**Actuarial Colloquia 2022**

# Modelling Cyber Risk of Insurance Companies by Hybrid Methodology - An Aggregation of Scenario Analysis and Loss Distribution Approach


Dr Madhu Acharyya

Senior Lecturer in Risk & Finance

Glasgow Caledonian University, London,

E-mail: Madhu.Acharyya@gcu.ac.uk

# Outlines of the Presentation

- Defining cyber risk
- Literature on cyber risk
- Key issues on Cyber Risk
- Insurability
- Cyber Risk Vs Operational Risk Vs Terrorism Risk
- Dynamic Nature - Human Intelligence & Skill
- Estimating the Impact of Hypothetical Cyber Attack Using LDA [six steps]
- Generating Aggregate Loss Distributions & Estimation of CaR from Historical Data Using Scenario Analysis (three steps)
- Empirical Testing of the Methodology & Results

# What is Cyber Risk?

- "The risk involved with malicious electronic events that cause disruption of business and monetary loss" (Mukhopadhyay, A. et al, 2006)

- "Information security risk or risk resulting in failure of information systems" (Böhme and Kataria, 2006).

# Issues in Insuring and Pricing Cyber Risks – Insurability

- In Biener et al (2015), the focus is placed on the different criteria of insurability and the difficulties in insuring cyber risks are emphasized.

- The different criteria used to test the insurability of a risk are exposed along with the assessment of these criteria for cyber risks

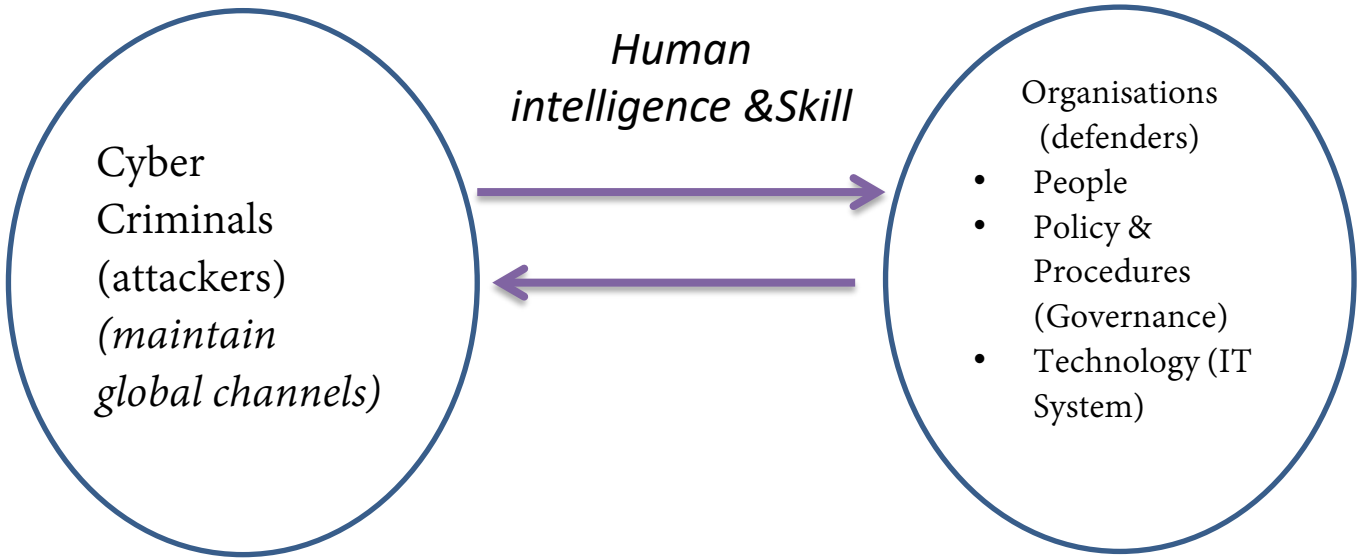
1. "**randomness of loss occurrence criteria**" (Criteria 1) requires "***independence and predictability of loss exposures***"

2. ***Moral Hazards*** and ***Adverse Selections*** are also too excessive for cyber risks for the **"information asymmetry**" (Criteria 5) criteria to be satisfied.

3. Finally, **indirect costs** caused by cyber-attacks such as the "***reputational loss"*** are often very complicated to measure. This makes it difficult to set up acceptable cover limits (Criteria 7).

# The dynamics of Cyber Risks

*"defender predicts attacker's best response to defender's own actions, and then chooses his or her own actions taking into account these best responses".*




Experts with clear mission & vision
- Where to target?
- When to target?
- How to target?

Digitalisation (Automation) Mathematical Algorithms
- Data Analytics
- Machine Learning

- Risk
- Reward

# Issues in modelling and quantifying cyber risks

- Brown & Cox (2011) state the main reason why cyber risks cannot be treated as traditional risks is that they involve **human intelligence, intent and adaptability**.

- Attackers collect specific intelligence associated with their targets, modify and optimise their strategies periodically to enable them to strategically adapt to situations before perpetuating their attacks.

- traditional risk analysis tools, such as **Probabilistic Risk Assessment (PRA)**, do not have the capability to integrate human intelligence and are not suitable to model and quantify cyber risk.

- Cox, (2008) introduced the "**Hierarchical Optimization Model**" as an alternative to PRA in *Terrorism Risk Analysis*.

# Focus of This Paper

- Two Key Issues

1. Capital Charge
2. Pricing

- Two Key Papers

1. Cambridge Center for Risk Studies. (2014a,b; 2015; 2016)
2. Rodriguez, E., & Dominguez, J. (2008).

# Aim & Objectives

- Aim:
  - The overriding aim of this study is to propose a methodology to Quantify the cyber risk.
    - The output of this study will assist insurers to identify their exposures and risk appetite on cyber risk
    - This will help insurers to price cyber risk in the presence granular and inadequate data.
- Objectives:
  - Understanding the general parameters and nature of cyber risks.
  - Creating Hypothetical Cyber Risk Data using LDA & Scenarios
  - Collecting Historical Data (4 Case Studies) & Scenarios
  - Generating aggregated Loss Distributions integrating Hypothetical Data & Historical Data
  - Estimating Capital at Risk (CaR) for insurance companies

# Lack of Data

- Information asymmetry – organisations try to hide
- Unreliable third party data – unclear sources,
- Also non-homogeneous way of capturing the data
- It takes time to crystalize the total severity of loss
- May never be possible to calculate the total loss – due to both tangible [regulatory fines, litigation] and intangible [reputational] losses: insurance policies do not cover such losses

# Parameters of Cyber Risk

1. Category (3)
2. Sub-Category (11)
3. Actors (4)
4. Motivations (5),
5. Type of Institution (6),
6. Key Risk Indicators (13),
7. Environmental Variables or Factors (5),
8. Level of Loss Impact (3)

(Source: Cambridge Center for Risk Studies, 2014).

