PartnerRe

Cyber Risks from a reinsurers perspective
DVfVW, Düsseldorf

Markus Bassler, PartnerRe

April 20, 2016

Reinsurance in the Cyber Space

Technology

Exposure

Accumulation

Market and Products

Outlook

PartnerRe

Technology

Today`s Internet

Over 7 bn humans on earth

Over 25bn connected devices

More "things" than computers connected

Still less than 1% "things" connected

PartnerRe

Sources: Lloyds Cyber Seminar 2014 and market information

Tomorrow`s Internet

2016: around 25bn connected devices

2024: 50bn to 1 trillion connected devices and 7.6bn humans

In 2014, 80 “things” connect to internet every second

By 2020, 250 things will connect to the internet every second

PartnerRe

Sources: Cisco Systems

IoT – Internet of Things

IoT captures and aggregate data - e.g. platform software, application software, telecom infrastructure, service infrastructure

Applications: Retail, manufacturing, infrastructure and public sector, consumer health and fitness, vehicles, consumer products

Hacks

Critical infrastructure control systems (ICS, SCADA, DCS)

Yacht GPS systems

Light bulbs

Video cameras

Medical devices

Home control hubs

Cars

…

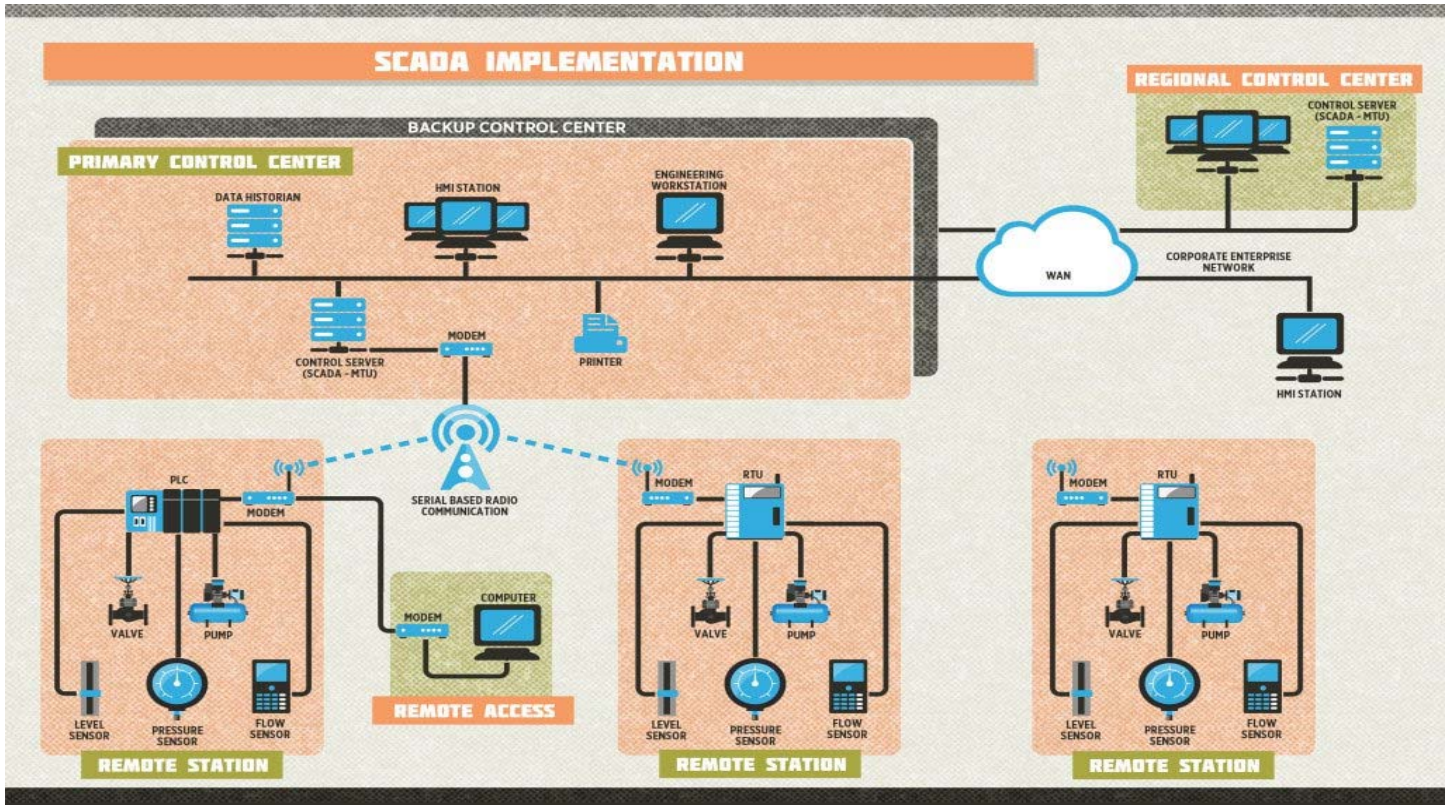
Everything can be hacked!

