Cyber Risks on the Rise

SCOR Global P&C Annual Conference
30 September 2016, Paris

State of the Cyber (Re)insurance Market

Didier PARSOIRE, CUO Cyber Solutions
Sébastien HEON, Deputy CUO Cyber Solutions

SCOR The Art & Science of Risk | P&C

AGENDA

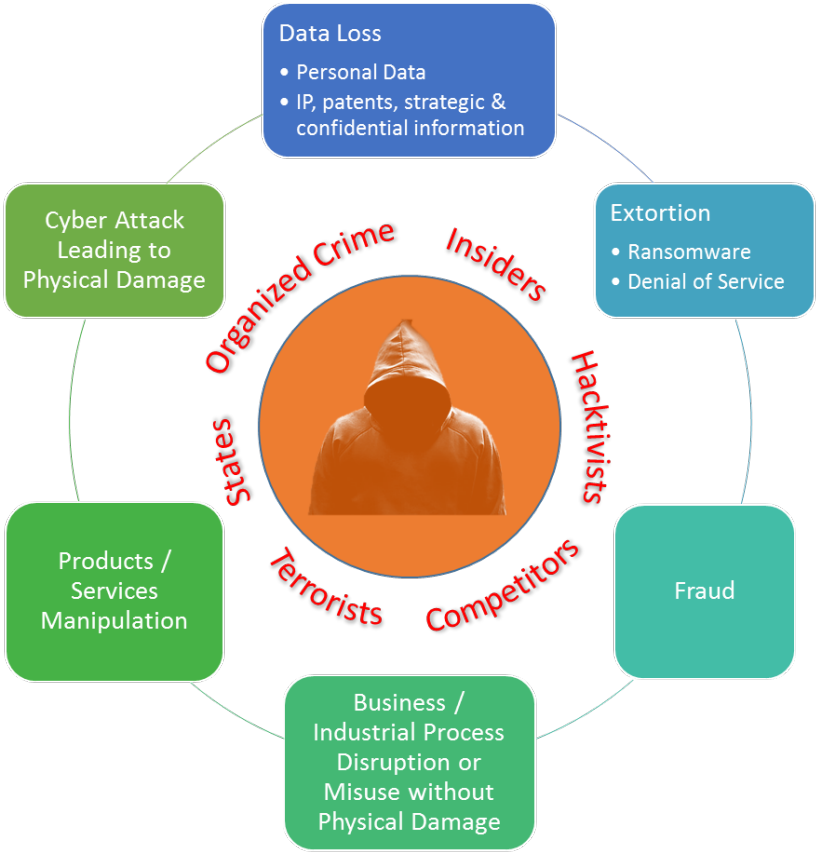
1. **Cyber Threats: Panorama & Trends**
2. Cyber Insurance products
3. Market Figures & Perspectives

Cyber Risks and Cyber Threats are very diverse

Cyber Risk has no standard definition

Organization	Definition of IT/Cyber Risk
ISACA Information Systems Audit and Control Association	IT risk is the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise
IUA International Underwriting Association	Cyber risk […] essentially encompasses any risk arising out of the use of technology and data
IMIA International Association of Engineering Insurers	Risks arising from the storage, use, computation, and/or transmission of electronic data. Such cyber risks may be malicious, for example caused by individual hackers or nation states, or inadvertent, for example caused by a coding error.
CRO Forum	The definition of cyber risk covers: • Any risk emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks • Physical damage that can be caused by cyber attacks • Fraud committed by misuse of data • Any liability arising from data use, storage and transfer • The availability, integrity and confidentiality of electronic information, be it related to individuals, companies or governments

Cyber Threats encompass many different cases, types of loss and motives



Cyber Threats: Panorama & Trends

In the last 18 months, all types of cyber threats have significantly increased

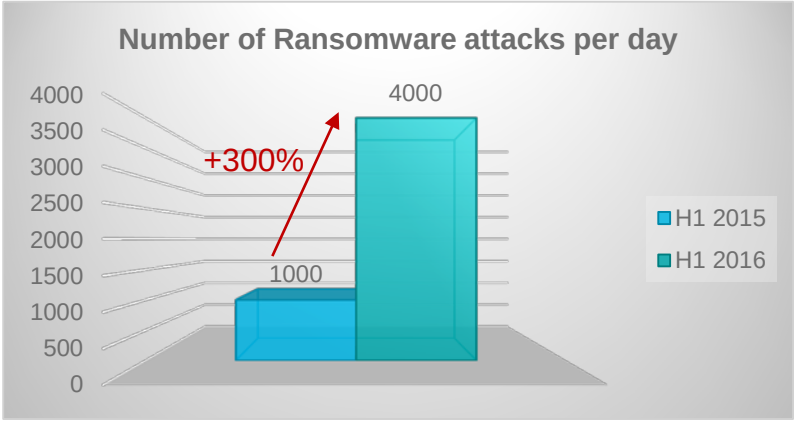
Ransomware / Cyber Extortion

Scope: Untargeted
Motive: Money

- Malicious software that encrypts data. A ransom must be paid to have the data decrypted
- Massive wave of ransomware in Q1/Q2 2016 against US hospitals
- Ransoms vary from ~$100 for individuals up to ~$20,000 for enterprises. Prices on the rise
- Pure profit for attackers – Customer Care Service to help people pay the ransom

Ransomware in 2015
-
2,453 cases
$24m losses

Source: FBI



- Feb. 2016, Hollywood Presbyterian Medical Center - **$17,000**.
- Apr. 2016, MedStar Health (10 hospitals in Maryland) - **$19,000**

