MARSH

SOLUTIONS…DEFINED, DESIGNED, AND DELIVERED.

CYBER INSURANCE & CYBER RESILIENCE

Qu’est-ce qu’une cyber-assurance ? Comment peut-elle protéger mon entreprise ?

Guillaume Del Pizzo
Client Executive
MARSH LUXEMBOURG

Anne-Sophie COPPENS
Cyber Practice Leader
MARSH BELGIQUE LUXEMBOURG

MARSH & McLENNAN COMPANIES

Que sont les risques informatiques ?

Attaque malveillante **Evénement accidentel**

Système informatique y compris toutes ses **Données**,

Interne & **Externe**

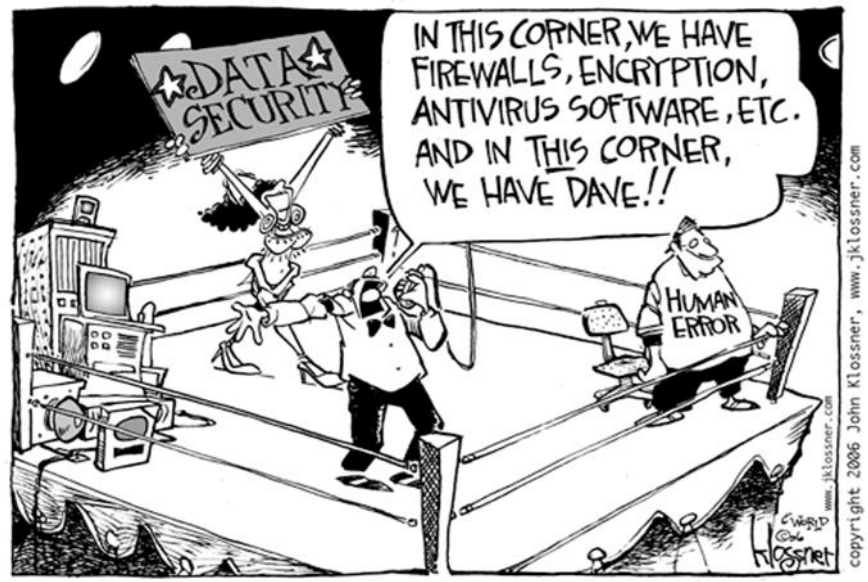
Impact opérationnel

