

CYBERSECURITY AND INSURANCE

Prof. Avv. Fabio Maniori
Maniori Studio Legale
Università Cattolica del Sacro Cuore

New Challenges From The Online Environment In Insurance
15 October 2020

Covid 19

54%

- Organizations using smart working as a consequence of COVID-19

76%

- Participants to the survey declaring that smart working would increase time to identify and contain a data breach

70%

- Participants to the survey declaring that smart working would increase the cost of data breach

Sorce: IBM Security, Cost of a Data Breach Report 2020

Cyber Risk Defined

Cyber Security

- Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
- Source: Adapted from ISO/IEC 27032:2012

Cyber Risk

- The combination of the probability of cyber incidents occurring and their impact.
- Source: Adapted from CPMI-IOSCO, ISACA Fundamentals(definition of “Risk”) and ISACA Full Glossary (definition of “Risk”)

Cyber Incident

- A cyber event that: i. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
- Source: Adapted from NIST (definition of “Incident”)

Role of Insurance Companies

Insurance Companies

Provide insurance coverage against
cyber risk



Are subject to cyber incidents

Insurance Companies are Exposed to Cyber Risk Too

- EIOPA issued on 12 October 2020 **Guidelines on information and communication technology security and governance**
- Approach based on governance and technology neutral
- 25 Guidelines, including
 - Governance, Information Security Policy, ICT Project Management, Business Impact Analysis
 - Strategy
 - Role of the Key Functions
 - Information security reviews, assessment and testing
 - ICT incident and problem management, Business Continuity Management, Response and Recovery Plans
 - Information security training and awareness