# Category & Sub-Category

| 3 Categories | 11 Sub-categories |
|---|---|
| Theft | Past data/historical data theft |
| Theft | Password/Identity/Credit Card data theft |
| Theft | Intellectual property / Secrets data theft |
| Theft | Money theft |
| Damage | Amendment/deletion of data |
| Damage | Amendment of algorithm /software |
| Damage | Disable hardware, Hard drive /Server |
| Disruption | Denial of service |
| Disruption | Blocking communications |
| Disruption | Downtime of websites |
| Disruption | Shut down power grid |



Source: Cambridge Center for Risk Studies (2014).

# Actors, Motivation & Type of Institutions

| 4 Actors | 5 Motivations | 6 Types of Institution |
|---|---|---|
| Hacktivists | Political | Financial Services |
| Terrorists | Financial | Health Care |
| Nation state | Social & cultural | IT |
| Lone wolf hackers | Economic | Entertainment & Media |
| | Personnel | Retail |
| | | Energy |

# 13 [Key] Risk Indicators and 3 Impact Levels

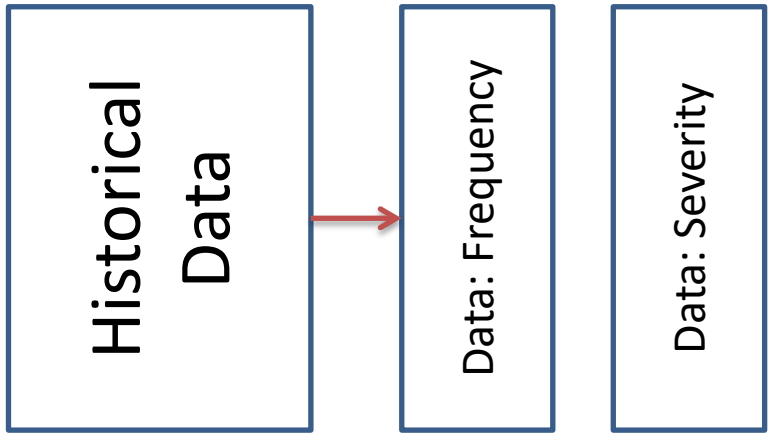
| | |
|---|---|
| 1. Reputation | 8. Property loss |
| 2. Percentage of returning customers | 9. Financial assets |
| 3. Number of clients | 10. Physical assets |
| 4. Market value | 11. Security |
| 5. Business Interruption<br>6. Income loss | 12. Administrative expenses |
| 7. Cost of operation/service, | 13. Insurance expense |

| |
|---|
| 1. Small |
| 2. Medium |
| 3. Large |

# Five Environmental Variables (Factors)

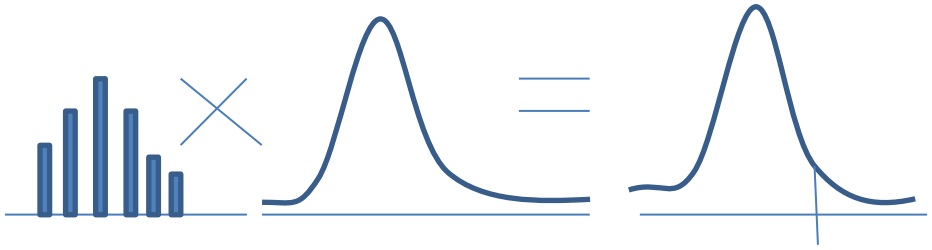
| |
|---|
| 1. Number of employees and/or Machines targeted |
| 2. Level of information or security |
| 3. Country wealth |
| 4. Country growth |
| 5. Sector growth |
| |

## Loss Distribution Analysis (LDA)




F & S Distributions

Aggregated Distribution



One scenario: Poisson

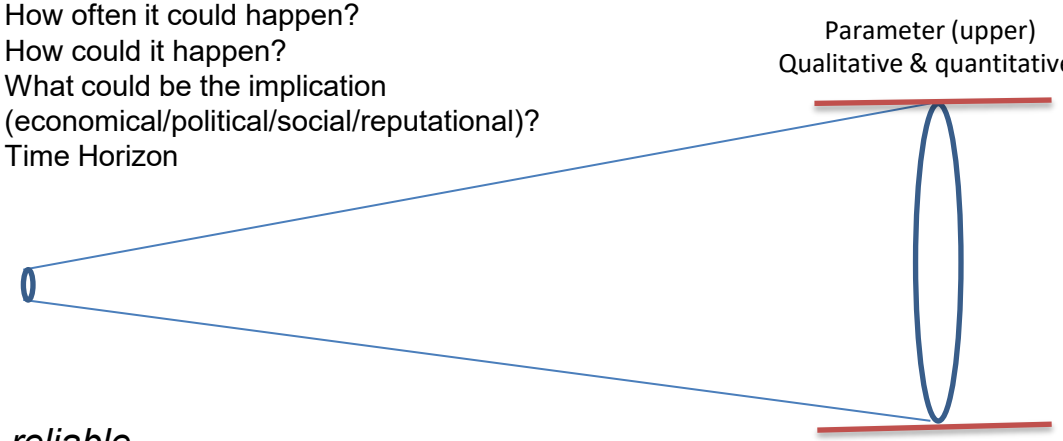
Two Scenarios: Log Normal & Pareto

VaR

Scenario Analysis

1. What could happen?
2. How often it could happen?
3. How could it happen?
4. What could be the implication (economical/political/social/reputational)?
   Time Horizon

Historical data




*The past is not a reliable predictor of the future*

LDA and Case Studies [Severity]

Scenario 1 Log Normal

Scenario Pareto

# Estimating the Impact of Hypothetical Cyber Attack Using LDA

We develop and employ **SIX** steps methodology

- **Step 1: Computation of Frequency**
  - assumed that the frequency depends on the sub-category of the cyber-attacks and all have low frequency
  - logically assigned the within a range from **8 (very low)** to **48 (very high)**
- **Step 2: Computation of Severity**
- Initial severity
  - assigned hypothetical quantitative and qualitative (i.e., categorical) severities to each sub-category
  - assign quantitative value of severities within a range from **US$1 million (very low)** to **$115 million (very high).**

*[Source: Cambridge Center for Risk Studies (2016)]*

# Estimating the Impact of Hypothetical Cyber Attack Using LDA (Cont'd)

- **Measuring the Impact of the Parameters of Cyber-attacks on the Indicators of Values at Risk (termed as "Impact (1)")**
- We measure the impact of the **parameters** of cyber-attacks ***(i.e.,*** *actors*, *motivations*, *types of institutions)* in terms of 'Values at Risk' indices.
- In this study we use **Values at Risk** to categorically measure the impact of a cyber-attack on business activities (or performance indicators) in three indices i.e., "*intangible*", "*tangible*" and "*operational*".
- We assume that these business activities (or performance indicators) are vulnerable (or "at risk") to cyber-attacks.
- Each of these indices is linked to a selection of [Key Risk] Indicators (i.e., *reputation*, *% returning customers*, etc.).

