Cyber exposures in traditional lines of business

AqabaConf, 16 May 2017

Fabian Willi, Cyber Risk Reinsurance Specialist, Swiss Re

Affirmative cyber

Silent cyber

Silent cyber – why does it matter?

Silent cyber exposure matters because...

...it constitutes a real risk

German Steel Mill Meltdown: Rising Stakes in the Internet of Things

Traditional property all risk policies are expected to cover physical damage and business interruption from incidents like the cyber attack to a German steel mill in 2014

Source: https://securityintelligence.com/german-steel-mill-meltdown-rising-stakes-in-the-internet-of-things/

...it's getting on regulators' agenda

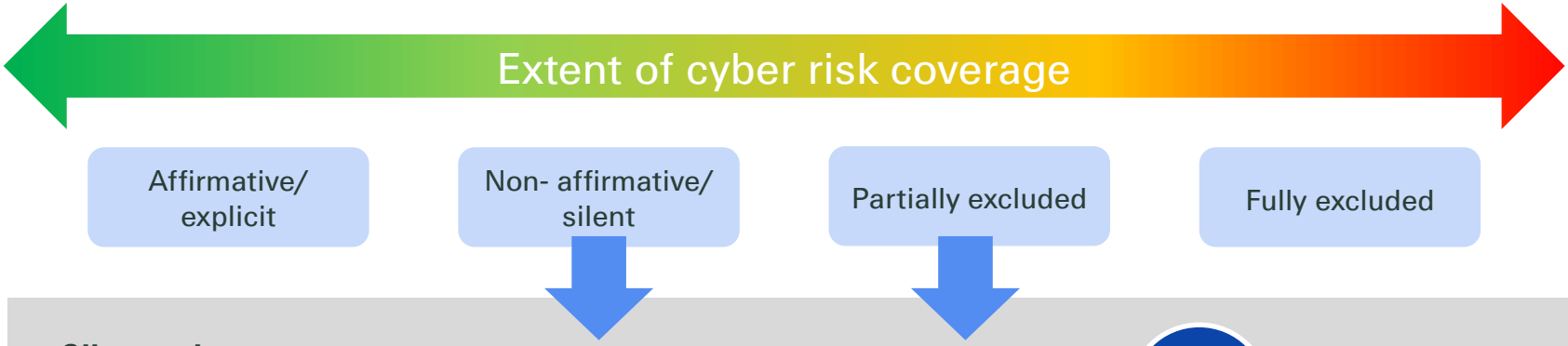
"By its nature, silent cyber risk is not always identified, managed and monitored and may be a material risk for firms"

The PRA expects firms to

"robustly assess and actively manage their insurance products with specific consideration to silent cyber risk exposure"

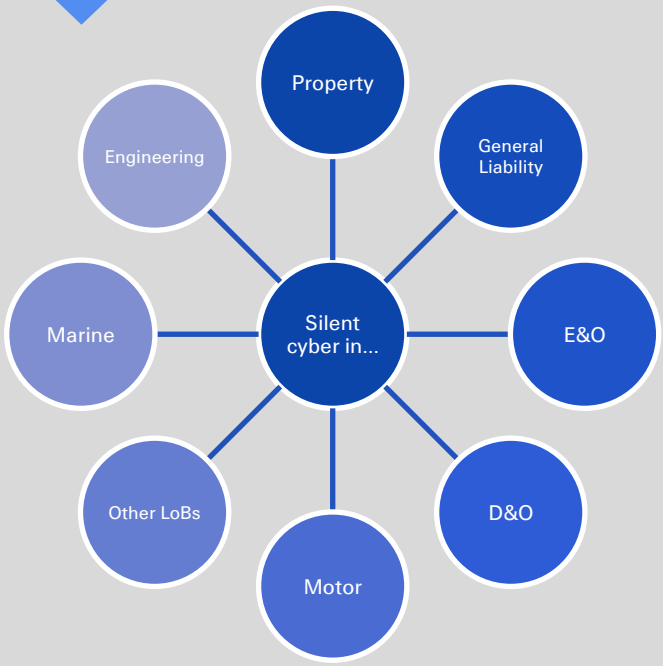
Source: PRA consultation paper CP 39/16

Unless explicitly excluded, cyber risks might be covered by most traditional insurance policies