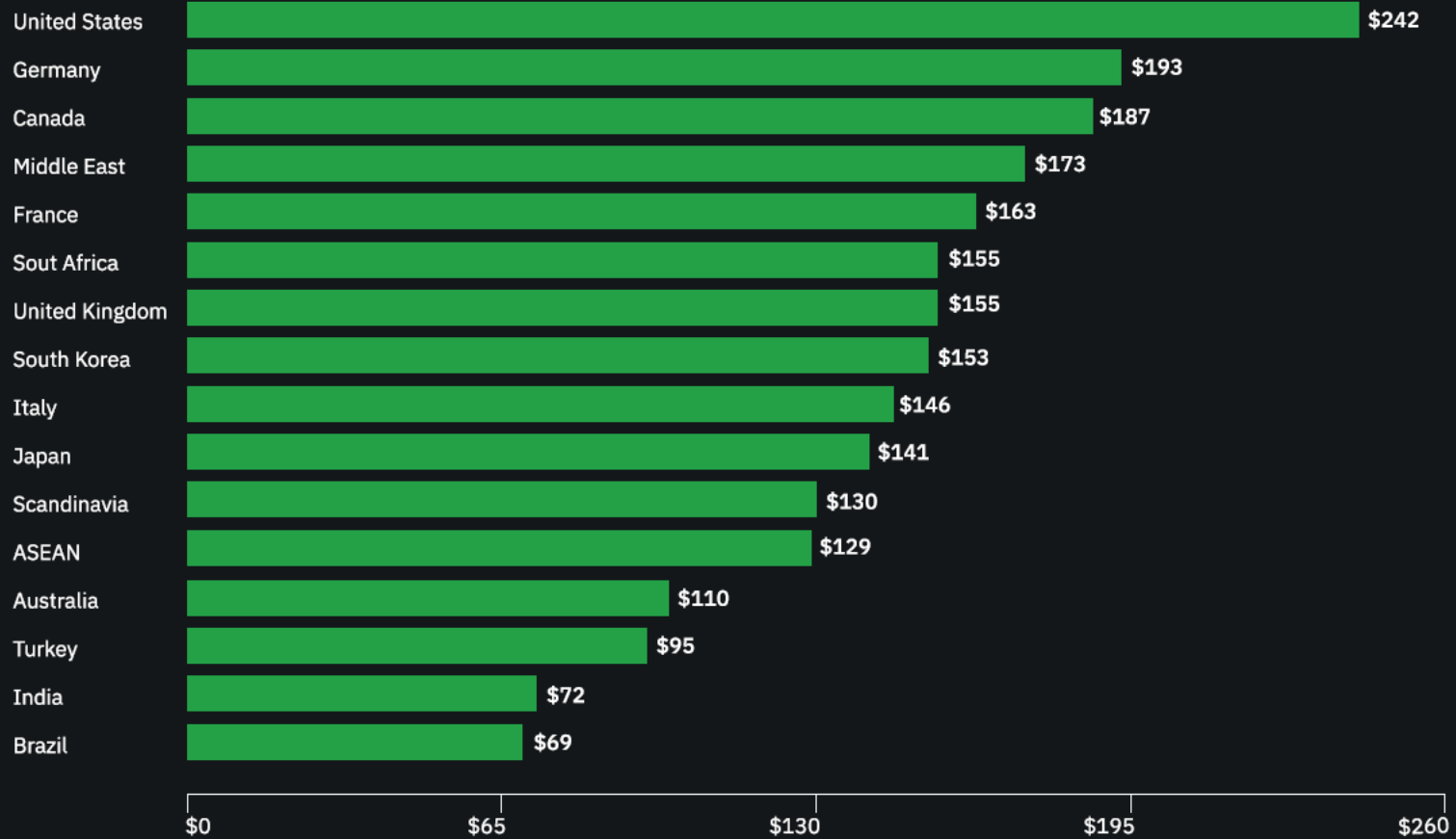
Cyber Insurance: A Brief History

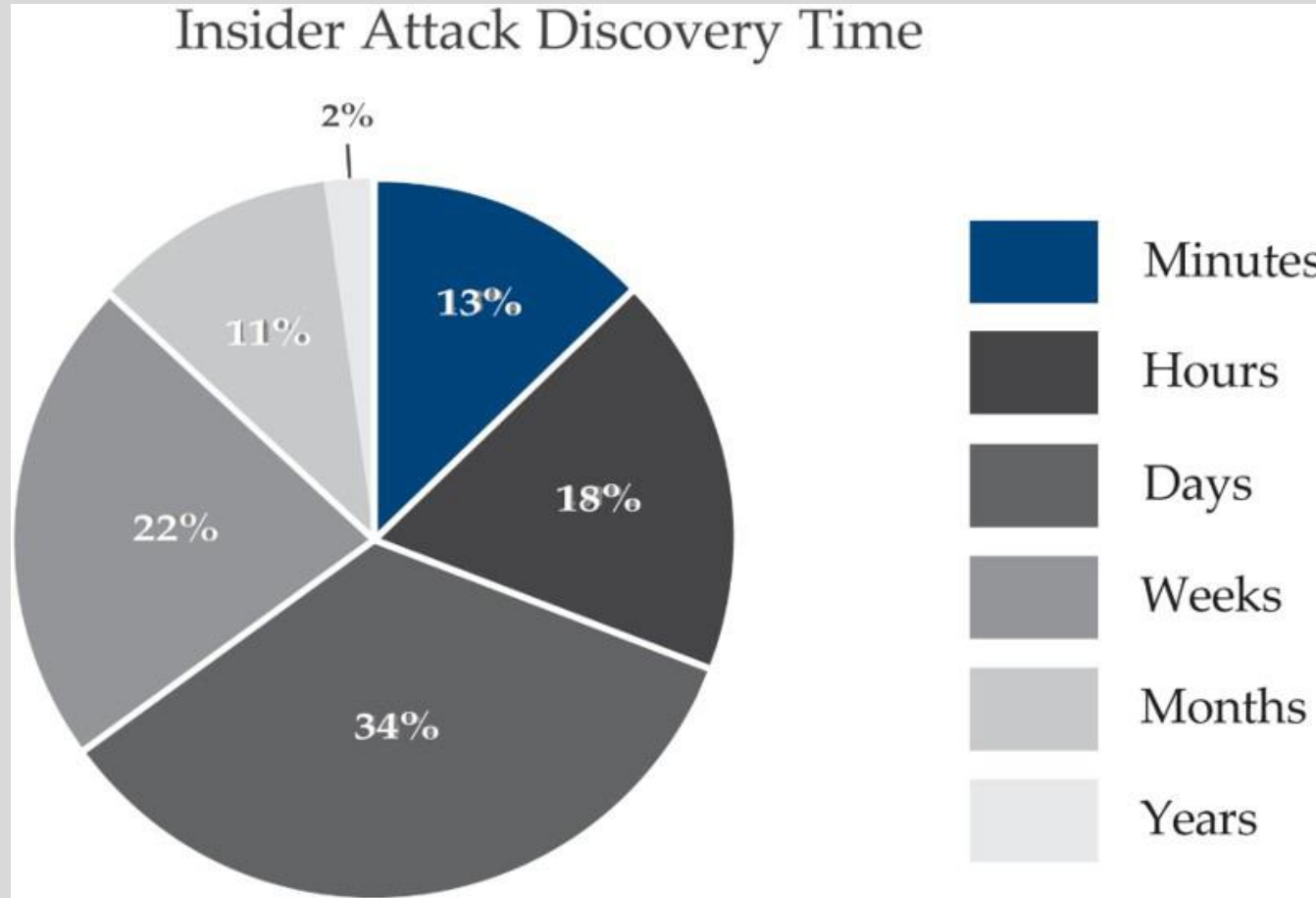
- First appeared in the late 1970s
 - Errors and Omissions (E&O)
- Cyber insurance as a stand-alone product
 - in response to the Y2K problem, aka the Millennium Bug
 - designed to fill gaps in traditional property and casualty (P&C) products
- Until early 2000s
 - Corporate expenditure concentrated on loss mitigation and network security
 - Insurers reluctant to offer cover, also due to lack of statistics
- New privacy regulation both in US and EU
 - Coverage focused on data breach
 - Information on average cost of data breach and average length of time before attack discovery become available

