SCOR
The Art & Science of Risk

SCOR Annual Conference

Pushing the edges of risk awareness and insurance:
The role of the (re)insurance industry to cover risks affecting societies and governments including new applications of artificial intelligence

28 & 29 September 2017

SCOR
The Art & Science of Risk

SCOR Annual Conference
28 & 29 September 2017

Cyber risks, where we are

Sébastien Héon, Deputy Chief Underwriting Officer, SCOR Global P&C

AGENDA

1. **Evolution of Cyber Risks**
2. Evolution of the Cyber (Re)insurance market
3. Understanding Cyber Risks

Cyber risks: What we said in 2016

- Cyber risks has high impact and likelihood, above terrorist attacks and not so far away from large scale involuntary migration!

Denis Kessler
(quoting the WEF Global Risk Report)

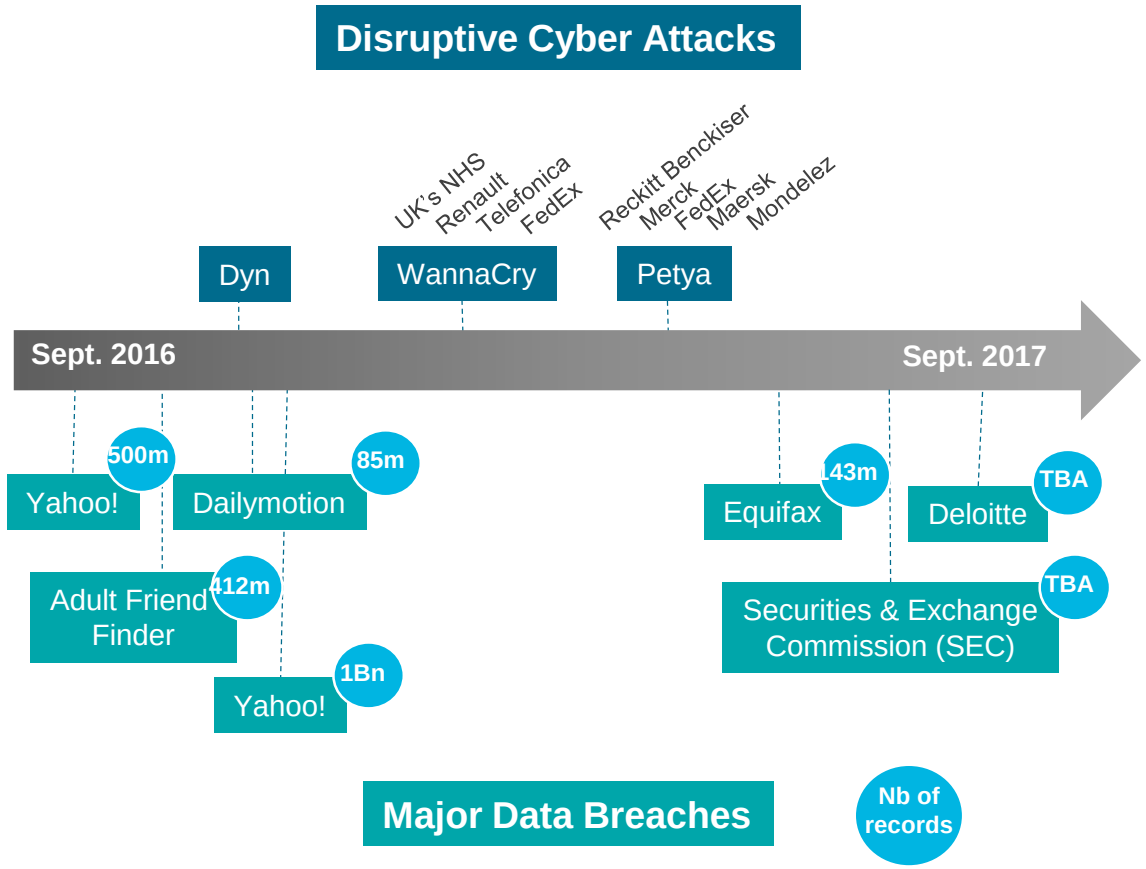
- Risks are increasingly connected and ubiquitous: technology everywhere
- Risks are increasingly systemic: same technology standards used globally
- Blurred time and space boundaries change risk accumulation and aggregation patterns (easy to cross borders online)

