Cyber Risk: Quantification, Stress Scenarios, Mitigation, and Insurance

Laurent Devineau & Arthur Maillart, Detralytics

5th European
Congress of Actuaries
www.eca2024.org

About the speaker

- **Laurent Devineau –** *Innovation Lead, Detralytics*
  Laurent is Innovation Lead at Detralytics. Previously, Laurent held the position of R&D Director within major consulting firms during almost 15 years. Before joining Detralytics, Laurent was head of on-site reviews within the Internal Models team of the French insurance supervisor (ACPR).

- Detralytics supports companies in the advancement of actuarial science and help them to solve their challenges. We guarantee to go beyond traditional consulting, by offering a unique combination of academic expertise, deep career and market knowledge.

About the speaker

- **Arthur Maillart –** *Innovation Lead, Detralytics*

  Arthur is Innovation Lead at Detralytics. Before joining Detralytics, Arthur wrote his PhD thesis on interpretable machine learning. Over the past three years at Detralytics, Arthur has developed his expertise in non-life modeling.

- Detralytics supports companies in the advancement of actuarial science and help them to solve their challenges. We guarantee to go beyond traditional consulting, by offering a unique combination of academic expertise, deep career and market knowledge.

Agenda

- **Introduction**
- Portfolio composition
- Frequency model
- Volume of data compromised
- Focus on the business interruption
- Applications

Introduction

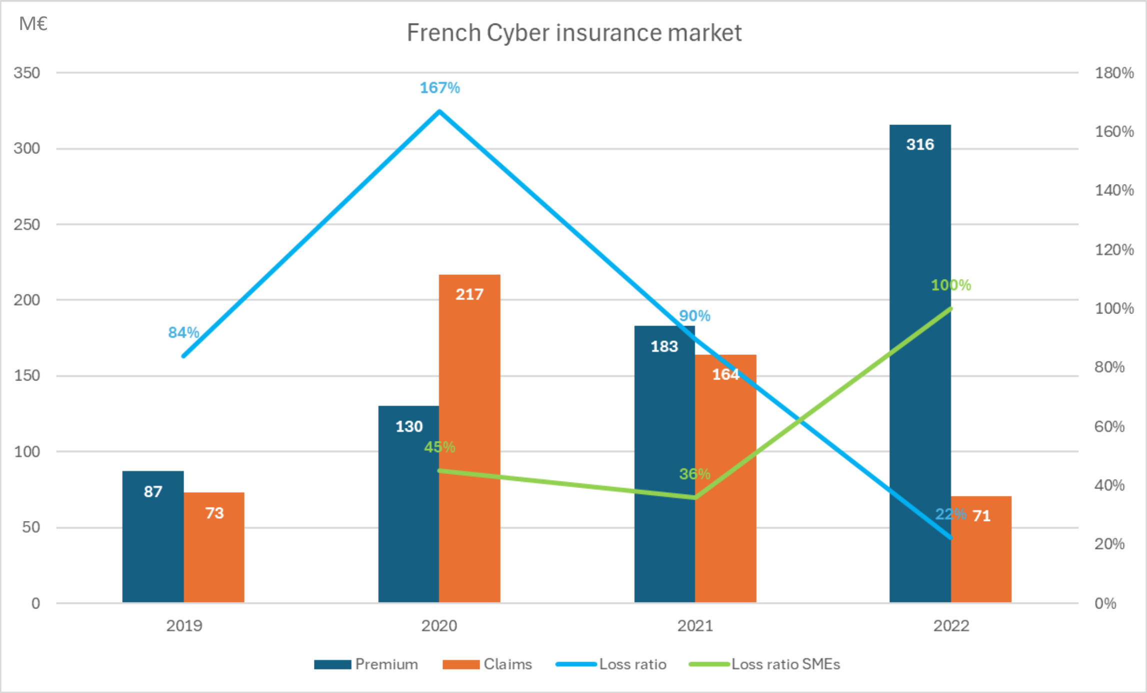
In full generality, cyber risk refers to a failure in the information systems leading to damages. This definition includes:

- Malicious events triggered by attacks from criminal groups:
  - DDoS, Ransomware, Data breach, Cryptojacking, …
- Non-malicious events
  - Accidental data leak, Accidental deletion of data,…

Here we focus on malicious cyber.

French market figures and context

- As time passes, the French cyber insurance market continues to evolve and exhibit notable differences.
- In 2020, 4 claims from large companies accounted for 65% of the year’s total claim amount. This shows that the French market is essentially driven by big companies.
- After 2020, insurers have opted for stricter conditions: higher premium rates and higher deductibles.
- This tightening of conditions reflects a lack of understanding of the risk.