Cyber Crime — State Sponsored

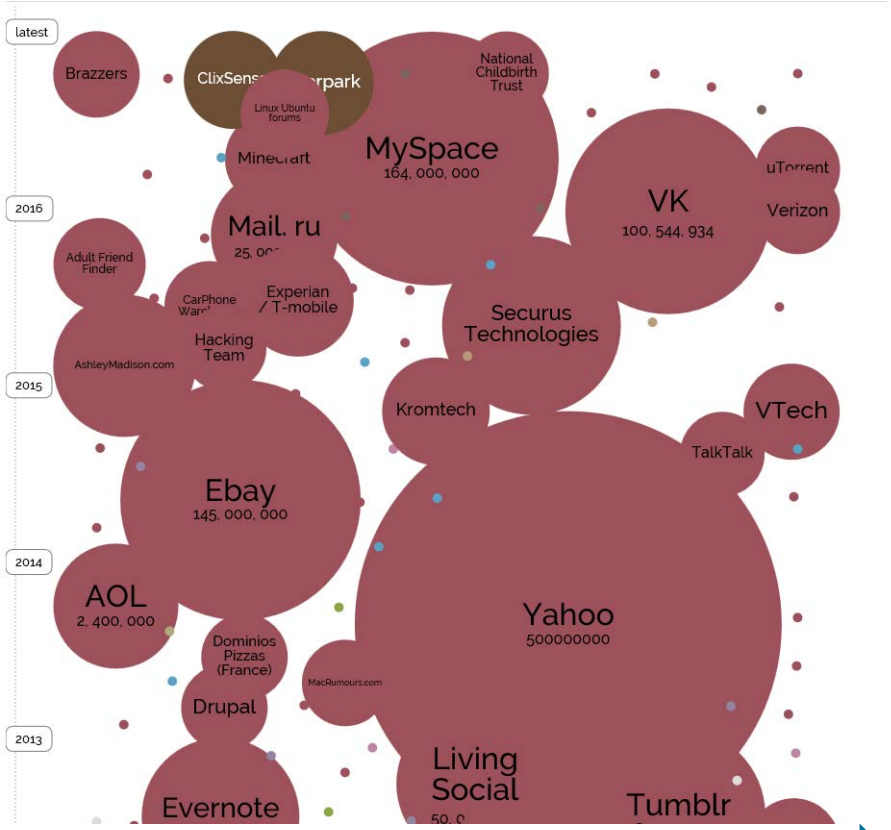
Cyber Threats: Panorama & Trends

In the last 18 months, all types of cyber threats have significantly increased

Data Theft / Privacy Breach

Scope: Targeted to Data Repositories
Motive: Money, Intelligence

- Attackers target the following:
  - Personal information: PII, PHI, PCI, credentials & passwords
  - Strategic, company confidential information (M&A, IP, financial statements…)
- US Regulation to impose reporting & notification to end-users



Ransomware

Cyber Crime — State Sponsored

Cyber Threats: Panorama & Trends

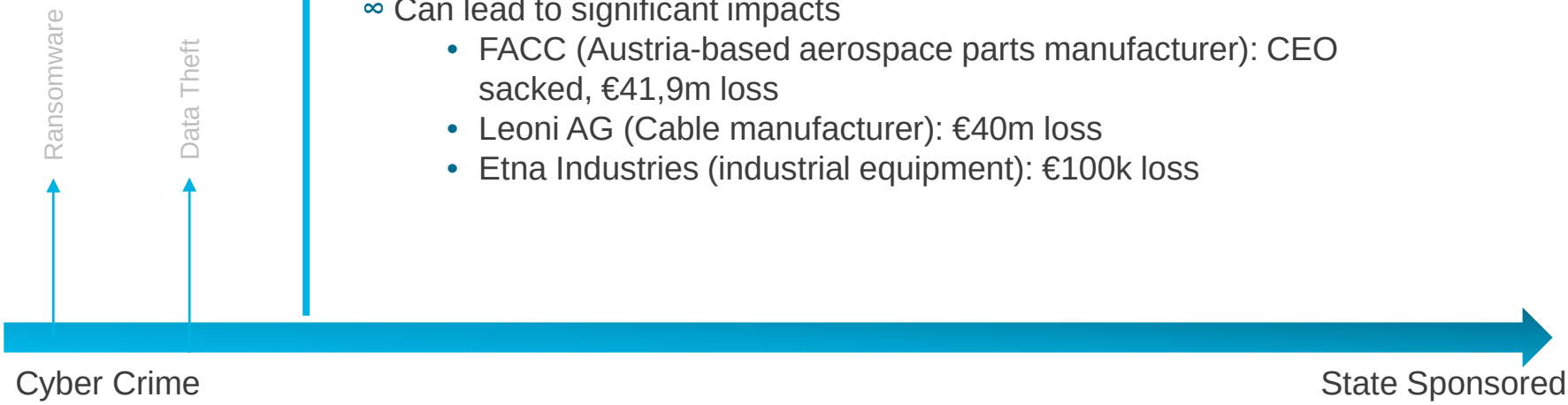
In the last 18 months, all types of cyber threats have significantly increased

“Fake CEO” fraud ***(Is it really a cyber threat ?)***

Scope: Untargeted but very specific
Motive: Money

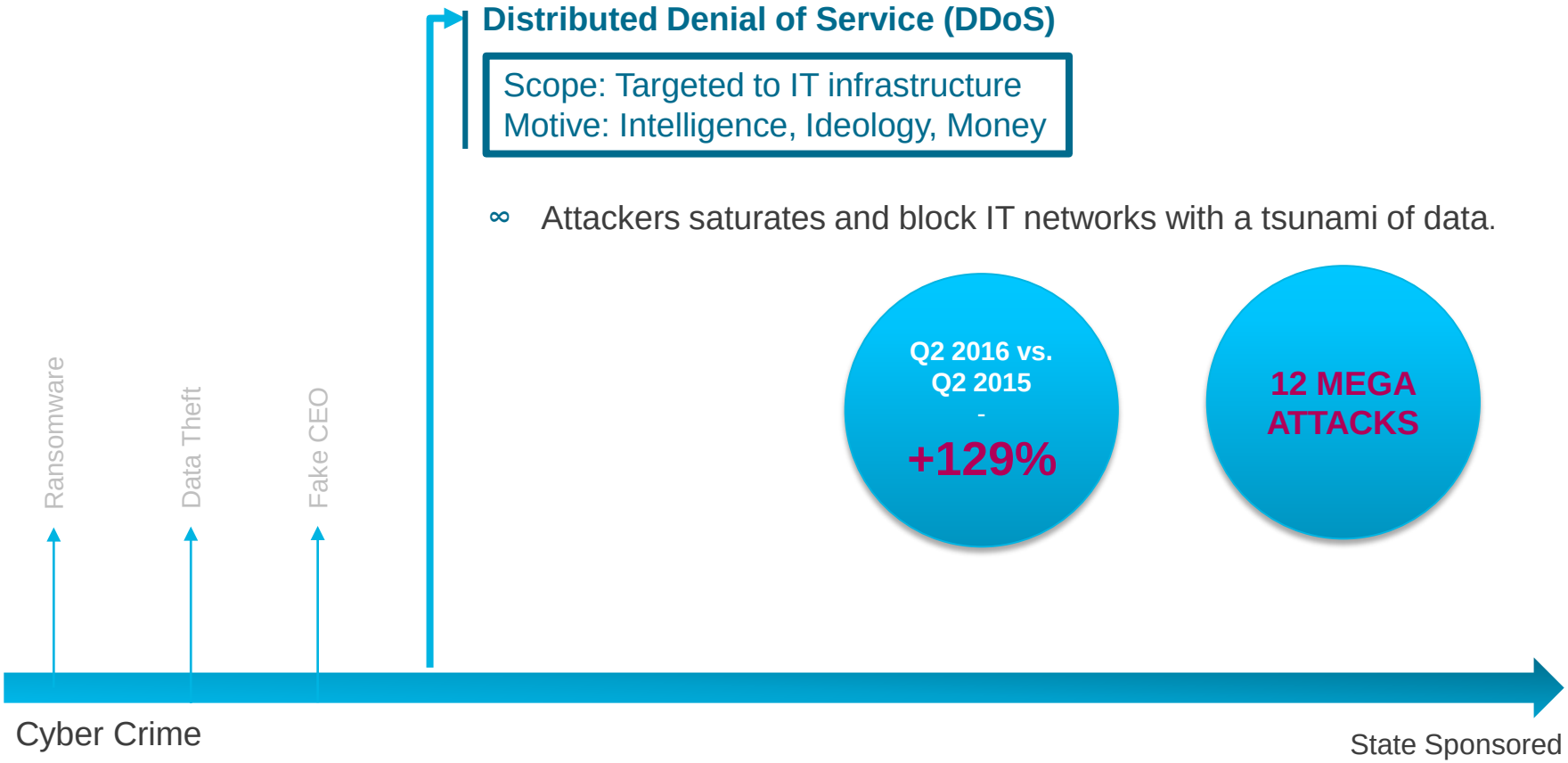
∞ Attackers impersonate the CEO to manipulate employees into transferring funds

