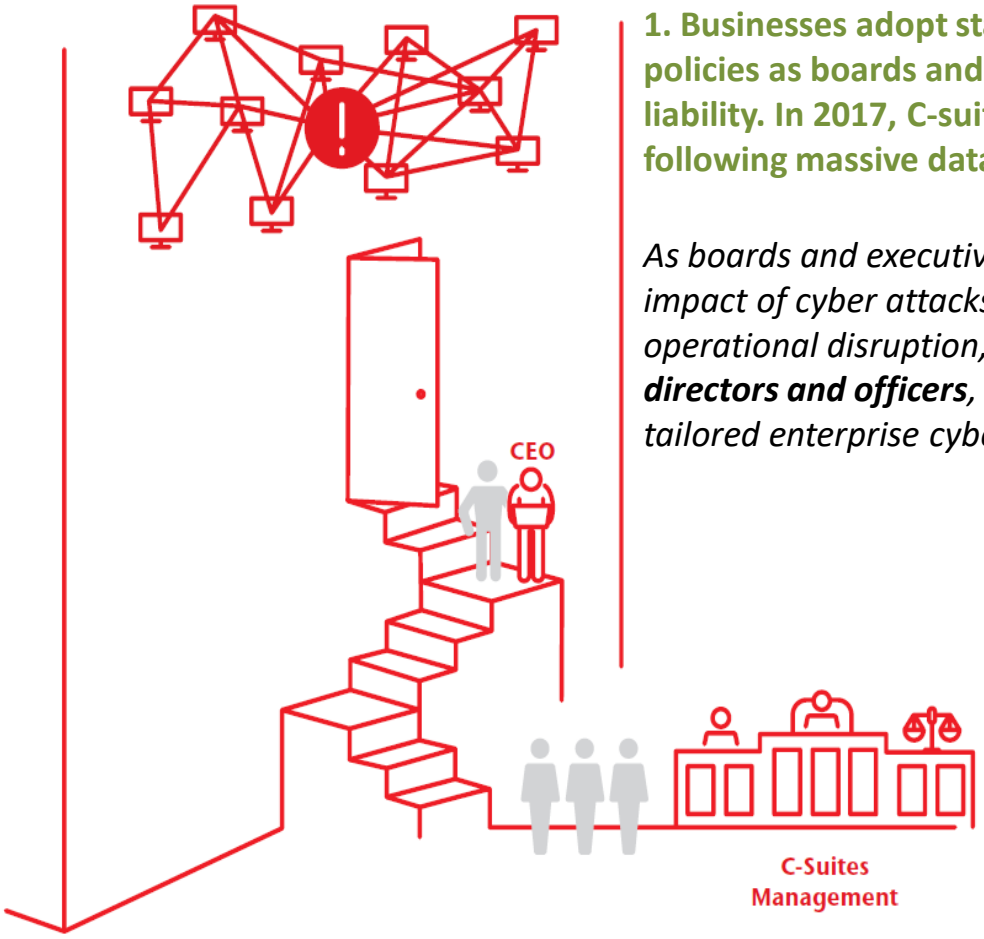

“How will cyber risk management affect tomorrow's business?”
AON
Empower Results®

The "integrated" path towards continuous improvement of information security

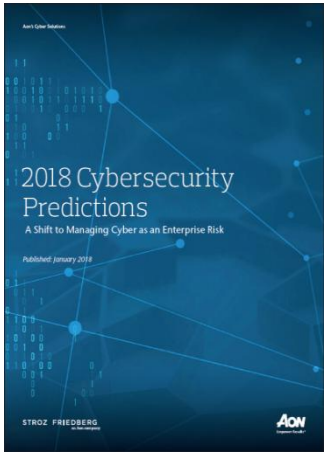
Cyber Risk as a Balance Sheet Risk … exposing Board and C-Levels