Victor Peignet

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

Didier Parsoire / Sébastien Heon

Recent Cyber attacks evidenced disruptive potential - Data Breaches remain significant



Key take-aways

- SCOPE
  - Cyber is not only Data Breach / Privacy liability
  - Manufacturing / industrial accounts are also impacted, worldwide
  - Geopolitical tensions are a risk driver
  - Accumulation

- SEVERITY
  - Some companies impacted by Petya issued profit warnings
  - Several companies released Petya impact on earnings in the range of $100m - $300m

> Mondelez International, maker of Oreo cookies and Cadbury chocolates, estimated the attack would shave three percentage points from second-quarter sales growth because of disruptions to shipping and invoices. The US company's net revenues were $6.4bn in the first quarter.

Source: Financial Times – 7 July 2017

AGENDA

1 Evolution of Cyber Risks

2 **Evolution of the Cyber (Re)insurance market**

3 Understanding Cyber Risks

The (re)insurance market: What we said in 2016

- 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

c.$500m ▪ Cyber insurance capacity available on the Market

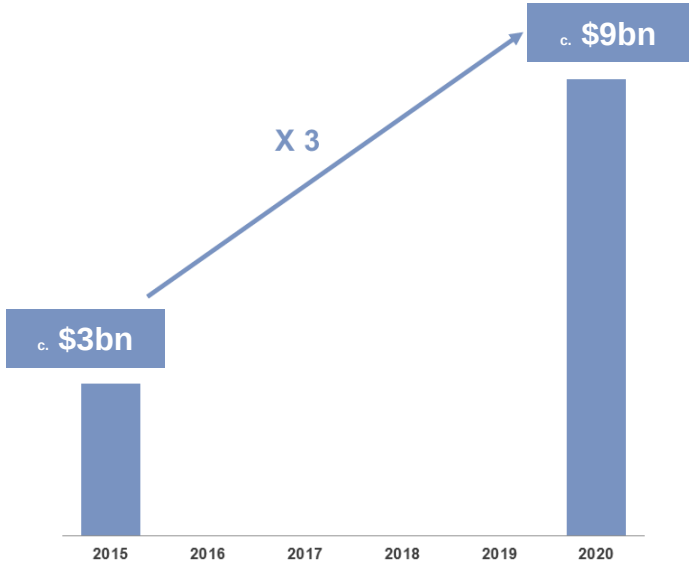
A Great Diversity of Cyber cover purchase:

Cyber Exclusion write-back / Cyber Endorsement

Cyber Standalone Policy

Cyber + E&O Bundled Policy

Comprehensive Cyber Package



The (re)insurance market: What we see in 2017

Stability of insurance capacity & reinsurance structure – Market growth as expected

- Insurance capacity remains overall stable – carriers more cautious in allocating capacity
- Some large programs (ca. $600m) have been placed in the US
- Take-up rate increases and expands now to manufacturers & utilities
- However, the SME market remains challenging
- Cyber insurance premium – depending on how you count! - reach $1.35 billion in 2016, +35% from 2015 - *source: Fitch Ratings and A.M. Best*
- A vast majority of reinsurance treaties remains QS

Unclear purchase pattern results in cyber exposure scattered in different insurance policies

- Risk Managers adopt a large variety of response to cyber exposure: exclusion write-back; cyber extension to standard policies; Cyber standalone, comprehensive Cyber product (encompassing 1st/3rd party cover for tangible risks)
- Some companies buy several of these solutions resulting in overlaps
- Wordings show unpreparedness / lack of maturity in front of reality of Cyber perils : Cyber extensions “Frankenstein-ed” in Property contracts which creates … strange creatures (e.g. misalignments in definitions)
- Reinsurers face the challenge of identiying exposures in various treaties

AGENDA

1 Evolution of Cyber Risks

2 Evolution of the Cyber (Re)insurance market

3 **Understanding Cyber Risks**

Understanding cyber risks: What we said in 2016

Structuring cyber insurance products and developing tools are challenges requiring cyber knowledge and out-of-the-box innovation

"Value of intangible assets is now a greater proportion than is the value of tangible assets for rich nations"
Global Intangible Financial Tracker 2015

- Intangible assets growing and vulnerable
  - Human Capital
  - Hacking of computer systems, software or code
  - Reputations & brands
  - Theft of intellectual property or trade secrets

