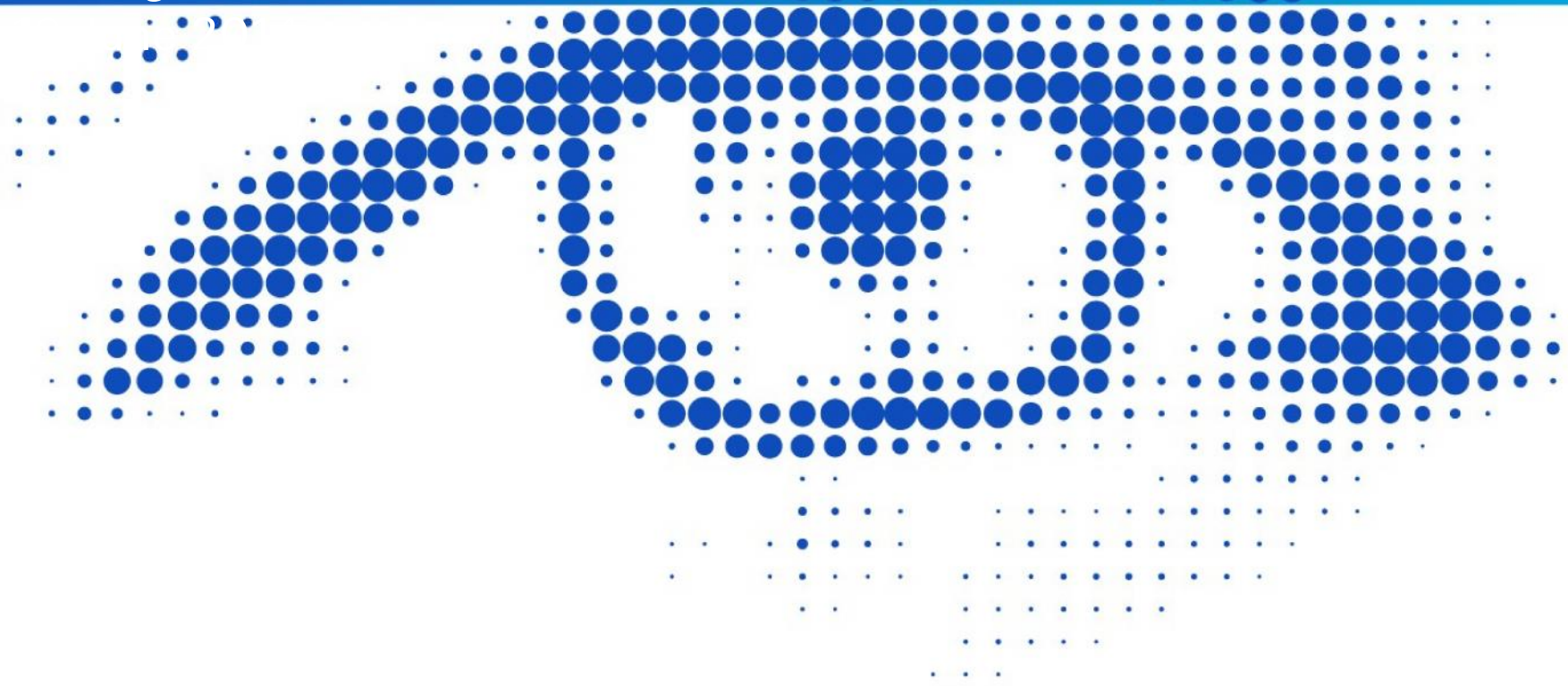
Swiss Re

Lost in Cyber Space? Cyber Risks and (Re-) Insurance

PIU - 10 June 2014

Constanze Brand, Swiss Re Europe S.A.,
New challenges and innovations in reinsurance



Lost in Cyber Space?
Cyber Risks and (Re-) Insurance

Topics
What is Cyber Risk?
Regulatory Environment USA & Europe
Cyber Products
Underwriting and Swiss Re´s Position
Outlook and Trends

Cyber Risk ...the growing awareness

- Greater use of e-commerce and the growth of the internet has led to developing liabilities.
- Greater awareness by individuals of the value of the identity to criminals.
- Greater involvement by regulatory bodies such as the Federal Trade Commission (FTC) and the European Union Commission.

This has led to greater legislation which is continue to broaden in scope and sanctions in future

Cyber Risk.... what is this?

Cyber Risk.... what is this?

"Cyber risk" means any risk emanating from the use of electronic data and its transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud committed by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information - be it related to individuals, companies, or governments.

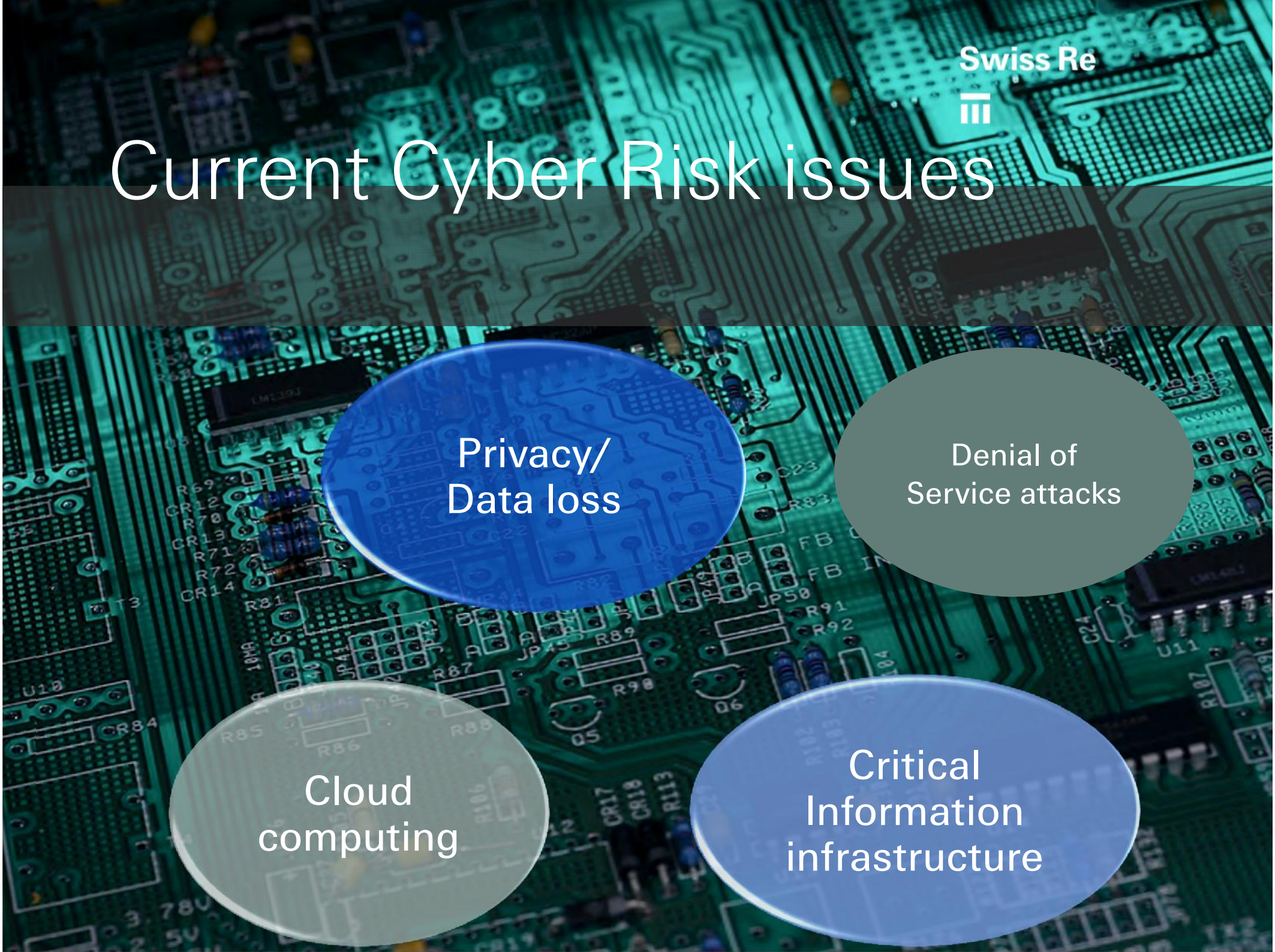
"Cyber Risk Insurance" addresses the first and third party risks associated with e-business, the Internet, networks and informational assets.