2018 Cybersecurity Predictions



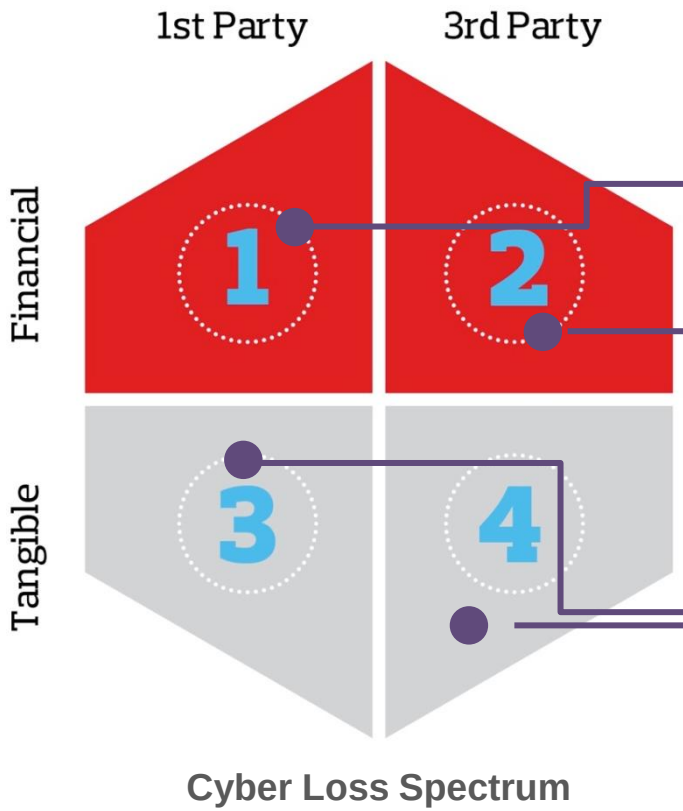
1. Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability. In 2017, C-suite executives resigned following massive data breaches.

As boards and executives witness the material impact of cyber attacks, including reduced earnings, operational disruption, and claims brought against ***directors and officers****, businesses will turn to tailored enterprise cyber insurance policies*



AON
Empower Results®

Cyber Risk Impacts All Loss Quadrants



Cyber Loss Spectrum

Any major cyber event will result in

- Public relations, response, and continuity costs
- Immediate and extended revenue loss
- Restoration expenses
- Defence costs

Third parties will seek to recover

- Civil penalties and awards
- Consequential revenue loss
- Restoration expenses

Physical damage is possible

- Property damage
- Bodily injury

Physical damage may cascade to others

- 3rd party property damage
- 3rd party bodily injury

AON
Empower Results®

Cyber Risk as a Balance Sheet Risk

Business Disruption

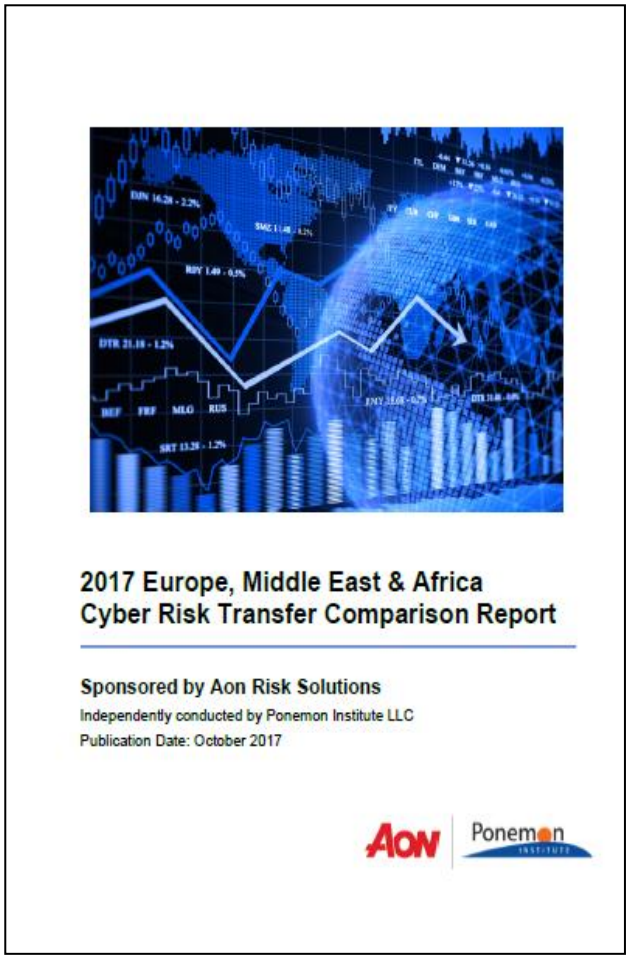
- **Financial statement impact of breaches shift to business disruption**
  - Denial of service & ransomware attacks can be more severe than data breaches
  - 2017 WannaCry and NotPetya ransomware attacks resulted in extended business disruption

D&O Claims

- **D&O follow on claims represent an increasing exposure**
  - **Wendy**'s derivative suit arising from a data security breach was settled for cybersecurity changes, corporate governance therapeutics, and $950,000 in plaintiffs' attorneys' fees (May 2018)
  - **Yahoo!**'s breach-related securities class action claim settlement of $80M is the first substantial data breach-related shareholder lawsuit recovery (March 2018)
  - **Home Depot** follow-on claim appeal settled for $1M+ corporate governance changes (May 2017)
  - Pending **Equifax** follow-on directors and officers claim arising out of a network security breach
  - **Wyndham** follow-on directors and officers claim: road map to effective litigation defenses

AON
Empower Results®

What do organizations in EMEA think?