∞ Can lead to significant impacts
- FACC (Austria-based aerospace parts manufacturer): CEO sacked, €41,9m loss
- Leoni AG (Cable manufacturer): €40m loss
- Etna Industries (industrial equipment): €100k loss



Cyber Threats: Panorama & Trends

In the last 18 months, all types of cyber threats have significantly increased



Cyber Threats: Panorama & Trends

In the last 18 months, all types of cyber threats have significantly increased

micros

Attacks against Core IT Components

Scope: Very Targeted
Motive: Intelligence, Money

- Attackers focus on key IT infrastructures that are common to a given business sector or type of industry
- Maximize effects by leveraging the systemic aspects of IT (standardization, solutions deployed globally)
- SWIFT Network
- Oracle Point-of-Sale
- CISCO routers and Firewalls

} Product manipulation

Cyber Crime — State Sponsored

SCOR The Art & Science of Risk | P&C

Cyber Threats: Panorama & Trends

In the last 18 months, all types of cyber threats have significantly increased

Over the past year or two, someone has been probing the defenses of the companies that run critical pieces of the Internet. These probes take the form of **precisely calibrated attacks designed to determine exactly how well these companies can defend themselves, and what would be required to take them down**.

Bruce Schneier – Sept. 13th, 2016

Attacks against Critical Infrastructures

Scope: Very Targeted
Motive: Warlike operations, Intelligence

- Attackers use cyber weapons to disrupt critical infrastructures and/or showcase their cyber war capabilities
  - Iran – 2012: Stuxnet against the Iranian nuclear program
  - Saudi Arabia – 2013: Cyber attack against Aramco
  - Germany – Dec. 2014: Steel factory disrupted
  - Ukraine – Dec. 2015: Electric grid switched-off
  - "**Someone Is Learning How to Take Down the Internet**" – Bruce Schneier

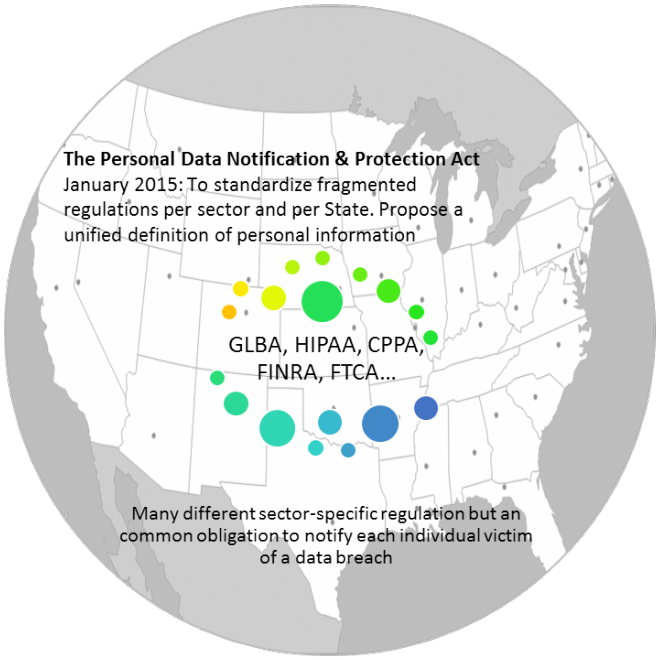
Cyber Crime → State Sponsored

SCOR The Art & Science of Risk | P&C

Cyber Threats: Panorama & Trends

In the last 18 months, Cyber Regulations have evolved, paving the way to improved cybersecurity

USA



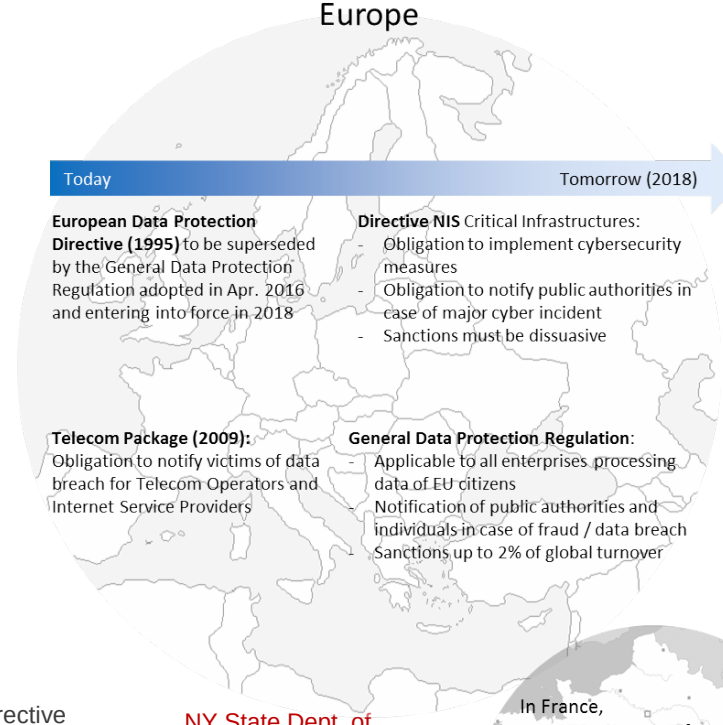
The Personal Data Notification & Protection Act
January 2015: To standardize fragmented regulations per sector and per State. Propose a unified definition of personal information

GLBA, HIPAA, CPPA, FINRA, FTCA…

Many different sector-specific regulation but an common obligation to notify each individual victim of a data breach

Safe Harbor – Cancelled in Oct. 2015 - Replaced by the Security Shield in Jul. 2016