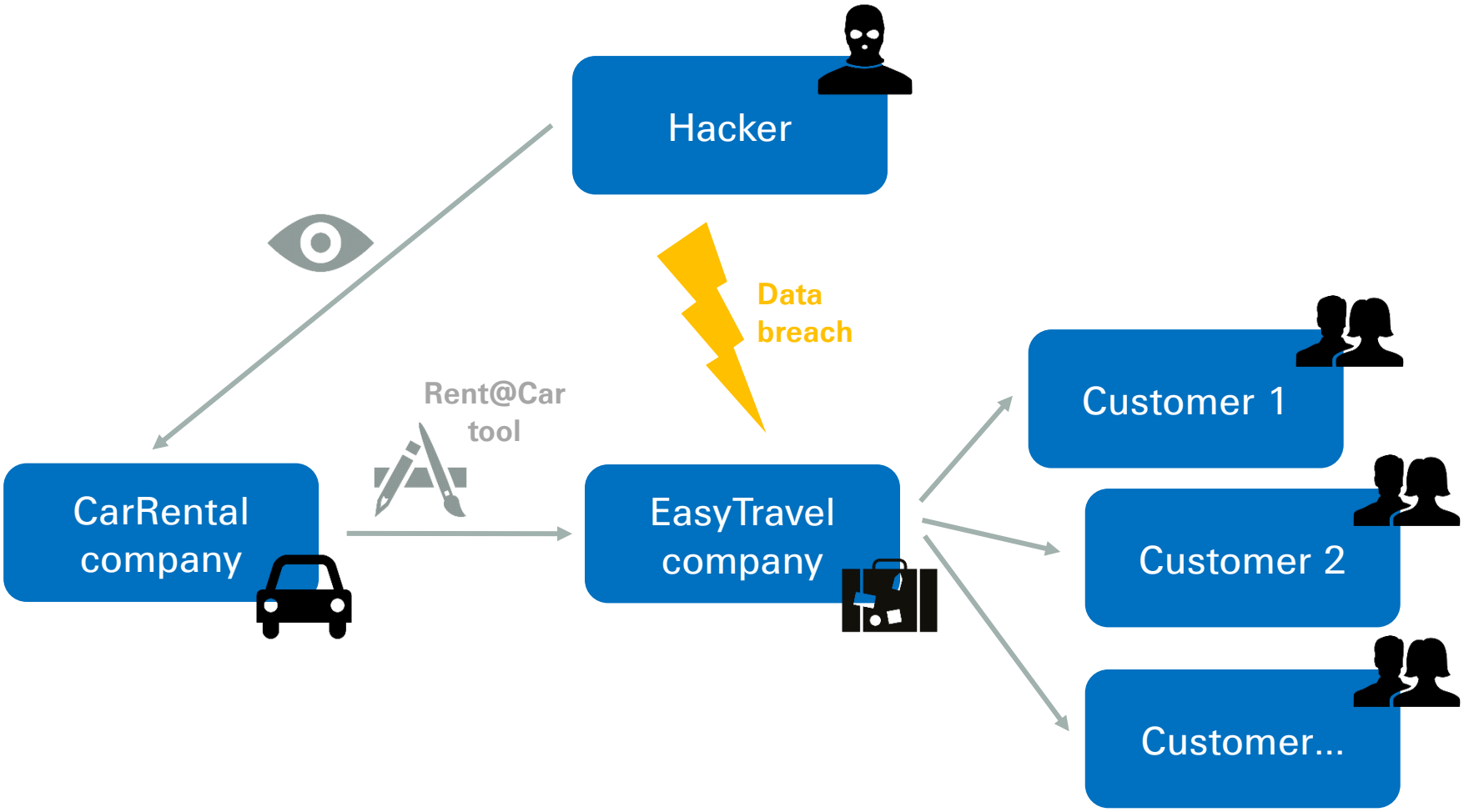
Silent cyber exposure:

- Depending on the scope of insuring agreements and exclusions, losses caused by cyber perils might be silently covered in most traditional insurance policies
- Silent cyber can creep into policies where cyber exclusions are not fully exhaustive
- Underwriters should assess how silent cyber exposure might impact loss severity and frequency



Cyber data breach case study
What is (not) covered in my traditional insurance policy?

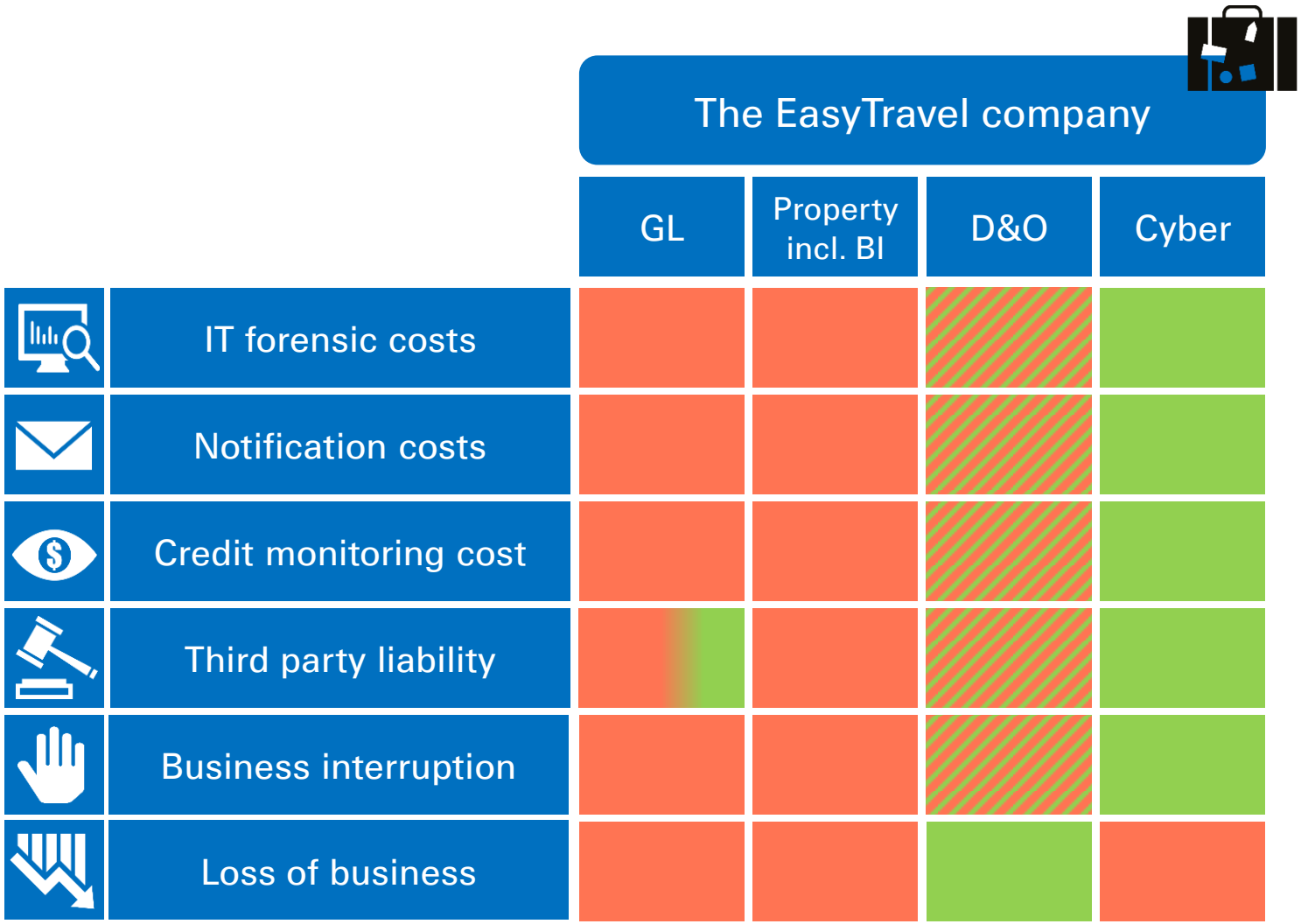
Data breach case study – what happened?