Note on this definition:

This definition is not intended to be used in wording or contractual documents. Its intention is merely to set the cyber topic into a consistent context be it from a regulatory, underwriting, or client management perspective. In particular, we consider cyber risk to also encompass material / physical damage. which is often provided in traditional coverages, as well as damage to (intangible) electronic data and liabilities arising therefrom, which is often only available through a specific policy.

Swiss Re

Current Cyber Risk issues



Threats & Loss Scenarios – a few examples

External data breach

TJ Maxx: Hacking of Wi-Fi network and link into the central database obtaining 95 million credit card numbers with total incurred costs over five years of $160 Mio as e.g. notification costs, forensic costs, credit monitoring costs and liability claims from banks,

Internal malicious breaches

Financial records of 680.000 Bank of America costumers were stolen by a disgruntled employee

Distributed Denial of Service (DoS) Attack

A DoS attack brought down the ticketing and sales platform of an air line for 24 hours. As a consequence they suffered significant loss of revenue, increased costs of working hours interruption (loss of revenue)

Password Theft

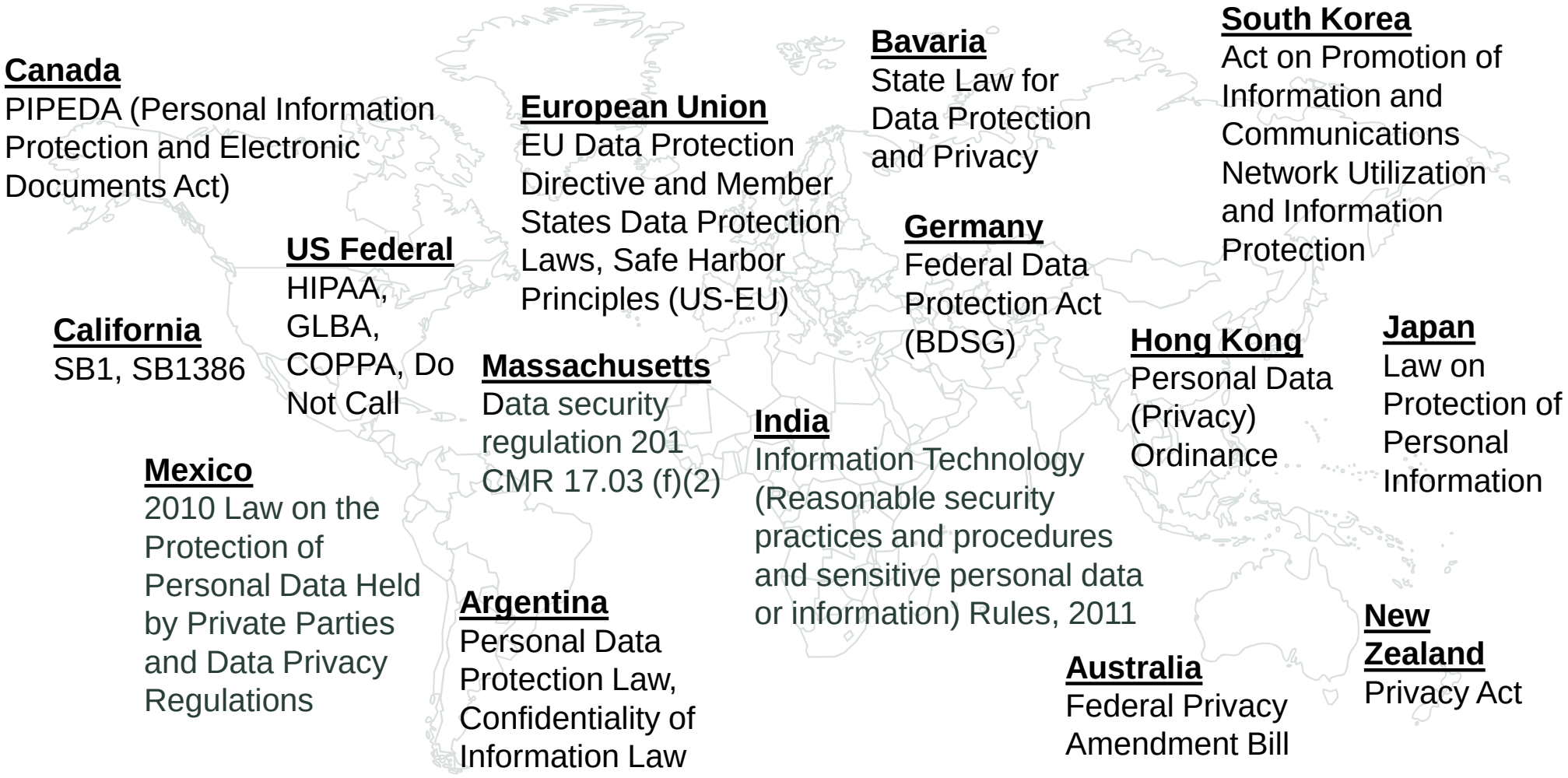
Linkedin password data base has been compromised with more than 6 million user´s details posted online. The social network is examining by security analysts that millions of encrypted passwords have been published on Russian hacker´s website

Critical infrastructure

The slammer worm got onto the controlling network of nuclear station in the US (2003) and blocked the digital controlling system. The controlling system was out of action for almost five hours. Damage was only avoided due to the existence of an analogue backup system.