Europe



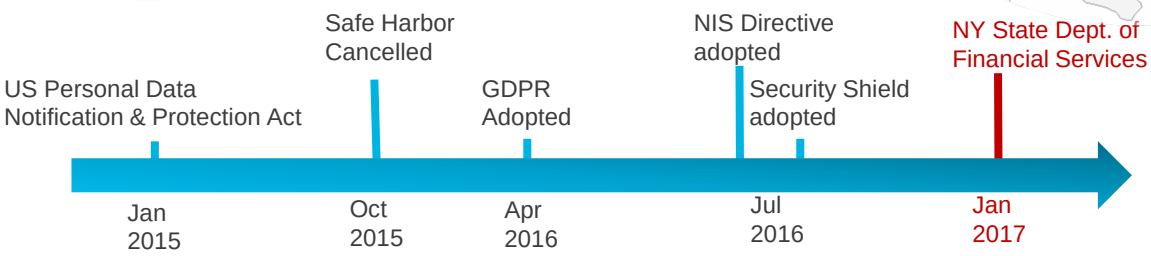
Today → Tomorrow (2018)

European Data Protection Directive (1995) to be superseded by the General Data Protection Regulation adopted in Apr. 2016 and entering into force in 2018

Directive NIS Critical Infrastructures:
- Obligation to implement cybersecurity measures
- Obligation to notify public authorities in case of major cyber incident
- Sanctions must be dissuasive

Telecom Package (2009):
Obligation to notify victims of data breach for Telecom Operators and Internet Service Providers

General Data Protection Regulation:
- Applicable to all enterprises processing data of EU citizens
- Notification of public authorities and individuals in case of fraud / data breach
- Sanctions up to 2% of global turnover



In France,
- 1978 – Act on information technology, data files and civil liberties
- EU Directive are applicable in French legal environment
- 2013 Military Programming Law is very similar to the NIS Directive