Key Findings

- ✓ The impact of business disruption to cyber assets is 50% greater than to property, plant and equipment assets (PP&E)
- ✓ Only 15% of the probable maximum loss (PML) potential for information assets is covered by insurance; almost two thirds (60%) of total PP&E asset values are protected
- ✓ Only 30% of respondents state they are 'fully aware' of the economic and legal consequences of an international data breach or security exploit

2017 EMEA Cyber Risk Transfer Comparison Report

AON
Empower Results®

Market Positioning and analysis

Overall cyber market tatus and growth.

The global cyber market is currently estimated to be worth approximately 3.4 billion dollars, of which 70% is related to stand-alone cyber products. Currently, a full 85% of this business originates in the U.S. The EU stand-alone cyber market, in contrast, is estimated to be worth approximately $190 million, but **could grow extremely rapidly to as much as $900 million (over 400 percent)** by 2020 as a result of the new **GDPR** directive, which is having a dramatic impact all over the EU and beyond.

Status and distribution of cyber security spending

As large and growing as the cyber security market is, a full 94% of the expenditures in that market is currently focused on loss prevention (whereby between 70 and 80 percent is spent on software and hardware, around 5% on risk assessment, 15% on consulting, and 6 percent on training and compliance).

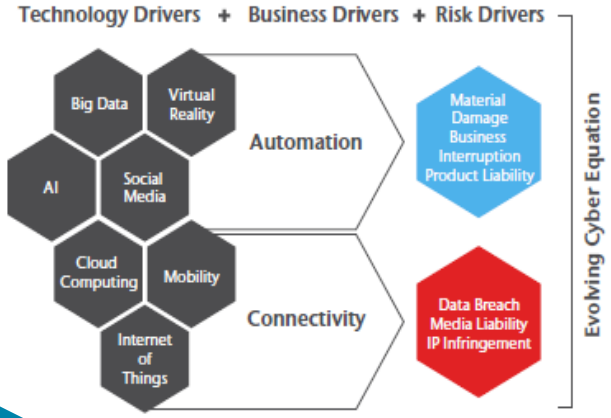
AON
Empower Results®

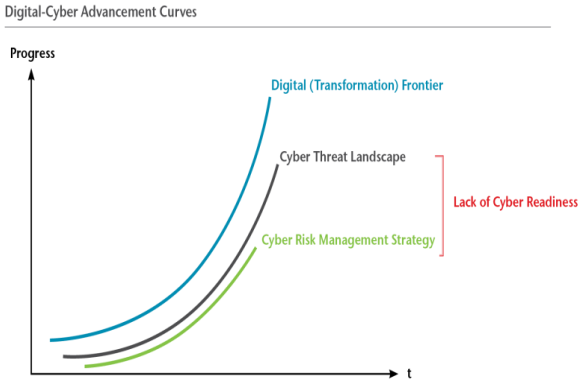
How to define an appropriate risk management strategy