Regulatory Environment USA & Europe

Complexity of data protection laws



Canada
PIPEDA (Personal Information Protection and Electronic Documents Act)

US Federal
HIPAA, GLBA, COPPA, Do Not Call

California
SB1, SB1386

European Union
EU Data Protection Directive and Member States Data Protection Laws, Safe Harbor Principles (US-EU)

Massachusetts
Data security regulation 201 CMR 17.03 (f)(2)

Mexico
2010 Law on the Protection of Personal Data Held by Private Parties and Data Privacy Regulations

Argentina
Personal Data Protection Law, Confidentiality of Information Law

Bavaria
State Law for Data Protection and Privacy

Germany
Federal Data Protection Act (BDSG)

India
Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

South Korea
Act on Promotion of Information and Communications Network Utilization and Information Protection

Hong Kong
Personal Data (Privacy) Ordinance

Japan
Law on Protection of Personal Information

Australia
Federal Privacy Amendment Bill

New Zealand
Privacy Act

Key Takeaways on the Legislative response US & EU

- The current EU legislation is an attempt to prevent a data breach. But it does not consider sufficiently some important aspects like globalization and technical developments like social networks and cloud computing, and the notification requirements and ability to take private actions is limited
- The American legislation is largely reactive with some ability to take private actions.
- Fines and Penalties – large fines in the US and recent increase in fines in Europe (the UK has increased it to GBP 500 000 and in Europe € 1 million).

Regulatory trends USA & Europe

USA:

- Duty to notify broadly established boosted market in the last 10 years.
- Issues around treatment of critical infrastructure, information sharing, improving risk management with SME are being addressed among other topics

Europe

- Risk awareness is increasing, driven by new EU Regulation and compliance Cyber Security Directive expected to come into force between 2014-2016 (next slide focuses on this legislation development)

Regulatory Trends – Europe (continued)

- The European Commission plans to unify data protection within the European Union (EU) with a single law, the **General Data Protection Regulation (GDPR)**.
- A proposal for a regulation was released on 25th of January, 2012. The EU´s European Council aims for adoption in late 2014 and the regulation is presently planned to take effect after a transition period of 2 years.
- Foreseen provisions of the proposed new EU data protection regime:
  - extends the scope of the EU data protection law to all foreign companies processing data of EU residents (so it will apply to organizations based outside the European Union if they process personal data of EU residents).
  - provides for a harmonization of the data protection regulations throughout the EU, thereby making it easier for non-European companies to comply with these regulations; however, this comes at the cost of a strict data protection compliance regime with severe penalties of up to 5 % of worldwide turnover, among other restrictions
  - increases responsibility and accountability for those processing personal data: for example, companies and organizations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible, within 24 hours).

Cyber Products

What is Cyber Insurance ?

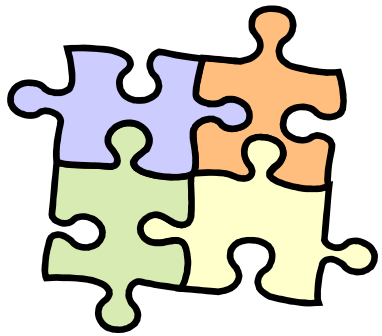
- At first insurers developed "Technology E&O" policies for e-commerce companies and technology providers that support e-commerce, such as internet service providers, technology consultants, and software developers.
- It is difficult to separate Technology E&O insurance from Cyber risk Insurance; for many insurers, the same base product is used, then adapted to fit the technology service provider insured or the Cyber risk insured.

Differentiation:

- As loss/damage linked to Technology Products and Services is main exposure, Technology Providers will purchase Tech E&O, ISBI, Multi-line packages

- As loss/damage linked to their use of IT Infrastructure is incidental to their core activities, Non-Tech companies will purchase Cyber products (mono-line or multi-line)

Standard Products and Cyber Insurance



Policy

GL polices	Tech, Media & Telecom (E&O)		Cyber		
Advertisement Personal Injury	**IP Infringement**	**Errors & Omissions**	**Business interruption and data restoration**	**Extortion**	**Privacy**
Libel	Copyright	Tech Services	Unauthorized Access	Investigation costs	Unintentional Disclosure
Slander	Trademark	Tech Products	Hacking	Extortion moneys due to a credible threat, e.g. to introduce Malicious Code	Breach of Confidentiality
Defamation	Patent *		Denial of Service		
			Virus		

* excluded from standard product

Traditional existing standard products

Liability	**Errors and Omissions (E&O) Technology**
Coverage	➢ Negligent errors acts or omission of the Insured in the provision of Technology Services and/or Products ➢ Unintentional Breach of Contract ➢ Intellectual Property Infringement (e.g. copyrights, trademarks..) BUT: Swiss Re does not insure patent infringement ! ➢ Coverage as an annex : Breach of any duty of confidentiality, invasion of privacy or violation of any other legal protections for personal information.
Liability	**Advertisement Personal Injury**
Coverage	➢ Coverage for negligence arising from libel, slander or defamation (e.g. publishers) ➢ Most personal liability coverage via householders policy and home insurance

Coverage overview under existing policies

- Property:

  Courts have consistently held that data isn't "property" – "direct physical loss" requirement not satisfied, however
  - Cost for reinstatement of data which is lost or destroyed due to physical damage can be covered under conventional Property and Engineering covers
  - Cost for reinstatement of data and BI losses which incur due to non-physical damage (virus, hacker attacks etc.) are offered as special covers only;
    No coverage e.g. for value of intellectual property, BI loss due to design errors of non-tested programmes

Coverage overview under existing policies (2)

- Error & Omissions (E&O):
  E&O wordings are tied to professional services and often to the requirement of negligence
- Commercial General Liability (CGL):
  Coverage for bodily injury and tangible property
  Advertising Injury/Personal Injury (AI/PI) section has potential exclusions / limitations in the area of web advertising
- Crime:
  Only coverage for covers money, securities and tangible property; Intent required
- Kidnap and Ransom (K&R):
  Special amendment for "cyber-extortion" required
- Since 2005 the privacy liability market has been developing to meet this gap in coverage