France

SCOR The Art & Science of Risk | P&C

AGENDA

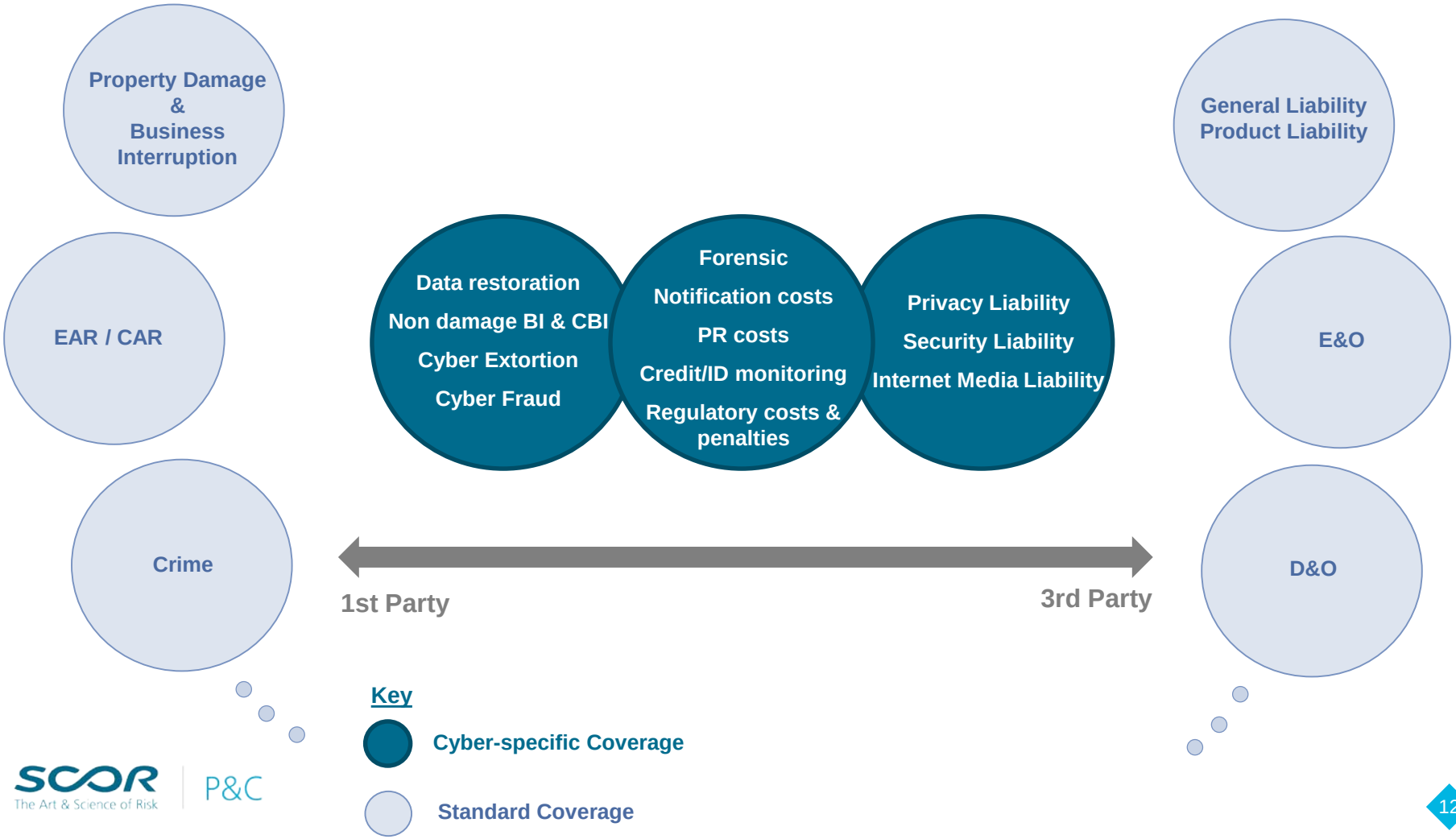
1 Cyber Threats: Panorama & Trends

2 **Cyber Insurance products**

3 Market Figures & Perspectives

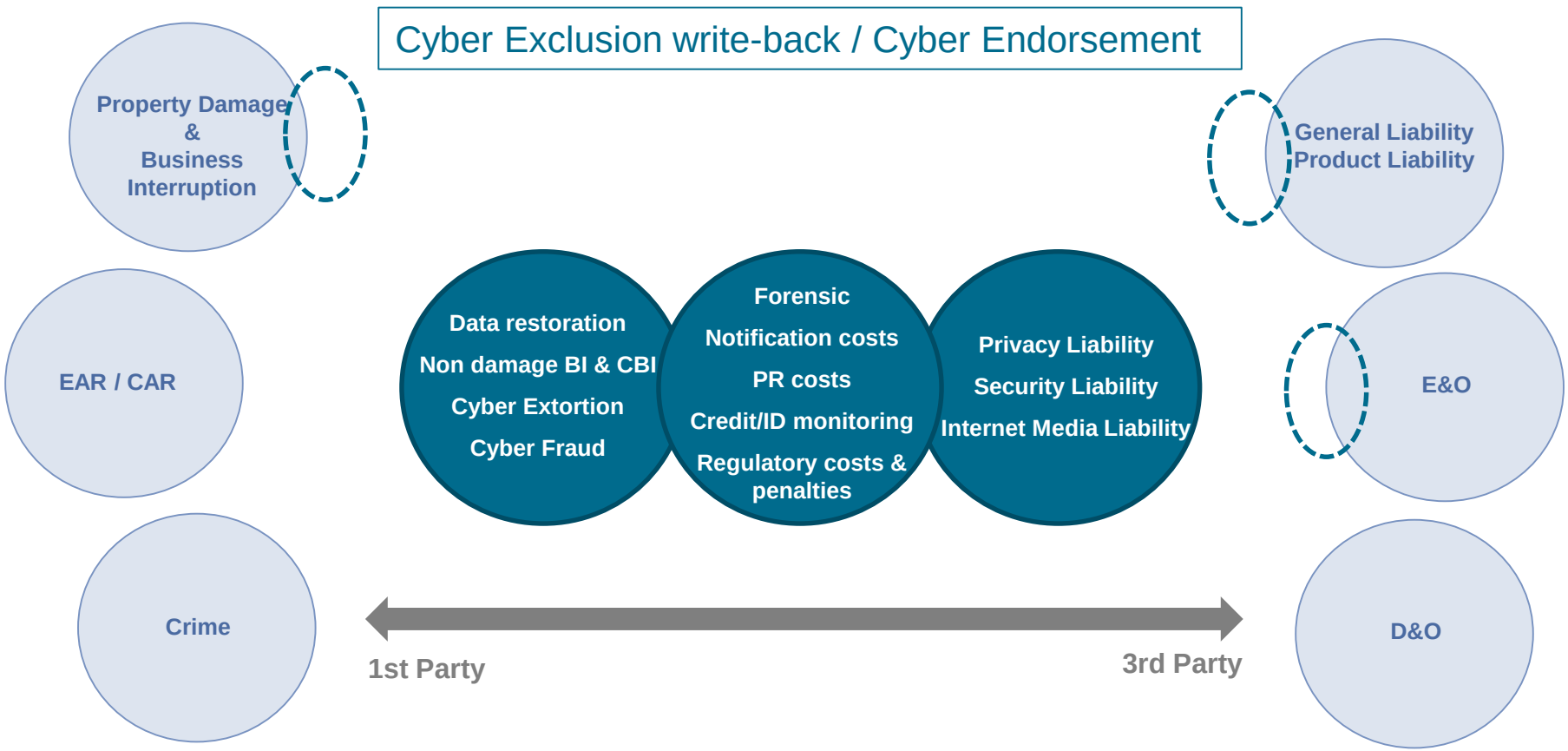
Cyber Insurance Products (1)

A Wide Range of Coverages possibly responding to Cyber Events



Cyber Insurance Products (2)

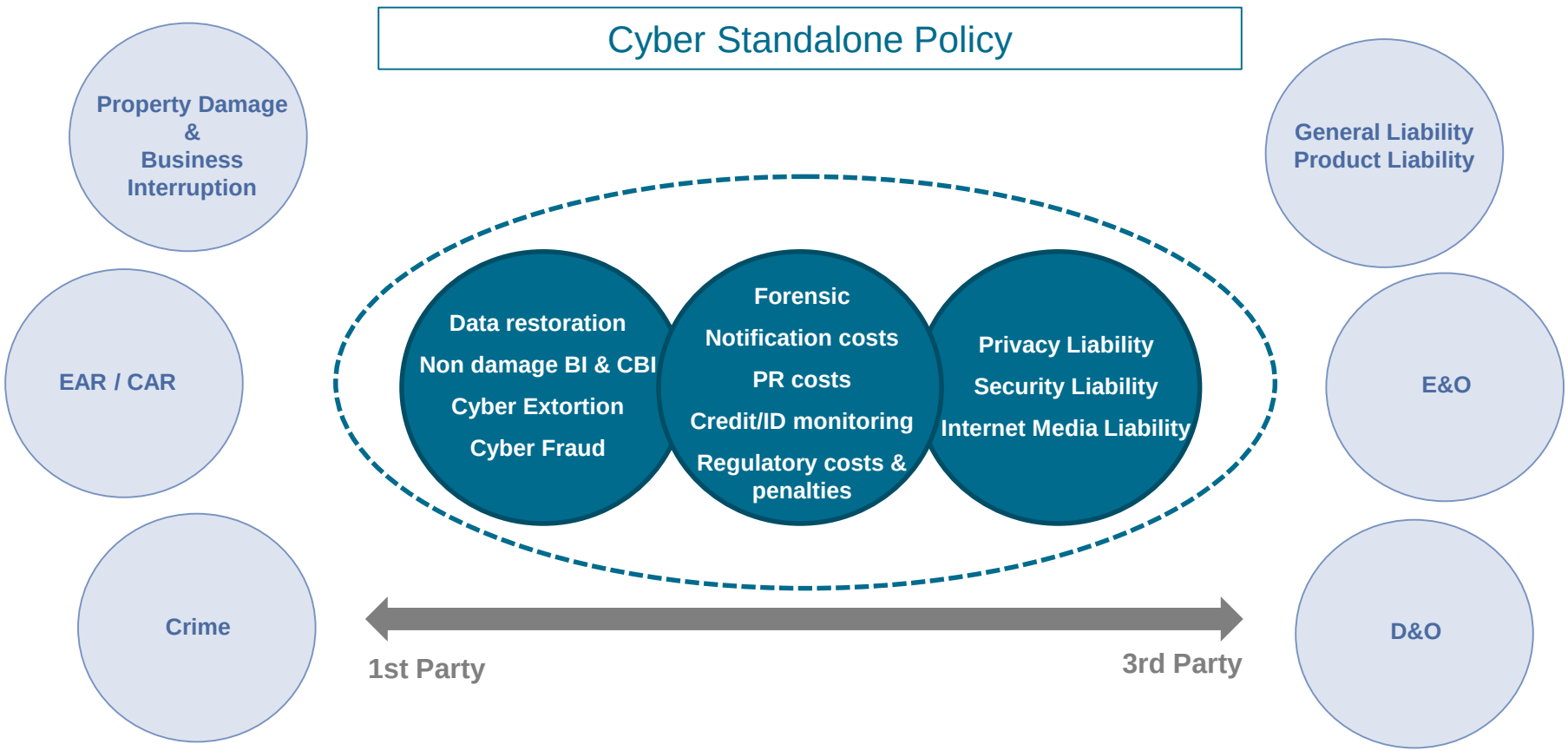
A Great Diversity of Cyber cover purchase:



SCOR The Art & Science of Risk | P&C

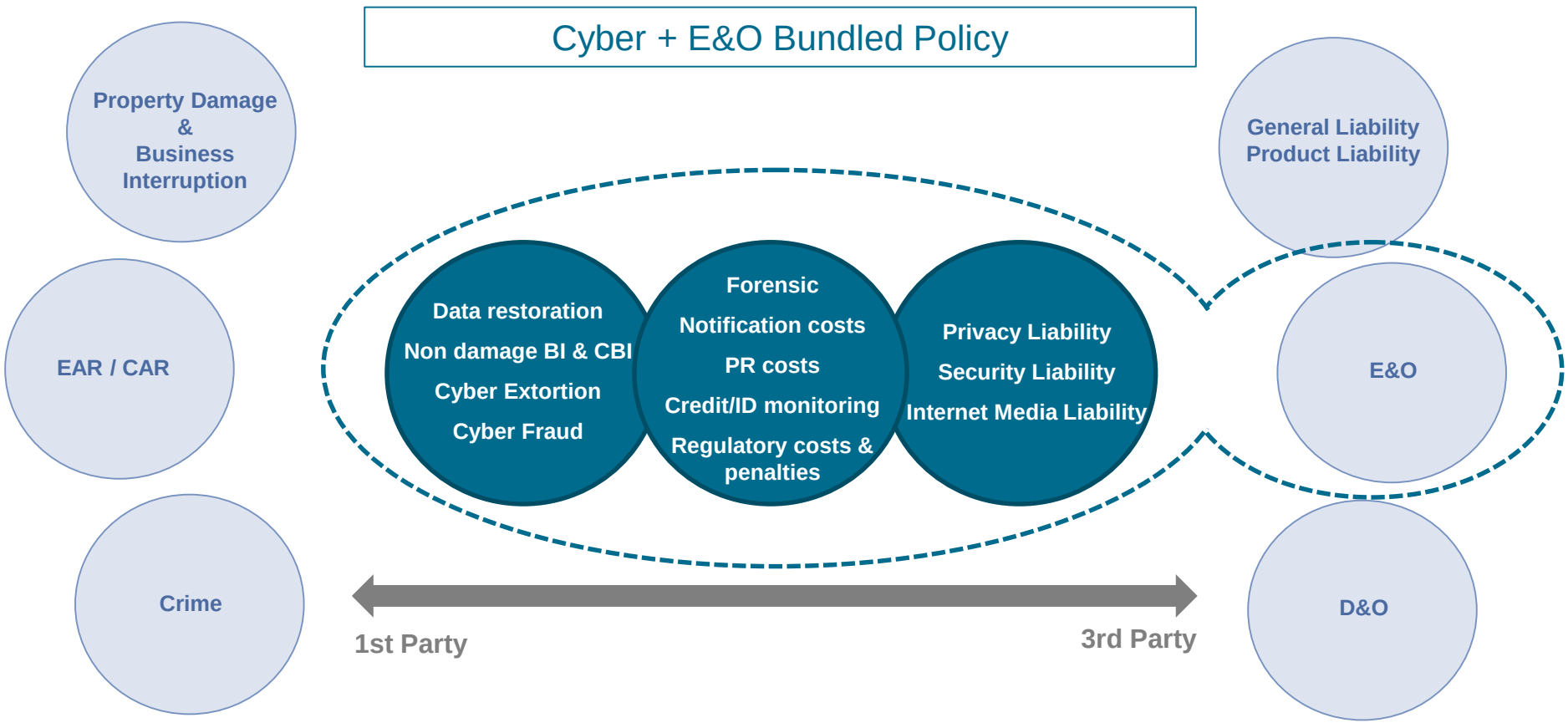
Cyber Insurance Products (3)

A Great Diversity of Cyber cover purchase:



Cyber Insurance Products (4)

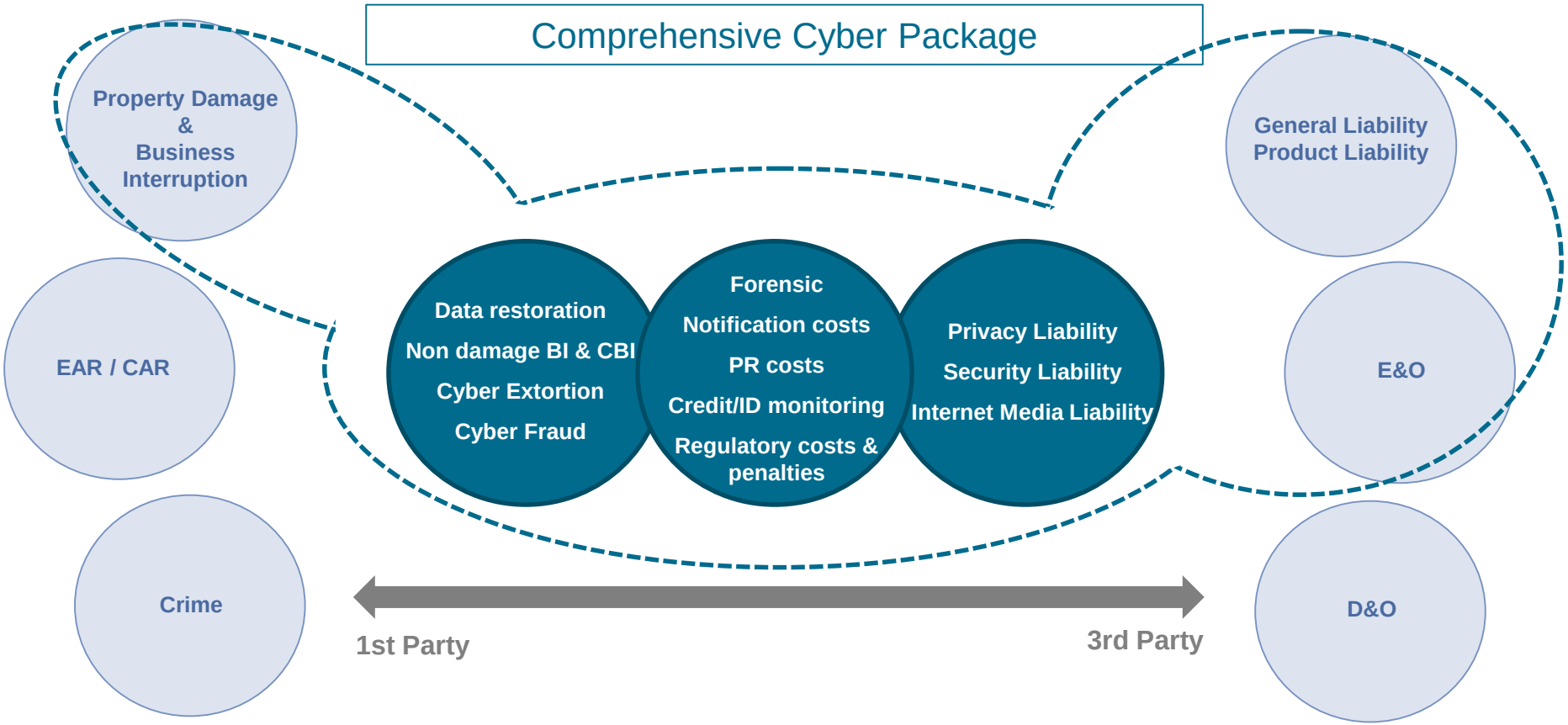
A Great Diversity of Cyber cover purchase:



SCOR The Art & Science of Risk | P&C

Cyber Insurance Product (5)

A Great Diversity of Cyber cover purchase:



What's unique with Cyber Insurance ?