LUCY report from AMRAE 2023:
https://www.verlingue.fr/app/uploads/2023/05/amrae-lucy-2023.pdf

Lack of data

Data exist, for example:

- **PRC** and **VERIS** databases document personal data leaks,
- Annual reports from **IBM** and **Hiscox** monitor risks,
- Annual reports **IBM, Flexera** and **Lloyd’s** document attacks on clouds and business interruptions,
- **NSFocus** 2022 report focus on DDoS.

Unfortunately:

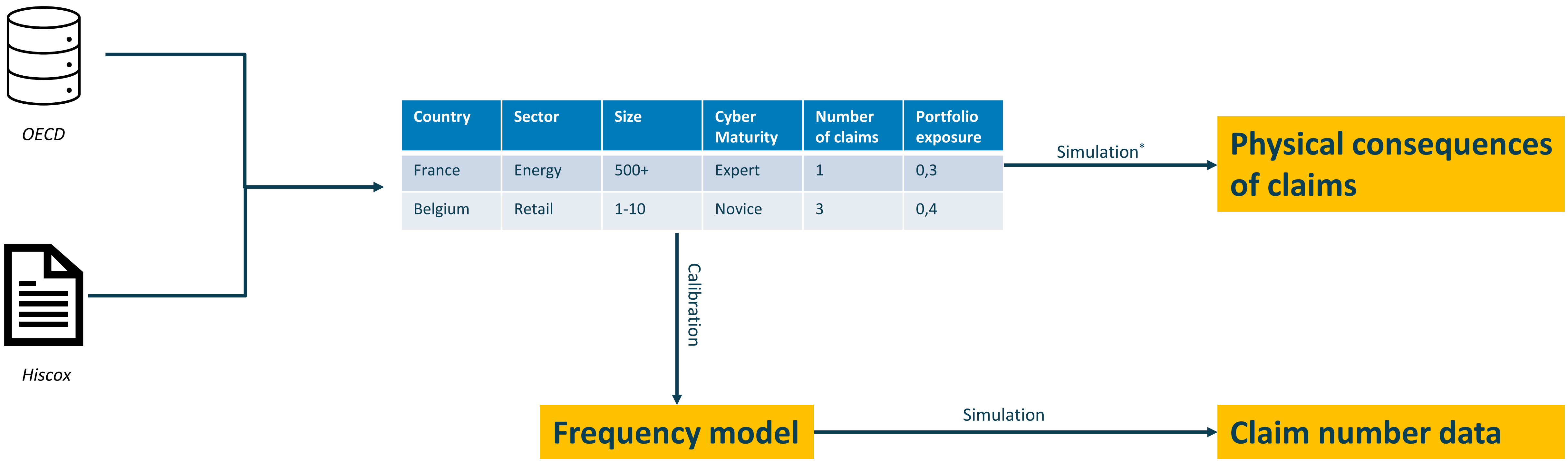
- Risks evolve rapidly and historical data can quickly become obsolete,
- Any database is potentially biased (US, big companies, …),
- It is difficult to extrapolate severity.

We have developed a package that allows to simulate data and quickly adapt portfolio composition, distribution parameters and severity functions.

Agenda

- Introduction
- **Portfolio composition**
- Frequency model
- Volume of data compromised
- Focus on the business interruption
- Applications

Modeling overview



Country	Sector	Size	Cyber Maturity	Number of claims	Portfolio exposure
France	Energy	500+	Expert	1	0,3
Belgium	Retail	1-10	Novice	3	0,4

[*] Functions implemented from the our litterature review.

Agenda

- Introduction
- Portfolio composition
- **Frequency model**
- Volume of data compromised
- Focus on the business interruption
- Applications

Target properties for the frequency model

Cyber-attacks tend to increase the claim frequencies for policyholders sharing common characteristics without systematically resulting in additional claims. Hence, we want in our frequency model that:

- Companies from the same country share a common random effect,
- Companies from the same sector share a common random effect,
- Companies from the same country and sector share a common random effect,

Generalized Linear Mixed Models offer a convenient way to model such grouping structure.

