ORGANIZED BY

FIWARE

SUPPORTED BY

GUARD

cyberwatching.eu
The European watch
on cybersecurity & privacy

Emerging challenges in cyber risk assessment and management

Paolo Roccetti

Head of cybersecurity research unit

Engineering R&D Labs

Setting up the context

what is cyber risk?

how to properly assess it?

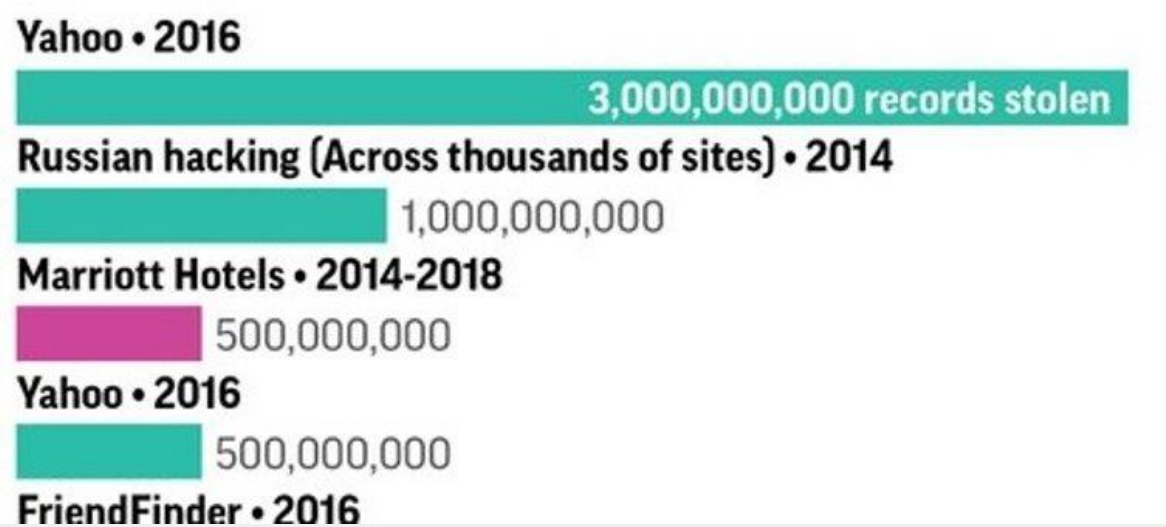
how to effectively manage it?

Defining cyber risk

“the potential of loss or harm related to technical infrastructure or the use of technology within an organization” (RSA)

“the risk of depending on cyber resources, i.e., the risk of depending on a system or system elements which exist in or intermittently have a presence in cyberspace” (NIST)

Marriott International data breach (2018)