Cyber coverages are not so New

They exhibit similarities with existing coverages:

Cyber Coverages	Standard coverages
Data loss notification & Event Management costs	Product Recall
Cyber Extortion	Kidnap & Ransom
Computer Fraud	Crime
Business/Process Disruption	Business Interruption
Data Restoration costs	Property Damage
Privacy / Security Liability	E&O

But Cyber Perils raise new challenges

- Intangible assets:
  - How to insure them ?
  - How to value data ?
  - Is loss of reputation insurable ?
- Non-physical losses:
  - How to adjust a Business interruption loss without physical damage ?
- Dynamics of the threat landscape:
  - How to cope with and model fast growing and fast changing nature of perils ?
- Systemic Risk:
  - How to manage risk accumulation due to common vulnerabilities or cascading effects (core provider failure) ?
- Pervasive technology:
  - With connected objects, Cyber risk is now entering the physical world: Are standard policies (Property, Liability) ready to respond ?

AGENDA

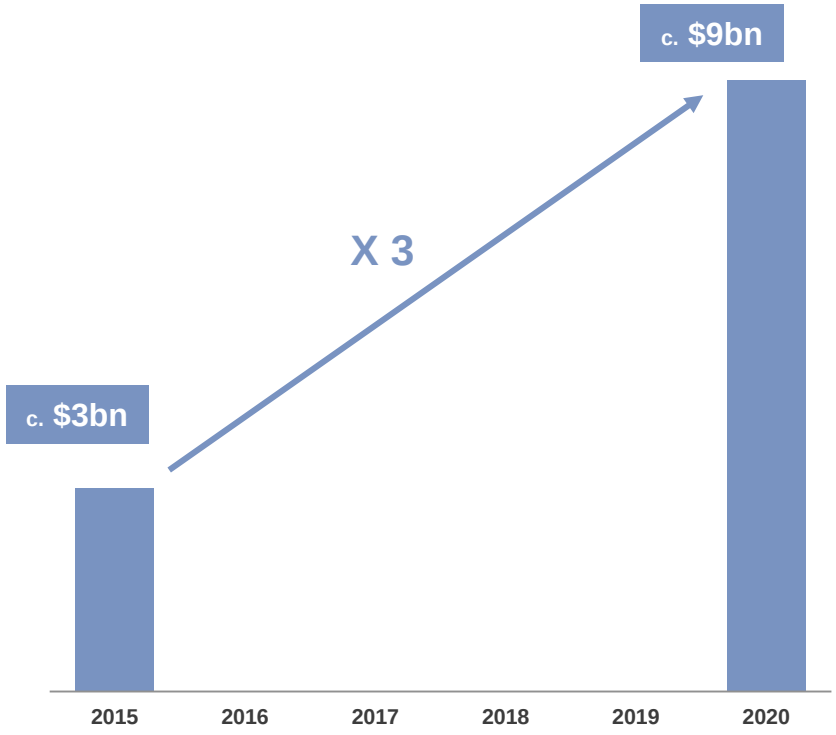
1 Cyber Threats: Panorama & Trends

2 Cyber Insurance products

3 **Market Figures & Perspectives**

Promising Outlook for the Cyber insurance market

Premium volume
Standalone Cyber + bundled products



Premium split in 2015

Key Facts [1]

c.$500m	▪ Cyber insurance capacity available on the Market
$1.7bn	▪ c.$1.7bn of Cyber Standalone GWP written in 2015 ▪ Figure excludes Cyber coverage bundled with more traditional products (e.g. PI/ E&O)
90%	▪ c.90% of Cyber Standalone GWP is US business (c.$1.5bn) ▪ Europe / APAC account for the bulk of the remainder
$450m	▪ c.30% of US Cyber Standalone GWP (c.$450m) flows to Lloyd's of London
c.45%	▪ The top 3 Cyber carriers are estimated to have a 45% combined share of the US market

1) SCOR & Aon Inpoint

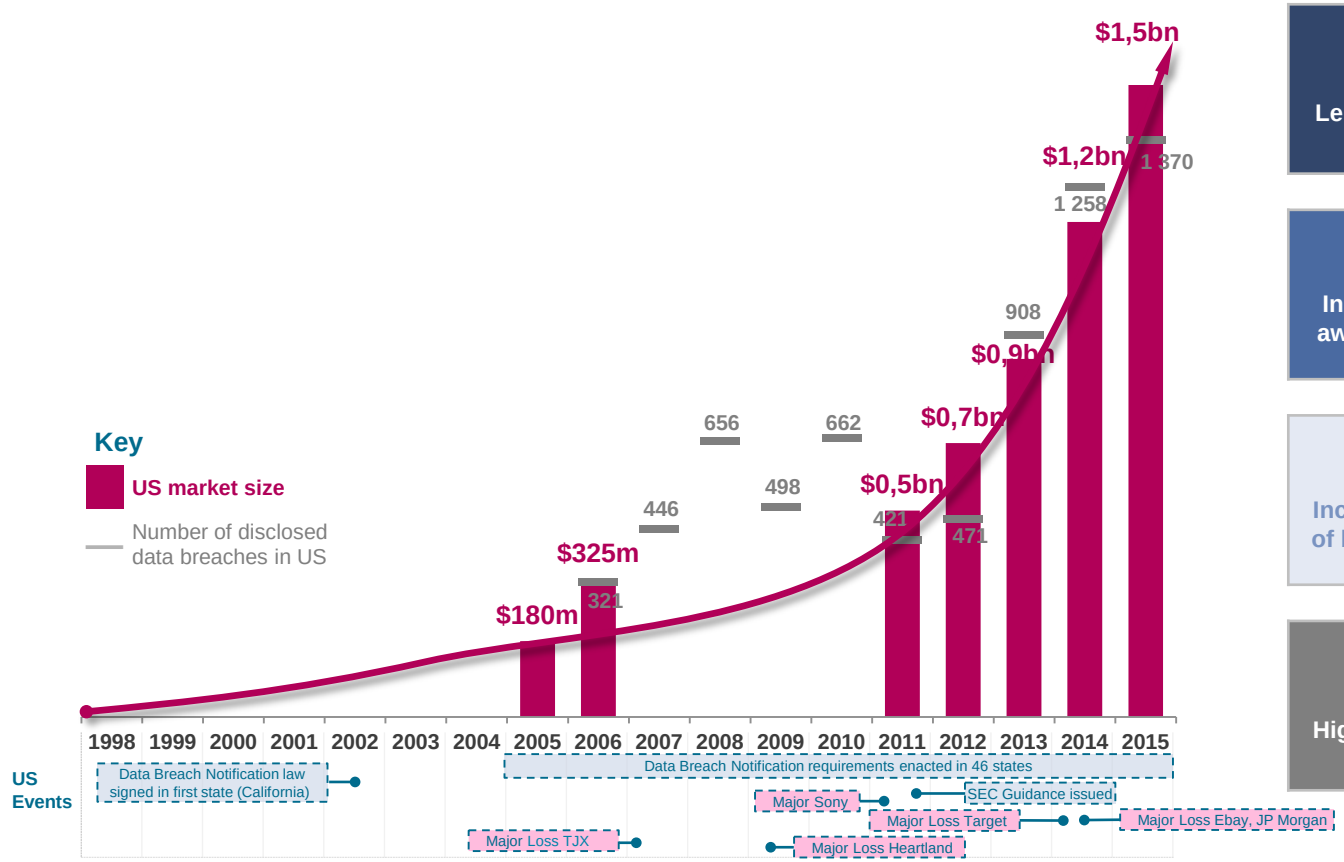
SCOR The Art & Science of Risk | P&C

Stricter legislation, highly publicised data breach incidents and increased awareness have driven strong demand for Cyber cover in the US