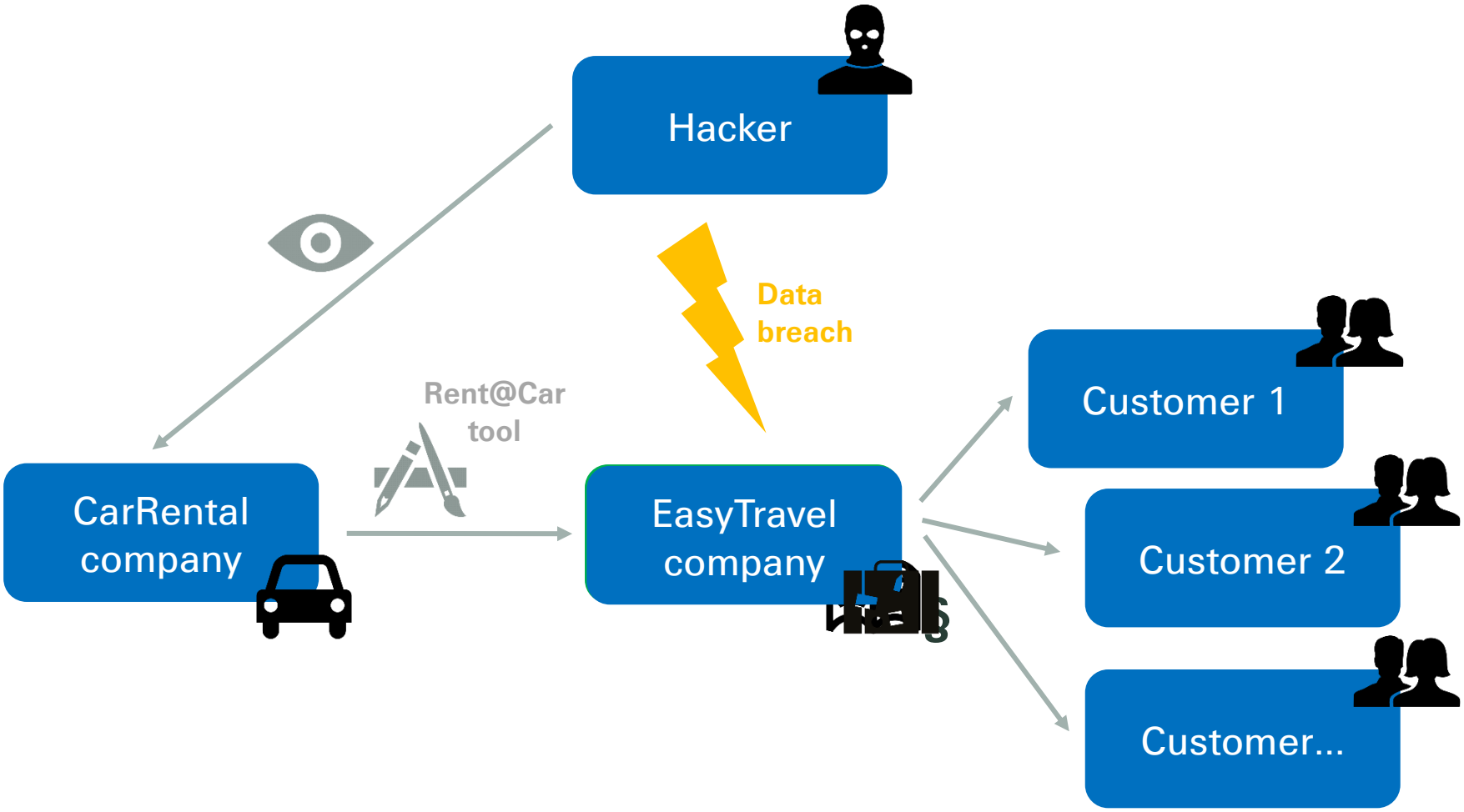
Data breach case study – the details

Actors	What happened
CarRental company	• The CarRental company offers car rental via their booking tool Rent@Car • The booking tool has been developed by an external IT software company
EasyTravel company	• EasyTravel is a travel agency using the Rent@Car booking tool to arrange car rentals for their customers • Their IT system was hacked and sensitive customer data from their database stolen • Stolen data includes personal information such as driver's licence and credit cards • In order to clean-up their compromised IT system, EasyTravel has to engage an IT forensic company and needs to go offline for one day • Based on applicable law EasyTravel notifies their customers about the data breach • EasyTravel offers one year free credit monitoring to their affected customers • Due to reputational damage EasyTravel loses customers and business
Hacker	• Hacker discovered backdoor in Rent@Car booking tool allowing him to attack and infiltrate EasyTravel's IT system
Customers	• Customers whose personal data was stolen file privacy breach class action against EasyTravel company