Frequency model

The number of claims N_i for the i-th policyholder is modeled using a Poisson random variable with mean parameter $\lambda_i = -\log(1 - p_i)$. The value p_i is taken as:

$$logit(p_i) = \alpha_i + \beta_0 + \beta^T \boldsymbol{X}_i + \Delta_{country,\, i} + \Delta_{sector,\, i}$$

- α_i a parameter fitted at policyholder level,
- β_0, β^T the fixed effects weights,
- $\boldsymbol{X}_i$ is the vector of covariates,
- $\Delta_{country,\, i}$ the coordinate of $\Delta_{country}$ corresponding to the country of policyholder i,
- $\Delta_{sector,\, i}$ the coordinate of Δ_{sector} corresponding to the sector of policyholder i

*p_i is easiest to calibrate from available data.

Types of attack

For each cyber event occurring in the simulated data, we need to define the type of attack. We denote by q the type of attack, and one (or more) entry point(s), denoted by v, except for DDoS attacks, for which we do not specify the entry point.

Type of attack q	Probability
DDoS	29.6%
Ransomware	17.6%
Loss of data (other than ransomware)	9.8%
Business e-mail compromise	30.8%
Other	12.2%

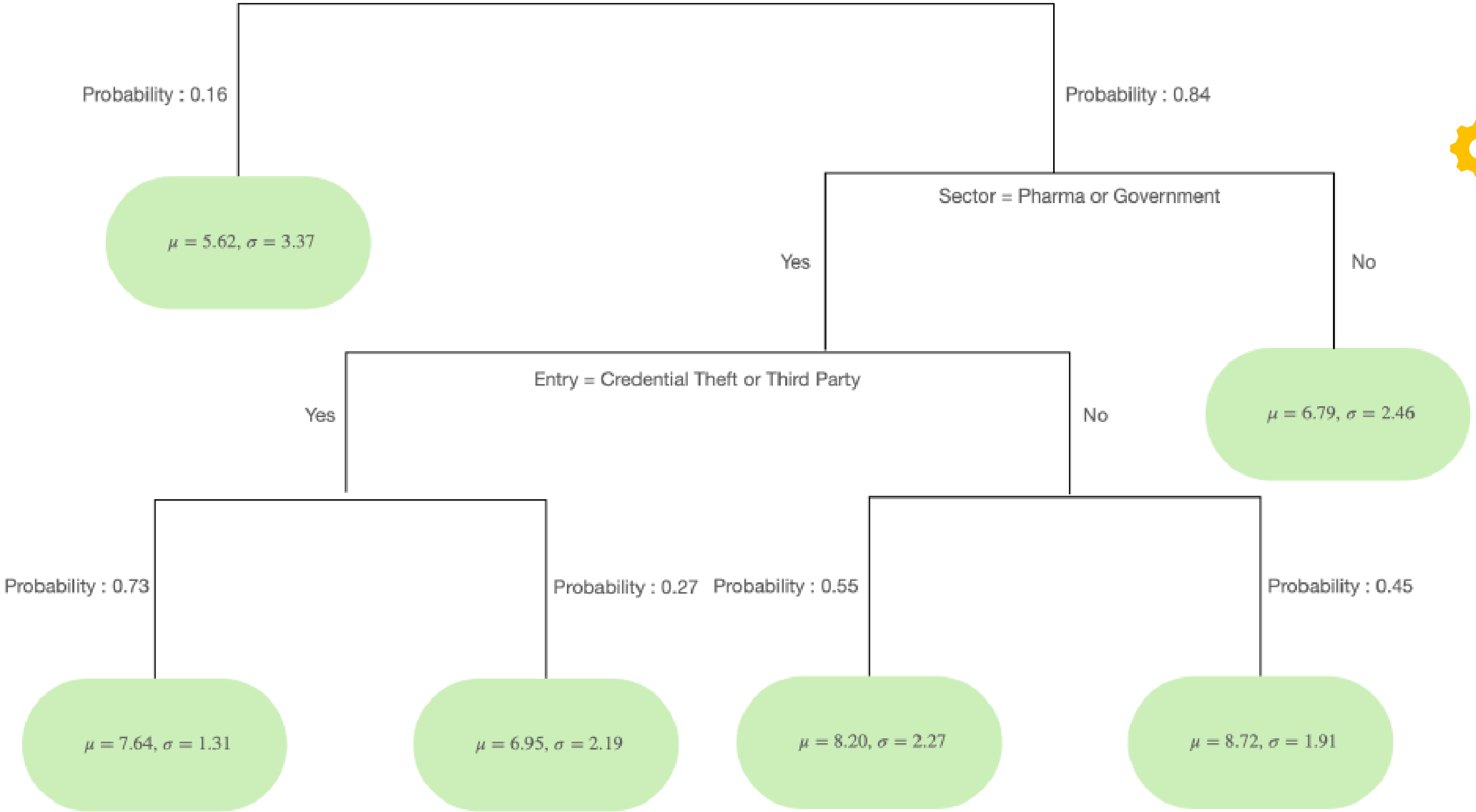
Entry point q	Probability
Phishing email	63%
Credential theft	44%
Third party	40%
Unpatched server	28%
Brute force server credential	17%