Confidentialité Et/ou **Intégrité** Et/ou **Disponibilité**

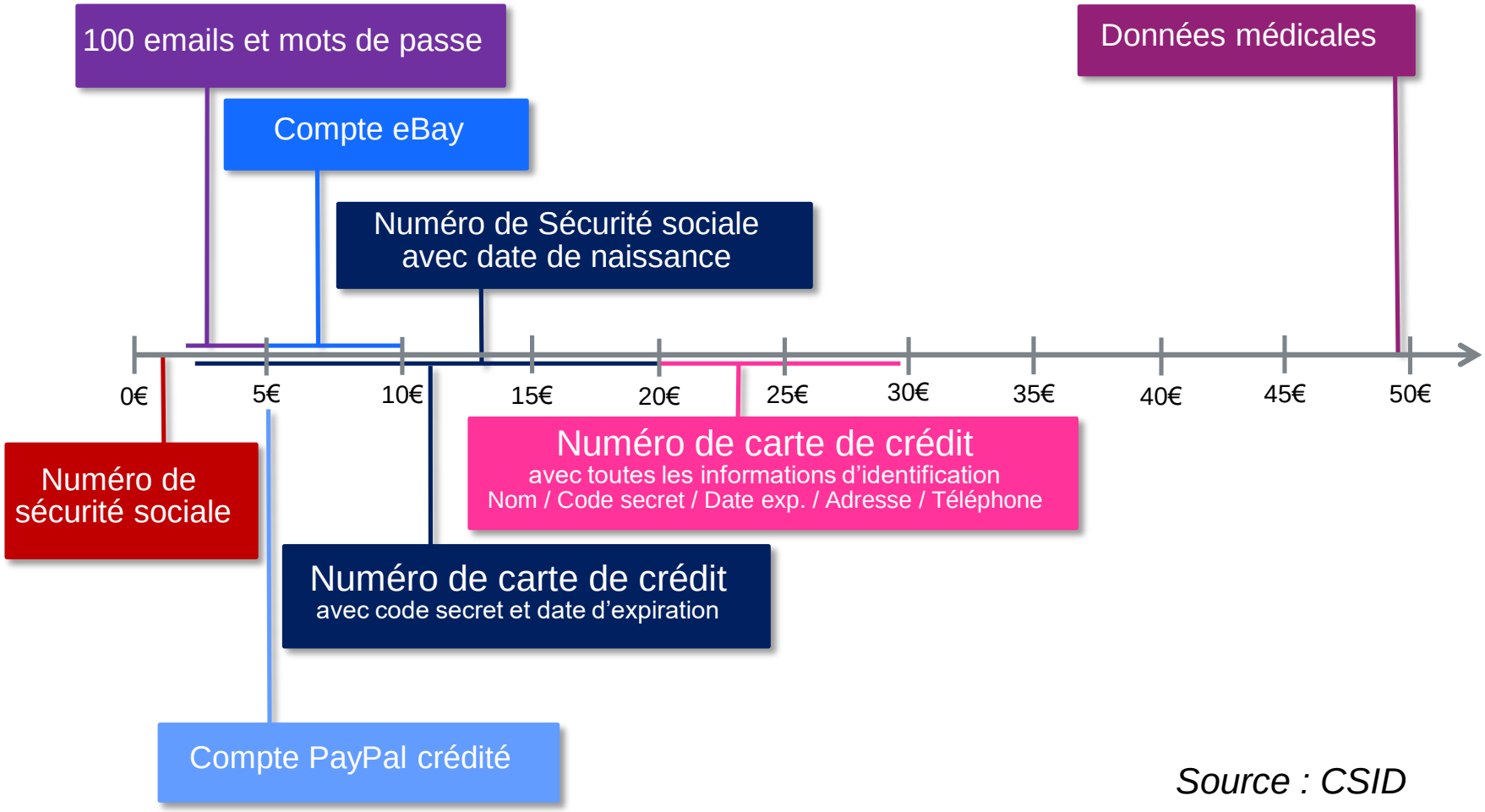
Impact financier

Perte de chiffre d'affaires	Frais et dépenses	Réclamations	Actifs

#WeAreDave


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 John Klossner, www.jklossner.com
www.jklossner.com
Klossner

Focus **confidentialité** : Estimation de la valeur marchande de données volées par un hacker

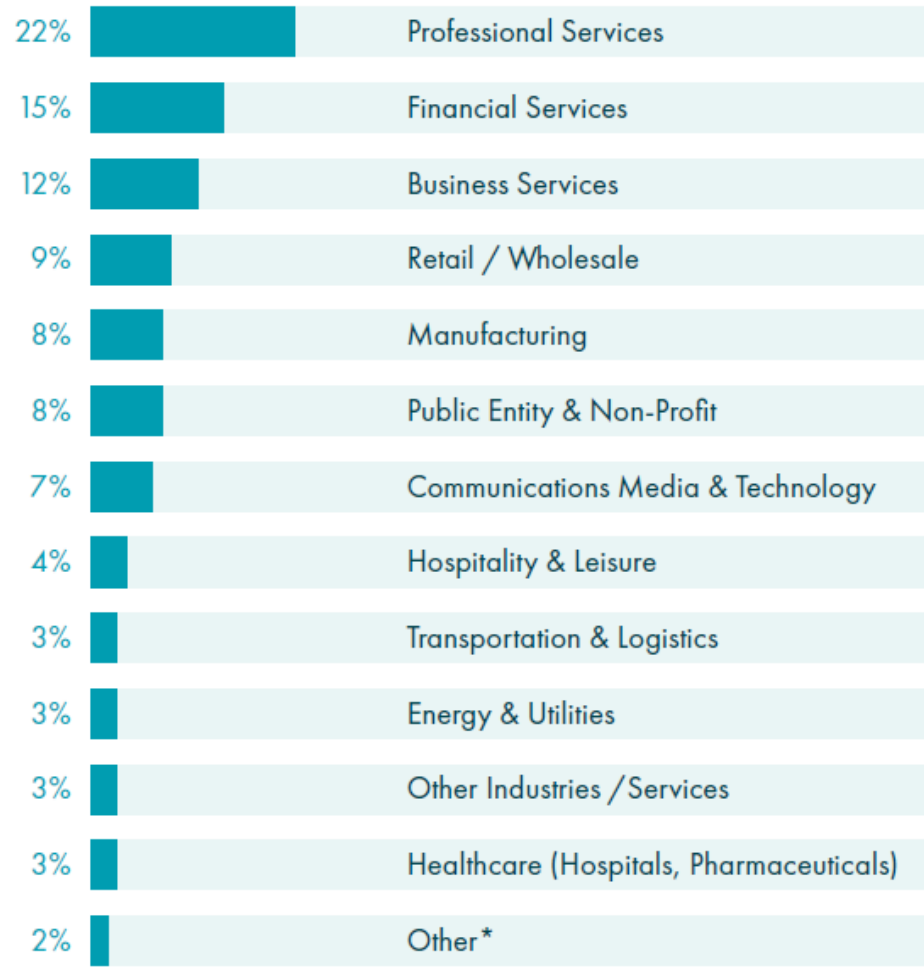


Source : CSID

Quelles types de société peuvent être confrontées aux risques Cyber?