Historical estimated Cyber market size in US

(figures where available)

c.30% growth p.a. between 2011-15



Key Growth Drivers

Legislation

Laws in 47 States

Legislation has been enacted in 47 states, as a result firms are obligated by law to notify affected parties in the event of a data breach

Increased awareness

5th biggest risk

Cyber is now on the C-Suite agenda, US firms ranked Cyber as their 5th biggest risk compared to 18th just four years before[1]

Increased # of breaches

Breaches up 425%

More companies are uncovering data breaches, reported breaches in the US have risen by c.425% since 2006[2]

Higher cost

Costs up 60%

Breaches are getting more costly, The cost of data breaches are 60% higher per capita than they were in 2006[3]

Source: Aon Inpoint

Source: Betterley Report, Advisen, PropertyCasualty360, Business Insider, Marsh, Aon, datalossdb.org, Identity Theft Resource Center, NCSL, Ponemon Instituite, 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

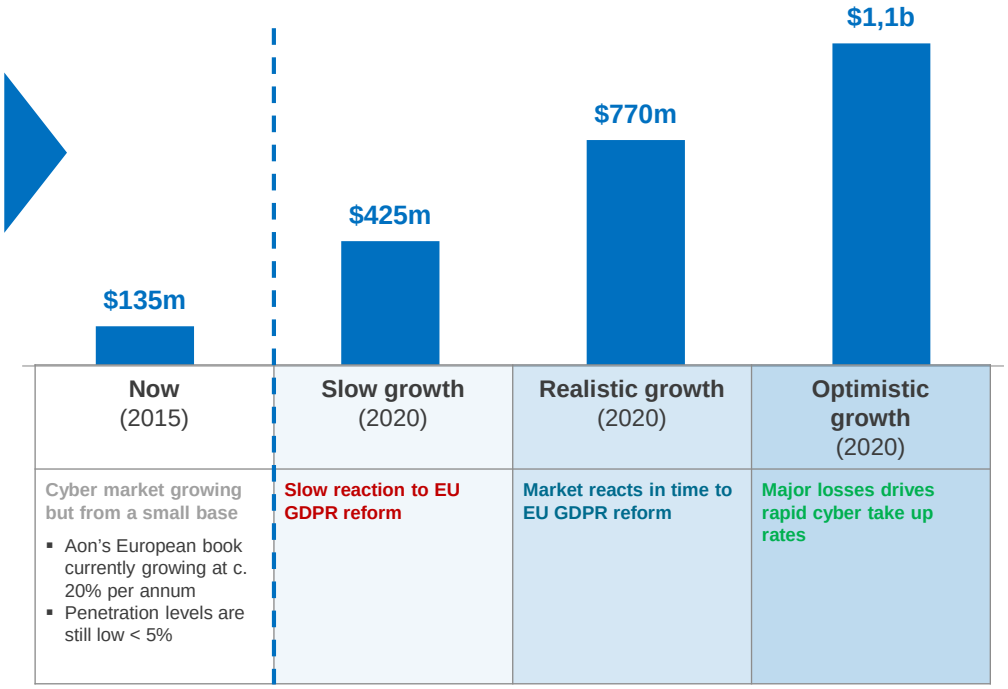
SCOR The Art & Science of Risk | P&C

Upcoming GDPR regulation is expected to be a catalyst for accelerated growth of Cyber in Europe

2018 - GDPR Implemented

Key growth drivers	Pre GDPR	Post GDPR
Legislation	• No general legislation mandating notification following a breach[1] • Weak regulators with limited ability to sanction firms • EU laws enforced with varying degrees of severity	• Strict regulation with a general requirement to notify in the event of a breach • GDPR regulations allow for a fine of up to 2% of global turnover • EU wide enforcement of GDPR
Awareness	• Cyber already recognised as an emerging risk in Europe • Aon clients currently view Cyber as 14th biggest risk	• Increased awareness expected to be driven by GDPR with higher numbers of data breaches likely to be publicised • Aon clients already expect Cyber to be their 8th biggest risk by 2018
Breach numbers	• European breach rates are already growing fast, 36% since 2011[2]	• Mandatory notification is likely to drive known breach numbers much higher • In the US where similar legislation already exists there were 1.1k (c.85%) more publicised breaches compared to Europe in 2015
Costs	• The cost of data breaches in Europe currently lags that of the US by 35% on average	• European firms are likely to suffer higher costs as a result of GDPR • US firms have seen the cost of data breaches rise at a rate of 9% a year since 2012

Cyber Market Growth estimates:



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

Notes: 1. Aon Global Risk Survey
2. The Breach Level Index
3. IBM

Source: Aon Inpoint

The Global Cyber Reinsurance market is estimated to be worth c.$525m in premium, the majority of which is placed on a Quota Share basis with a few reinsurers

Assessment of Cyber Reinsurance Market Key facts

$525m

- The global Reinsurance market is estimated to be worth c.$525m

c.95%

- Approximately 95% of reinsurance premiums are written by reinsurers on a Quota Share basis

New Market

- A large portion of standalone Cyber business would still be reinsured within traditional financial lines treaties
- Most reinsurers have only just started playing in the market

Issues

- The market faces two major challenges
  - need to develop modelling capabilities to get a better understanding of aggregate exposure
  - lack of underwriting talent with expertise required to develop and make the market

Source: Aon Grip Data, Company websites, Insurance day, Insurance insider, Aon Practitioner Insight

Cyber market insights

- While most business is US domiciled a large proportion of risks are reinsured outside of the US
- Cedents remain cautious about holding Cyber risk on their balance sheets, many are concerned by silent Cyber aggregates
- Reinsurers, like cedents, remain cautious on writing Cyber and are unwilling to take large lines
- Often require to have occurrence or loss cap on QS

Source: Aon Inpoint

Key Take-aways

1. Cyber Threat landscape is undergoing tremendous changes in nature, frequency and size of risks

2. Insurance client base is expanding with cover demand evolving from « data breach » to more comprehensive 1st and 3rd party cover

3. Incursion of IT into « real world » increases exposure to Physical loss, blurring lines between Cyber coverages and Standard ones

4. While Market outlook is promising, Cyber science has to infuse in the (Re)insurance industry to really apprehend Cyber Perils and overcome hurdles to market development