Agenda

- Introduction
- Portfolio composition
- Frequency model
- **Volume of data compromised**
- Focus on the business interruption
- Applications

Volume of data compromised : attritional losses

- Modeling of **attritional breaches** based on **mixture** of **LogNormal** distributions

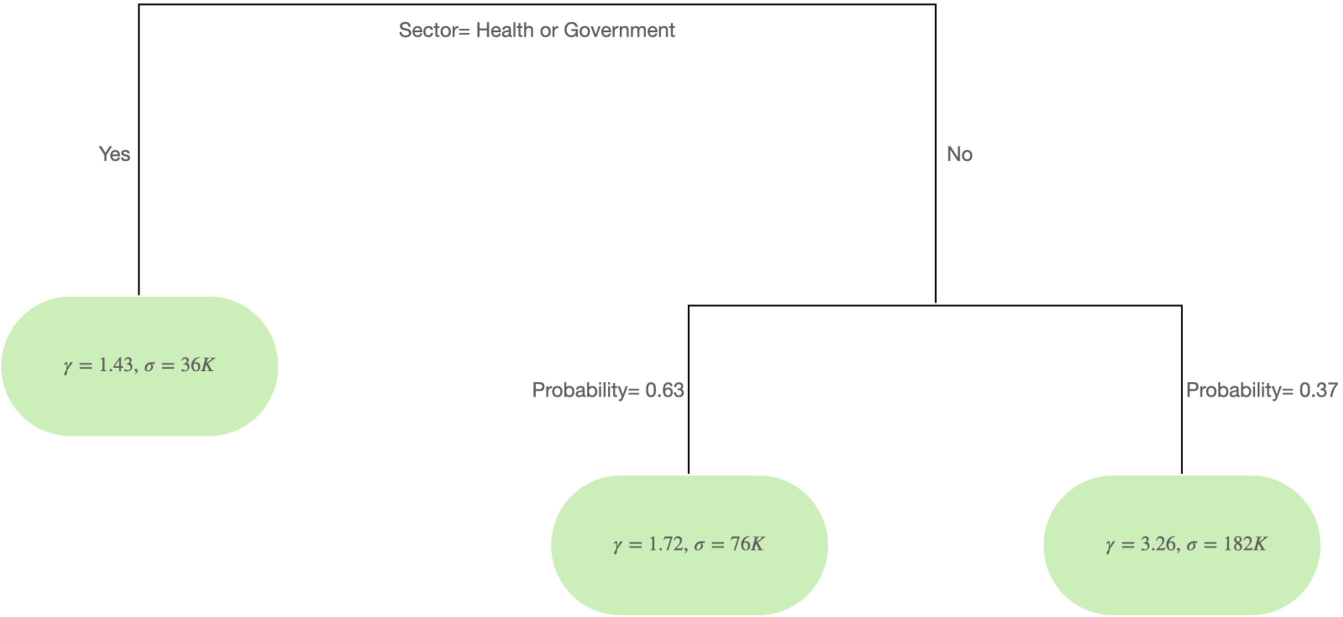

Probability : 0.16
Probability : 0.84
$\mu = 5.62, \sigma = 3.37$
Sector = Pharma or Government
Yes
No
Entry = Credential Theft or Third Party
Yes
No
$\mu = 6.79, \sigma = 2.46$
Probability : 0.73
Probability : 0.27
Probability : 0.55
Probability : 0.45
$\mu = 7.64, \sigma = 1.31$
$\mu = 6.95, \sigma = 2.19$
$\mu = 8.20, \sigma = 2.27$
$\mu = 8.72, \sigma = 1.91$

- The volume of lost data is assessed in **number of records**
- Statistical information from several sources (PRC, Veris...)
- The **point of entry** has an impact on the volume of leaked data

Adaptation of Farkas, Lopez, Thomas (2021)

Volume of data compromised : extreme losses

- Modeling of **extreme breaches** based on **mixture** of **Pareto** distributions