Quelques Chiffres par industrie

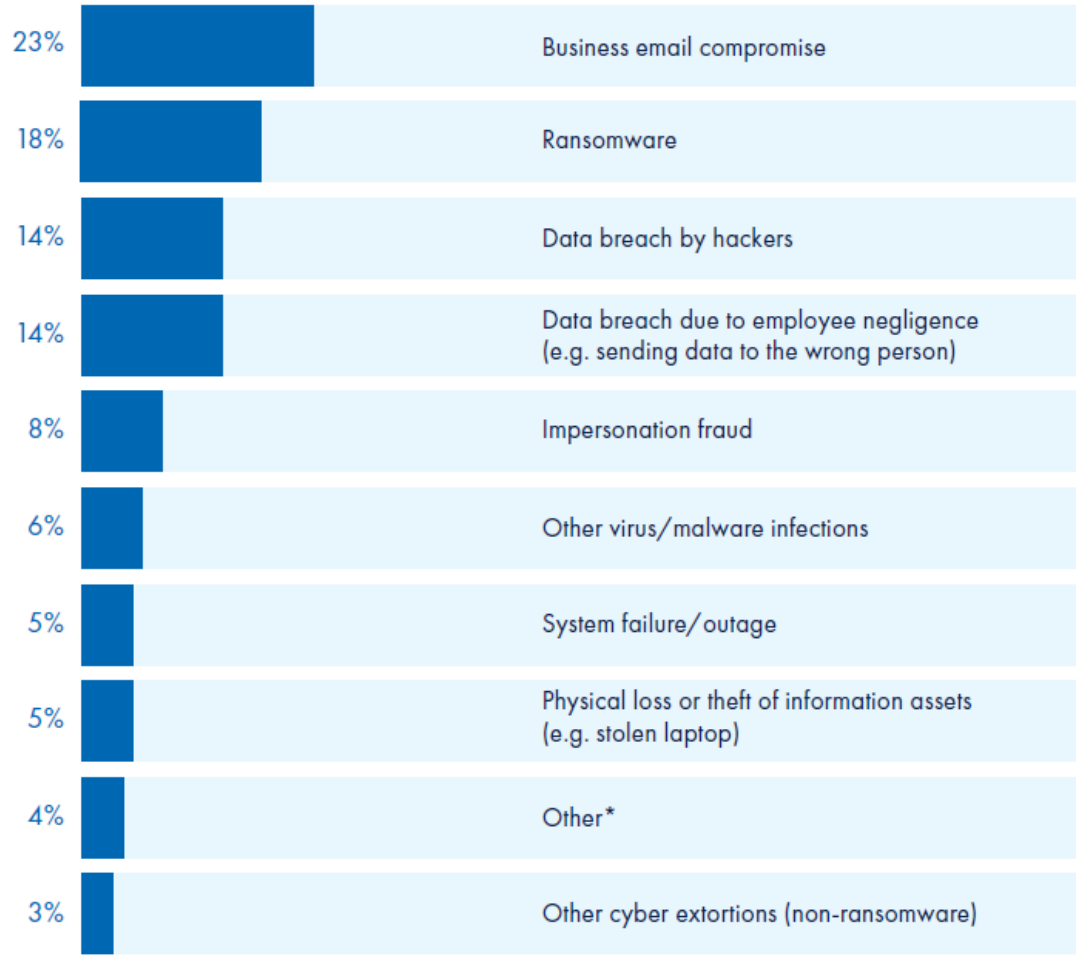
Cyber claims reported to AIG EMEA in 2018



*Food & Beverage, Construction, Education

Quels types d'incidents?

Cyber claims reported to AIG EMEA in 2018



*Denial of Service Attacks, Legal/Regulatory Proceedings based on violations of data privacy regulations

En quelques mots…

Les conséquences des cyber-attaques peuvent être importantes voire dramatiques. Il est indispensable de mettre en place des moyens de gestion de crise et être capable de les financer.

Ainsi, en complément des mesures en place, l’assurance Cyber vous offre une protection optimale. Afin de vous offrir le meilleur du marché, nous avons créé nos propres « Polices d’assurance Cyber » basées sur une couverture « Tous Risques Sauf ». Ceci permet au client d’avoir un texte simple, efficace et écrit à son avantage.

Nous limitons au maximum les sous-limites et les exclusions au strict minimum.

Les éléments déclencheurs de l’assurance Cyber sont l’Atteinte malveillante, l’Atteinte à la confidentialité des données personnelles et l’Evènement accidentel.

Cyber insurance a necessary tool in the cyber risk management process

AVOIDANCE
CYBER PREVENTION

MITIGATION
CYBER SECURITY

FOCUS ON FREQUENCY

TRANSFER
CYBER INSURANCE

ACCEPTANCE
CYBER ASSESMENT

FOCUS ON SEVERITY

DEFENSE, DEFENSE, DEFENSE

Gestion des risques Cyber

- **Understand**
  - Provide **cyber context** within a **business perspective**.
- **Measure**
  - Quantify the **financial impact** of cyber exposures.
- **Manage**
  - Actionable steps to **secure**, **insure** and **recover**.