Cyber Risk - Scope

3 Key Points

1. Complex and dynamic risk
2. IT and Business relationship
3. Risk is always > 0





AON
Empower Results®

Cyber Risk Management

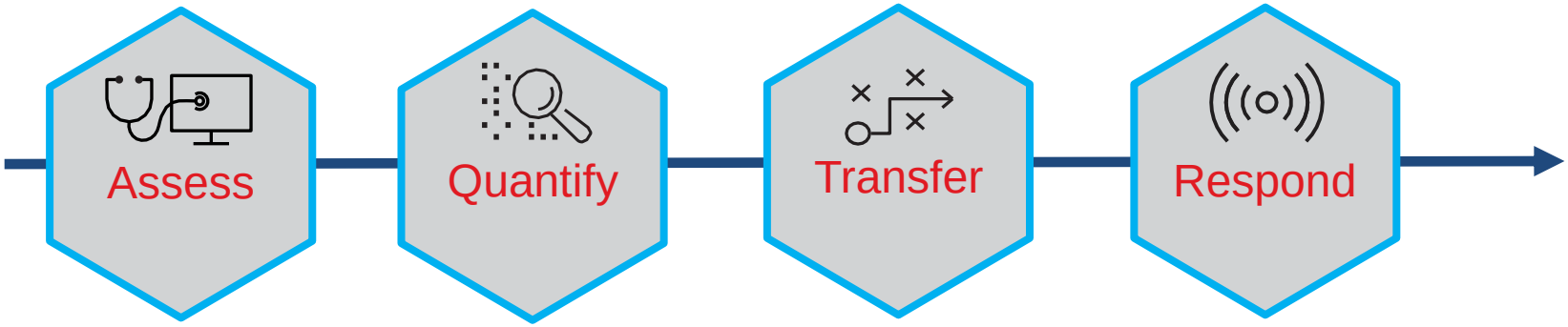
Objectives and methods

The process, designed according to the sector's Best Practices (ISO 27001 and ISO 27005), aims to improve the degree of protection, security from any type of internal and external Cyber risk to:

- **Provide a view of the risk scenarios applicable to organizations**
- **Manage and control the risk of information security**
- **Identify the "critical" areas of the Organization,**
- **Define a process of continuous improvement of information security**

AON
Empower Results®

Cyber Risk Management | Adopting a Risk-Based Cyber Insurance Strategy



- Helping clients optimise the total cost of risk associated with cyber exposures

Holistic integration with Enterprise Risk Management (ERM) framework: appetite, financing, and insurance

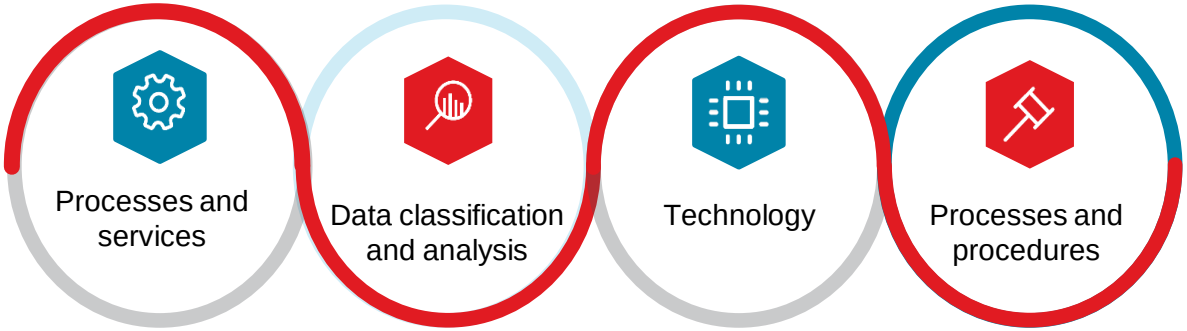
Includes harmonized input from Compliance, Legal, Finance, HR, BUs, Internal Audit + Cybersecurity and IT