Sector= Health or Government
Yes
No
$\gamma = 1.43, \sigma = 36K$
Probability= 0.63
Probability= 0.37
$\gamma = 1.72, \sigma = 76K$
$\gamma = 3.26, \sigma = 182K$

Adaptation of Farkas, Lopez, Thomas (2021)

- **Breach size** is not the only marker of severity (e.g. DDOS)
- **Business Interruption**

- **Generalized Pareto** distribution with parameters (σ, γ) with $\gamma > 0$ and $R > u$

$$P(R - u \geq t) = \frac{1}{\left(1 + \frac{\gamma t}{\sigma}\right)^{1/\gamma}}$$

- **Financial losses** can be tricky to deduce from the volume of **compromised data** => possibility to consider proxies. Below an example of a proxy design$^{(*)}$:

$$\boldsymbol{\log(L) = \alpha + \beta . log(R)}$$

(*) See Jacobs (2014) and Farkas et al. (2021)

Agenda

- Introduction
- Portfolio composition
- Frequency model
- Volume of data compromised
- **Focus on the business interruption**
- Applications

Business interruption: DDoS attacks

The **modeling** of **Distributed Denial Of Service (DDoS)** attacks may rely on **rate costs** and **duration parameters**

- **Short interruption**, usually less than a day
- DDOS attacks **don't** necessarily involve **compromised data**, but imply **high** and **variable interruption costs**
  - **Ponemon Institute** (2012) estimates the average cost at **$22K/minute**
  - The **NSFocus** report (2022) estimates the cost at between **$1 and $100K/minute**

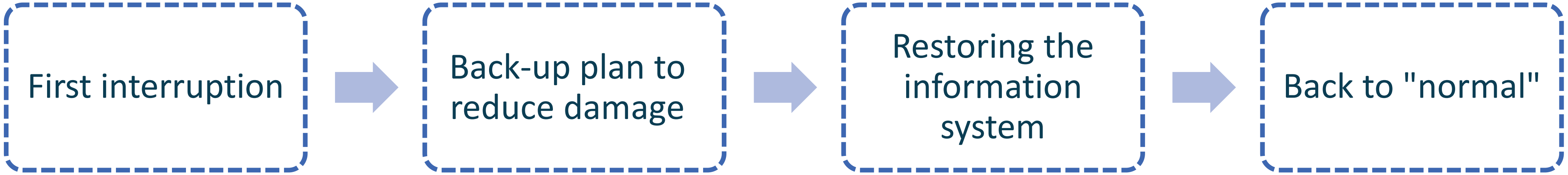
Duration	**< 5 min**	**5-10 min**	**10-60 min**	**1-12h**	**>12h**
Probability	25%	36%	30%	7%	2%

Distribution of the duration of a DDOS attack - NSFocus,2022

- In view of the rarity of these events, **several assumptions** must be considered in order to deal with this **specific case**
- **Few statistics** available on DDOS attacks **lasting > 12h**

Business interruption: Long business interruption

The modeling of **Long business interruption** (ransomware, cloud unavailability...) may be based on **back-up plan** implementation and **restoration** assumptions



First interruption

Back-up plan to reduce damage

Restoring the information system

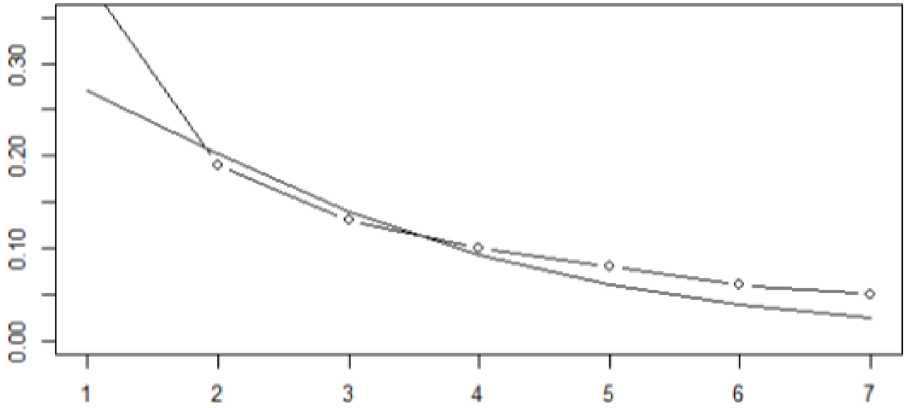
Back to "normal"

