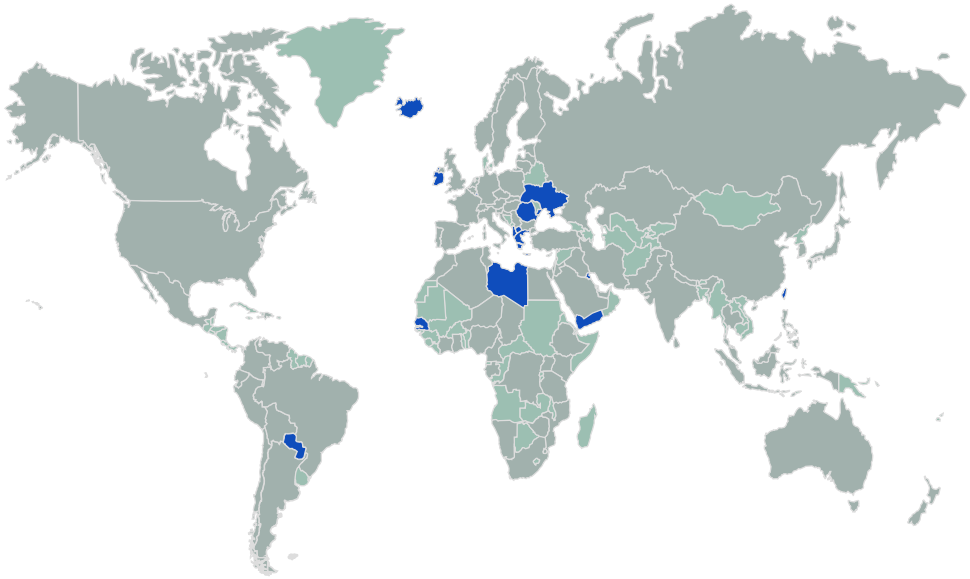

Swiss Re
Corporate Solutions
The Road to Resilience – Managing Cyber Risks
Willy Stoessel, Head Cyber, Technology & Construction, Swiss Re Corporate Solutions
Energietag 2016, 29. September 2016, Berlin

Energy leaders identify key issues critical for energy transition



- 90 contributing countries
- Over 1,200 energy leaders
- Main concerns of energy leaders

WEC Issues Monitor confirmed the importance of three main concern areas:

- Cyber threats
- Extreme Weather Events
- Energy-Water-Food nexus

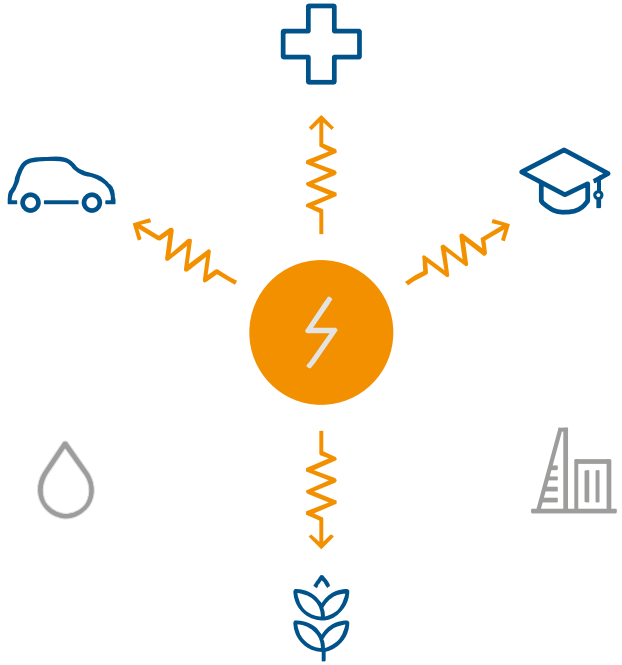
Cyber-attacks, a core threat to business continuity

- Increased **digitisation continues to improve efficiencies** but comes with associated **increased vulnerabilities.**
- Attacks on energy infrastructure have the potential to **cross from the cyber realm to the physical world.**
- Cyber risks today are growing in terms of both their sophistication and the frequency of attacks.
- Companies are increasingly recognising **cyber as a core risk to business continuity.**
- By 2018 the oil and gas industries alone could be **spending US$1.87 billion each year on cyber security**.