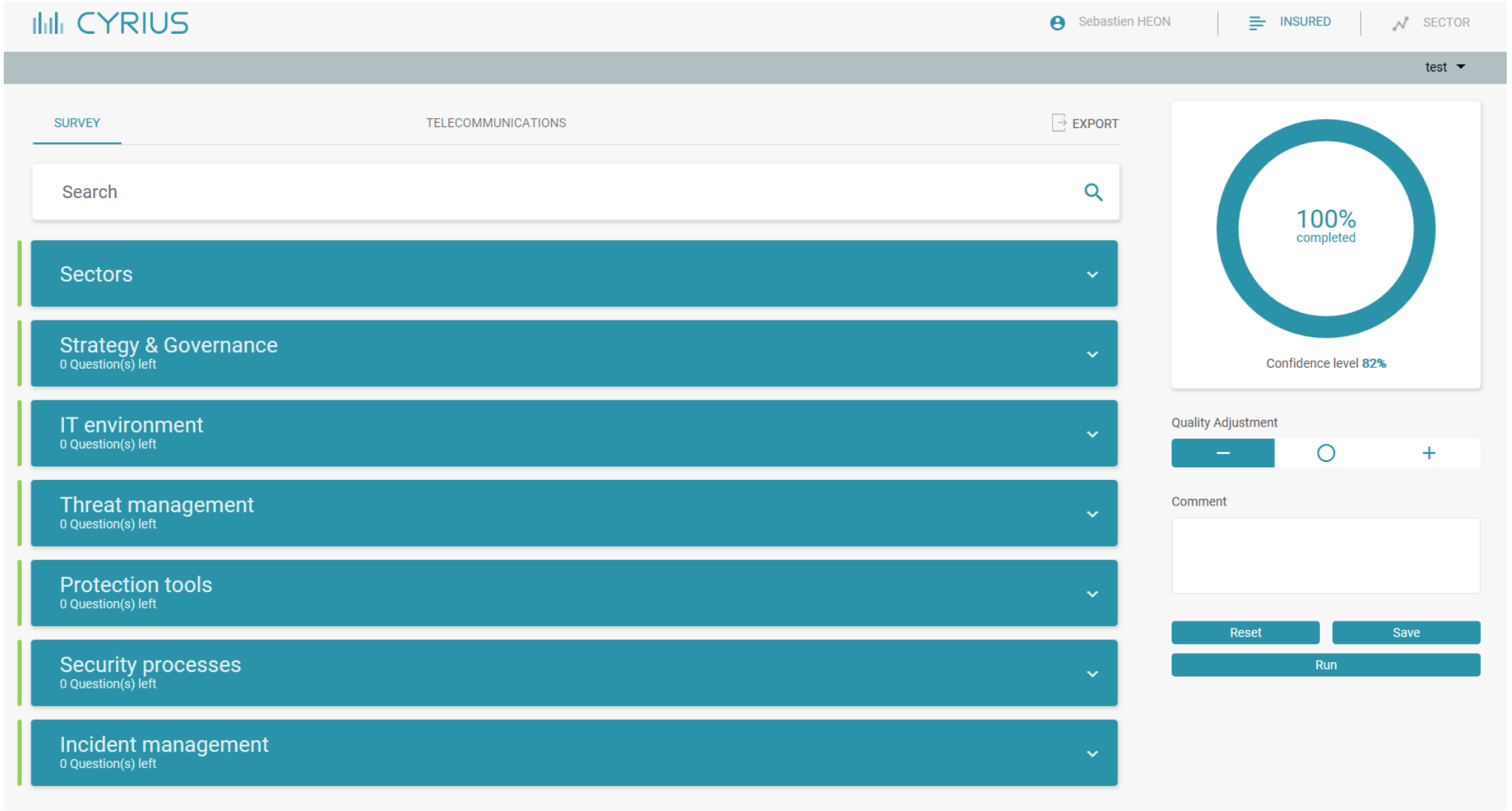
Cultural change required, too

- Multi-dimensional / cross-class approach
- Attract talent, including from outside the industry
  - Cultural adaptation
  - Career paths
- Interconnectedness and complexity requires modelling improvements
  - Historically models addressed physical events with defined geographies
- Predictive analysis, not experience rating
  - Requires access to data
  - Confidentiality issues