- Estimating the **business interruption** from **cloud interruptions**

Duration	1	2	3	4	5	6	7
Probability	39%	19%	13%	10%	8%	6%	5%

Time required (in days) to reach zero loss of information once the service to the cloud is restored - Lloyd's Cloud Down Impacts on the US economy

Gamma distribution

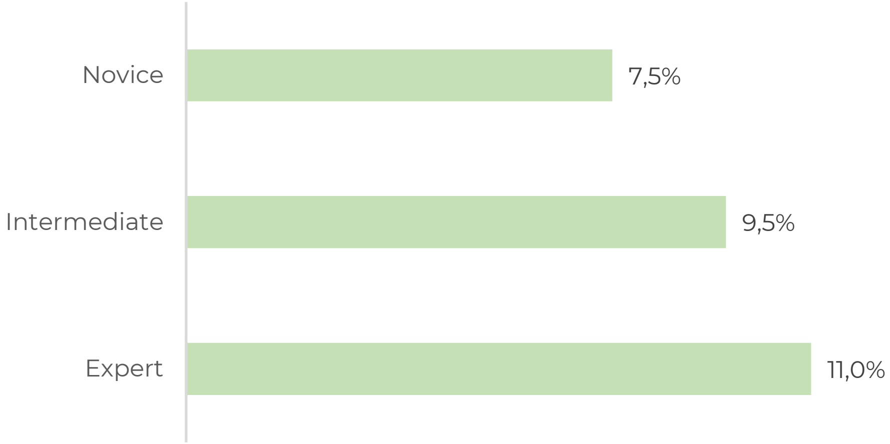


Calibration of a gamma distribution to capture longer interruptions

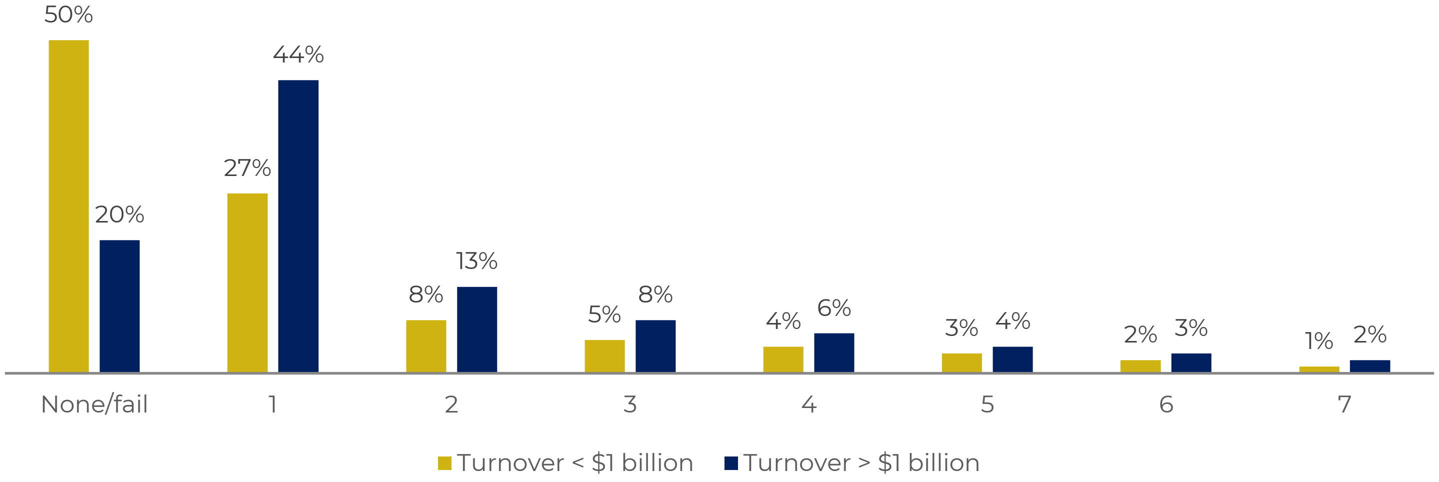
Business interruption: Long business interruption

Below assumptions of **ability to defend** against a Cyber attack and **back-up plan implementation**