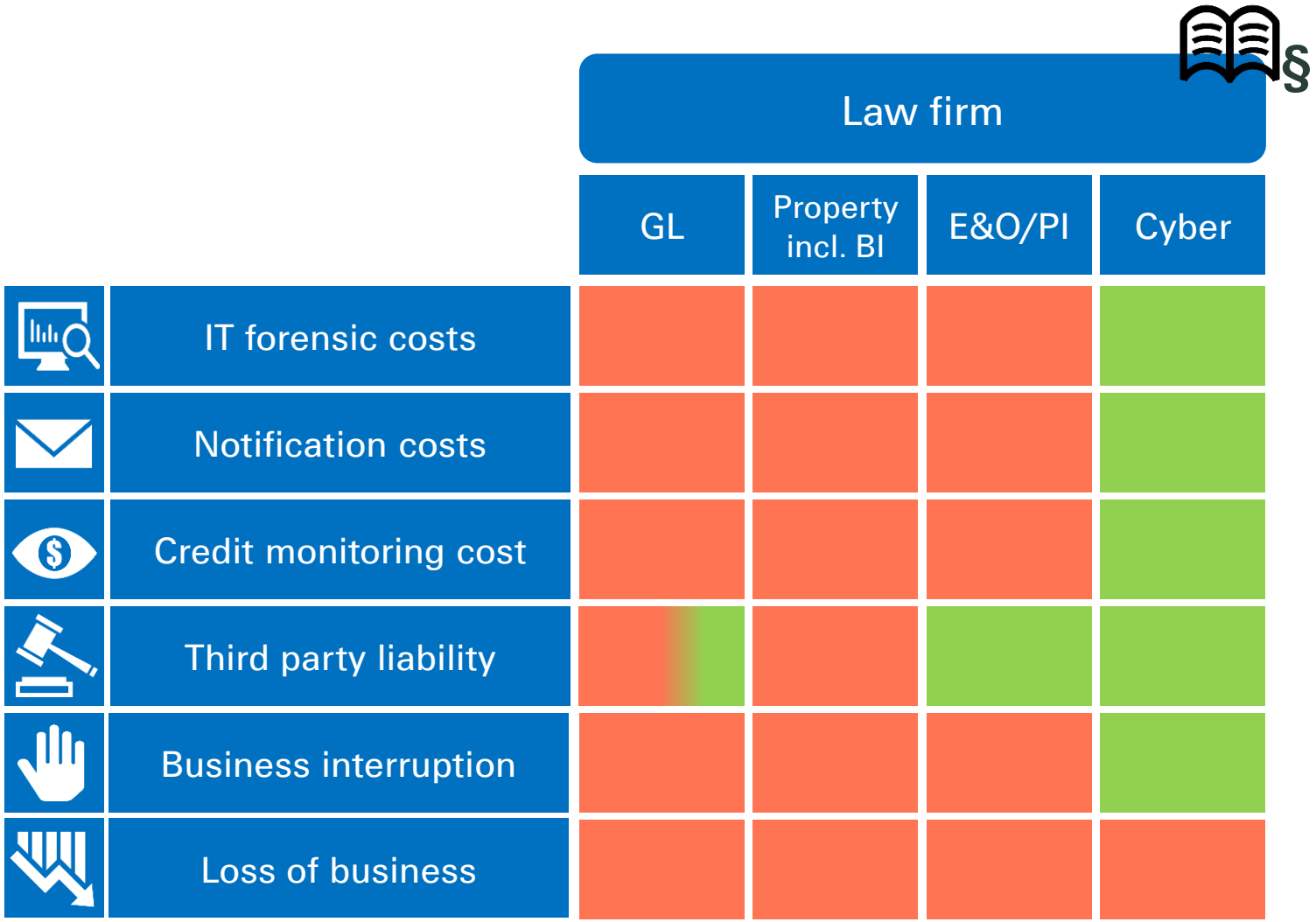
Data breach case study – what is covered?



Data breach case study – let's swap the breached company



Data breach case study – what is covered now?



Data breach case study - conclusion

- General Liability insurance generally does not respond to data breach (unless endorsed with pure financial loss coverage)
- Property insurance generally does not respond to data breach
- In selected regulated professions Errors & Omissions/Professional Indemnity insurance might respond to cyber third party liability claims in case of data breach
- Directors & Officers insurance might respond to any type of cyber-related losses (incl. loss of business) if duty of care is violated
- Stand-alone cyber insurance generally provides coverage far beyond traditional products. This is in particular the case for 1st party breach response costs (IT forensics, notification, credit monitoring etc.) which are generally not covered in traditional lines of business

Silent cyber exposure in the light of accumulation

Cyber accumulation

Understanding silent cyber is key to actively manage accumulation

DoS / IO

(Denial of Service / Interruption of Operations)

- Example 1: Coordinated attack that puts down many on-line sales portals
- Example 2: Attack on clouds or cloud-of-clouds
- Example 3: Large scale internet outage

Affirmative coverage - affects mainly dedicated cyber products

Data Breach

(Impact on personal and/or financial data)

- Personal data and credit card information stolen from a widely used database system

Affirmative coverage - affects mainly dedicated cyber products

Critical Infrastructure

(with or without property damage)