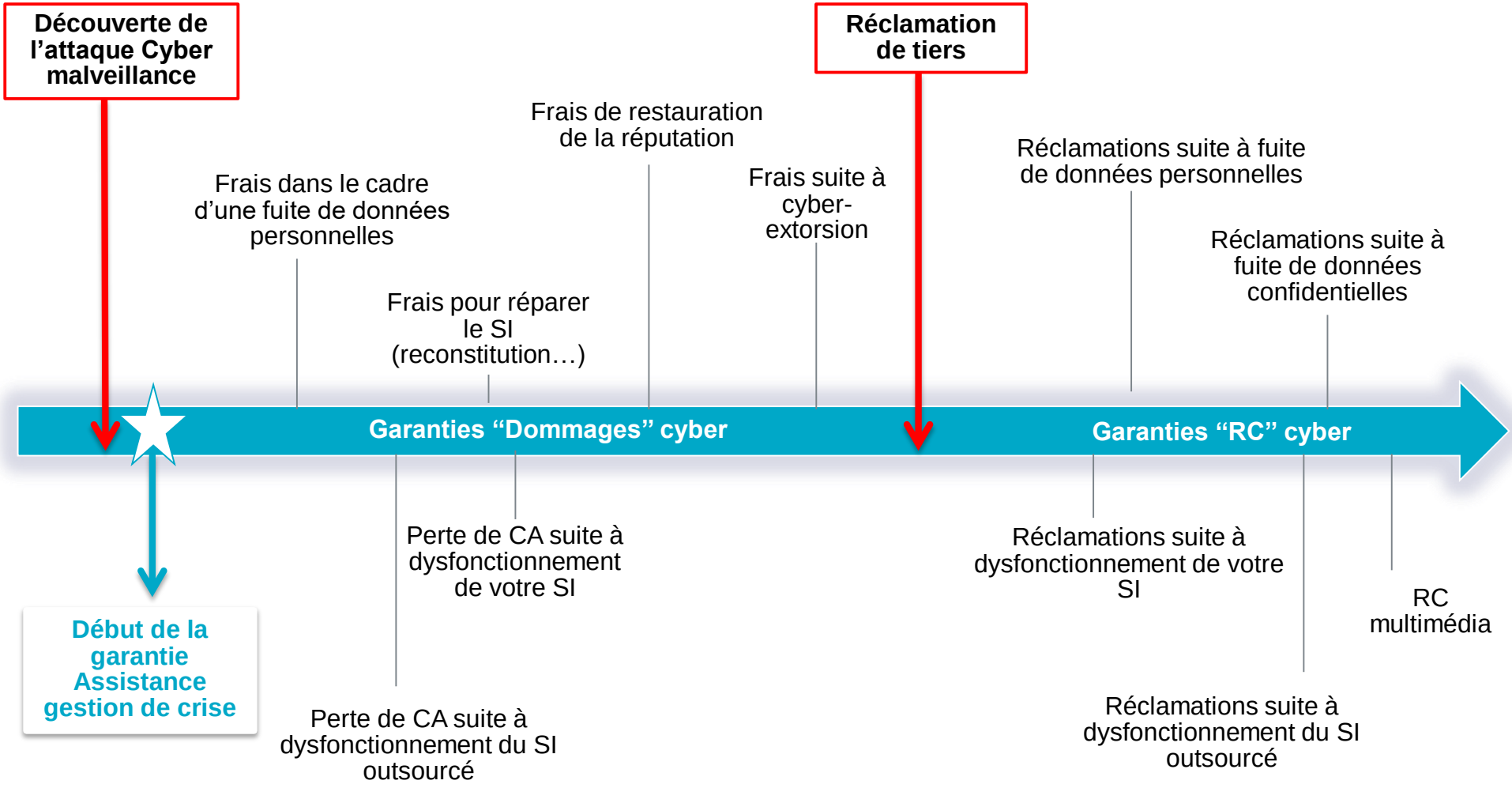
Nos outils pour objectiver le montant de garantie nécessaire

benchmark : afin de savoir ce que des sociétés comparables achètent en termes de couverture cyber (Limite / Franchise).

NotPetya: Cet outil permet de calculer les conséquences financières d'une attaque telle que NotPetya. Cet outil se base uniquement sur le chiffre d'affaires de la société et non sur son activité.

Cyence: Cette outil permet de mesurer le risque informatique d'après des données en Open-source.

Business Case N°1
Focus sur les couvertures – cyber assurance



Les Principales Garanties et Exclusions

LES COUVERTURES

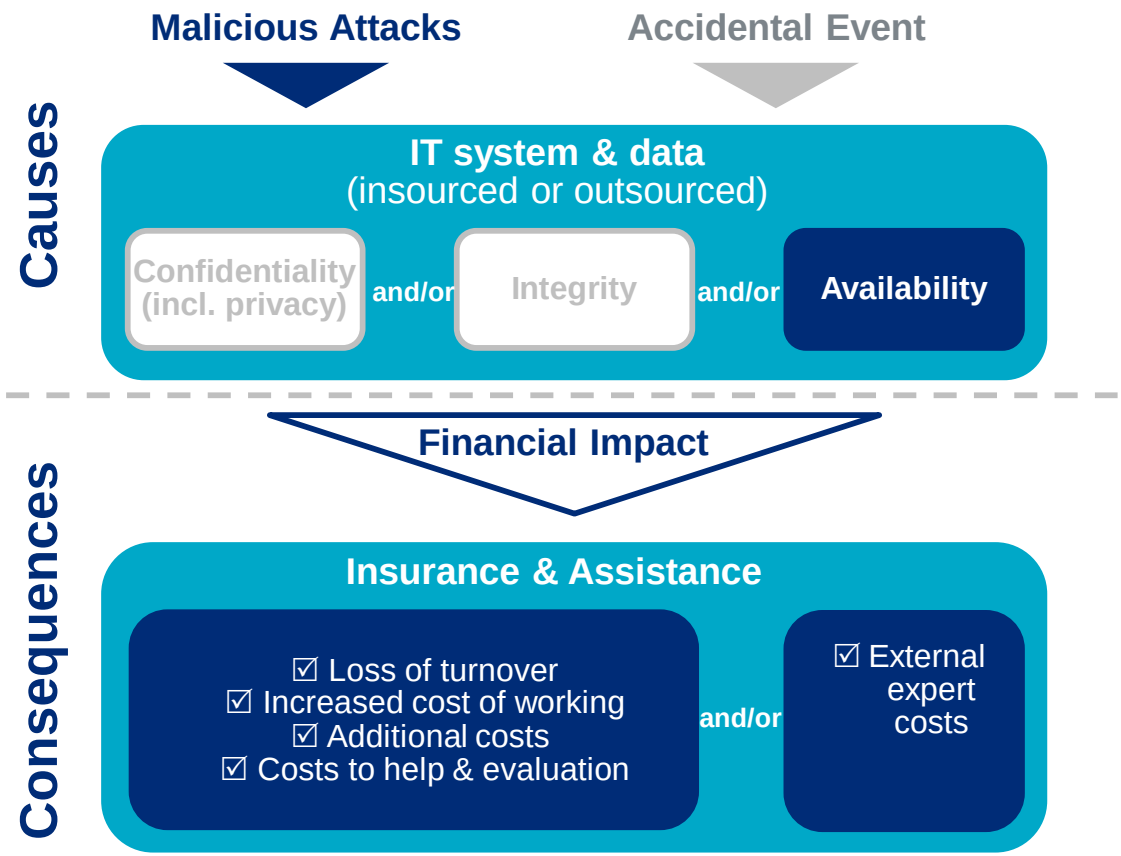
- Assistance et Gestion de crise
- Frais d'un expert en sécurité informatique
- Frais d'assistance juridique
- Frais de notification
- Pertes d'exploitation
- Frais d'assistance en matière de réputation
- Frais de communication de crise
- Cyber-Extorsion
- Responsabilité Civile
- …