Probability of defending against an attack



Probability of implementing a back-up plan with regards to a company's turnover

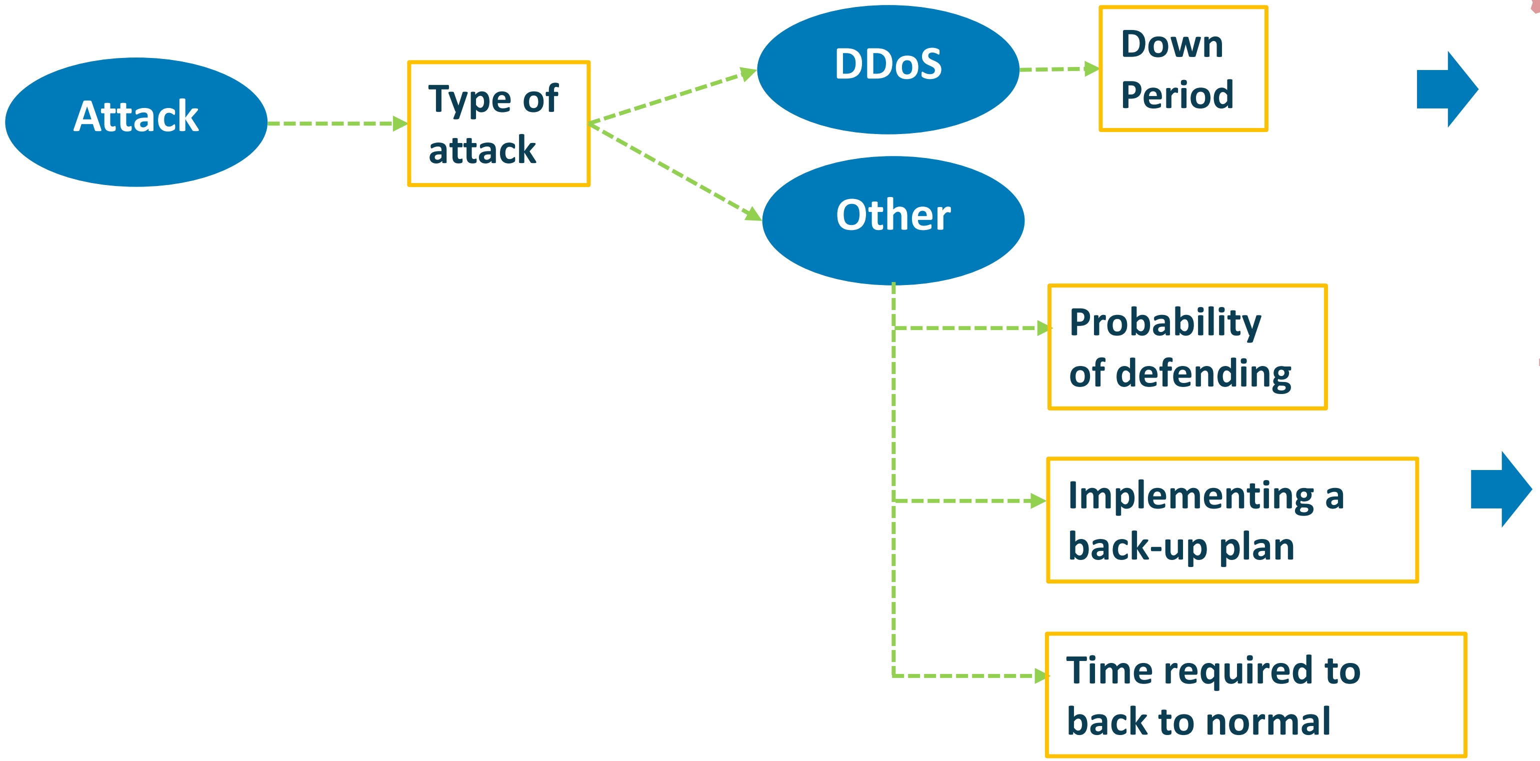


Lloyd's Cloud Down Impacts on the US economy

Focus on business interruption

Summary of **methodologies** allowing to generate **business interruption events** associated with different types of attacks:

Business interruption events



Attack

Type of attack

DDoS

Down Period

Other

Probability of defending

Implementing a back-up plan

Time required to back to normal

Conversion into loss values

- Assumption of average cost (e.g **$22K/minute** Ponemon Institute estimation)

- Loss based on turnover value
$$turnover \times T/365$$

- Use of more sophisticated valuations (e.g. Lloyd’s reports formula)