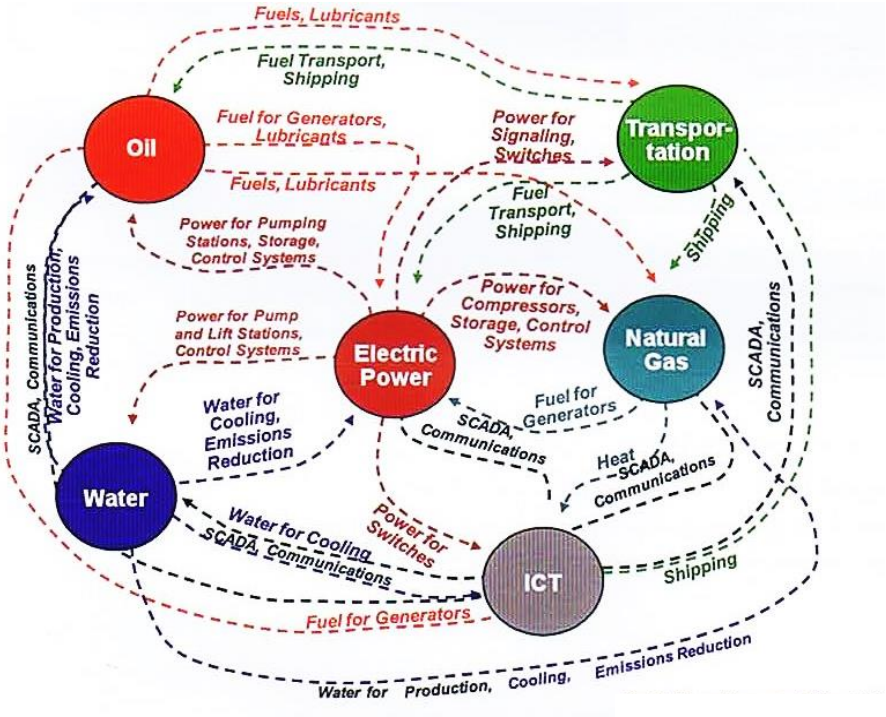
- Virus blocks cooling system of several power plants which catch fire/explode
- Malware brings electricity transmission down w/o property damage

"Silent" coverage embedded in traditional products


Critical
Infrastructure

Critical Infrastructures

Electric power is most critical infrastructure in the light of cyber attacks

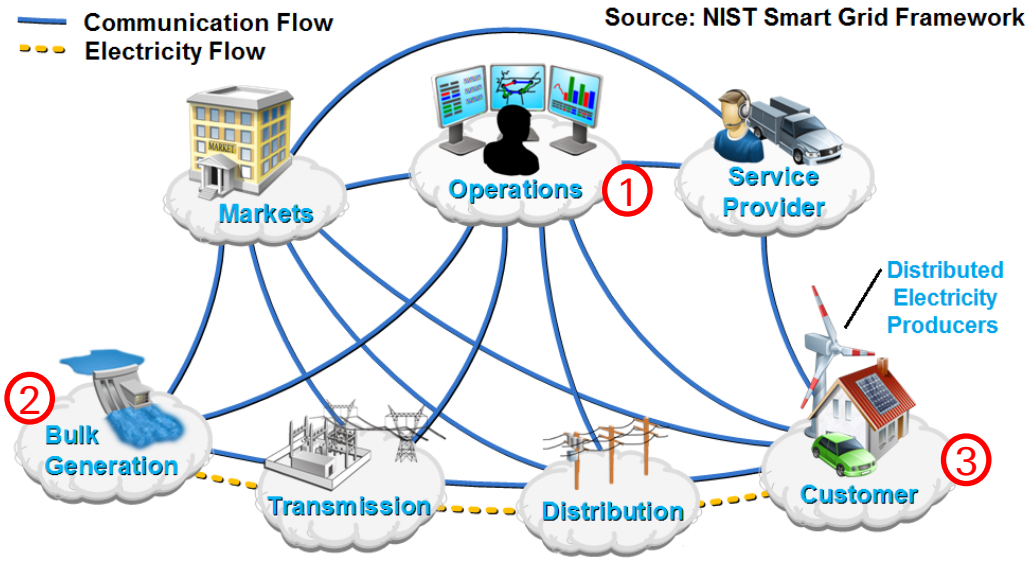


Source: M. Rinaldi, P. Peerenbom and K. Kelly – Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies

- **Interdependencies** between **critical infrastructures** have been studied since 2001 in the US in response to a series of outages of critical services
- Several **power disruptions** in California in 2001 had **cascading effects** on other critical infrastructures:
  - Outage of **public transportation**
  - No operations of **gas/oil pipelines** → **no fuel** → no traffic → no airport
  - No **water transport** → dehydration and crop failure
  - Outage of **communication**

There is widespread consensus that **electric power** is the **central component** of all critical infrastructures with by far the highest degree of **interdependency.** Almost all other critical infrastructures depend on it.

How to attack the electric power grid?



① **Control centres of TSO/ISO/RTOs[1]**
→ **Generally well protected, but single successful attack can cause large blackouts**

② **Power plants control centres, power generators**
→ **Attacks on single plant not critical thanks to the security reserves kept within the grid. A high number of plants need to be attacked synchronously for large-scale outage (very unlikely)**

③ **"Smart Grid" consumers and producers**
→ **"Smart Grid" is still in its infancy. Attack might be a concern in 10-15 years, but not today.**

[1] TSO: Transmission System Operator, central entities that control the flow of electric power in European Countries
ISO/RTO: Independent System Operator / Regional Transmission Operator (same function in the USA)

Cyber attack to power grid – not a theory anymore!

Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html

CYBER SCARE

Ukraine Power Grid Goes Black After Cyber Attack

Source: https://www.the-american-interest.com/2016/12/20/ukraine-power-grid-goes-black-after-cyber-attack/

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

Source: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

OPINION

Why the Ukraine power grid attacks should raise alarm

The cyber-attacks in Ukraine are the first publicly acknowledged incidents to result in massive power outages. Grid defenders should develop anticipatory responses to these and other ICS attacks.

Source: http://www.csoonline.com/article/3177209/security/why-the-ukraine-power-grid-attacks-should-raise-alarm.html

Are cyber attacks to power grids covered in traditional property policies?

Potentially exposed covers

- Electricity producers: **business interruption**
- Electricity consumers: **contingent business interruption** due to failure of utility provider (suppliers, off-premise power and service provider extensions)
- **Food and product spoils**

Insurance trigger condition met or not?

- In most policies **physical damage** is insurance trigger condition → cyber attack to power grid most likely not covered
- However, not all policies require physical damage → **accidental occurrence** trigger
- Some property insurance products treat data manipulation as physical damage

Legal ambiguity

- Physical damage trigger is not an unequivocal term
- Recent legal court rulings suggest that there is some **room for interpretation** ("loss of functionality doctrine")

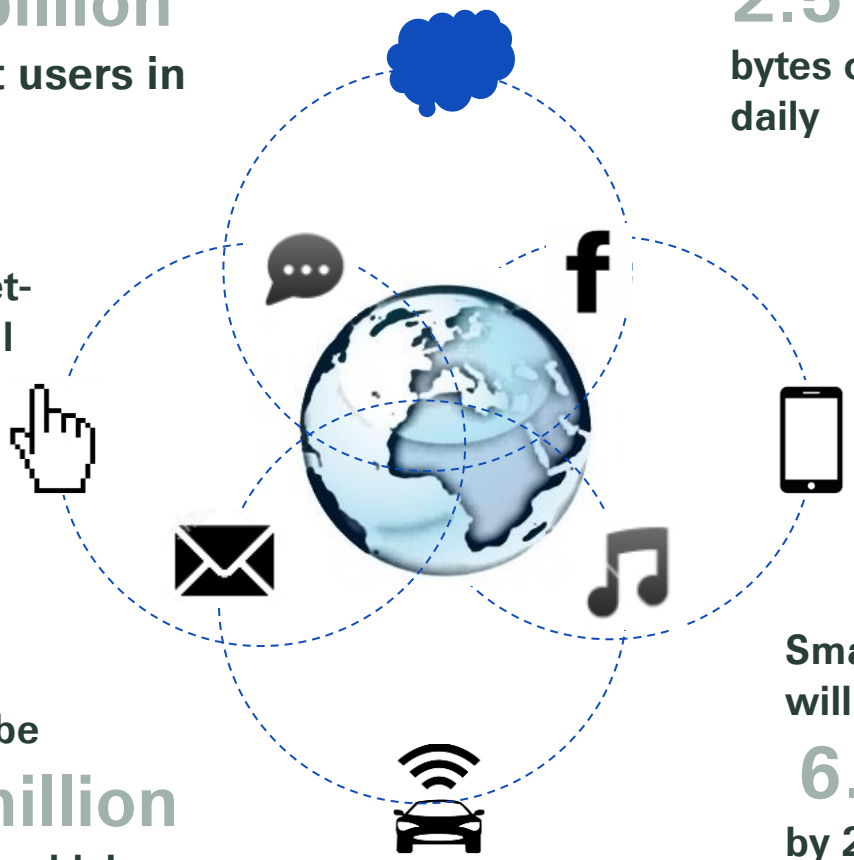
Impact of digitization on traditional lines of business

The world is becoming increasingly interconnected...