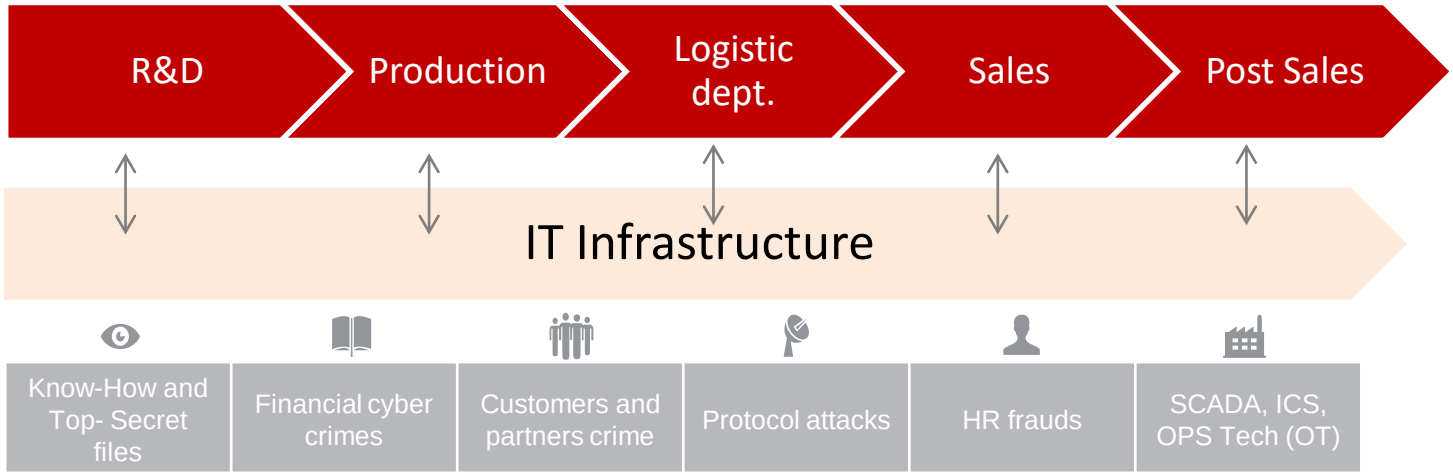
AON
Empower Results®

The "integrated" path towards continuous improvement of information security

Cyber risk Holistic analysis

The analysis to be carried out with the managers of the various areas of the organization, assessing:

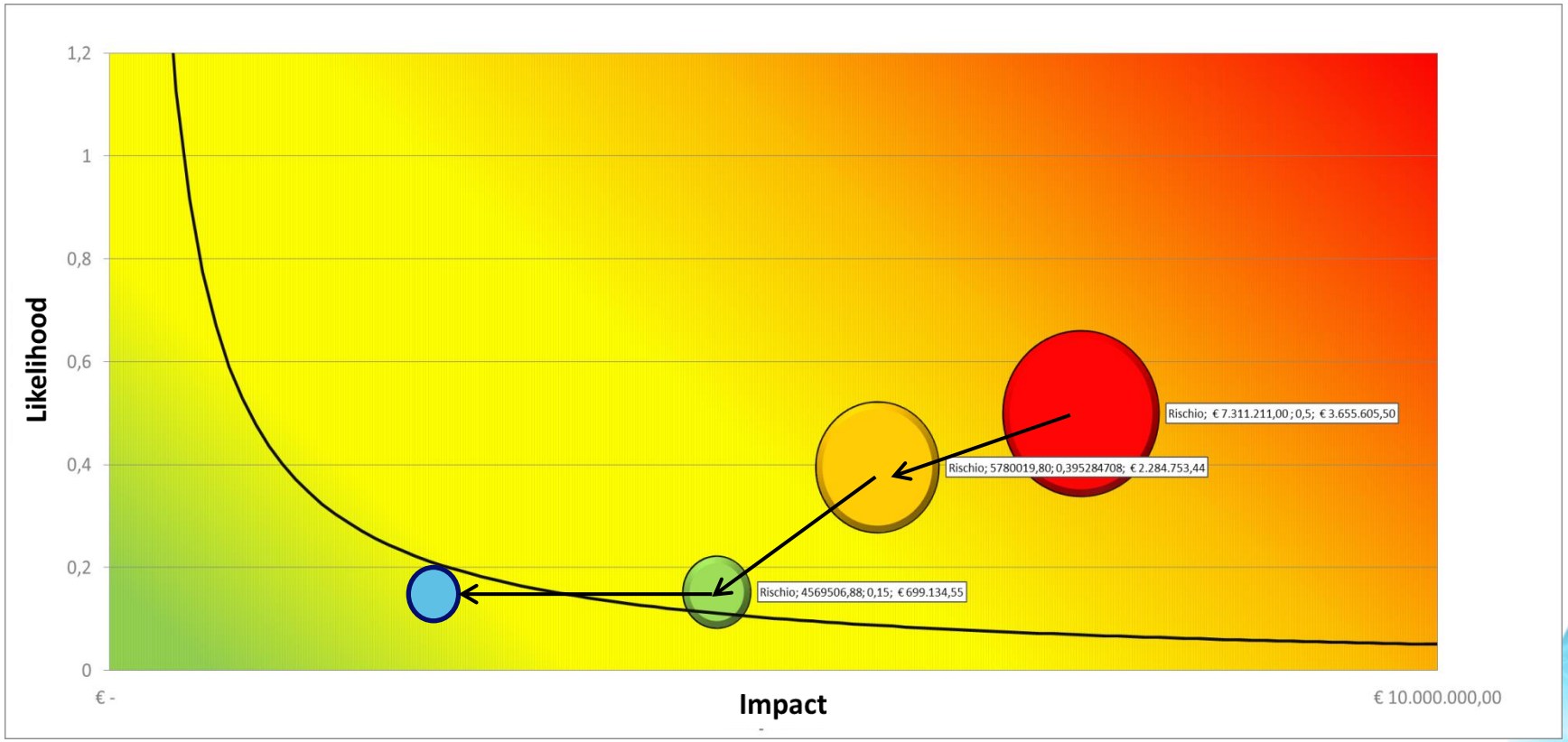




AON
Empower Results®

Cyber risk «integrated» path

Synthesis and standards

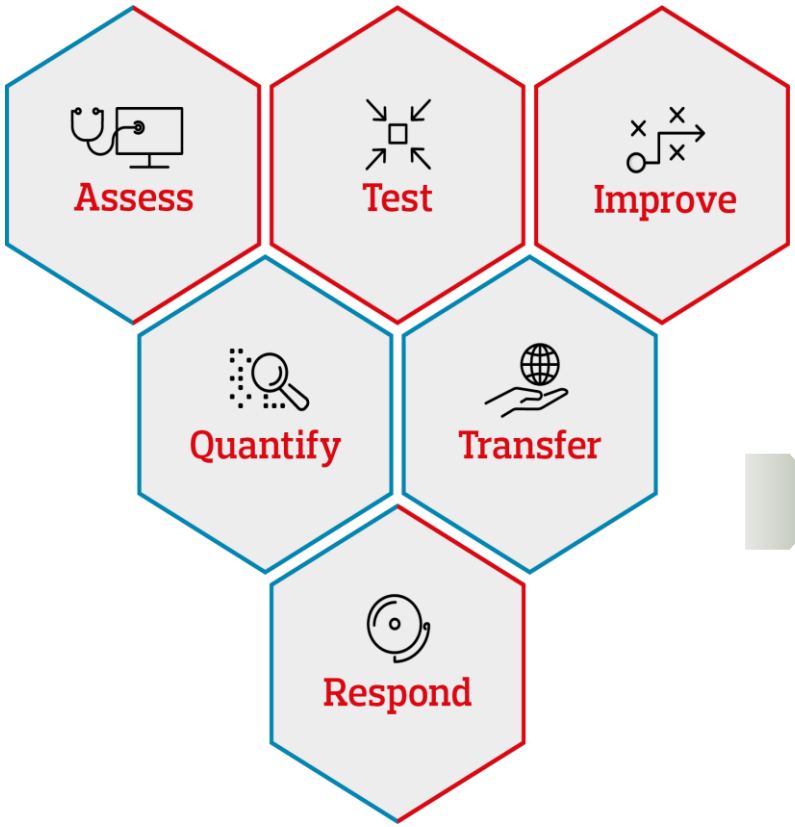


- Intrinsic Risk
- Actual Risk
- Residual Risk
- Post Insurance – Transfer

AON
Empower Results®

The main factors that determine the price and the perimeter of a tailor made cyber insurance

The "integrated" path towards continuous improvement of information security



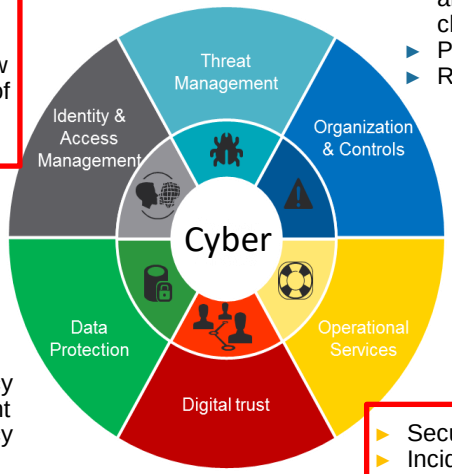
Cyber Risk Management

Cybersecurity Management

- Identity and access management
- Access review
- Segregation of duties
- Ecc.

- Threat intelligence
- Vulnerability Management
- Penetration Test
- Ecc.

- Strategy
- ISMS
- Training and awareness
- Governance and processes
- Asset evaluation and data classification
- Policy
- Reporting



- GDPR
- Data privacy management
- Data privacy governance

- Cloud Protection
- IOT cybersecurity
- Security Awareness
- …

- Security Monitoring
- Incident Response e Data Breach MGMT
- Network & host security
- Business Continuity Management & DR
- Change Management