# Value at Risk Examples

| | Impact on Values at Risk (4) | | | | |
|---|---|---|---|---|---|
| | Intangible | Tangible (i) | Tangible(ii) | Operational | Global impact (5) |
| 1.1.1.1.1.1.1.1 | 1.5875 | 2.791666667 | 6.808333333 | 3.983333333 | 3.792708333 |
| 1.1.1.1.1.1.1.2 | 1.5875 | 2.758333333 | 6.833333333 | 3.983333333 | 3.790625 |
| 1.1.1.1.1.1.1.3 | 1.65 | 2.858333333 | 6.875 | 3.991666667 | 3.84375 |
| 1.1.1.1.1.1.2.1 | 1.575 | 2.783333333 | 6.8 | 4.008333333 | 3.791666667 |
| 1.1.1.1.1.1.2.2 | 1.575 | 2.75 | 6.825 | 4.008333333 | 3.789583333 |
| 1.1.1.1.1.1.2.3 | 1.6375 | 2.85 | 6.866666667 | 4.016666667 | 3.842708333 |
| 1.1.1.1.1.1.3.1 | 1.65 | 2.841666667 | 6.883333333 | 4.05 | 3.85625 |
| 1.1.1.1.1.1.3.2 | 1.65 | 2.808333333 | 6.908333333 | 4.05 | 3.854166667 |
| 1.1.1.1.1.1.3.3 | 1.7125 | 2.908333333 | 6.95 | 4.058333333 | 3.907291667 |
| 1.1.1.1.1.2.1.1 | 1.6 | 2.808333333 | 6.825 | 3.95 | 3.795833333 |
| 1.1.1.1.1.2.1.2 | 1.6 | 2.775 | 6.85 | 3.95 | 3.79375 |
| 1.1.1.1.1.2.1.3 | 1.6625 | 2.875 | 6.891666667 | 3.958333333 | 3.846875 |

# Estimating the Impact of Hypothetical Cyber Attack Using LDA (Cont'd)

**Step 3:** Computation of the Impact of the Environmental Variables of the cyber-attacks on the Key Indicators of the Values at Risk **(termed as "Impact (2)")**

**Step 4:** Computation of Total Impact of Cyber Attacks on the Key Indicators of Values at Risk (termed as "Impact 3")

$$\text{Total Impact (3)} = \text{Impact (1)} + \frac{\text{Impact (2)}}{10}$$

…… Equation [1]

# Why one-tenth of Impact 2?

- In Equation 1, we deliberately include only a tenth of Impact (2).

- This is with the assumption that the impact of the parameters [**Impact (1)**] plays a bigger part in the computation of total impact rather than the impact on the environmental variables [**Impact (2)**] of the cyber attack.

# Estimating the Impact of Hypothetical Cyber Attack Using LDA (Cont'd)

**Step 5:** Computation of the Impact of Cyber Attacks on each of the Values at Risk (4) and of their global impact on the Values at Risk (5)

**Step 6:** Computation of the Final Severity of Cyber-attacks (6)

$$\text{Final Severity (6)} = \text{MinInitalSev} + \frac{\text{Global Impact (4)} - \text{Min( Global Impacts)}}{\text{Max(Gobal Impacts)} - \text{Min(Global Impacts)}} * (\text{MaxInitialSev} - \text{MinInitialSev}) \ldots\ldots \text{Equation [2]}$$

# Definitions of Variables in Equation 2

- Where, **MinInitialSev** and **MaxInitialSev** are respectively the minimum and maximum initial severities of each cyber-attack
- **Min(Global Impacts)** and **Max(Global Impacts)** are respectively the minimum and maximum of all the global impacts on the 243 cyber-attacks' Values at Risks (5).
- The results for the 243 cyber events are displayed in the "**Risk Register**" tab, in the column marked as "**Final Severity**".

# Historical Data

## Four Case Studies

# Case Studies

| | | |
|---|---|---|
| **Bangladesh Bank heist**<br>**(2016)**<br>**[near miss loss]** | thieves tried to illegally transfer US$951 million to several fictitious bank accounts around the world | • weaknesses in the security of the Bangladesh Central Bank<br>• possible involvement of some of its employees |
| **Sony Pictures hack**<br>**(2014)**<br>Two breaches –<br>1. a breach of its Playstation network in 2011<br>2. North Korean attack on its movie studios in 2014 | a hacker group which identified itself by the name "Guardians of Peace"<br>(GOP) leaked a release of confidential data from the film studio Sony Pictures. | The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information |
| **Talk-Talk (2015)**<br><br>***Identity theft*** | cyber attack accessed the data of nearly 157,000 customers using a well known hacking technique called SQL injection | a record £400,000 fine by the Information Commissioner's Office |
| **Anthem (a health insurer)**<br>**(2015)**<br><br>***Identity theft*** | criminal hackers had broken into its servers and potentially stolen over 37.5 (later known to 78.8 billion) million records that contain personally identifiable information from its servers | there is fear that the stolen data will be used for identity theft. |

http://breachlevelindex.com/data-breach-database

# Generating Aggregate Loss Distributions & Estimation of CaR from Historical Data Using Scenario Analysis

- We employed a **THREE** step methodology to compute aggregate loss distributions to measure CaR

**Step 1: Fitting Frequency and Severity Distributions Using Scenario Analysis**

**a) Frequency distribution**

- model the frequency by fitting into **Poisson** distribution

**b) Severity distributions**

- model the severity of cyber attack loss using **Lognormal** distribution [$\mu$ = €18,909 and $\sigma$ = €98, 226] (Scenario 1) and **Pareto** distribution [$\alpha$=2] (Scenario 2).

Source: Rodriguez & Dominguez (2008)