→ Traditional policies may respond only partially to this developing area of liability

Cyber Risk Insurance - examples

Risks	Coverage	Traditional Policies	Cyber and Privacy Policy
Legal liability to others for privacy breaches	Privacy liability: harm suffered by others due to the disclosure of confidential information		
Legal liability to others for computer security breaches	Network security liability: harm suffered by others from a failure of your network security		
Regulatory actions	Legal defense for regulatory actions		
Identity theft	Expenses resulting from identity theft		
Privacy notification requirements	Cost to comply with privacy breach notification statues		
Loss or damage to data / information	Property loss: the value of data stolen, destroyed, or corrupted by a computer attack		
Extra expense to recover / respond to a computer attack	Cyber extortion: the cost of investigation and the extortion demand		
Loss of revenue due to a computer attack	Loss of revenue: business income that is interrupted by a computer attack		
Loss or damage to reputation			

= coverage provided = restrictive coverage may be provided = not covered

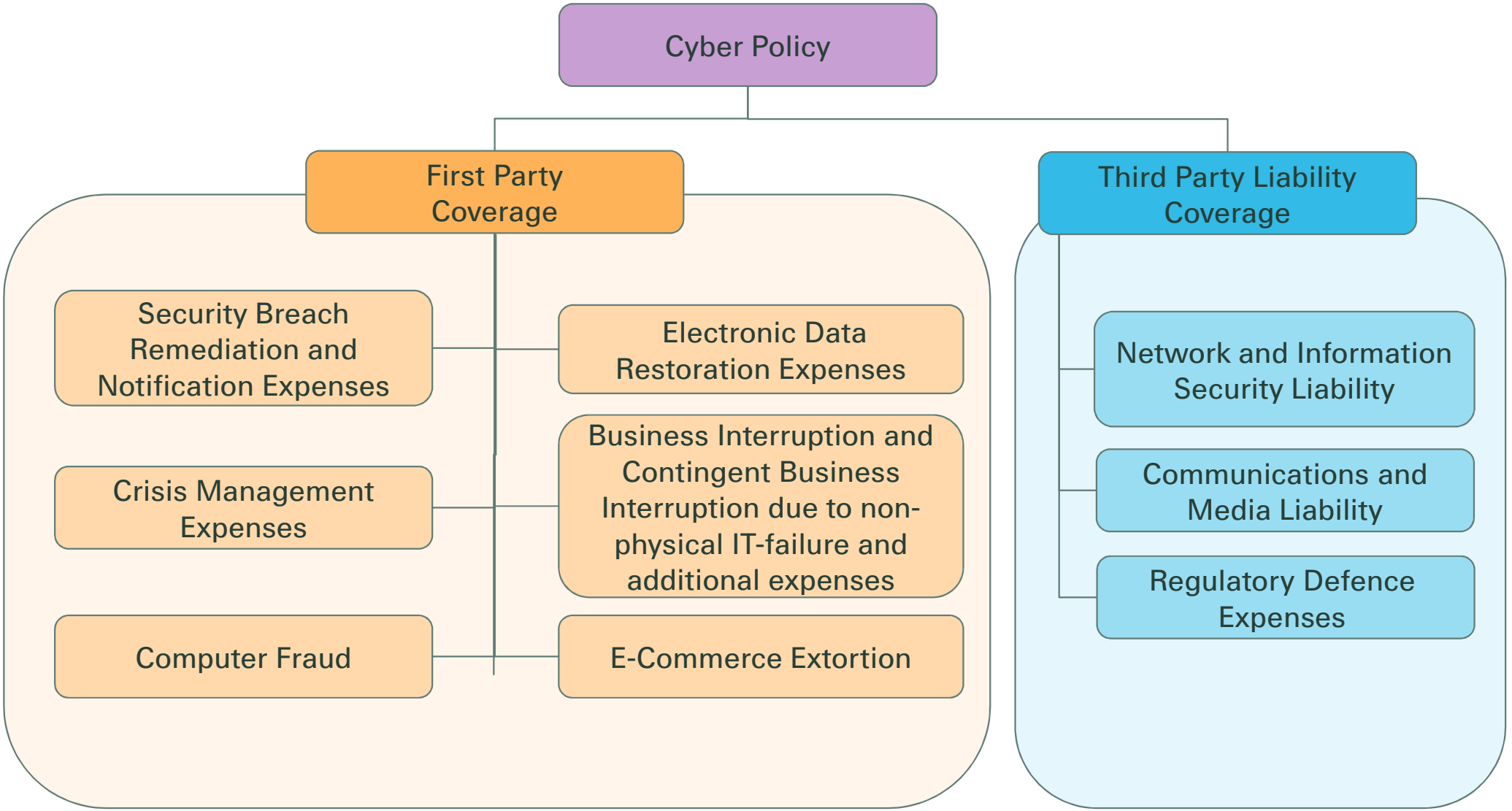
New Cyber Coverage:
First Party Cyber Coverage

First Party	**Non–physical IT Failure**
Coverage	➢ Business Interruption loss incl. malicious attack ➢ Contingent Business Interruption loss due to lack of IT or public services ➢ Costs for reinstatement of data ➢ Investigation cost to determine cause of security failure
First Party	**Cyber Extortion (Extension)**
Coverage	➢ Covers the funds paid by the assured as a result of a credible threat or series of relate threats directed at the Insured to introduce Malicious Code; corrupt, damage or destroy the Insured's computer system, or restrict or hinder access to the Insured's computer system; release, divulge, disseminate, destroy or use confidential information stored in the Insured's computer system

New Cyber Coverage:
Third Party Privacy Coverage

Liability	Privacy Liability for non-Technology Companies
Coverage	➢ **Liability :** the defence and settlement costs for the liability of the insured arising out of his failure to properly care for private data ➢ **Remediation:** The response costs following a data breach, including investigation. public relations, customer notification and credit monitoring. ➢ **Fines and/or penalties:** The costs to defend, settle fines and penalties that may be assessed by the regulator.