US$1.87 billion

Impacts of cyber risks on the energy sector

- The changing energy architecture creates an **increased number of entry points** for cyber intruders.
- Cyber risks include **non-physical and physical damage** from a cyber-attack:
  - Market disruption
  - Physical infrastructure damage
  - National security
  - Human harm
  - Network effects
  - Financial loss, liabilities



Building resilience to cyber threats

Technical measures

- Security measures for software and hardware
- Measures governing physical structures, such as limiting access to data centres, and
- Clear instructions and rules for using external hard drives

Human preparedness

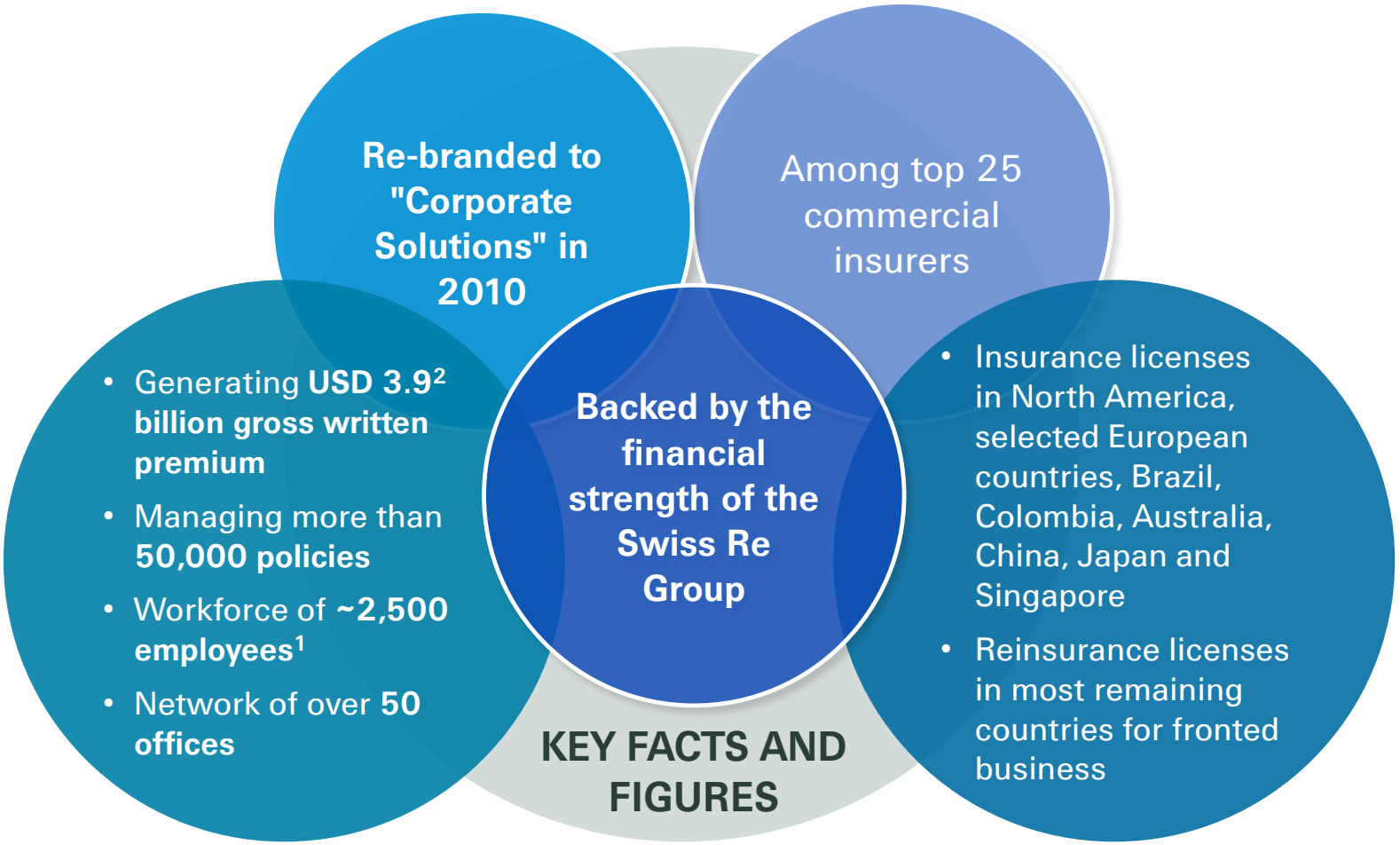
- Developing a robust cyber governance, cyber-awareness culture and cyber-awareness behaviours
- Implement at all levels of an organisation and between organisations
- Raise capabilities to prevent, detect and respond to cyber risks