LES EXCLUSIONS

- Faute Intentionnelle de l'assuré (la société, pas les employés)
- Passé Connu à la date d'effet du contrat
- Fraude: perte de fonds, détournement -> à couvrir dans une assurance **Fraude / Crime**. Cfr présentation ci-après.
- Responsabilité Civile Professionnelle
- Acte de violence* – Tout sinistre occasionné par la Guerre et/ou les Attentats. Cette exclusion ne s'applique pas aux Sinistres occasionnés par le Cyber-terrorisme.
- …

* *Suite à l'attaque NOTPETYA et la réaction polémique de ZURICH US sur une police Property, nous avons redéfini dans nos Polices la définition de Cyber-Terrorisme afin qu'elle soit la plus large possible.*

Business case N°2
Eurofins – Ransomware attack – June 2019

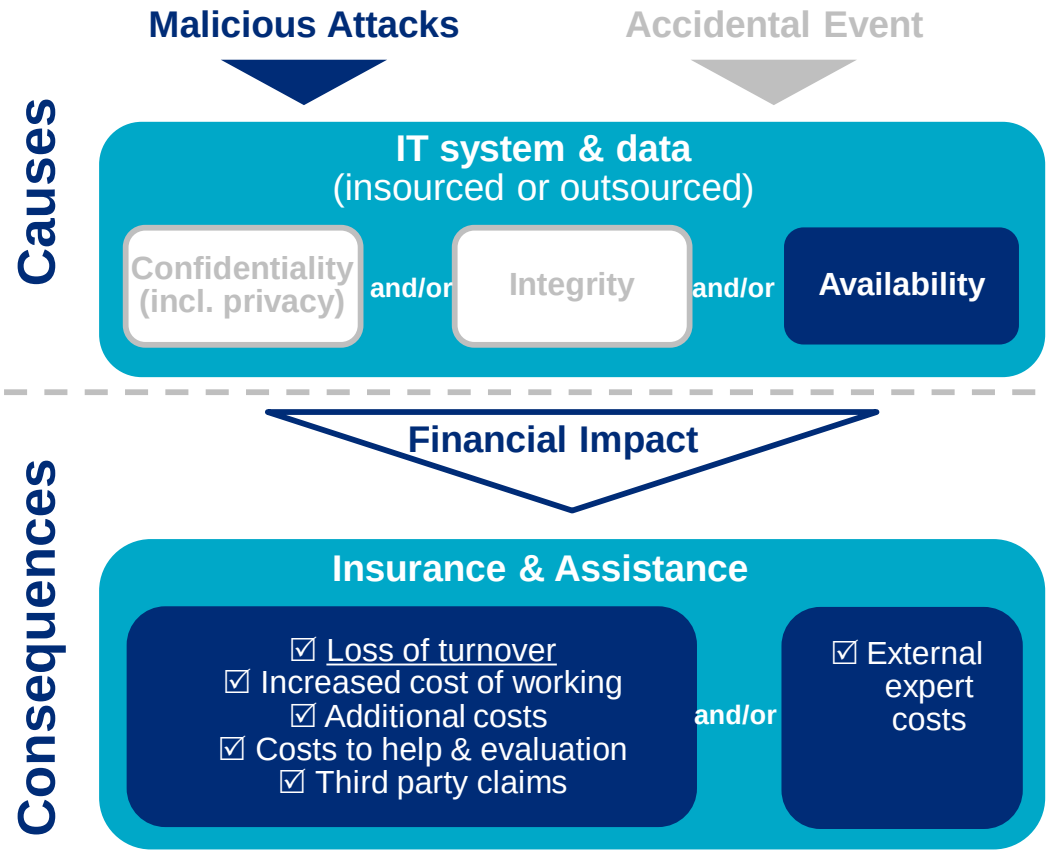


Comments

"The exact revenues and profits that were lost during the month of June will unfortunately never be known exactly. As can be judged today (29/8/2019), estimates based on extrapolation of year-to-date May 2019 growth figures, or taking into account July growth, lead to a range of values with an average impact of **EUR 62M** on revenues "

"Eurofins being fortunately well insured, it could well be that the full missing margin caused by this criminal act will be compensated by its insurers. **Coverage has been confirme**d and discussions about exact determination of damages will be on-going for some months" *

Business case N°3
Maersk (container ship) – Denmark – Ransomware - (NotPetya, 2017)



Comments

"We had to reinstall an entire infrastructure"
"It took **ten days**"