## Generating Aggregate Loss Distributions & Estimation of CaR from Historical Data Using Scenario Analysis (Cont'd)

### Step 2: Generating Aggregate Loss Distributions by Monte Carlo Simulation

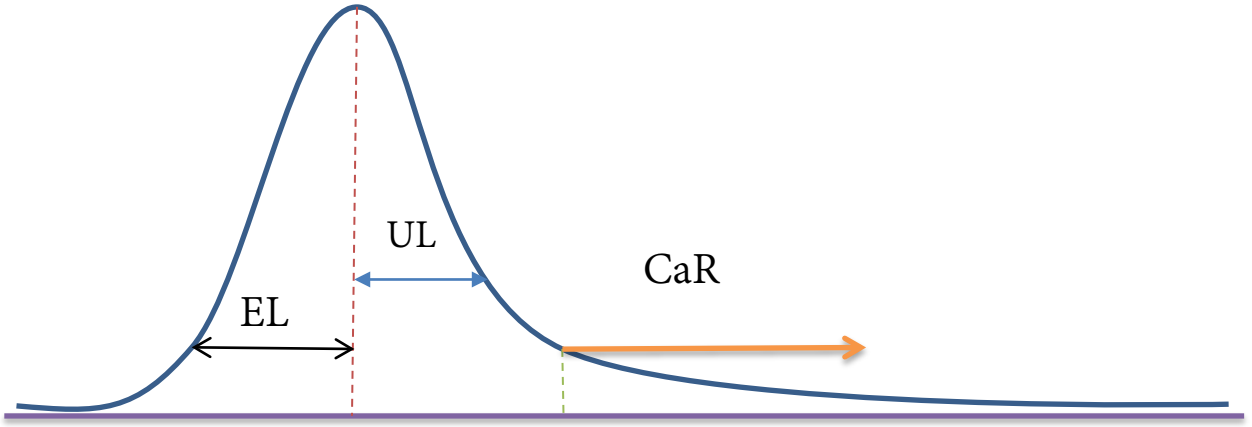
a) Closed form
   - analytical formulae, with the Convolution and Fourier Transform

b) Open form
   - implementing algorithms such as Monte Carlo simulation [100,000 simulations] and the Latin Hypercube

## Generating Aggregate Loss Distributions & Estimation of CaR from Historical Data Using Scenario Analysis (Cont'd)

### Step 3. Estimation of Capital at Risk (CaR)

We estimated the expected losses (EL), unexpected losses (UL) and the Capital at Risk (CaR) from the aggregate loss distributions



# Empirical Testing of the Methodology & Results

- Used Scenario Analysis to create both **hypothetical** [*derived by LDA*] and **historical** data [*Case Studies*]

- For the Hypothetical Data 320 000 hypothetical cyber-attack scenarios are created [permuting and combining]
  - 3 categories; 11 sub-categories; 4 actors; 5 motivations; types of institution; 13 indicators; 5 environmental variables

- In order for the program to run on basic computers the user requires **two** inputs; (a) parameters of the hypothetical cyber-attack scenarios; and (b) the categorical values of the indicators to be adapted for the company of interest. [see "**User Input**" tab]

- The 243 hypothetical attacks are assigned a "low" [categorical] frequency and 12 [quantitative] frequency (or occurrences) per year

# Risk Register of Hypothetical Data Generated Through LDA

| Reference | Category | Sub category | Actors | Motivation | Type of Institution | Environmental variables | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Number of Empoyees/machines targeted | Level of formation / Security | Country wealth | Country Growth | Sector growth |
| 1.1.1.1.1.1.1 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | S | S |
| 1.1.1.1.1.1.2 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | S | M |
| 1.1.1.1.1.1.3 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | S | L |
| 1.1.1.1.1.2.1 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | M | S |
| 1.1.1.1.1.2.2 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | M | M |
| 1.1.1.1.1.2.3 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | M | L |
| 1.1.1.1.1.3.1 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | L | S |
| 1.1.1.1.1.3.2 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | L | M |
| 1.1.1.1.1.3.3 | Theft | Intellectual Propei | Hacktivists | Financial | Financial Services | S | S | S | L | L |

243 cyber attacks [low frequency and 12 occurrence per year] [see "**Risk Register**" Tab]

The user has input a medium value for all the indicators and the following parameters for the attack: theft (category), intellectual property/secret data theft (sub-category), hacktivists (actors), financial (motivation), financial services (type of institution).

# Creation of Hypothetical Data

5 Environmental Variables

| #employees/machine targeted | level of formation/security | country wealth | country growth | sector growth |
|---|---|---|---|---|
| | | | | |

13 Key Risk Indicators

| Tangible i | Tangible ii | Intangible | Operational |
|---|---|---|---|
| Business interruption | Property loss | Reputation | Security |
| income | Financial assets | % returning customer | Administrative |
| cost of operation / service | Physical assets | #clients | Insurance expenses |
| | | Market value | |

# Computation of "Impact (1)" for "Attack 9"

| Parameters | Inputs | Impact |
|---|---|---|
| Sub-category | Intellectual property | 1 |
| Authors | Hacktivists | *1.5 |
| Motivation | Financial | *1 |
| Type of institution | Financial service | *2 |
| Impact (1) on reputation =3 | | |

- Use of the 1st matrix using CA of line 9.
- Showing the impact of the CA parameters on the reputation indicator.

# Matrix for Impact (1)

| Impacting event | Reputation | % of returning customers | nb of clients | market value | business interuption | income | cost of operation/ service |
|---|---|---|---|---|---|---|---|
| Past data / historical trades data theft | 1 | 0.5 | 1 | 1 | 0.5 | 1 | 0.5 |
| Password/Identity/Credit cards data theft | 2 | 2 | 2 | 2 | 1 | 2 | 1 |
| Intellectual Property / Secrets data theft | 1 | 1 | 1 | 1.5 | 1.5 | 1.5 | 0.5 |
| Money theft | 1.5 | 1 | 1.5 | 1.5 | 2 | 2 | 1.5 |
| Amendment/deletion of data | 1.5 | 1 | 1.5 | 0.5 | 1.5 | 1 | 1 |
| Amendment of algorithm / software | 0.5 | 0.5 | 0.5 | 1 | 1.5 | 0.5 | 1.5 |
| Disable hardware. Hard drive / Server | 1 | 0.5 | 0.5 | 0.5 | 2 | 0.5 | 1.5 |
| Denial of services | 1 | 1 | 1 | 1 | 1.5 | 0.5 | 1 |
| Bloking communications | 1.5 | 1 | 1.5 | 1 | 1.5 | 1 | 1.5 |
| Downtime of websites | 1 | 1 | 1 | 1 | 1.5 | 1 | 1.5 |
| Shut down Power Grid | 0.5 | 0.5 | 0.5 | 0.5 | 1.5 | 0.5 | 1 |
| Hacktivists | 1.5 | 1 | 0.5 | 1 | 1 | 1 | 1 |
| Terrorists | 2 | 2 | 1.5 | 2 | 1 | 1 | 1 |
| Nation state | 1.5 | 1 | 1.5 | 2 | 1.5 | 1.5 | 1 |
| Lone wolf hackers | 0.5 | 0.5 | 0.5 | 1 | 1 | 0.5 | 1 |
| Political | 1.5 | 1 | 1.5 | 1.5 | 1.5 | 1 | 1 |
| Financial | 1 | 0.5 | 1 | 1 | 0.5 | 2 | 1.5 |
| Social & cultural | 0.5 | 1.5 | 1.5 | 1.5 | 1 | 1.5 | 1 |
| Economic | 1 | 1 | 0.5 | 1 | 1.5 | 1.5 | 1 |
| Personnal | 0.5 | 0.5 | 0.5 | 0.5 | 0.5 | 1 | 1 |
| Financial Services | 2 | 1 | 1 | 1 | 1.5 | 2 | 1 |
| Health Care | 1.5 | 1.5 | 1 | 1 | 0.5 | 1 | 1.5 |
| IT | 1.5 | 1.5 | 1.5 | 1.5 | 1 | 1.5 | 1.5 |
| Entertainement & Media | 1 | 0.5 | 0.5 | 1 | 1 | 1 | 1 |
| Retail | 1 | 1.5 | 1.5 | 1.5 | 1.5 | 1.5 | 1.5 |
| Energy | 0.5 | 0.5 | 0.5 | 1 | 0.5 | 1 | 1 |