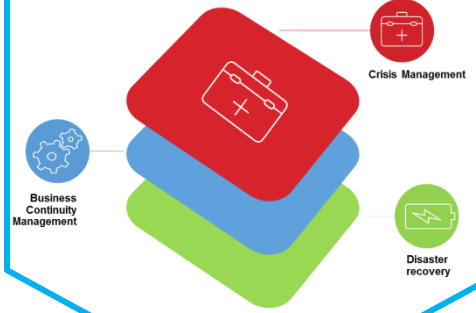
AON
Empower Results®

Elements aimed at mitigating the cost of the insurance policy

Revenues from Online activities

IAM

BCM & DR



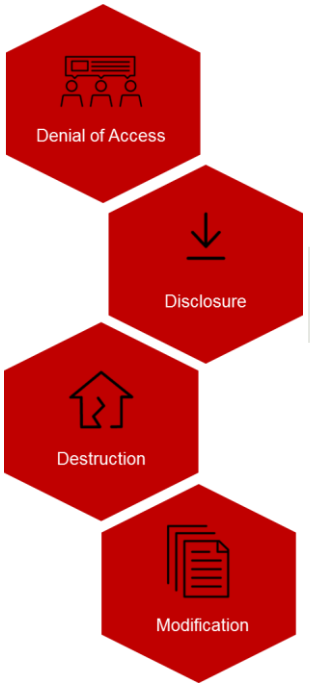
BACKUP

AWARENESS

AON
Empower Results®

Adopting a Risk-Based Cyber Insurance Strategy

Identify Scenarios



Define Impact

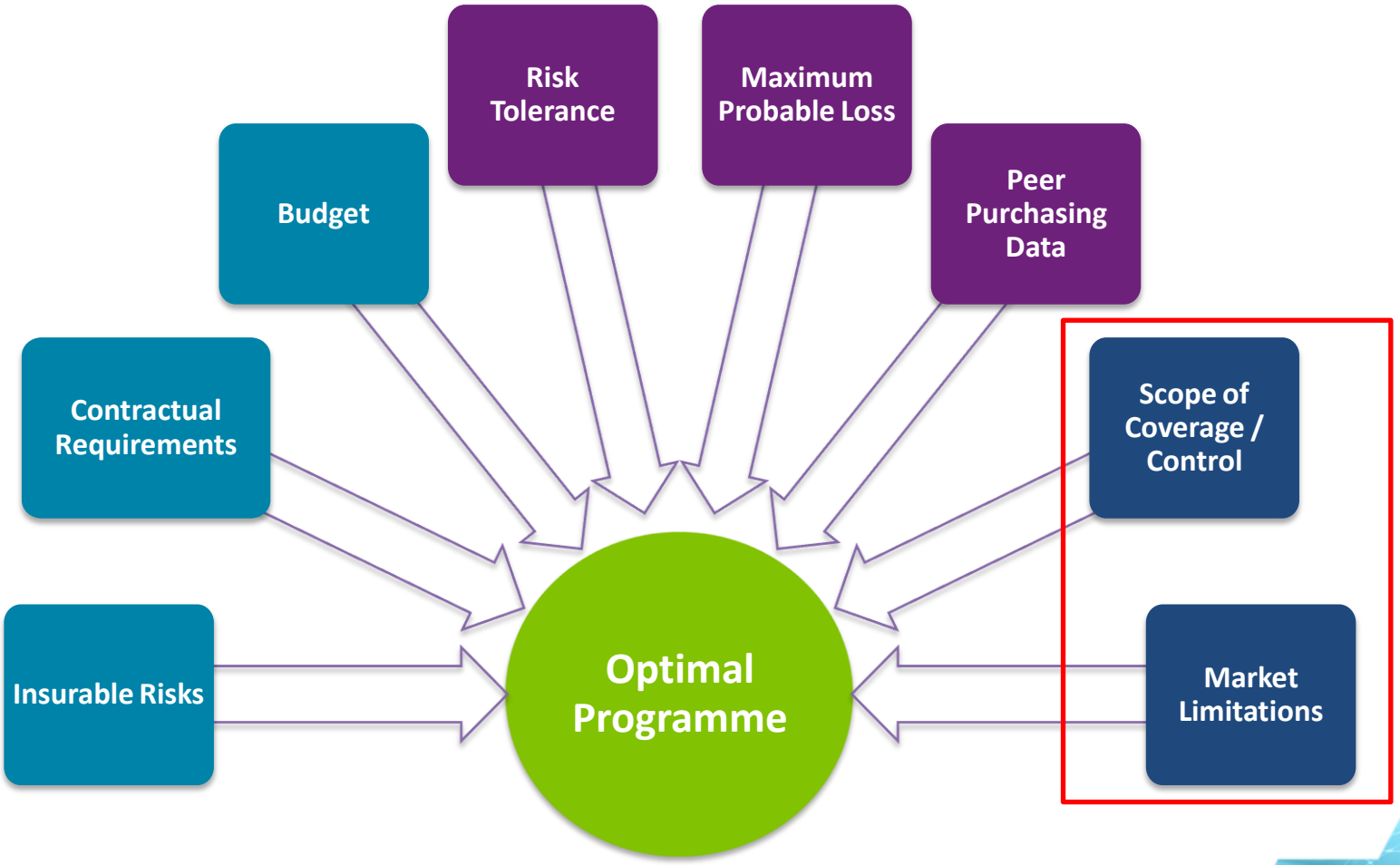
Evaluate Insurance Position

Cyber risk — No coverage | Limited coverage | coverage

	Property	General liability	Crime/Bond	K&R	Professional indemnity	Cyber
1st Party Privacy/Network Risks						
Physical damage to data only						
Virus/hacker damage to data only						
Denial of service attack						
B.I. loss from security event						
Extortion or threat						
Employee sabotage of data only						
3rd Party Privacy/Network Risks						
Theft/disclosure of private info.						
Confidential corporate info. breach						
Technology E&O						
Media liability (electronic content)						
Privacy breach expense/notification						
Damage to third party's data only						
Regulatory privacy defense/fines						
Virus/malicious code transmission						

AON
Empower Results®

Placement Strategy



AON
Empower Results®

Cyber Risk: Main Topics

Relevant Elements

01

Risk Mitigation & Coverage: define a correct strategy for risk analysis and management, combining strategic risk mitigation plans in the Cyber Security (Risk Management Plan) and any policies.

02

Dynamicity: The cyber risks are constantly evolving and the analysis of these aspects is always recommended to be entrusted to experts in the sector.

03

Regulatory risks and certifications: Risk analysis today is a recurring element in most new mold laws and regulations, as well as in ISO standards (9001, 27001).

AON
Empower Results®

ANNEX

Notable NotPetya Commercial Impacts

Organisation	Commercial Impact	Financial Components	Source
A.P. Moller – Maersk	$250--300 million	Earnings Reduction	Q4 2017 Financials