PartnerRe

Intelligent Control Systems and SCADA

The move from historically ICS isolated systems, controlled by engineers and isolated from the internet to a more modern, integrated network - like the SCADA system, the operating system and the network equipment used to connect the two - leaves greater points of access for hackers and cyber terror attacks.

As unspecialised operating systems using internet networks are operated by lesser trained employees, the networks created become increasingly vulnerable.



PartnerRe

Changing Business and IT environment

New Business Models – Cloud, Mobile

Globalisation and increased interconnection

Enterprise IT environment disrupted – rogue IT

Regulatory changes with SEC rules

PartnerRe

Sources: Deloitte Development LLC, Emerging Risks – a focus on cyber security

First summary

Greater vulnerability through globalisation and interconnection

Critical infrastructure is a target

Supervision, legislation and compliance

Outsourcing data (cloud computing) creates new risks

Constant availability changes everyday life

Exposure

Targets of Cyber Attacks – Critical Infrastructure

- Energy
- Communications
- Emergency Services
- Financial Services
- Food
- Health
- Transport
- Government
- Water

Energy sector targeted disproportionately

PartnerRe

Critical infrastructure attacks by pattern

Energy and Utilities: 38% web application attacks, 31% crime ware, 14% denial of service

Transportation: 24% espionage, 16% insider missuse, 15% web application attacks

Manufacturing: 30% espionage, 24% denial of service, 14% web application attacks

Financial Services: 27% web application attacks, 26% denial of service, 22% card skimmers

Hospitality: 75% POS intrusion, 10% denial of service, 8% insider misuse

PartnerRe

Sources: Verizon, Data Breach Investigations Report, 2014

Where are the exposures?

Hacking

Malware/Virus

Phishing

Loss or theft of Computer

Unintentional Disclosure

Rogue Employees

Potential Damages

Property

Pipelines

- Power Grid

Denial of Service

- Unable to provide services to customers – BI/CBI

Theft of personal information

- Name/Passwords
- Social Security Numbers
- Credit Card information
- Bank/Financial information

Examples from the Energy sector

Saudi Aramco, 2012 Shamoon Virus

RasGas, 2012 Hacker Attack

Chevron, 2010 Virus

Natanz, Uranium Enrichment Plant, 2010 Stuxnet

Stuxnet was a game changer!

PartnerRe

Data Breach Exposures

Industries Targeted

- Retailers
- Healthcare
- Financial Institutions
- Social Media
- Content Aggregators
- Gaming
- Entertainment
- Cloud/Saas Providers

Customer Data

- Credit Cards
- Address
- Social Security Numbers
- Login Credentials

Employee Data

- Personal Information
- Personal Health Information

Loss of Profits

- Network Outage
- Security Failure

Cyber Exposure in the Insurance Market

Affirmative Stand-Alone Cyber Cover

Affirmative Cyber Endorsements

Silent Cyber Exposure – gaps in cyber exclusions

Silent Cyber Exposure – policies without cyber exclusions

PartnerRe

Sources: RMS, Cambridge Center for Risk Studies, February 2016

Accumulation

Classification for managing cyber accumulation

- Information technology
- Retail
- Financial Services
- Healthcare
- Energy incl. Utilities, mining and pharmaceuticals
- Telecommunications
- Manufacturing
- Defense and military contractor
- Public authorities
- Transportation, Aviation, Aerospace
- Real Estate
- Food and Agriculture
- Education

Lloyds cyber peril coding

Cyber Security data and Privacy BreachEnergy

CY code, 1st and 3rd party claims from a datat breach without physical damage

Cyber Security Property Damage

CZ code, 1st and 3rd party claims from physical property due to a data breach of security even

Recognition loss cause through peril codehelps to identify related policy wordings and loss types