# Results For Impact (1)

| 1 | Reference | Reputation | %of returning customers | nb of clients | market value | business interuption | income |
|---|---|---|---|---|---|---|---|
| 2 | 1.1.1.1.1.1.1 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 3 | 1.1.1.1.1.1.2 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 4 | 1.1.1.1.1.1.3 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 5 | 1.1.1.1.1.2.1 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 6 | 1.1.1.1.1.2.2 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 7 | 1.1.1.1.1.2.3 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 8 | 1.1.1.1.1.3.1 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 9 | 1.1.1.1.1.3.2 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |
| 10 | 1.1.1.1.1.3.3 | 3 | 0.5 | 0.5 | 1.5 | 1.125 | 6 |

The impacts noted above range from 1/16 (0.5^4) to 16 (2^4).

*All the values displayed in each line are identical because all the hypothetical attacks have the same parameters (fixed by the user).*

*For example, in the instance of an attack for financial motivation by hacktivists, it is considered the choice of values for impacts will have more impact on the reputation of a business than an attack perpetrated by a lone- wolf hacker.*

# Matrix for Impact (2)

| A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| Environmental situations↓ | Indicators→ | Reputation | | | %of returning customers | | |
| | | S | M | L | S | M | L |
| umber of Empoyees/machines targete | S | -1 | 0 | 1 | -0,5 | 0 | 0,5 |
| | M | 0 | 1 | 1,5 | 0 | 0,5 | 1 |
| | L | 1 | 1,5 | 2 | 0,5 | 1 | 1,5 |
| Level of formation / Security | S | 1,5 | 1 | 0,5 | 0,5 | 1 | 2 |
| | M | 1 | 1 | 0,5 | 0 | 0,5 | 1 |
| | L | 0,5 | 0,5 | -0,5 | -1 | -0,5 | 0,5 |
| Country wealth | S | 0 | 0,5 | 0,5 | 0 | 0,5 | 0,5 |
| | M | 0,5 | 0,5 | 1 | 0,5 | 0,5 | 1 |
| | L | 0,5 | 1 | 1,5 | 0,5 | 1 | 1,5 |
| Country Growth | S | 0 | 0,5 | 0,5 | 0 | 0,5 | 0,5 |
| | M | 0,5 | 0,5 | 1 | 0,5 | 0 | 1 |
| | L | 0,5 | 1 | 1,5 | 0 | 1 | 1,5 |
| Sector growth | S | 0 | 0,5 | 0,5 | 0 | 0,5 | 0,5 |
| | M | 0,5 | 0,5 | 1 | 0,5 | 0 | 1 |
| | L | 0,5 | 1 | 1,5 | 0 | 1 | 1,5 |

"Impact 1" is varied depending on the **Environmental Variables** of the attack; the [Key Risk] Indicators in this study have been fixed at a medium value by the user.

# Computation of Impact (2) for "Attack 9"

| Environmental Variables | Values for Attack 9 | Impacts |
|---|---|---|
| Number of employees | S | 0 |
| Security | S | +1 |
| Country wealth | S | +0.5 |
| Country growth | M | +0.5 |
| Sector growth | L | +1 |
| Impact (2) of Attack 9 on Reputation Indicator = 3 | | |

- Use of the 2nd matrix using CA of line 9.
- Showing the impact of the CA Environnemental Variables on the reputation indicator.

# Results For Impact (2)

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Reference | Reputation | %of returning customers | nb of clients | market value | business interuption | income |
| 2 | 1.1.1.1.1.1.1.1 | 2.5 | 2.5 | 1.5 | 2 | 1.5 | 1.5 |
| 3 | 1.1.1.1.1.1.1.2 | 2.5 | 2 | 2 | 2 | 1 | 1.5 |
| 4 | 1.1.1.1.1.1.1.3 | 3 | 3 | 2.5 | 2.5 | 2 | 2.5 |
| 5 | 1.1.1.1.1.1.2.1 | 2.5 | 2 | 2 | 1.5 | 1.5 | 1.75 |
| 6 | 1.1.1.1.1.1.2.2 | 2.5 | 1.5 | 2.5 | 1.5 | 1 | 1.75 |
| 7 | 1.1.1.1.1.1.2.3 | 3 | 2.5 | 3 | 2 | 2 | 2.75 |
| 8 | 1.1.1.1.1.1.3.1 | 3 | 3 | 2.5 | 2.5 | 2 | 2 |
| 9 | 1.1.1.1.1.1.3.2 | 3 | 2.5 | 3 | 2.5 | 1.5 | 2 |
| 10 | 1.1.1.1.1.1.3.3 | 3.5 | 3.5 | 3.5 | 3 | 2.5 | 3 |

The impacts range from -7.5 (= -1.5-1.5-1.5-1.5-1.5) to 10 (= 2+2+2+2+2). Where the user has input a 'medium' value for the reputation indicator and the hypothetical attack has a 'medium' value for the environmental variable 'sector growth'; it is considered that the impact of an attack on the reputation indicator is lower than if the 'sector growth' was 'large'.

# Step 4: Computation of Total Impact of Cyber Attacks on the Indicators of Values at Risk (3)

We use Equation [1] from Section 2 to compute the total impact of the cyber event on the Indicators (3):

$$\text{Total Impact (3)} = \text{Impact (1)} + \frac{\text{Impact (2)}}{10}$$

In the examples below, the total Impact (3) for "Attack 9" on the reputation indicator is = 3 + 3/10=3.3.

The 243 hypothetical cyber-attacks are listed along with their total Impact (3) in the "Impact (3)" tab:

# Results For Total Impact (3)

| 1 | Reference | Reputation | %of returning customers | nb of clients | market value | business interuption | income |
|---|---|---|---|---|---|---|---|
| 2 | 1.1.1.1.1.1.1.1 | 3.25 | 0.75 | 0.65 | 1.7 | 1.275 | 6.15 |
| 3 | 1.1.1.1.1.1.1.2 | 3.25 | 0.7 | 0.7 | 1.7 | 1.225 | 6.15 |
| 4 | 1.1.1.1.1.1.1.3 | 3.3 | 0.8 | 0.75 | 1.75 | 1.325 | 6.25 |
| 5 | 1.1.1.1.1.1.2.1 | 3.25 | 0.7 | 0.7 | 1.65 | 1.275 | 6.175 |
| 6 | 1.1.1.1.1.1.2.2 | 3.25 | 0.65 | 0.75 | 1.65 | 1.225 | 6.175 |
| 7 | 1.1.1.1.1.1.2.3 | 3.3 | 0.75 | 0.8 | 1.7 | 1.325 | 6.275 |
| 8 | 1.1.1.1.1.1.3.1 | 3.3 | 0.8 | 0.75 | 1.75 | 1.325 | 6.2 |
| 9 | 1.1.1.1.1.1.3.2 | 3.3 | 0.75 | 0.8 | 1.75 | 1.275 | 6.2 |
| 10 | 1.1.1.1.1.1.3.3 | 3.35 | 0.85 | 0.85 | 1.8 | 1.375 | 6.3 |

The impacts range from -7.4375 (=1/16-7.5) to 26 (=16+10).