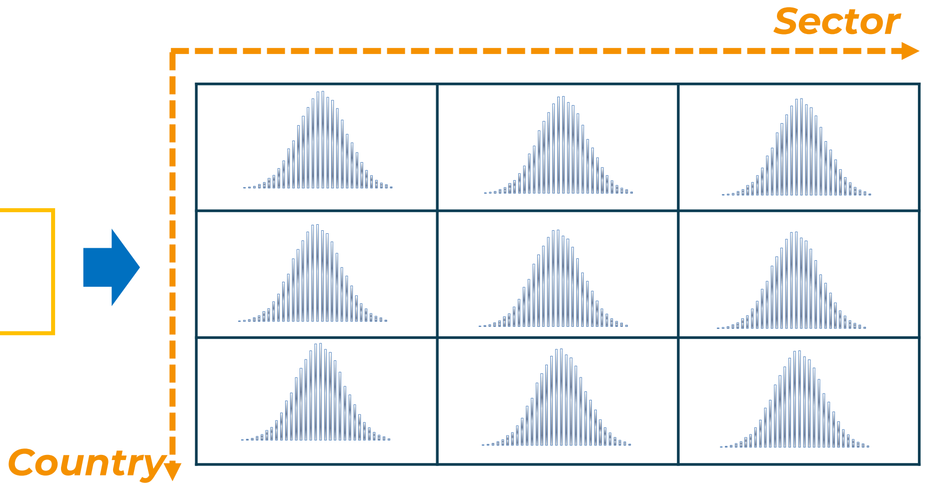
Agenda

- Introduction
- Portfolio composition
- Frequency model
- Volume of data compromised
- Focus on the business interruption
- **Applications**

Application #1: stress scenarios construction and application

- Application of the **Cyber events database** construction methodology to the **generation of stress scenarios** in various frameworks: calculation of a **Cyber SCR** within a **Solvency 2 Internal Model (IM)**, **ORSA multi-year adverse scenarios** construction,…
- Below the **main steps** to compute IM Cyber SCR:
  - Preliminary **mapping of the insured portfolio** according to the underlying **segmentation** of the cyber events database (company size, Cyber maturity, country, sector)
  - Obtaining **loss scenarios** associated with the portfolio guarantees and adjusted by contractual parameters (eg deductibles)
  - Calculation of **Cyber SCR** using the **generated scenarios**

Cyber losses simulation at 1 year



Impact of dependency modeling on SCR

$$SCR_{cyber} = q_{99,5\%}\left(\sum_i L_i\right) - E\left(\sum_i L_i\right)$$

$$logit(p_i) = \alpha_i + \beta_0 + \beta^T X_i + \boxed{\Delta_{c,i} + \Delta_{s,i}}$$

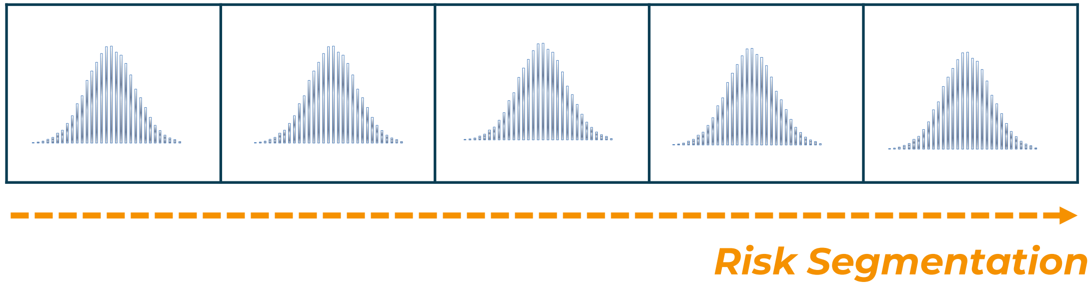
Application #2: optimizing exposures of cyber risk coverages

- **Objective**: for an insurance group offering Cyber coverages => **optimization of underwriting process** taking into account **underlying systemic risk** and **diversification limits**
- **Methodology**: the construction of **Cyber scenarios** allows to **objectify / rationalize** the **weight of risk exposure** of each **segment** (company size x Cyber maturity x country x sector), thereby **minimizing** the impact in terms of **risk** (SCR, loss volatility, etc.)

How to distribute new exposures while minimizing risk?

$$\overline{L_{new}} = E(L_{new})$$

???



Impact of dependency modeling on the following indicators

$$Min \begin{cases} \sigma(L_{new} + L_{stock}) \\ Or \\ SCR_{cyber} \\ = q_{99,5\%}(L_{new} + L_{stock}) - E(L_{new} + L_{stock}) \end{cases}$$

Thank you

Laurent Devineau
Innovation Lead - Detralytics
l.devineau@detralytics.eu

Arthur Maillart
Innovation Lead - Detralytics
a.maillart@detralytics.eu