ISSUES OF THE DIGITAL REVOLUTION. BETWEEN GPDR AND CYBERATTACK: GADGET, THREAT OR OPPORTUNITY? ELEMENTS OF RESPONSE THROUGH THE INSIGHT OF AN INSURER

CIRIEC – 1er juin 2018

Valerie Kriescher

ethias

What is considered as a cyber attack ?

- Data loss
- Cyber extortion / ransomware
- “Fake CEO” fraud
- Business/industrial process disruption or misuse without physical damage
- Cyberattack leading to physical damage
- Products and services manipulation

How should companies react?

According to “Fortune” magazine, intangible assets represent 80% of companies’ value.

First step : having a dedicated person (a CCSO – Chief Cyber Security Officer) in charge of cybersecurity for all facets of the company at the highest level of the organization.

Second step : defining a cybersecurity strategy through analysing the risks (what are the possible targets ? What attacker profile ?)

Third step : everybody in the company should be involved and trained (a cybersecurity governance should be settled)

Fourth step : the necessarily resources have to be identified and implemented (e.g. : building a surveillance centre or use external service providers)

The regulatory landscape in Europe has evolved :

Under the new European Union (EU) General Data Protection Regulation (GDPR) which took effect in 25th may 2018, European companies will face significant fines if they fail to protect data.

Firms must also be able to purge an individual's details from their systems if that information is no longer relevant or necessary, which can be difficult if data are fragmented across organizations and/or there is limited visibility on information held externally.

⇒ **Companies could face serious financial and legal consequences of non-compliance.**

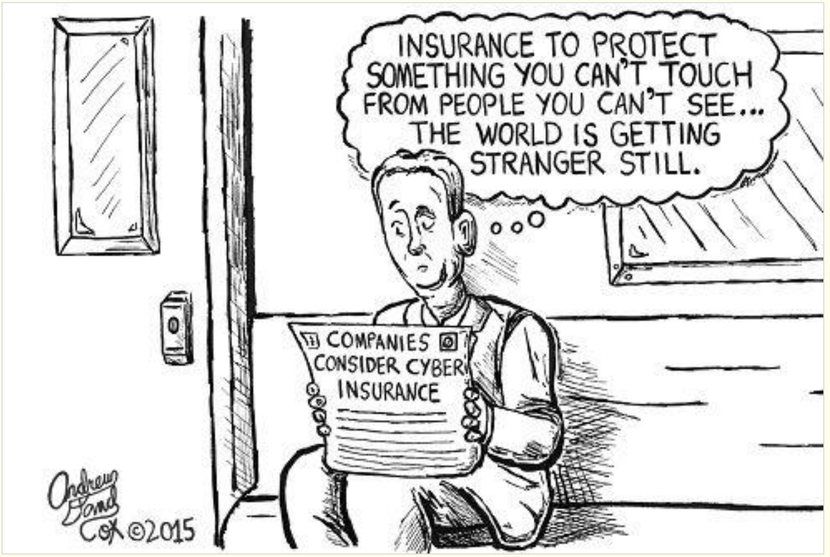
⇒ **The need of being insured for these expenses increases (like it happened in the US)**

How reacted the insurance industry ?

There are different options offered to the clients :

1) In some cases, cyber risks are covered in “silent form” by traditional policies

(for example : fire or explosion caused by a cyber attack, medical malpractice caused by loss of data as a consequence of a cyber risk, etc.…),



2) The clients can ask to extend the coverage of their existing property or liability policies by:

- Removing the cyber exclusion from the property policy or the general liability policy;
- Purchase an extension to the property policy (for example) in order to cover restoration costs or business interruption without physical loss

3) The companies can subscribe a cyber-stand alone policy (or bundled with an E&O policy)

Standalone products emerged in the US in the mid/late 1990s, evolved from professional liability policies,

Overview of cyber insurance products

Cyber-specific policies provide usually three main types of guarantees :

1. First-party coverages:
   - Restoration or rebuilding of lost data;
   - Costs of recollection;
   - Cyber extortion;
   - Fraud;
   - Business interruption (but without material damage) following a cyber event.