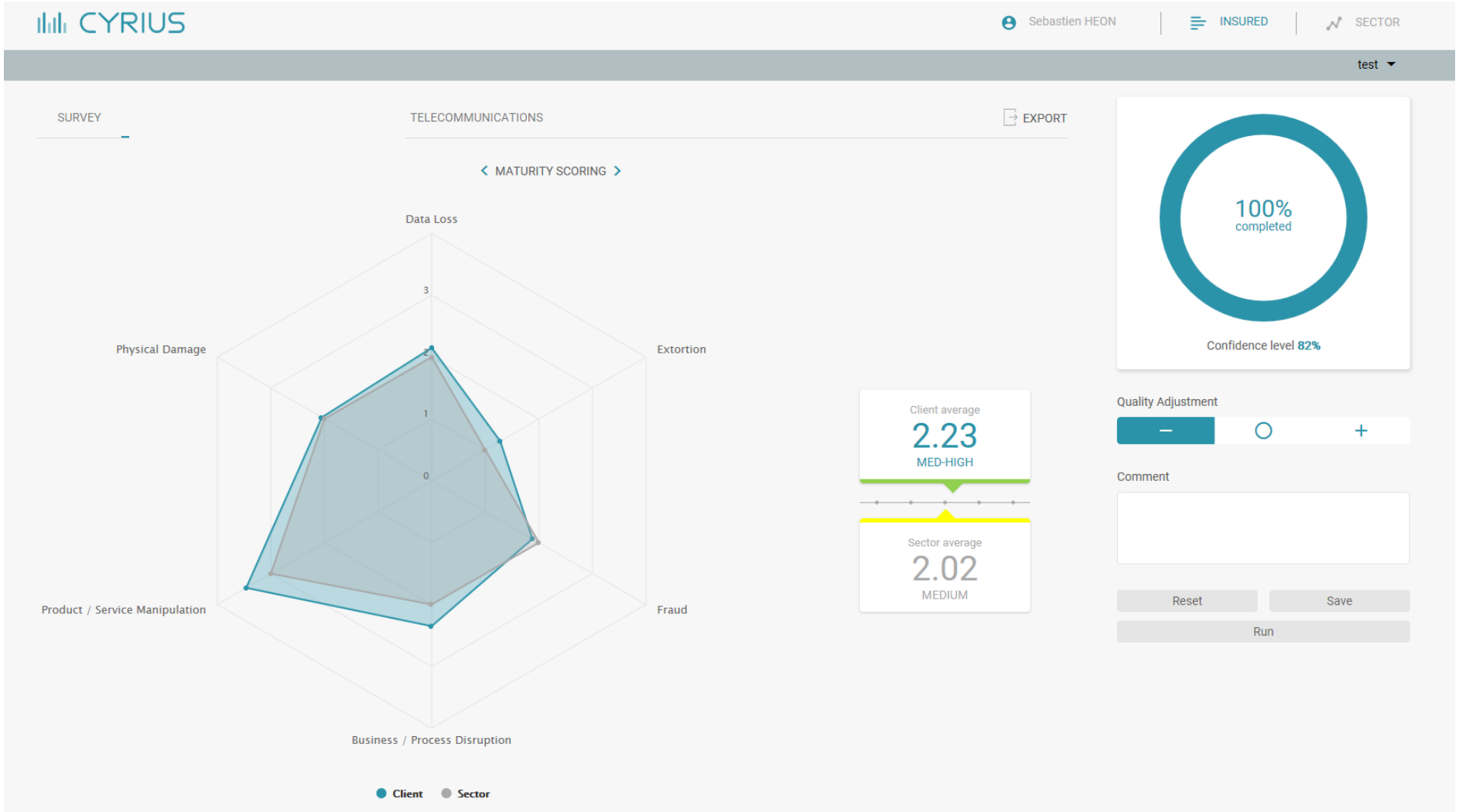
But from an insurer's point of view, given our limited knowledge of consequences, we are talking much more about unknown risk than known risk.

There is an amazing lack of actuarial data.

Understanding cyber risks: An example of what we have done



Understanding cyber risks: An example of what we have done



As a Lead reinsurer, we contribute to the improvement of the whole Cyber Chain to collectively build a sustainable Cyber (Re)insurance Market

Addressing challenges at each step of cyber risk management and risk transfer

Brokers

Insureds

- Exposure analysis & scenarios
- Risk reduction & transfer strategy

Insurers

- Matching demand and offer in a competitive environment
- Risk selection
- Streamlining wordings & programs
- Pricing

Reinsurers

- Aggregation modeling & control
- Development of proper reinsurance offer
- Pricing