3.4 billion
internet users in 2016

2.5 quintillion
bytes of data created daily

The number of internet-connected devices will touch
50 billion
by 2020

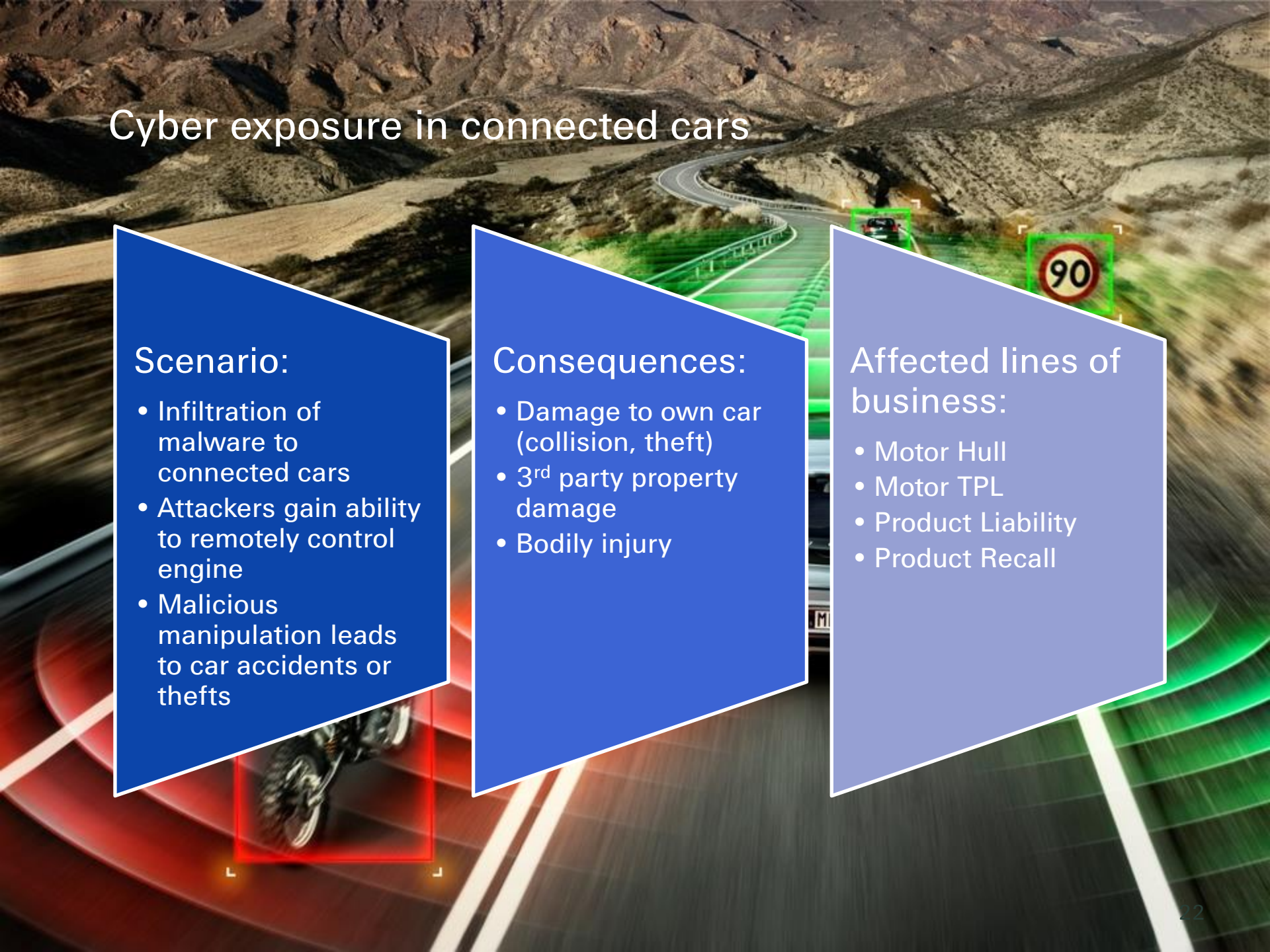


Facebook users like over
4 million
posts a minute

There will be
250 million
connected vehicles on the road by 2020

Smartphone users will reach
6.1 billion
by 2020

Cyber exposure in connected cars



Scenario:

- Infiltration of malware to connected cars
- Attackers gain ability to remotely control engine
- Malicious manipulation leads to car accidents or thefts

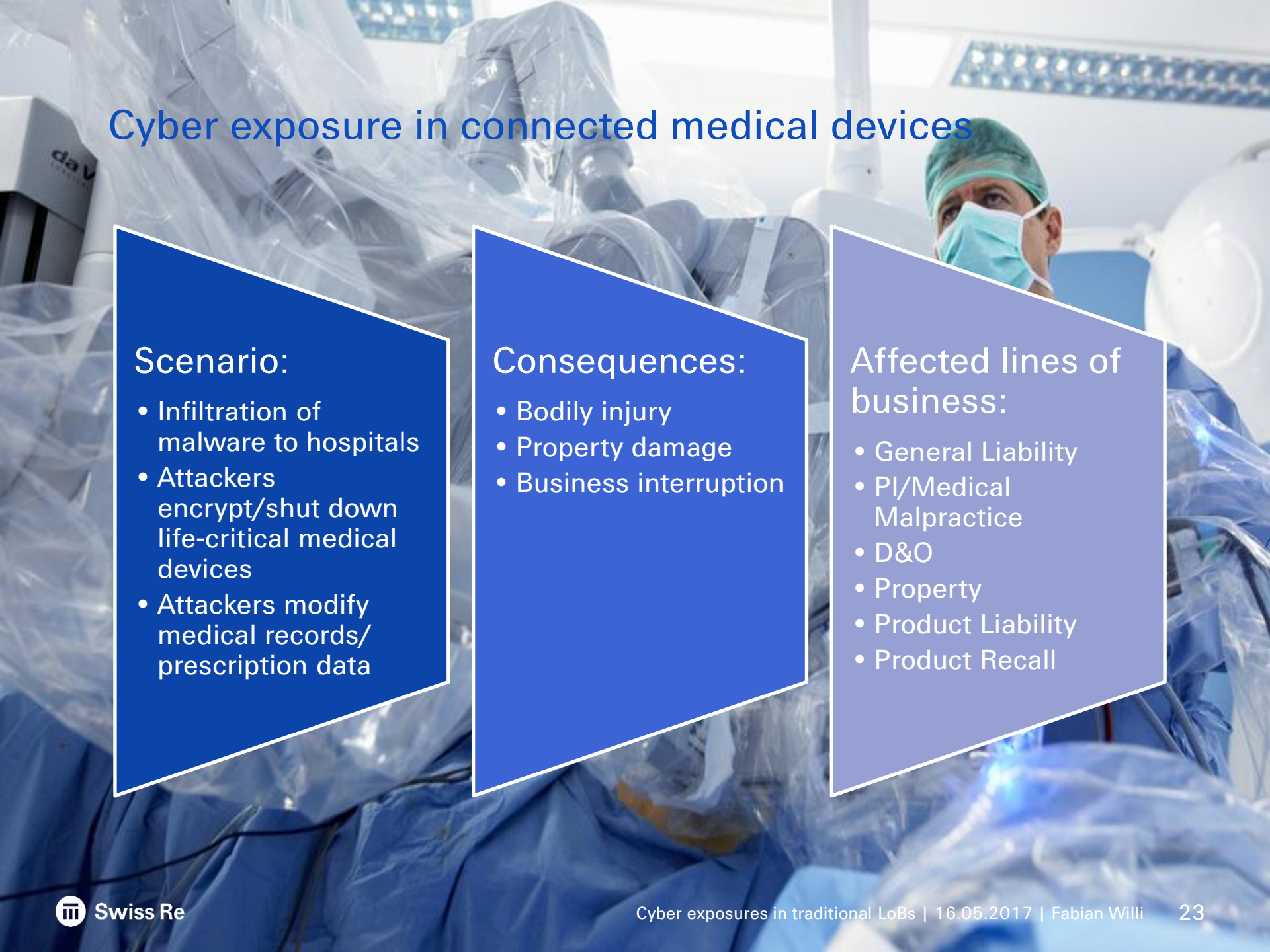
Consequences:

- Damage to own car (collision, theft)
- 3rd party property damage
- Bodily injury

Affected lines of business:

- Motor Hull
- Motor TPL
- Product Liability
- Product Recall

Cyber exposure in connected medical devices



Scenario:

- Infiltration of malware to hospitals
- Attackers encrypt/shut down life-critical medical devices
- Attackers modify medical records/ prescription data

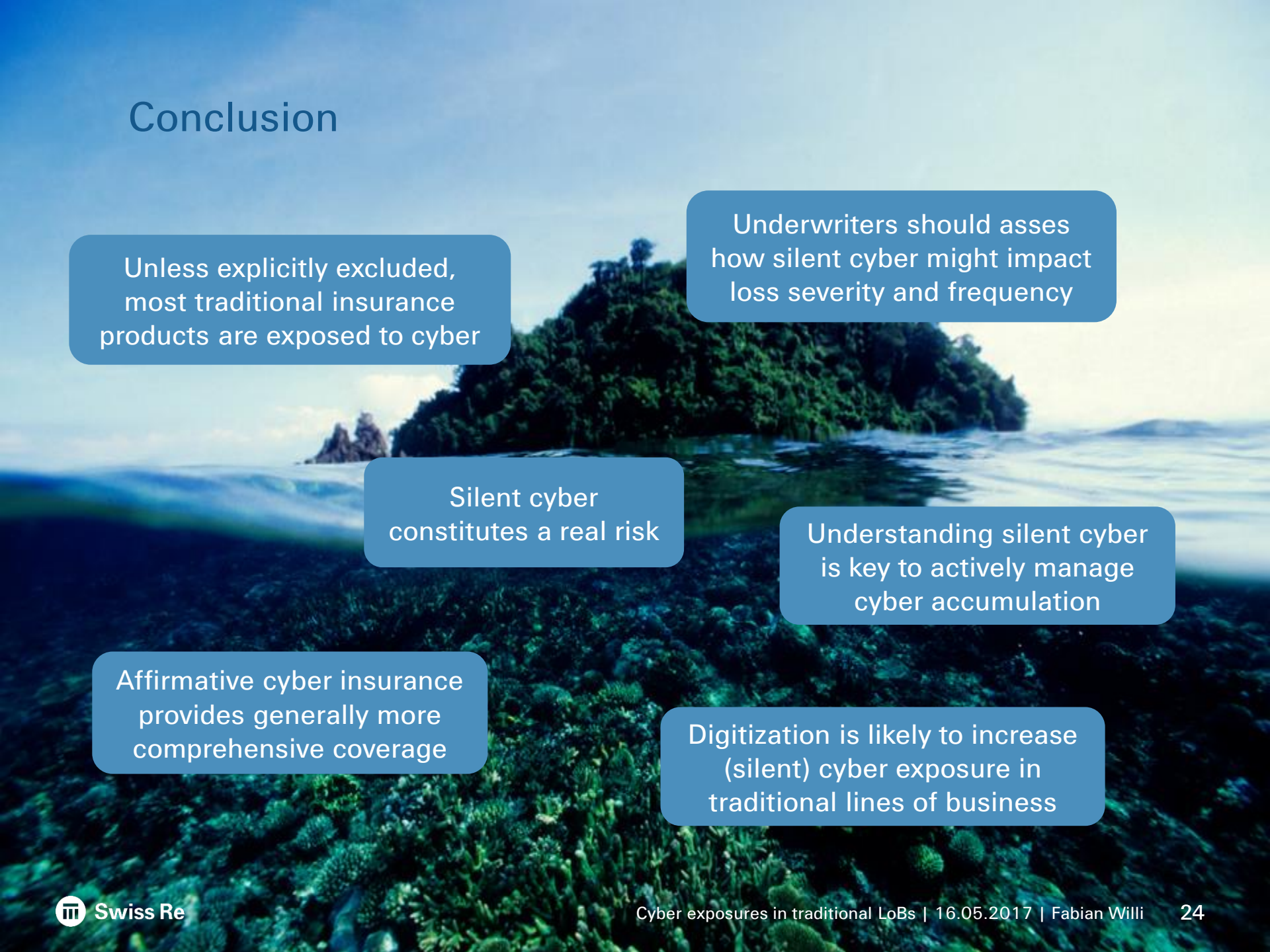
Consequences:

- Bodily injury
- Property damage
- Business interruption

Affected lines of business:

- General Liability
- PI/Medical Malpractice
- D&O
- Property
- Product Liability
- Product Recall

Conclusion



Unless explicitly excluded, most traditional insurance products are exposed to cyber

Underwriters should asses how silent cyber might impact loss severity and frequency

Silent cyber constitutes a real risk

Understanding silent cyber is key to actively manage cyber accumulation

Affirmative cyber insurance provides generally more comprehensive coverage

Digitization is likely to increase (silent) cyber exposure in traditional lines of business

Is your interest piqued?

Read more about cyber under http://www.swissre.com/library

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.