Accumlation scenarios and challenges

PML determination difficult

Claims experience limited

Cyber threat is rapidely evolving, older losses are less credible

Systemic nature of cyber is apparent – but lack of truly systemic cat loss

Start with an evidence-based assessment of loss potential

PartnerRe

Sources: RMS, Cambridge Center for Risk Studies, February 2016

High impact scenarios for affirmative standalone cyber policies

Scenario Leakomania: a/ Breach of privacy event b/ data and software loss

Scenario Mass DDoS: Business Interruption

Scenario Cloud Compromise: Business Interruption

Scenario Financial Transaction Interference: Financial Theft

Scenario Extortion Spree: Cyber Extortion

PartnerRe

Sources: RMS, Cambridge Center for Risk Studies, February 2016

Pre-conditions and thoughts about insurability

- Transparency between insured, risk career and external IT consultant
- Access to loss data, sharing of information, standardized data structure
- Cooperation with governamental bodies
- Future development of cyber accumulation management systems
- Constant stress testing of the cyber business
- Enhance regulatory/rating reporting requirements

The market needs to price for the additional cover/exposure
Most covers require a sub-limit
The market introduces occurence limits

Market and Products

Segmentation

1st party coverage	3rd party coverage
Property	Liability Product and Operations
BI	Liability Technology E&O
Data and software loss	Liability Professional Services E&O
D&O	CBI
Incident response cost	Network service failure liability
Financial theft and fraud	
Reputational damage	
Cyber extortion	
Intelectual property theft	
Breach of privacy	

Standard Cyber Coverage

- **First Party Liability**
  - Remediation costs to respond to breach
    - Investigation, public relations, customer notification, credit monitoring
  - Business Interruption
  - Fines and/or penalties
    - Regulatory fines
    - PCI - DSS fines
- **Third Party Liability**

Market for cyber insurance

The market is growing 2bn in 2014 (thereof 1.3bn from the US) – currently around 30 different insurers

Market potenial $10B by 2020

$250m to $500m Data Breach Cyber Liability

$100m Non-Damage BI (requires further science)

Physical damage from Cyber event not offered or very limited

Manuscript cyber policies available on All Risk basis

Cyber Insurance penetration

Cyber Insurance Penetration Rates by Company Size	
Revenue Range ($)	% purchasing Cyber
<2.5M	3.4%
2.5M<5M	4.1%
5M<10M	5.4%
10M<25M	6.9%
25M<100M	9.0%
100M<300M	16.1%
300M<1B	19.2%
1B<5B	19.3%
5B+	21.9%

ADVISEN Insurance Intelligence

Highest penetration in healthcare, retailing, hospitality and financial services

PartnerRe

Products

Prominent carriers such as AIG, Ace, Beazely, Chubb, CNA, Hiscox, LIU, Trafelers, XL, ZFS etc. offer a broad varity of products

What`s covered? Not always clear…

Capacity offered between $10-25m (50m)

Deductibles between $1.000-25.0000

Average Limit $5m, average premium $50.000

PartnerRe

Sources: Advisen Cyber Risk Conference London 2014

Cyber Liability Insurance Marketplace

- **Over 25 markets offering coverage on stand-alone basis. Many more endorsing coverage on existing policies**
  - Competitive market
  - Not standardized product
- **Betterley Report estimates $2B Market**
- **Limits up to $25M (Offered by about 10 markets)**
- **Market Capacity ~ $450M**

Changing regulatory and statutory landscape

Federal Requirements

- **FTC**
  - FACTA (Fair and Accurate Credit Transaction Act)
  - Gramm-Leach-Bliley Act (financial institutions)
- **HIPAA (Health Ins Portability and Accountability Act) – governs use and disclosure of PHI**
- **HITECH - The Act extends HIPAA rules for privacy and security safeguards, including increase enforcement, penalties and audits**
- ***Sarbanes Oxley – CEO/CFO responsible for data security***
- ***SEC requirements on cyber disclosure***
- ***In the US legal requirements vary by state***
- ***Different regulatory environment in Europe***

PartnerRe

Outlook

Conclusion and Outlook

Cyberization - the world is changing, and fast!

Increase of data dependancy and interconnections

Compliance with regulatory requirements becomes more challenging

New cat exposure from IT/Network Security and more complicated by cloud, mobile technology

Accumulation becomes an issue

Clients need to identify, understand, map and share the expsosure related to Cyber

The demand for cyber products is growing fast

Disclaimer

This presentation is for general information, education and discussion purposes only.

Views or opinions expressed, whether oral or in writing do not necessarily reflect those of PartnerRe nor do they constitute legal or professional advice.

PartnerRe