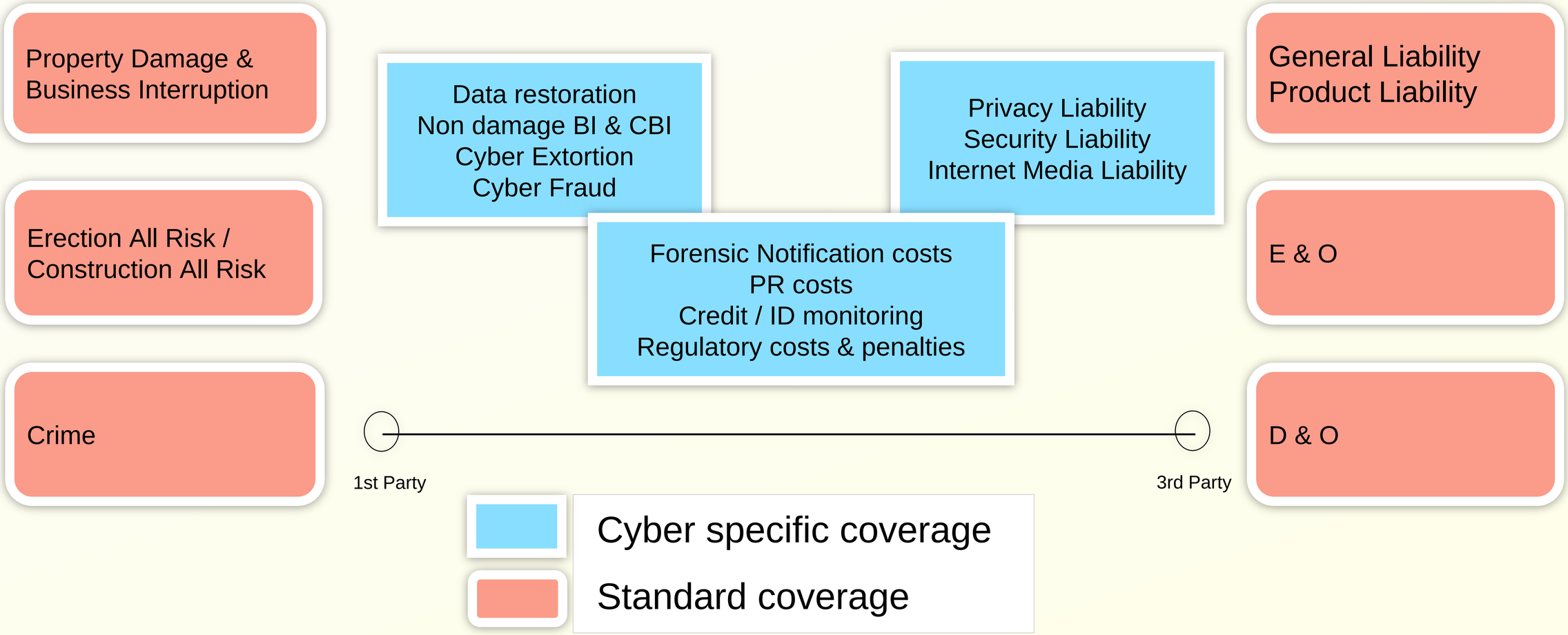
Overview of cyber insurance products

2. Liability coverages:
   - Privacy liability arising from the loss or theft of personal data from third parties;
   - Liability for the lack of notification of the personal data breach;
   - Liability for any damage caused to third parties due to misuse or breach of security of a company's IT system;
   - Internet media liability.

3. Costs and services:
   - Forensic and investigation costs;
   - Public relation costs;
   - Notification or assistance to the individuals subject to breach of personal data
   - Regulatory inquiries (sometimes including defence costs and penalties)

It's not unique as a product : it's a bundle of product recall coverage, kidnap & ransom, crime/fraud policy, business interruption and replacement costs in a property policy and E&O cover…..but :

How reacted the insurance industry ?



Overview of cyber insurance products

Cyber-specific policies – what pricing ?
Insurers are facing a lack of actuarial data

- We only know the cyber-attacks targeting companies which accepted to report…and only those being aware of it.
  => very little knowledge about the actual or potential consequences of a given cyber attack
- No official information (besides from mandatory reports of data breaches, and especially the lost of personally identifiable information)
- There are no generally accepted underwriting standards
- There are no standards for risk management

⇒ cyber pricing is very disjointed across insurers, probably because of different rating tools and limited historical loss data

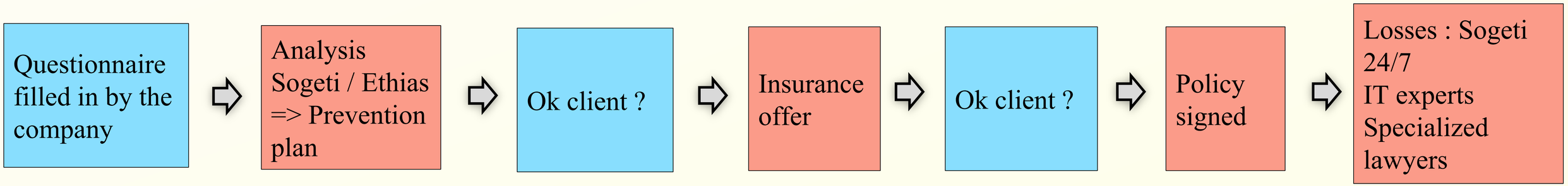
Cyber-specific policies – particularities?