Resilience – an evolving approach

- To date, the energy industry has typically relied on **"hard" resilience,** focused on resistance:
  - Single-asset approaches ensuring that individual infrastructures can withstand a sudden event and return to full performance.
  - Marginal improvement is increasingly costly.
- **"Soft" resilience** is more focused on absorption:
  - Allows for partial system failure that tries to control impact.
  - Aims to be prepared to absorb a hazardous event and limit its impact.
  - May reduce the cost of adaptation by shifting from expensive protection solutions to more flexible systems.
- Industry and policymakers should take **an integrated approach** and use a **combination of hard and soft resilience measures.**

Swiss Re Corporate Solutions position on cyber

Corporate Solutions in a nutshell



1) Excluding employees in Shared Service Centers and other Group Functions

2) Gross premiums written and premiums for insurance in derivative form

Corporate Solutions Offering

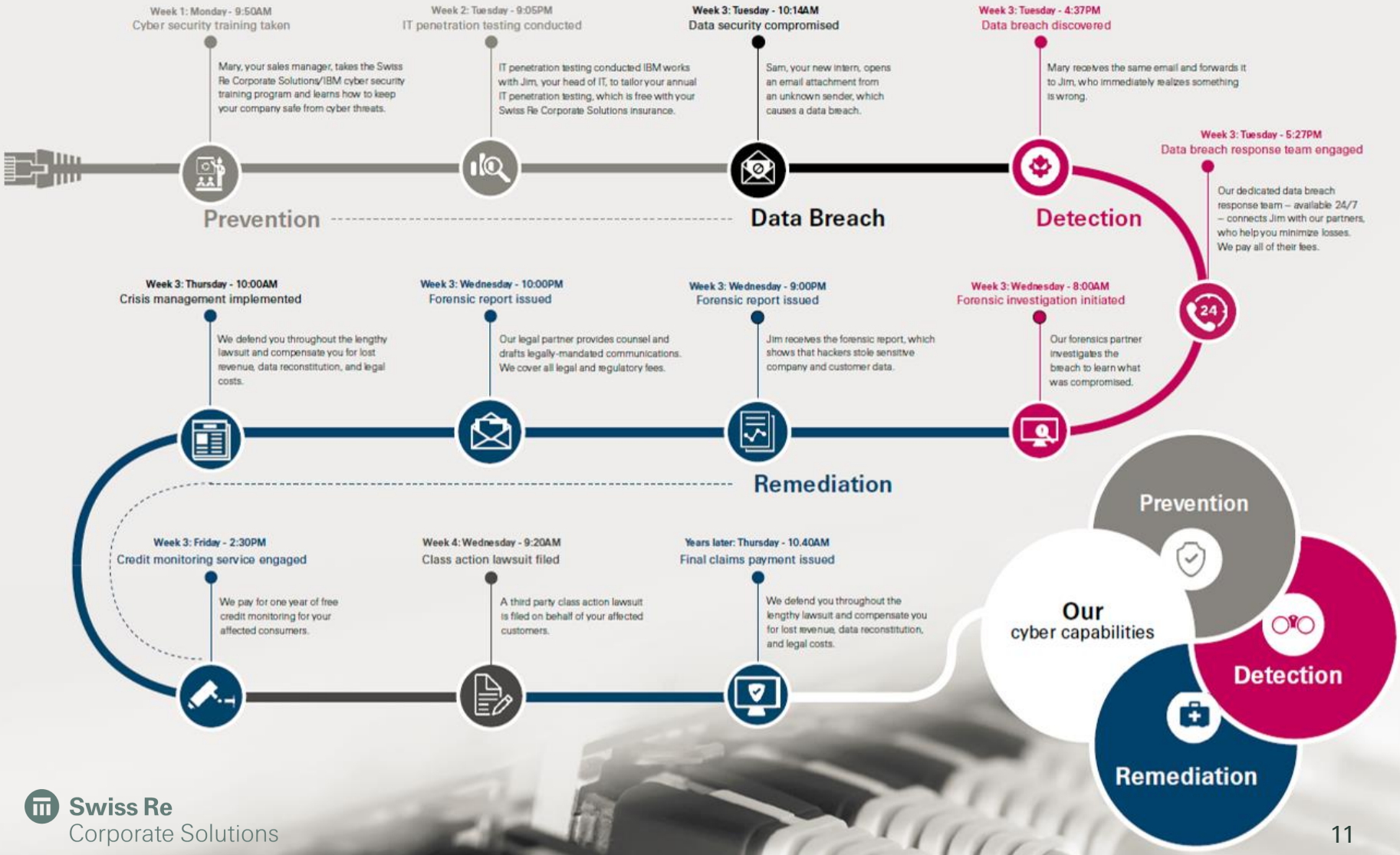
Includes First Party/ISBI, extortion and privacy coverage