Summary : Coverage Structure for a cyber policy



Swiss Re´s view on market Cyber coverage

No coverage for

- Patent Infringement
- Value of data as e.g. intellectual property
- Value of reputation (e.g. drop in share price)
- Stand alone coverage for Extortion or Contingent Business Interruption
- Contractual Liability
- Fines and penalties unless following decisions by regulatory authorities
- Losses from untested or badly maintained software, wrong programme design

Standard Market Exclusions

- War/Terrorism
- Bodily Injury/Property Damage
- Anti Trust
- Patent Infringement
- RICO (Rackeeter Influenced and Corrupt Organization Act)
- Loss of use of property
- Service Interruptions
- Contractual Liability
- Breach of warranties / guarantees
- Pollution
- Nuclear Energy

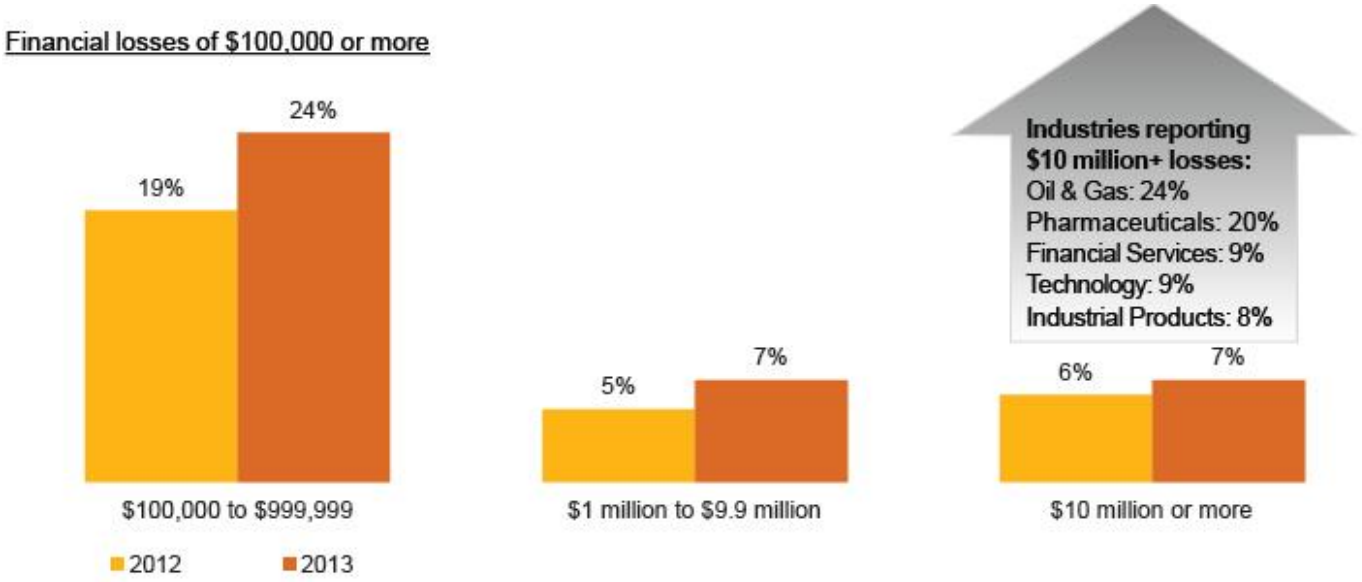
Swiss Re´s View on market Cyber coverage

- There is no worldwide uniformity in policy forms or coverage (though Claims Made or Claims Made reported trigger with Extended Reporting Period is a common feature)
- Coverage varies depending on a business's particular exposures
- Sub-limits (i.e. Remediation costs, Fines and Penalties – often coverage limited to defence costs) and monetary retention amount apply to Privacy coverage – Policy limit based on an annual aggregate limit (or combined single limit if multiline)
- Changes in regulation and technological evolution can quickly render policy wordings obsolete
- Case law influence => early 2014 ‚New York Trial Court Denies Coverage For Cyber Claims Under Commercial General Liability Policies (Sony case)

Claims ?

Cyber Loss Costs

- **PWC–Financial Services Global Info Security Report 2014**



- ❑ 169% increase in cyber incidents from 2012 to 2013
- ❑ 18% increase in average financial losses

- **Willis (Feb 2014)**

	2012	2013
Average records per breach	83,870	383,000
Total breaches	260m	822m

- ❑ No reduction in frequency or severity despite security and regulatory improvements

- ❖ **Main Targets**: Accommodation & Food Services (54%), Retail (20%), Financial Services (10%)
- ❖ Increase in attacks against **retailers (+100%), pharma, chemical, electronics, and mining (+600%)**

Cyber Insurance Claims

- NetDiligence – Cyber Liability & Data Breach Insurance Claims (2013)

	Median	Average
Total Claim Payment	$242k	$954k
Per Record cost	$107.14	$6,790
Per record cost excluding outliers	$97	$307
Crisis Services (forensics, notification, credit monitoring)	$209k	$737k
Legal Defence	$7.5k	$574k
TP Settlement	$22.5k	$258k

- ❑ Sample of 145 data breaches 2010-12
- ❑ 88 claims settled @ total $84m
- ❑ Median claim payments 25% increase
- ❑ Individual per record costs up to $251k.
- ❑ No correlation between number of records breached & total claim payment.
- ❑ Crisis Services = 50% claim payment. Legal defence = 35%. TP settlements = 13%
- ❑ Defence costs range up to 10m
- ❑ Settlement range up to 4m

Statistics

- **US** NetDiligence® 2013 **- study on insurance pay outs**
  - Most Frequent cause of loss: Lost/Stolen Laptop/Devices (20.7%) and Hackers (18.6%).
  - Most frequently breached sector: Healthcare (29.3%) and Financial Services (15.0%).
  - Median number of records lost:1,000. Average number of records lost: 2.3 million. Median cost per record: 97USD (excl. outliers). Not always correlation between #records and loss cost. www.NetDiligence.com
- **UK** Information **Security Breaches Survey** 2014, by Department for Business, Innovation and Skills together with PWC
  - Average cost of organizations' worst breach of the year: £65,000-£115,000 for small businesses and £600,000-£1,150,000 for large organizations.
  - Business disruption: 7-10 days /£40,000 to £70,000 for small businesses and 5-8 £350,000 to £650,000 days for large companies. www.gov.uk/government/uploads/system/uploads/attachment_data/file/307296/bis-14-767-information-security-breaches-survey-2014-technical-report-revision1.pdf
- **Hewlett-Packard** study
  - Ponemon Institute's 2013 *Cost of Cyber Crime study* finds the participating 60 US companies experienced more than 100 successful cyber attacks each year at an average cost of $11.6M, (between 1,3m to 58m USD) http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports

Statistics (2)

a couple of other reports

-
- **US Identity Theft Resource Center;**

  http://www.idtheftcenter.org/id-theft/data-breaches.html

- **Ernst & Young;** Cyber hacking and information security in mining 2013

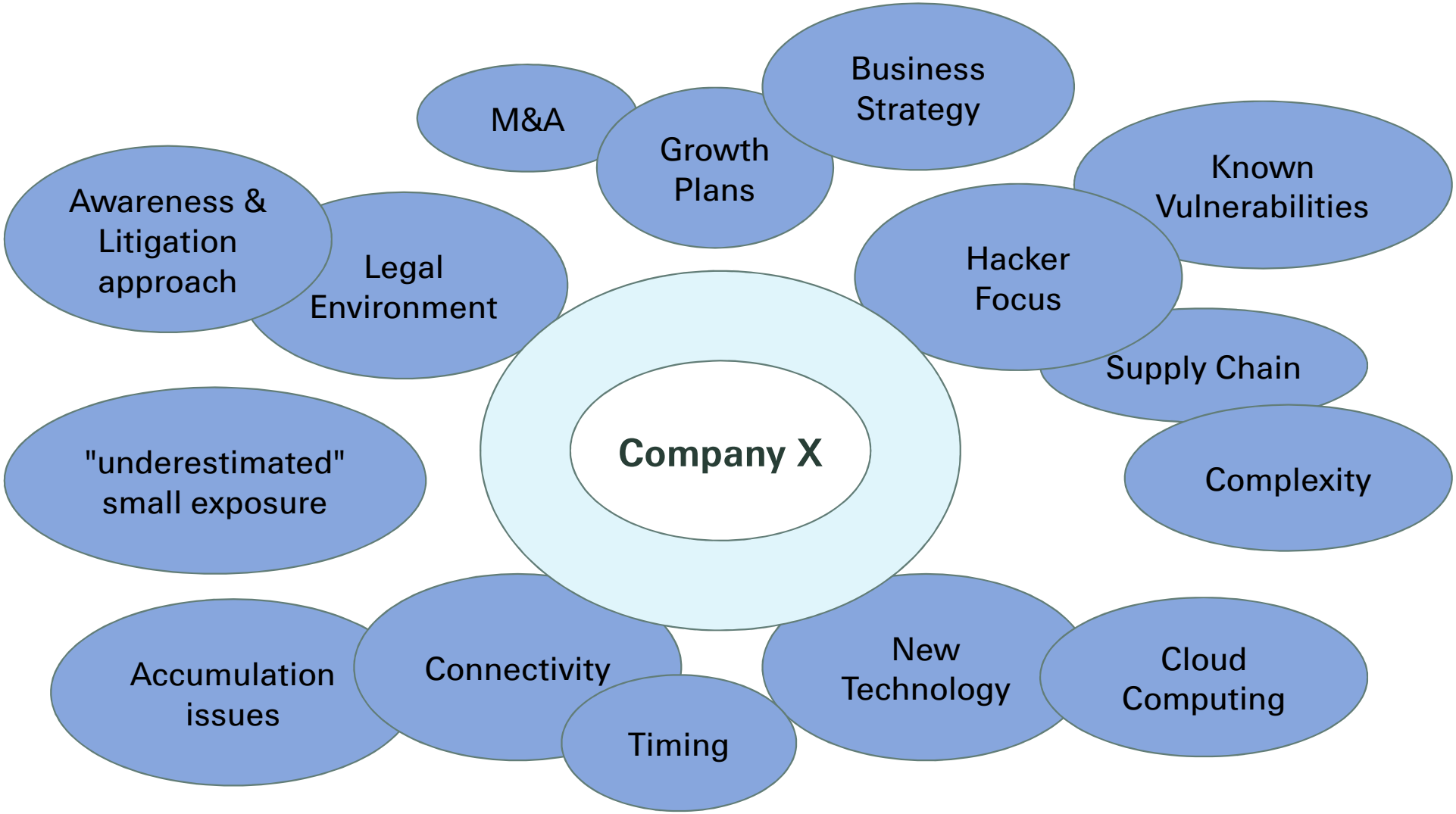
  http://www.ey.com/GL/en/Industries/Mining---Metals/EY-Cyber-hacking-and-information-security-in-mining