"We had to install 4,000 new servers, 45,000 new PCs, 2,500 applications" *

"We only had a 20% drop in volume, so we managed 80% of that volume manually"

"The damages caused by NotPetya to be between $250 and **$300 million**" *

Cyber risks, un sujet C-Suite

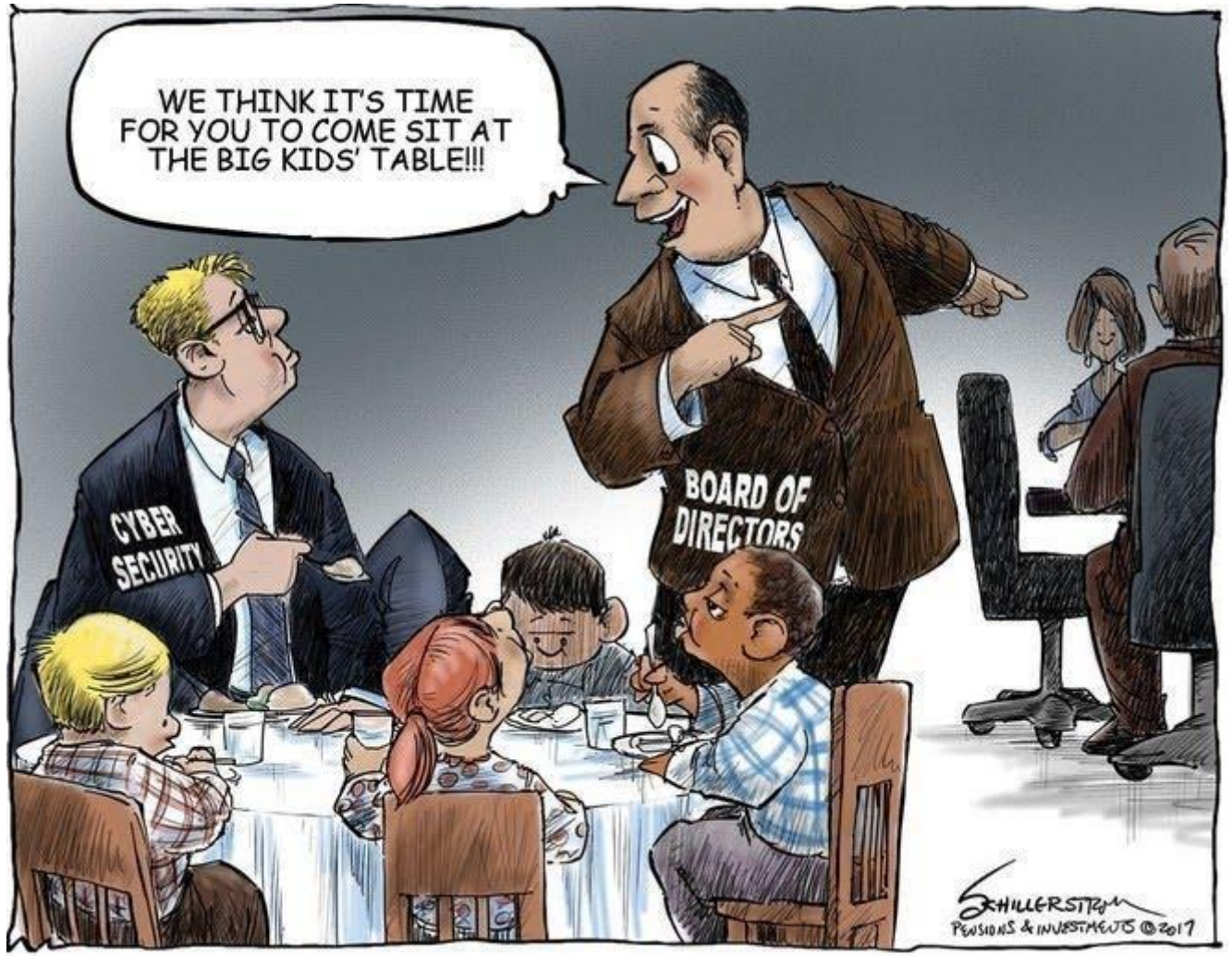
Dans tous les sinistres Cyber importants, la police **D&O** (responsabilité des Dirigeants) a été déclenchée avec comme raison principale que le Management n'avait pas suffisamment investi dans la sécurité informatique. Ainsi, l'assurance Cyber est un moyen pour les dirigeants de montrer qu'ils ont pris des mesures afin de réduire l'impact d'une attaque informatique contre l'entreprise.

De plus, il est possible que certains de vos clients vous demandent un **certificat d'assurance** cyber (RFP).

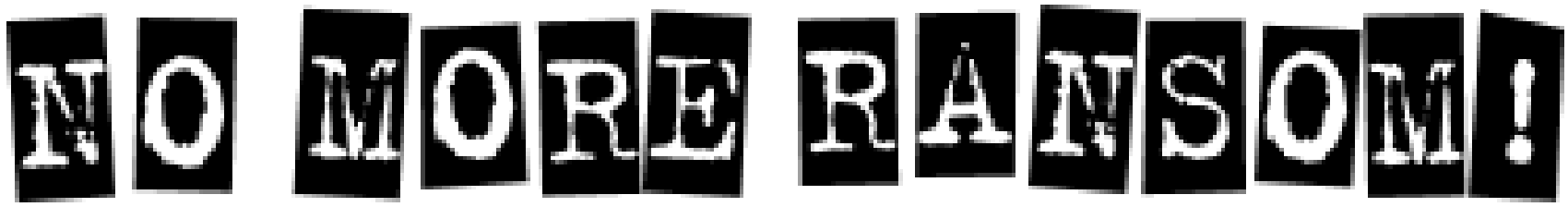
Enfin, certaines **agences de notation** prennent en considération la sécurité informatique pour noter les entreprises.