Global Averages 		Italy Averages 	
Average total cost of a data breach \$3.92M		Average total cost of a data breach \$3.52M	
Average size of a data breach 25,575 records		Average size of a data breach 24,577 records	
Cost per lost record \$150	Time to identify and contain a breach 279 days	Cost per lost record \$146	Time to identify and contain a breach 283 days
Highest country average cost of \$8.19 million United States	Highest industry average cost of \$6.45 million Healthcare	Country rank for total cost 8	Highest industry average for cost per record Financial

Cost per record by country or region

Measured in US\$





Source: Verizon Data Breach Investigations Report 2014

Content of Cyber Insurance

- Lack of standardisation
- First- and third-party exposures, including
 - loss or damage to digital assets
 - data recovery
 - business interruption
 - notification costs
 - liability in respect of data breaches
 - multimedia liability
 - employee dishonesty
 - cyber extortion
 - regulatory defence costs
 - Possibly damage to property and equipment
 - Possibly bodily damage
- Insurers also offer a number of services to their insureds (customers), most notably crisis management, forensic IT, security advice and legal consultation.

A Comprehensive Risk-Management Approach



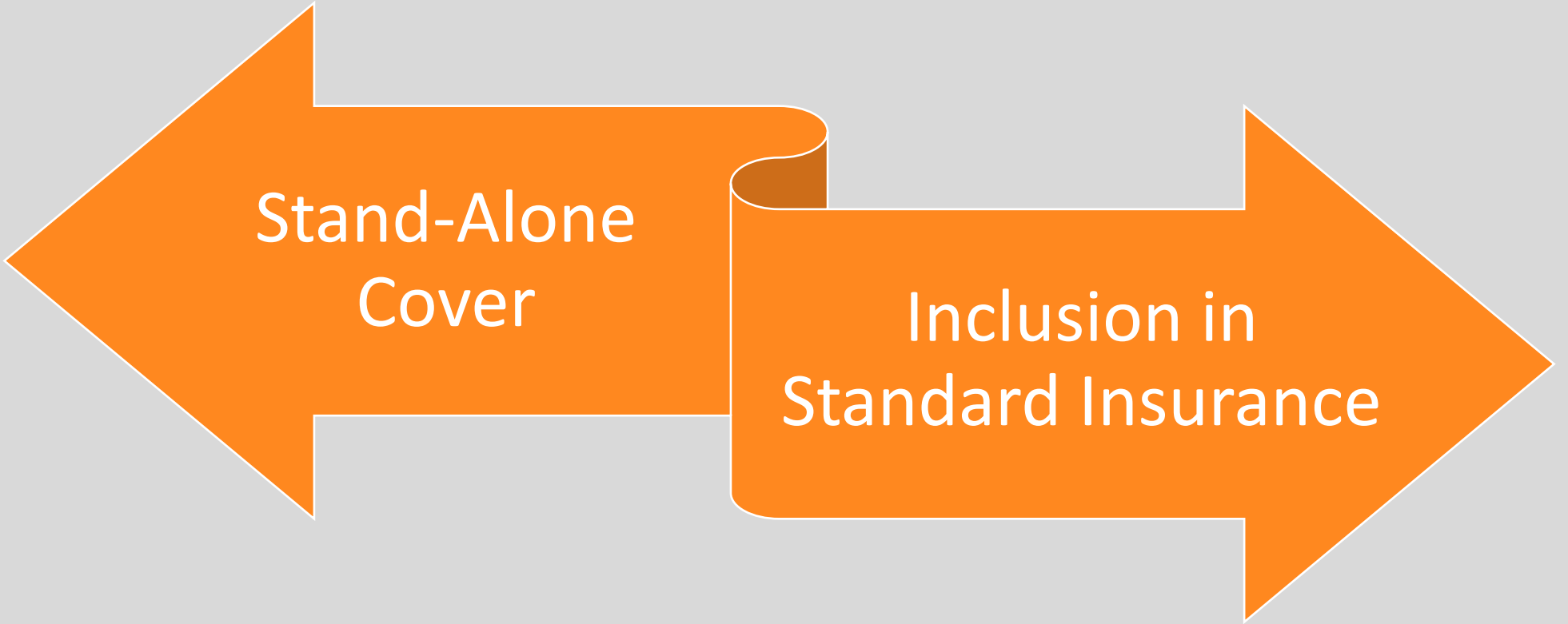
Role of technology

Tools

- Remote Browsing to reduce risks from accessing websites
- AI to monitor anomalies in a corporate network
- Sensor on networks

Consequences

- Dynamic risk management and premium adjustment



Cyber Risk as a War or Terrorism Risk

- Catastrophic events are excluded by law from coverage in some jurisdictions
- The Italian Civil Code lists some risks that are excluded from coverage unless the Insurer explicitly agrees to coverage
- Such risks include war but not terrorism
- It is widely believed that the list is provided by the Civil Code by way of example of catastrophic risks and it is not exhaustive
- Transparency is required when drafting insurance contract
- Controversies may possibly arise

Cyber Risk as a Catastrophic Risk

- According to one study of ARIA - American Risk and Insurance Association (2016)
 - Solvency II massively underestimates the threat to insurers from operational cyber risk
 - Capital requirements are only sufficient if carriers are underwriting a significantly large and well-diversified book of business
- Lloyd's Study
 - hypothetical scenario, which envisages hackers shutting down parts of the U.S. power grid, causing a total blackout in 15 U.S. states and Washington, D.C.
 - total impact on the U.S. economy was estimated at \$243 billion, rising to over \$1 trillion in the most extreme scenario

Governments Role

- Define standard data formats, in co-operation with industry
- Establish minimum assessment standards
- Collect high-level data
- Authorise information-sharing
 - (e.g. Block Exemption Regulation as far as EU Law is concerned)
- Possible role as a final insurer for catastrophic risks

Conclusion

Complex coverage
in constant
evolution

New business
model implying
partnership

Transparency
issues need to be
addressed

Government role
to be clarified



QUESTIONS?

Studio Legale Prof. Avv. Fabio Maniori

Via Boncompagni, 61

00187 ROMA RM

www.maniori.com

E-mail: fabio.maniori@maniori.com

Mobile: +39 335 57.56.322