Beiersdorf AG	Minimal sales impact €15 million	€35mm sales shifted Q2 to Q3 Additional expenses	Q2 2017 Financials Q4 2017 Earnings Call
FedEx (TNT Express)	$400 million	Earnings Reduction	Q3 2018 Financials
Merck & Co.	$460 million $355 million	2017, 2018 Sales Reduction Additional Expenses	Q4 2017 Financials Q1 2018 Financials
Mondelez International	~$104 million $84 million	2017 Sales Reduction Additional Expenses	Q4 2017 Earnings Call Q4 2017 Earnings Release
Nuance Communications	$68 million $30 million	2017 Sales Reduction Additional Expenses	Q1 2018 Financials
Reckitt Benckiser	~£114 million	2% Q2 Sales Reduction 2% Q3 Sales Reduction	Press Release Q2 2017 Financials Q3 2017 Financials
Saint-Gobain	~€220-250 million €80 million	2017 Sales Reduction 2017 Earnings Reduction	Q3 2017 Earnings Release Q1 2018 Earnings Release

Notable Data Breach / Intrusion Commercial Impacts

Organisation	Commercial Impact	Financial Components	Source
Anthem	$263 million	Gross Expenses ($148mm) Security Improvements ($115mm)	Regulator Settlement U.S. District Court
Equifax	$242.7 million $439 million	Gross Expenses to Date Total Estimated Gross Expenses	Q1 2018 Earnings Release Q1 2018 Earnings Call
Global Payments	$141 million	Gross Expenses	10-K Filing 2015
Heartland Payment Systems	$148 million	Gross Expenses	10-K Filing 2013
The Home Depot	$298 million	Gross Expenses	10-K Filing 2017
Sony Corporation (2011)	~$171 million ¥14 billion	Consolidated Operating Income	2010 Forecast Revision
Sony Corporation (2014)	~$41 million ¥4.9 billion	Investigation & Remediation Expenses	Q4 2014 Financials
Target Corporation	$292 million	Gross Expenses	10-K Filing 2017
The TJX Companies	$187 million	Gross Expenses	10-K Filings
Yahoo! Inc. (Altaba Inc.)	$350 million $35 million $80 million	Reduced Acquisition Price SEC Fine Securities Class Action	Verizon Press Release SEC Press Release U.S. District Court