Sans oublier les situation de **fusion-acquisition** où l'aspect sécurité informatique fait désormais partie des volets analysés en plus des autres paramètres de santé financière d'une société.

SECURITY & BUSINESS



Besoin d’aide pour libérer votre vie numérique sans avoir à payer?



https://www.nomoreransom.org/

MARSH

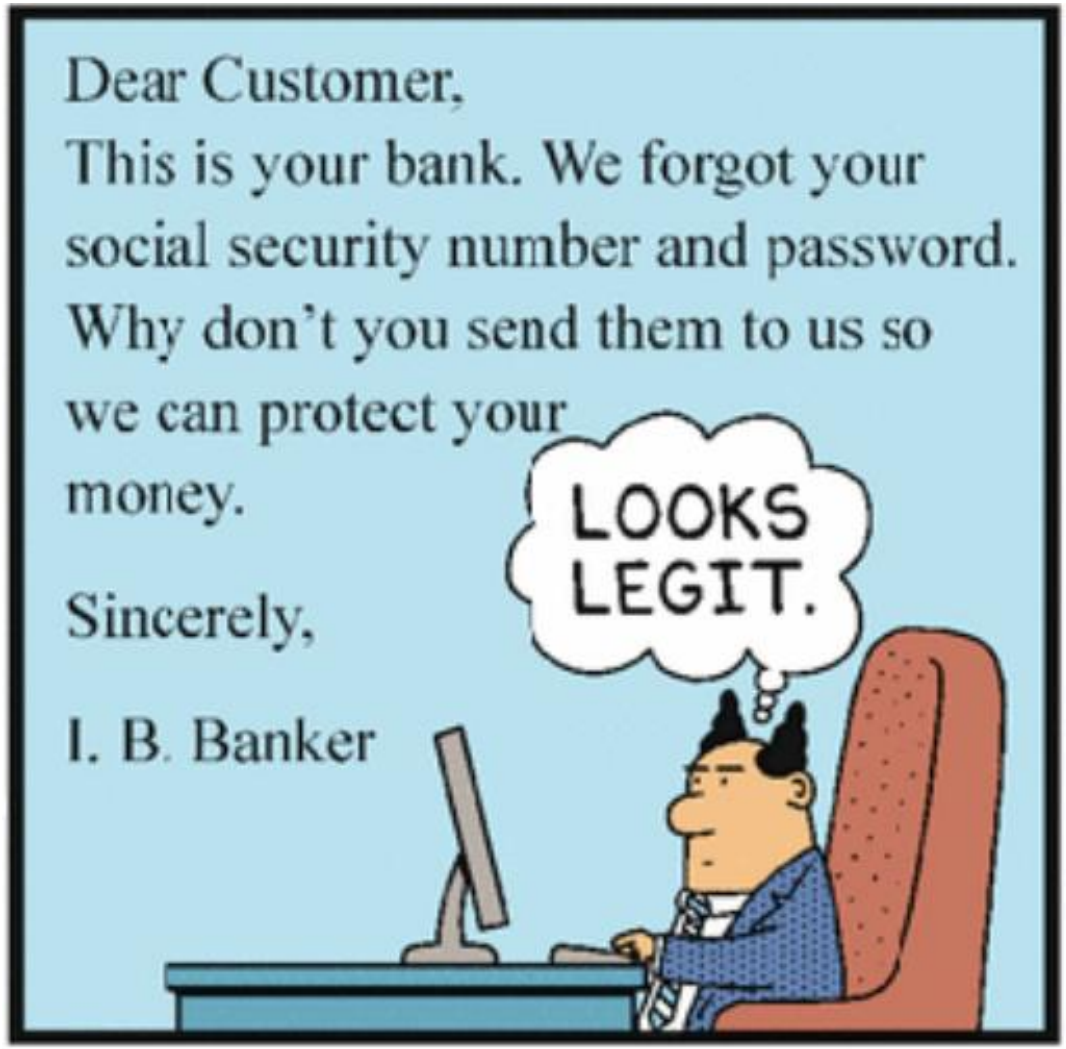
SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

Assurance Fraude et l' "arnaque au faux president"

Anne-Sophie Coppens

MARSH & McLENNAN COMPANIES

Changing nature of Crime insurance claims



Changing nature of Crime Insurance claims

Social Engineering: A Fraudulently Induced Funds Transfer loss received and acted upon by an Insured employee caused by someone purporting to be:

Employee or Officer

Ex: A criminal convinces an employee in the Finance Department to electronically transfer money for a "secret" M&A deal, a tax payment, or a "war chest" to help save jobs at a money-losing subsidiary

Vendor

Ex: Claiming to be a business vendor, a criminal sends an official-looking email requesting a change to the account where payments are sent

Client or Customer

Ex: A social engineer poses as a wealthy client and persuades a business manager to transfer $3 million

Why purchase a Crime insurance cover?