## Step 5: Computation of Impact on each of the Values at Risk (4) and of their Global Impact on the Values at Risk (5)

The impact of cyber-attacks on each Values at Risk (4) creates an average for the total impact of the Cyber Attack (3).

The impact is dependent upon the indicators selected by the user.

For example, the indicators relating to the intangible Values at Risk are the reputation, the percentage of returning customers, the number of clients and the market value.

Therefore, the impact attaining to "Attack 9" on this Value at Risk is 1.6375 (= (3.3 + 0.75 + 0.8 + 1.75)/4).

## Step 5: Computation of Impact on each of the Values at Risk (4) and of their Global Impact on the Values at Risk (5) (Cont'd)

- In order to calculate the global impact of the attacks on all the Values at Risk (5), the average impacts of cyber-attacks on all the values at risk is computed.

- Therefore the impact for "Attack 9" on all the Values at Risk is 3.84 (= (1.64+2.85+6.87+4.01+3.84)/5).

- All the 243 cyber events are listed in the "Risk_Register" tab along with their Impacts (4) and (5). A sample of these is seen below (Illustration 10).

# Results For Total Impact (4) & (5) [Illustration 10]

| Impact on values at risk (4) | | | | |
|---|---|---|---|---|
| Intangible | Tangible (i) | Tangible (ii) | Operational | Global impact (5) |
| | | | | |
| 1.5875 | 2.791666666 | 6.808333333 | 3.983333333 | 3.792708333 |
| 1.5875 | 2.758333333 | 6.833333333 | 3.983333333 | 3.790625 |
| 1.65 | 2.858333333 | 6.875 | 3.991666666 | 3.84375 |
| 1.575 | 2.783333333 | 6.8 | 4.008333333 | 3.791666666 |
| 1.575 | 2.75 | 6.825 | 4.008333333 | 3.789583333 |
| 1.6375 | 2.85 | 6.866666666 | 4.016666666 | 3.842708333 |
| 1.65 | 2.841666666 | 6.883333333 | 4.05 | 3.85625 |

## Step 6: Computation of the Final Severity of Cyber Attacks (6)

- The Final Severity (6) of "Attack 9" is:

$$\text{Final Severity (6)} = 12000 + \frac{3.8427-3.65}{4.071875-3.65} * (50000 - 12000) = 29\ 358\ (000\$)$$

- All the results for the 243 cyber-attacks are displayed in the "Risk_Register" tab, in the column "Final Severity (6)" (see Illustration 10);

# Historical Data

Four Case Studies

# Use of Scenario Analysis on Historical Data

## Two scenarios of each case study are considered

| Scenarios | Frequency distribution | Severity distributions | Bangladesh Bank [money-theft] | |
|---|---|---|---|---|
| | | | Frequency | Severity |
| Scenario 1 | Poisson | Lognormal | $\lambda = 36$ | $\mu = 9.467;$ $\sigma = 1.825$ |
| Scenario 2 | Poisson | Pareto | | |

# Descriptive statistics of a sample of the Hypothetical Data

| ***m*** | ***s*** | ***a*** | ***q*** |
|---|---|---|---|
| LogNormal [Scenario 1] | | Pareto [ Scenario 2] | |
| *Mu* | *Theta* | *Alpha* | *Beta* |
| 8.29709281 | 1.82528501 | 2.1 | 30991.70091 |
| 8.289514 | 1.82528501 | 2.1 | 30757.70834 |
| 8.46681798 | 1.82528501 | 2.1 | 36724.51903 |
| 8.29331058 | 1.82528501 | 2.1 | 30874.70463 |
| 8.28570294 | 1.82528501 | 2.1 | 30640.71205 |
| 8.46362711 | 1.82528501 | 2.1 | 36607.52274 |
| 8.50433472 | 1.82528501 | 2.1 | 38128.47448 |
| 8.49817886 | 1.82528501 | 2.1 | 37894.48191 |
| 8.64440557 | 1.82528501 | 2.1 | 43861.29259 |
| 8.30835441 | 1.82528501 | 2.1 | 31342.68978 |
| 8.30086079 | 1.82528501 | 2.1 | 31108.6972 |
| 8.47632994 | 1.82528501 | 2.1 | 37075.50789 |

Scenario 1

Scenario 2

# Descriptive Statistics of a Sample of Historical Data

| Cases | m | s | a | q |
|---|---|---|---|---|
| | LogNormal | | Pareto | |
| | Mu | Sigma | Alpha | Theta |
| Sony | 10.277018 | 1.825285 | 2.1 | 224,448 |
| TalkTalk | 9.1784058 | 1.825285 | 2.1 | 74,816 |
| Bangladesh Bank | 9.4660878 | 1.825285 | 2.1 | 99,755 |
| Anthem | 9.6892314 | 1.825285 | 2.1 | 124,693 |

Scenario 1

Scenario 2

# Parameters of Severity Distributions in a Sample Using Hypothetical Data

| Final Severity (6) | μ | σ | α | θ |
|---|---|---|---|---|
| | LogNormal | | Pareto | |
| 24854,32099 | 8,2970928 | 1,825285 | 2,1 | 26465,92489 |
| 24666,66667 | 8,289514 | 1,825285 | 2,1 | 26266,10269 |
| 29451,85185 | 8,466818 | 1,825285 | 2,1 | 31361,56886 |

# Parameters of Severity Distributions For Historical Data

| Severity | μ | σ | α | θ |
|---|---|---|---|---|
| | LogNormal | | Pareto | |
| 180 000 | 10.27701804 | 1.8252850100 | 2.1 | 191671.56017726 |
| 60 000 | 9.178405753 | 1.8252850100 | 2.1 | 63890.5200590867 |
| 80 000 | 9.466087825 | 1.8252850100 | 2.1 | 85187.3600787824 |
| 100 000 | 9.689231377 | 1.8252850100 | 2.1 | 106484.200098478 |

we can observe that as the severity increases, $\theta$ and $\mu$ increase and the parameters $\alpha$ and $\sigma$ are fixed.