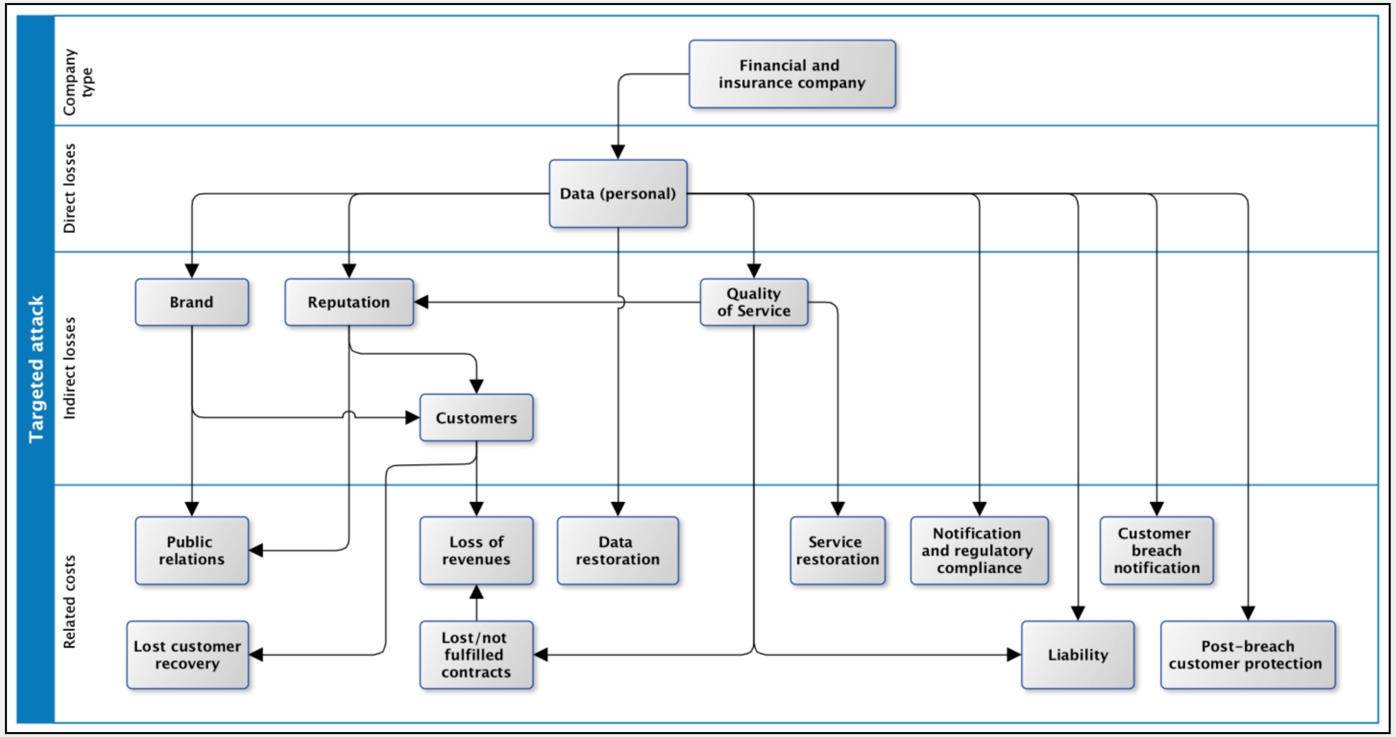
discovered after 4 years (ouch!)

estimated cost of 23 M$ (fines)

mostly covered by the cyber insurance

+ 1 year of endpoint protection subscription to each affected client (100$ each)

Challenge #1 – Estimating cyber risks on intangibles



HERMENEUT project (www.hermeneut.eu)

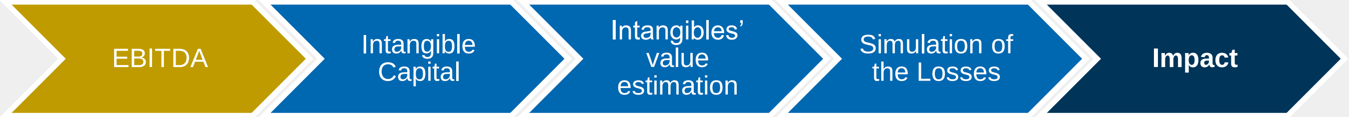
define intangibles: Reputation, Human capital, Intellectual properties, Data

consider the domino effect (cascading risks) from IT/OT on intangibles

reliability of current models (top-down and bottom-up)

Challenge #1 – Estimating cyber risks on intangibles

Top-down approach



- From Balance sheets

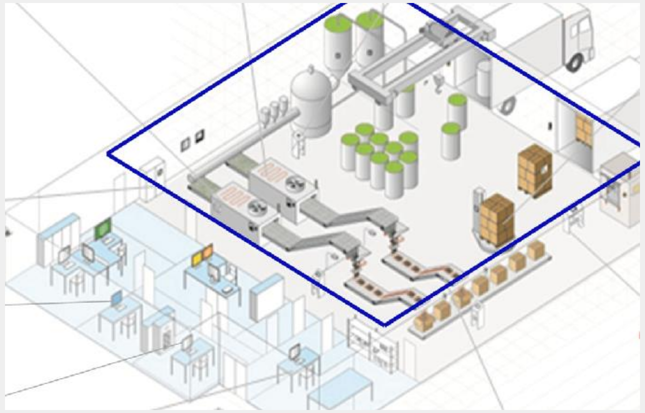
- Economic performance
- Intangible Driving Earnings