- Annual claims surveys indicate a higher trend of fraud
  - at companies of all size
  - recovery rate is low
  - severity has increased
- Higher risk profile at
  - mergers and acquisitions
  - decentralising
- New sophisticated fraud techniques as social engineering
- Balance sheet protection
- Prevention on its own is simply not sufficient
- The human factor…

What does a Crime insurance cover?

- Coverage for loss sustained where discovery occurs during the Policy Period
- **What type of fraud?**
  - **Internal Fraud** (employee dishonesty acting alone or in collusion with other)
  - **External Fraud** (acts of frauds by others, e.g. extortion)
  - Acts of **Computer misuse** by others (e.g. introduction of malicious codes, impairment of computer programs, fraudulent electronic funds transfer, etc.)

What does a Crime insurance cover?

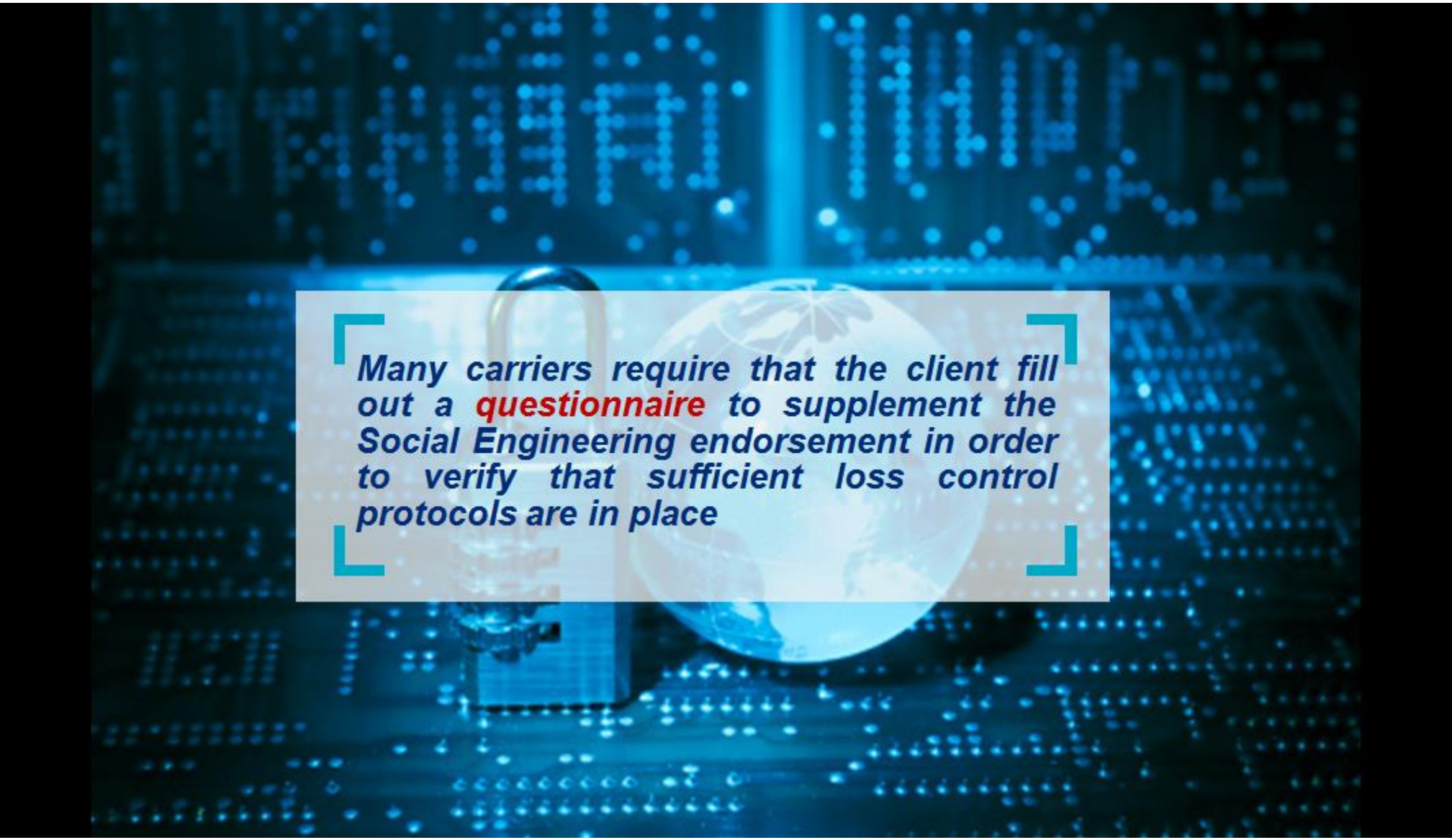
- **What type of impact?**

  - Direct financial loss + expenses (investigation/legal costs, claims preparation)

  - Physical loss, damage to, destruction of or disappearance of property

- ! **Fraudulent electronic fund transfer** is to be covered by a crime policy and not the aim of a Cyber policy
  - A sublimit may be provided under the Cyber policy
  - Cover under Cyber only when there has been an actual intrusion in the IT network of the victim

Social Engineering Endorsement Questionnaires



Underwriting of Impersonation Fraud cover

- Specific endorsement for affirmative Impersonation Fraud cover
- Obligations put forward by insurers on verification of payment instructions can be different from carrier to carrier
- Check any exclusions related to Impersonation Fraud
- Dedicated and limited number of insurers
- Capacity per insurer from 5 to 15M EUR

marsh.lux@marsh.com

+352 49 52 38