Cyber Insurance			
Product	**First Party / ISBI***	**Extortion**	**Privacy**
	▪ Unauthorized access ▪ Hacking ▪ Virus & Denial of Service	▪ Investigation costs ▪ Extortion of monies due to credible threat e.g., introduction of malicious code	▪ Unintentional disclosure ▪ Breach of confidentiality
Comment	➔ **Business Interruption or loss of data** due to a general malicious attack (e.g., generic virus: love bug virus) ➔ **Contingent Business Interruption** due to lack of internet connectivity caused by IT failure at providers' location ➔ **Costs for reinstatement of data** ➔ **Investigation costs** to determine cause of security failure	➔ **Covers the monies paid by the insured as a result of a credible threat/series of related threats directed at the Insured** ➔ e.g., to corrupt, damage or destroy the Insured's computer system, or to restrict or hinder access to the Insured's computer system ➔ e.g., to release, divulge, disseminate, destroy or use confidential information stored in the Insured's computer system	➔ **Liability:** the defence and settlement costs for the liability of the insured arising out of its failure to adequately protect its 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

*Stand-alone property/extensions to property

Swiss Re
Corporate Solutions

Swiss Re and IBM's cyber security solution



Concluding remarks

World Energy Council

- Cyber risks today are growing in terms of both their sophistication and the frequency of attacks
- Evolution from prevention of cyber risks to development of a comprehensive operational strategy is necessary
- Developing appropriate technical measures and human awareness is key
- Focusing on cyber resilience makes **business and political sense**

Swiss Re Corporate Solutions

- Cyber exposure must be underwritten by specialists with the corresponding underwriting authority
- Cyber must be covered under dedicated cyber liability policies
- Cyber is not an exposure susceptible of being included into a policy as a freebee

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.

Backup

WEC's Financing Resilient Energy Infrastructure initiative

- *'The road to resilience – managing cyber risks'* is the third risk dimension investigated as part of the Financing Resilient Energy Infrastructure initiative (previously extreme weather and energy-water-food-nexus).
- It is a joined project by WEC, Swiss Re Corporate Solutions and Marsh & McLennan Companies, Inc.
- The current report investigates how cyber risks can best be managed, taking into account the changing nature of the energy industry and energy infrastructure.
- Drawing on insights from a network of energy industry experts, the report assesses the ways in which vulnerabilities in current and new energy infrastructures are changing.
- The report recommends actions that energy decision makers and stakeholders can take – individually and collaboratively – to improve the sector's response to rising cyber threats, as part of a wider move towards resilience.