# Aggregate Loss Distributions and Estimation of CaR

- In order to calculate the aggregate loss distributions we integrate the discrete frequency distribution and the continuous severity distribution using 100,000 Monte Carlo simulations for both **Hypothetical** and **Historical** data.
- Noted the results for the EL, UL, and CaR obtained under both scenarios and for both kinds of data

# Aggregate Losses of Hypothetical Data [generated through LDA] Under Scenario 1

| LogNormal | | | | | | |
|---|---|---|---|---|---|---|
| CaR 99,9% | CaR 99% | CaR 95% | EL | UL | EL/CaR 99,9% | UL/CaR 99,9% |
| 3540524,454 | 1482790,475 | 708 797 | 252 015 | 3 288 510 | 7,12% | 92,88% |
| 4316194,622 | 1517094,575 | 721 488 | 257 777 | 4 058 418 | 5,97% | 94,03% |
| 4391199,806 | 1640653,44 | 823 712 | 294 456 | 4 096 744 | 6,71% | 93,29% |
| 4186340,646 | 1478795,97 | 713 303 | 255 029 | 3 931 311 | 6,09% | 93,91% |
| 3951173,693 | 1432263,62 | 695 511 | 248 836 | 3 702 337 | 6,30% | 93,70% |
| 4970887,793 | 1720667,734 | 834 668 | 302 769 | 4 668 119 | 6,09% | 93,91% |
| 5055729,178 | 1792097,084 | 888 050 | 316 469 | 4 739 260 | 6,26% | 93,74% |
| 4750557,302 | 1652226,096 | 867 440 | 313 186 | 4 437 371 | 6,59% | 93,41% |
| 5982622,646 | 2136016,99 | 1 016 861 | 362 884 | 5 619 739 | 6,07% | 93,93% |

EL represents the expected aggregate loss under a type of cyber-attack.
UL (difference between CaR and EL)
CaR is the amount of capital that is set aside to cover risks.

# Aggregate Losses of Hypothetical Data [generated through LDA] Under Scenario 2

| Pareto | | | | | | |
|---|---|---|---|---|---|---|
| CaR 99,9% | CaR 99% | CaR 95% | EL | UL | EL/CaR 99,9% | UL/CaR 99,9% |
| 2 550 334 | 1 522 155 | 1 058 240 | 612 509 | 1 937 825 | 24,02% | 75,98% |
| 2 621 234 | 1 418 611 | 1 045 017 | 601 320 | 2 019 914 | 22,94% | 77,06% |
| 3 902 204 | 1 728 721 | 1 249 363 | 723 557 | 3 178 647 | 18,54% | 81,46% |
| 3 089 179 | 1 465 927 | 1 057 483 | 614 873 | 2 474 306 | 19,90% | 80,10% |
| 2 613 565 | 1 445 297 | 1 057 309 | 606 010 | 2 007 554 | 23,19% | 76,81% |
| 3 221 620 | 1 713 932 | 1 249 736 | 715 467 | 2 506 153 | 22,21% | 77,79% |
| 3 453 902 | 1 783 992 | 1 280 555 | 744 134 | 2 709 769 | 21,54% | 78,46% |
| 4 159 565 | 1 749 890 | 1 267 636 | 745 082 | 3 414 483 | 17,91% | 82,09% |
| 3 988 957 | 2 098 039 | 1 494 189 | 863 623 | 3 125 333 | 21,65% | 78,35% |

A 99.9% CaR value of amount $X means that there is 0.1% chance for the CaR to be bigger than this current amount of $X.

The ratio $\frac{EL}{CaR}$ represents the proportion of EL over the CaR i.e. the proportion of CaR that comes from the EL.

$\frac{UL}{CaR}$ ratio represents the proportion of the UL over the CaR i.e. the proportion of CaR that is explained by the UL.

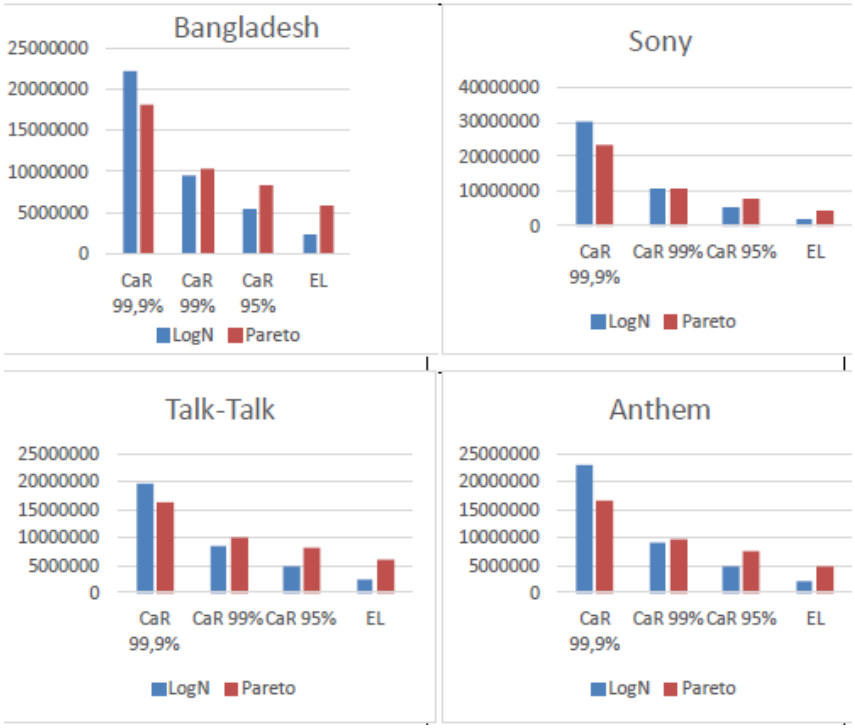
# Aggregate Losses of Historical Data [Case Studies] Under Scenario 1

| LogNormal | | | | | | |
|---|---|---|---|---|---|---|
| CaR 99,9% | CaR 99% | CaR 95% | EL | UL | EL/CaR 99,9% | UL/CaR 99,9% |
| 30176535,86 | 10795330,32 | 5 150 104 | 1 840 637 | 28 335 899 | 6,10% | 93,90% |
| 19751317,76 | 8454842,938 | 4 961 196 | 2 486 200 | 17 265 118 | 12,59% | 87,41% |
| 22132081,03 | 9464784,589 | 5 400 358 | 2 463 069 | 19 669 012 | 11,13% | 88,87% |
| 22691317,72 | 9208241,98 | 4 859 935 | 2 048 807 | 20 642 511 | 8,95% | 91,05% |