Swiss Re

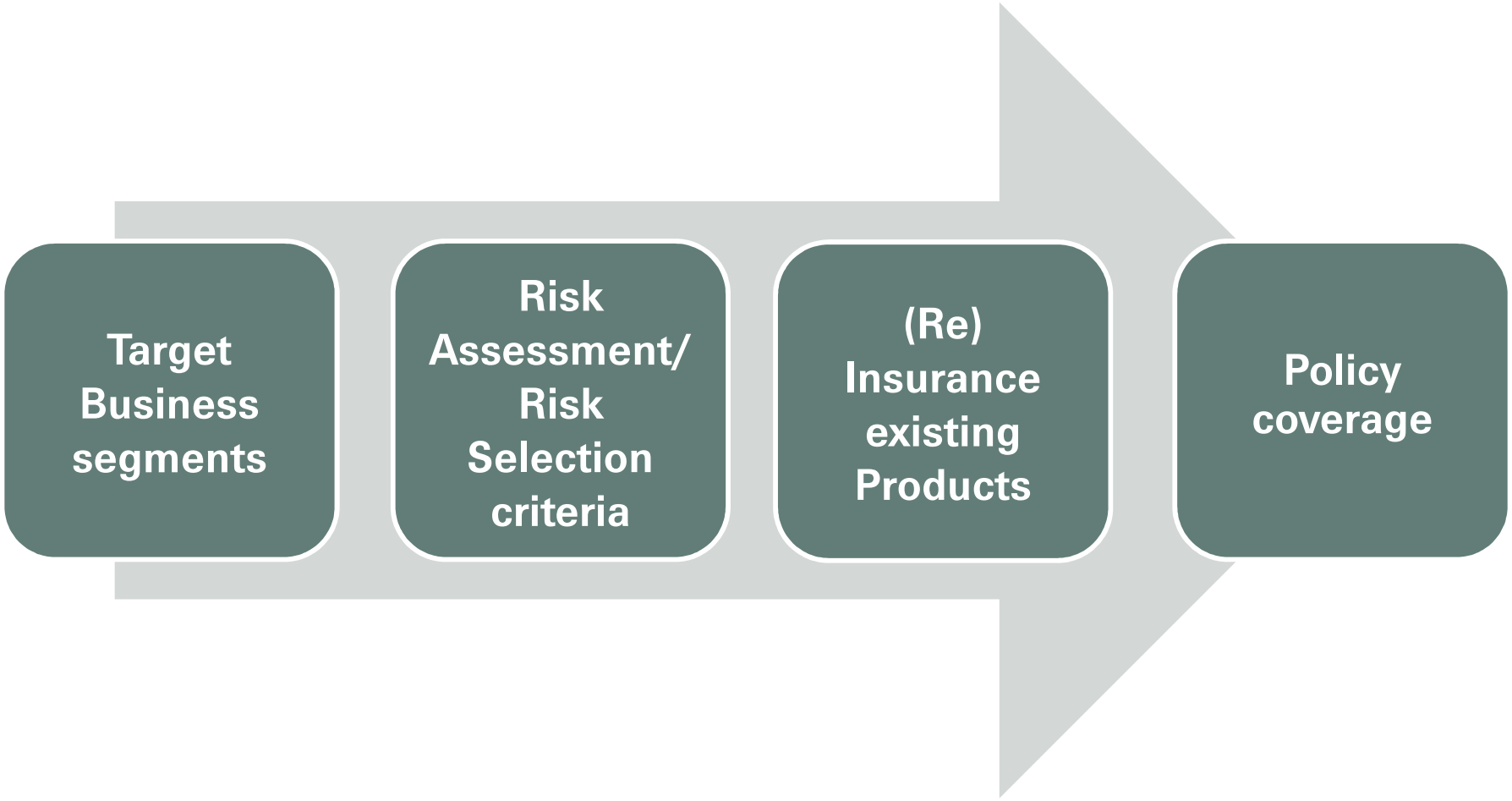
Underwriting and Swiss Re´s Position

Driving Factors for Technology E&O / Cyber Insurance

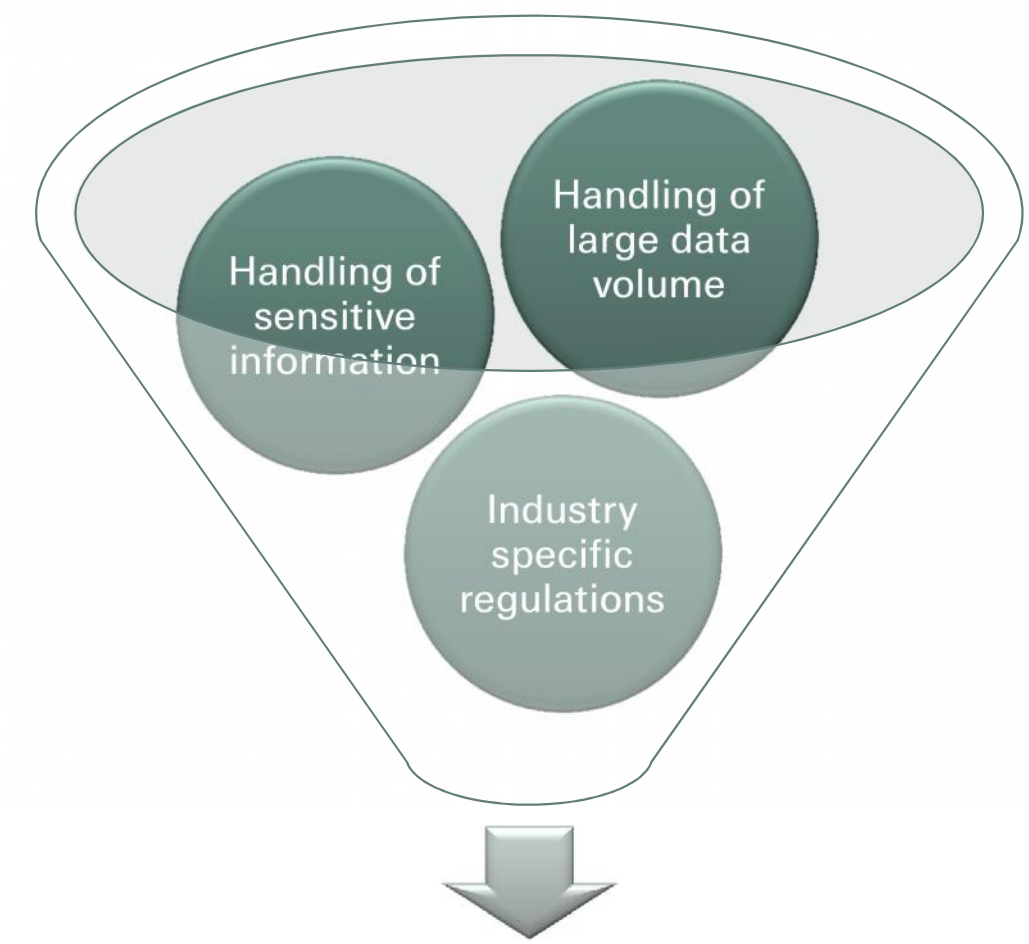
A Constantly Changing World



Underwriting Process



Highly exposed industries



Highly concerned industries for Cyber Attacks

Who are potential targets ?

Highest rate of data breach cases

- Healthcare providers / health insurers
- Financial Institutions

Heavy use of credit/debit card transactions

- Retailers
- Hotels/ restaurants and food retailers

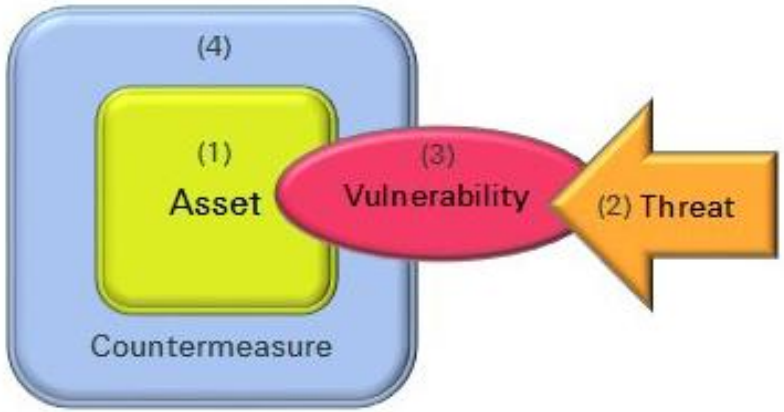
Other industries with the experience of large personal information security breaches:

- Universities / other educational institutionsPayment Processors
- Law Firms
- Real Estate Agents
- Insurance companies
- Manufacturers
- Law Firms
- Real Estate Agents

Cyber Risk Assessment Process

On a very high level, an information security / cyber risk assessment always involves the same five steps:

1. Identify the key assets > "What you are trying to protect?"
2. Identify threats to these assets > "What can go wrong, also through deliberate action by an attacker?"
3. Identify vulnerabilities that make it more likely that the threats actually materialise
4. Identify and verify the countermeasures that are in place to mitigate the vulnerabilities
5. Balance (4) against (2) and (3) to determine if the residual risk is at an acceptable level