Some insurers designed their cyber standalone policy as a totally new & different insurance product, offering additional services of a cyber security firm together with the cyber coverage.
That’s the choice Ethias made, and we chose Sogeti to assess the risk and help us in the claim handling.

Overview of cyber insurance products

Cyber-specific policies – particularities?

As Ethias does (e.g. below), a number of insurers have chosen for a complete service to the client, adding Prevention and Claims handling to insurance, in partnership with an IT/Cyber risks specialist and a specialized law firm :

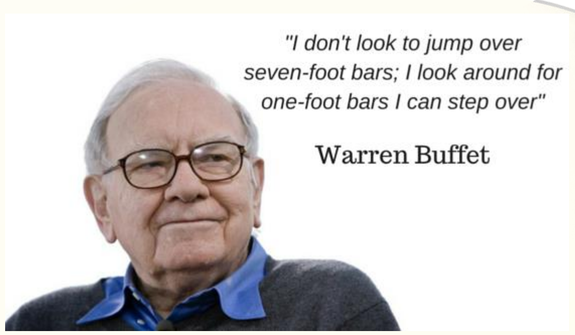


Overview of cyber insurance products

Cyber-specific policies – capacities ?

Dedicated cyber insurance typically provides core protection against data and network security breaches and associated losses, with capacity limits ranging from around 100.000 € to 100 million €. Most policies are written on a “claims-made and reported” basis meaning that claims must be notified to the insurer during the policy period, or at most within 36 months of policy expiration.

The reinsurers are cautious…



Berkshire Hathaway won't be a pioneer in cyber insurance: Warren Buffett

5th May 2018 - Author: Steve Evans

Speaking at the annual shareholders meeting of his conglomerate Berkshire Hathaway Inc. today, Warren Buffett said that he doesn't believe anyone understands cyber risk well enough today, so his firm will not seek to be a pioneer in underwriting cyber insurance.

Cyber risks are seen as an enormous opportunity by many in the insurance and reinsurance industry, but not by Warren Buffett.

The so-called Sage of Omaha doesn't feel that cyber risks are understood well enough by the industry and he insinuated that there could be cyber mega-catastrophes to come.

He said that "cyber is uncharted territory," explaining that he expects the risk to increase, saying it's going to get "worse, not better."

He explained that cyber risk is becoming increasingly material and the threat which didn't exist just a decade or so ago is only going to increase in the future.

"I don't think we or anybody else really knows what they're doing when writing cyber," he's quoted by Bloomberg as saying.

While CNBC cited him as saying, "We don't want to be a pioneer on this," although Buffett said he understands the need to write some to remain competitive in the area.

But Berkshire Hathaway will not be the number one, two or even three in terms of exposure to the cyber underwriting market, Buffett said, suggesting he is happy to leave others to pioneer in cyber insurance and reinsurance.

"I think anybody that tells you now they know in some actuarial way either what general experience is like in the future, or what the worst case can be, is kidding themselves," he explained.

Buffett cited challenges in policy wordings and the risk of clash between cyber events or contracts as two concerns, explaining that while Berkshire Hathaway has a good understanding of risks like hurricanes and earthquakes, cyber is a different challenge altogether.

Insurance & Reinsurance market – facts & figures

Most reinsurers & insurers have only just entered the market, which is therefore relatively small and concentrated.

Three insurers (AIG, Chubb and XL Group) reportedly have around 45% of the market in the US, and are also leaders for this product in Europe. That seems likely to change, however, with many insurers looking to expand their cyber protection capabilities. Half of the insurers questioned by a reinsurer who currently do not offer cyber insurance plan to do so in the next few years.

In summary, the cyber insurance market is growing strongly, but premiums and policy limits remain small relative to the value of the tangible and intangible assets that could be impaired by a cyber risk event.

According to a Aon/Ponemon study, only around 12% of information assets are covered by insurance, compared with 51% of property, plant and equipment.

Aon thinks that the European market could write between 0,5 and 1 billion USD in premiums by 2020.

Sources : SCOR, Swiss Re, AON