- Splitting of the intangibles:
  - Intellectual Property
  - Key Competences
  - Organizational Capital

RATING

Bottom-up approach

PrOTectME project (Protecting Operational Technologies of Medium Enterprises from Cyber Risks)



ENGINEERING

Assessing Social Engineering risks

as part of ENG contribution to the **CyberSec4Europe initiative**

phishing simulation targeting a large LPA (~5k targets)

balancing the hook, the target set, the date/time of the simulation

collecting SW fingerprints

anonymizing results

and then, the real challenge...

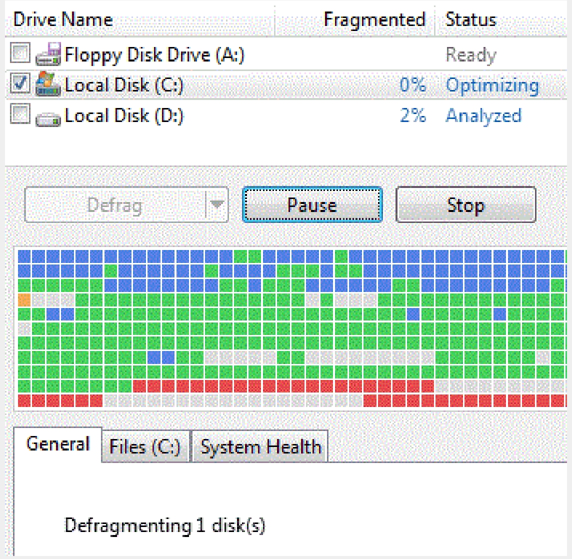
CyberSec4Europe initiative (https://cybersec4europe.eu/)

Challenge #2 – «defrag» your approach to cyber risks

different levels: Physical, OT, IT, human (incl. SE), organizational, supply-chain, sectoral, …

different methodologies: internal-vs-external, black-,white-, grey-box, …

different providers



Drive Name	Fragmented	Status
□ Floppy Disk Drive (A:)		Ready
☑ Local Disk (C:)	0%	Optimizing
□ Local Disk (D:)	2%	Analyzed

Defragmenting 1 disk(s)

Cyber Security for Europe

CyberSec4 Europe initiative also includes a roadmap for a progressive cyber risk management approach (in the context of smart cities)

Colonial Pipeline attack

[COLONIAL] «proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, ...»

classical double-extortion scheme

potential impacts to both sides of the supply chain: providers and distributors

impacts goes well beyond economic ones

[Darkside] «... goal is to make money and not creating problems for society »

Challenge #3 – «Assess globally, manage locally»

by considering and quantifying also non-economic impacts: psychological, social, environmental, ...

by enlarging the set of stakeholders involved in the impact assessment process: supply chain / sector / cross-sectors

by considering stakeholder's conflicting priorities: confidentiality vs. Sharing needs, strict policies vs. business continuity

CitySCAPE

CitySCAPE project (https://www.cityscape-project.eu/) is experimenting on how to assess non-economic impacts on organization assets across multimodal transport cases

ENGINEERING

Challenge #4 – Estimate the effectiveness of cyber mitigations

ease ante-adoption estimation: simulation-based (montecarlo, genetic algoritms) and ML-based models are appearing

requires deep knowledge of the market and of the adopting organization

include also non-economic aspects in the measurement: usability-flexibility tradeoff, digital sovereignty implications

CitySCAPE

CitySCAPE project (https://www.cityscape-project.eu/) is experimenting on how to conduct ante-adoption assessments for specific mitigations

Key takeaways

Don’t forget things you cannot touch (intangibles)

Keep your approach to cyber risks consistent

Assess (the impact) globally, manage it locally

Estimate the effectiveness of cyber mitigations (ante and post)

ORGANIZED BY

FIWARE

THANK YOU FOR LISTENING!

Paolo Roccetti

ENGINEERING

SUPPORTED BY

GUARD

cyberwatching.eu
The European watch on cybersecurity & privacy