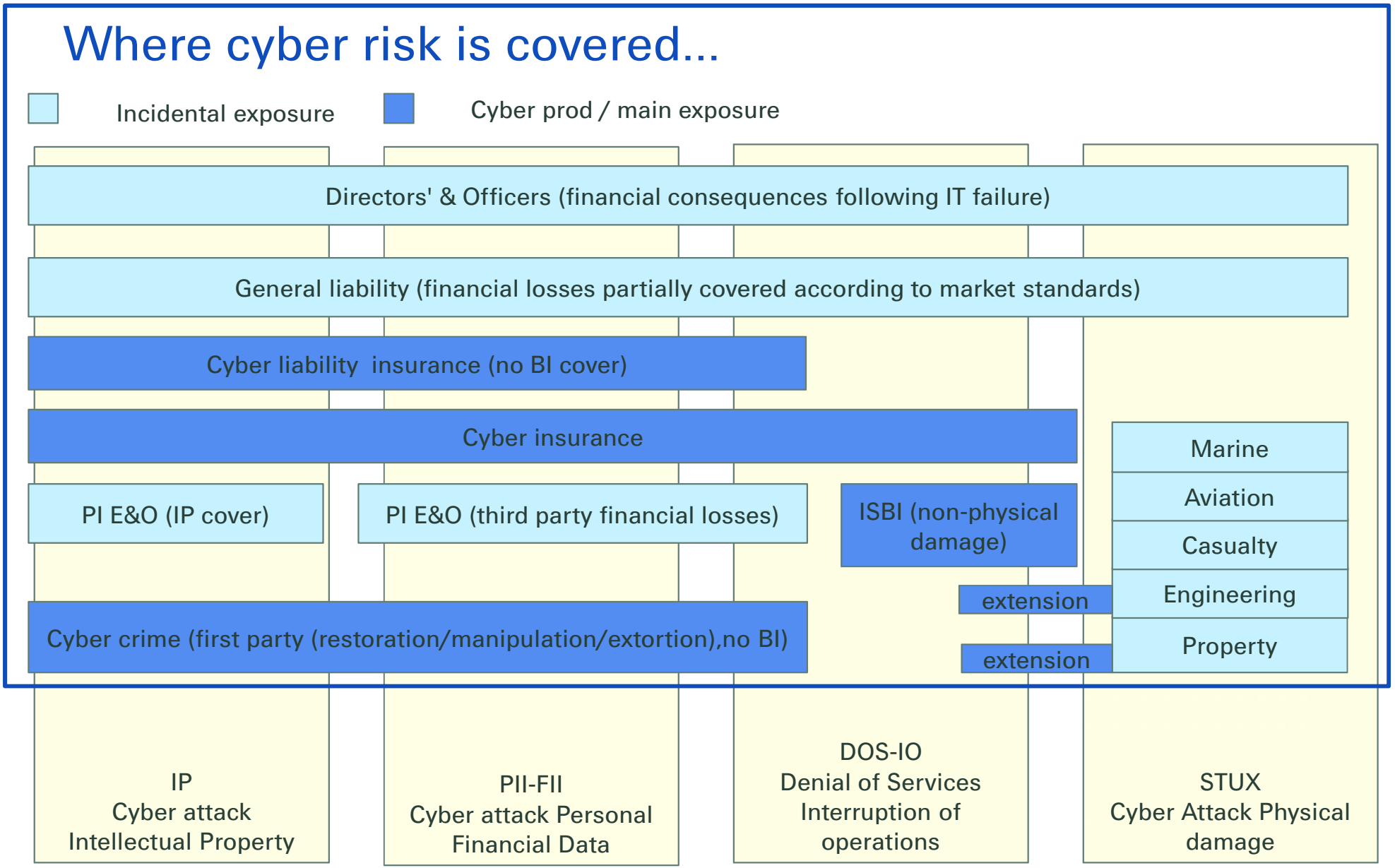
What it takes to make cyber risks insurable...

- IT & Insurance Industry must develop a common understanding on best practices in cyber security – these risks have to be actively managed by the insured!
- Information and Communications Technology is a recent discipline – deeper understanding of technical issues is needed
- Risk^assessments, costing, contracts, wordings and processes need to be developed with sustainable products based on reliable information

What it takes to make cyber risks insurable...(2)

- Clear interpretation of wordings
- Crisis management with specialized professionals
- Active steering: No overlapping of existing covers, thus incidental coverage crept into re-/insurer´s portfolio due to general wordings and absence of exclusions is identified
- Adequate accumulation methodology assessing exposure in all portfolio (incidental or direct)

Where cyber risk is covered...



... and how it accumulates.

Reinsurance Products Offering (1/2)

- Cyber coverage is opportunity for business growth and largely unknown and fast developing exposure
- Support clients in developing their cyber business subject to
  - sound risk management approach
  - underwriting and claims handling expertise
  - reasonable risk retention (alignment of interest)
  - portfolio transparency
  - limits of insurability (e.g. war exclusion)
  - availability of accumulation exposed capacity (i.e. for cyber attacks triggering first party exposures)

Reinsurance Products Offering (2/2)

- Offer both treaty and facultative business
- Accept facultative reinsurance offers of substantial size (large companies)
  - preferably as stand-alone first or third party coverage but also
  - as multi-line (combined first and third party) coverage, or
  - extension to conventional first or third party coverage
- Smaller original business reinsured via treaties or semi-automatic facultative facilities

Outlook & Trends

- New and changing exposures affecting one or more lines of business e.g Stuxnet
- Bodily injury – e.g. Cyber attacks against healthcare facilities (critical building facilities as well as critical medical devices, implants)
- Insurability of large retailers like e.g. Target, Michaels due to increasing costs of data breaches
- Tighter underwriting controls (e.g. higher retentions, higher premiums, more exclusions) observed
- Trigger ("occurrence" and "detection" are two very different things in cyber – an incident can spread across multiple policy periods..)

Conclusions

- Mature market in US, young market phase in Europe with several new entrants: many value propositions, heterogeneous wordings and players.
- Europe is not a vibrant market with currently limited potential in comparison with USA (USA estimated premium volume: $ 1Bn) with ISBI driving the demand so far
- Main offer is either privacy product (third party) or combined (including first party).
- Brokers trying to create value proposition by unique knowledge position (Marsh, Willis).
- First Party BI extensions seen more regularly on Cyber European market
- EU Regulation to be possibly in place in 2014 which will stimulate the demand for Cyber Insurance
- Growing awareness of European clients results in increasing number of enquiries, and proposals to work jointly on the product development

"In the middle of difficulty lies opportunity."
(Albert Einstein)

Thank you

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.