# Aggregate Losses of Historical Data [Case Studies] Under Scenario 2

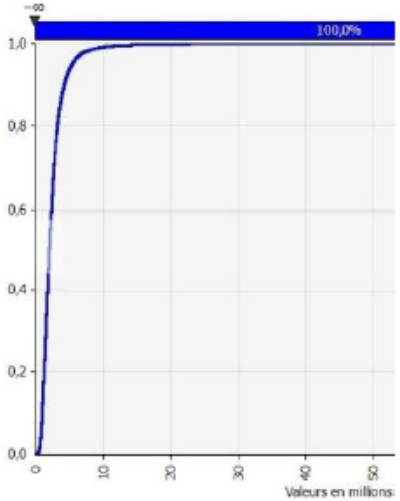
| Pareto | | | | | | |
|---|---|---|---|---|---|---|
| CaR 99,9% | CaR 99% | CaR 95% | EL | UL | EL/CaR 99,9% | UL/CaR 99,9% |
| 23 153 158 | 10 639 853 | 7 629 936 | 4 418 480 | 18 734 677 | 19,08% | 80,92% |
| 16 455 090 | 10 015 595 | 8 097 468 | 5 936 014 | 10 519 076 | 36,07% | 63,93% |
| 18 127 949 | 10 371 702 | 8 386 780 | 5 838 456 | 12 289 493 | 32,21% | 67,79% |
| 16 534 188 | 9 697 858 | 7 488 738 | 4 880 595 | 11 653 592 | 29,52% | 70,48% |

# CaR under both Scenarios (Log Normal, Pareto) for the Historical Data

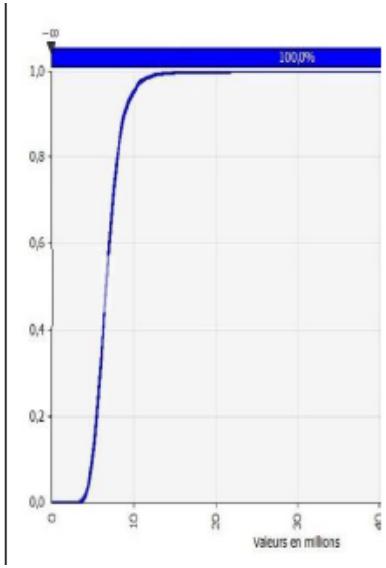



- CaR under both scenarios
- Scenario 1 (Log Normal - in blue) generates lower EL, EL/CaR ratio and higher UL, UL/CaR ratio.
- Although, up to 99% confidence, Scenario 2 (Pareto - in red) generates a higher CaR, at 99,9% confidence, the CaR is slightly smaller for this scenario

# CDF under both Scenarios (Log Normal, Pareto) for the Bangladesh Case Study



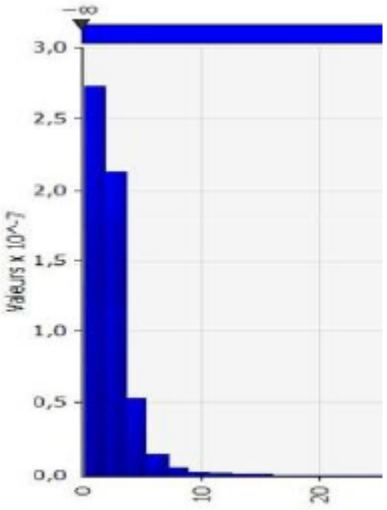

Scenario 1



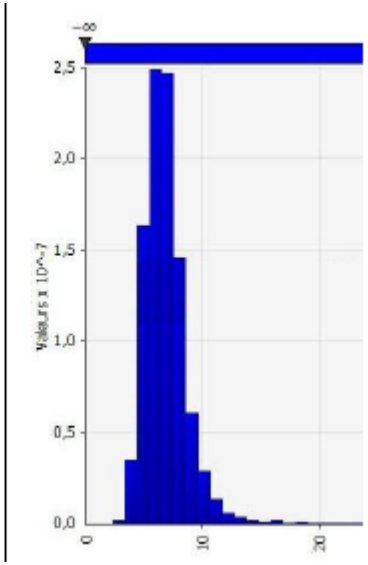

Scenario 2

- X-axis = values in billions $ of losses incurred
- Y-axis = probabilities of such losses incurring.
- 50% of losses under S1 are <3 billions $, under S2, 50% are <7 billions $
- Aggregate loss under S1 are much smaller compared to Under S2
- 50% of the losses under Scenario 1 are below 3 billion $
- whereas 50% of the losses under Scenario 2 are below 7 billion $

# PDF under both Scenarios (Log Normal, Pareto) for the Bangladesh case study




Scenario 1




Scenario 1

- X-axis = values in billions £ of losses
- Y-axis = probabilities of such losses incurring.
- 50% of losses under S1 are <3 billions $, under S2, 50% are <7 billions $
- Losses under S1 are concentrated on the left (values are between 0 and 3 billions) whereas in S2 values are between 5*10 billions
- Under S2, smaller UL, CaR Hence, S2 is suitable for risk-averse

# Conclusions

- Research outcomes: the findings allow insurers indentifying their risk appetite and exposure to cyber risk in order to implement a better pricing of cyber insurance products.

- Nobility: although the combination SA/LDA has been previously applied to operational risks, no previous research appeared to have specifically treated the lack of CR data using this method nor creating hypothetical CA

- Further Research: initial frequencies and severities, selection of indicators, environmental variables.
- developing an enterprise-wide solution for cyber risk.
- Will provide a Risk Registrer to capture the data in a comprehensive and systamatic way

# Key References


- Biener, C., Eling, M., & Wirfs, J. (2015). "Insurability of Cyber Risk: An Empirical Analysis", Geneva Papers on Risk & Insurance, Vol. 40, pp. 131-158
- Brown, G., & Cox, L. (2011). Making Terrorism Risk Analysis Less Harmful and More Useful: Another Try. Risk Analysis, 31(2), 193-195.
- Cambridge Center for Risk Studies. (2014a). Sybil Logic Bomb Cyber Catastrophe Scenario. Cambridge.
- Cambridge Center for Risk Studies. (2016). Managing Cyber Insurance Accumulation Risk;. Risk Management Solutions.
- Cambridge Centre for Risk Studies. (2014b). Cyber Insurance Exposure Data Schema V1.0. Cambridge, Cyber Accumulation Risk Management Working Paper. Available at http://cambridgeriskframework.com/page/20

# Key References


- CRO Forum (2014). Cyber Resilience - The cyber risk challenge and the role of insurance. Available at https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf
- CRO Forum (2016). Concept paper on a proposed categorisation methodology for cyber risk, Available at https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf
- Rodriguez, E., & Dominguez, J. (2008). Scenario analysis for modelling operational losses in the absence of data: the Spanish bank perspective. Journal of Financial Management and Analysis, 21(2), 1-10.
- Swiss Re (2017) "Cyber: getting to grips with a complex risk", Sigma, No. 1. Available at www.swissre.com/sigma
- Swiss Re (2016) "Cyber: in search of resilience in an interconnected world", Swiss Re and IBM joint survey. Available at http://media.swissre.com/documents/ZRH-16-09789-P1_Cyber%20Publication_web1.pdf