Telefónica Tech

PRACTICAL CASE

Quantification of Cyber Risk

A ransomware attack on a financial institution

Estevenson Solano
Senior GRC Consultant in Govertis, part of Telefónica Tech

telefonicatech.com

Índex

PREAMBLE

This case study presents a hypothetical scenario of a ransomware-type cyberattack on a financial institution with the objective of illustrating the application of cyber-risk analysis and quantification methodologies in a realistic context. Recognized frameworks such as ISO 27005, NIST 800-30 and the FAIR model are integrated through this exercise to estimate the potential financial loss, define mitigation strategies and evaluate the return on investment (ROI) in cyber security.

The analysis includes the use of advanced tools such as Monte Carlo simulation and Bayesian analysis, providing data-driven insights for informed decision making by senior management and corporate governance bodies. This approach allows prioritizing investments, aligning cyber security strategy with business objectives and strengthening resilience to new risks and cyber threats.

INTRODUCTION

This exercise analyzes a simulated ransomware incident affecting a financial institution, focusing specifically on the impact on its online banking services. The goal is to apply an integrated approach to cyber risk management and quantification that allows:

- Identify the threats, vulnerabilities and impacts associated with the attack.
- Quantify the risk using the FAIR model, estimating the frequency and magnitude of losses.
- Evaluate risk treatment options, such as mitigation or transfer through cyber insurance.
- Justify cyber security investment decisions based on return on investment (ROI) analysis.
- Integrate the results in corporate governance and strategic decision-making processes.

To this end, the ISO 27005 and NIST 800-30 methodological frameworks are combined as a reference for qualitative risk management, with FAIR for its financial quantification, complemented with analysis techniques such as Monte Carlo simulation and the Bayesian approach.

This case study is illustrative and didactic in nature and seeks to provide a replicable model for advanced cyber risk assessment in critical and highly regulated environments such as the financial sector.

Identify risk components taking into account existing ISO 27005 and NIST 800-30 approaches to identify threats, vulnerabilities, and impacts.

Threat Source

Organized ransomware groups targeting financial services.

Threat Event

A ransomware cyberattack encrypts critical banking systems.

Vulnerability

Outdated backup system and lack of proper segmentation in infrastructure and technology architecture.

Impact:

- Business interruption due to system failure.
- Financial losses due to ransomware payment **if paid**.
- Data recovery and forensic investigation costs.
- Potential legal and regulatory fines or penalties **GDPR, NIS2, DORA, SEC**.
- Loss of customers due to reputational damage.
- High impact economic and financial loss.

Quantifying cyber risk using the FAIR model

Identification of key factors

- **Loss Event Frequency (LEF):** Frequency with which this type of event is expected to occur in a year
- **Threat Event Frequency (TEF):** The probability that the cyberattack will occur.
- **Vulnerability (Vuln):** The probability that cyber defense controls and capabilities will fail.
- **Loss Magnitude (LM):** The financial impact of the event divided into **direct** primary and **indirect** secondary losses.

Estimation of FAIR Components

Loss Event Frequency (LEF) Estimation

Threat Event Frequency (TEF)

- Based on threat intelligence, **similar financial institutions face ransomware attempts every 2 months.**
- **LEF estimate:** 6 cyberattacks per year.

Vulnerability (Vuln) – Probability of a successful cyberattack

- **Existing security controls (backups, segmentation and endpoint) reduce the probability of success.**
- Security assessment indicates **40% probability of failure of cyber security controls by cyberattack.**
- **Vulnerability: 0,40**

Loss Event Frequency (LEF) Calculation

- LEF = TEF × Vulnerability
- LEF = 6 × 0.40 = 2.4 ransomware events per year.

Loss Magnitude Estimation (LM)

Loss magnitude estimation includes primary losses direct impact and secondary losses indirect **consequences such as legal and regulatory fines or penalties, reputational damage, etc.**

Primary losses (direct financial impact)	
Loss Category	**Estimated cost (USD)**
System downtime (2 days)	2.000.000
Ransom payment (if paid)	1.500.000
Data recovery and forensic investigation	800.000
Customer compensation	500.000
Total primary losses	4.800.000
Secondary losses (reputation and regulatory impact)	
Loss Category	**Estimated cost (USD)**
Regulatory fines(GDPR, SEC, etc.)	2.000.000
Customer chun and revenue loss	3.500.000
Increased cybersecurity investment	1.500.000
Total secondary losses	7.000.000

- **Total Loss Magnitude (LM) = Primary Loss + Secondary Loss**
- **LM = 4,800,000 + 7,000,000 = 11,800,000**

Annualized Loss Expectation (ALE) Calculation)ALE = LEF × LM

- **ALE = LEF × LM**
- **ALE = 2,4 × 11,800,000**
- **ALE = 28,320,000 for year**

Interpretation and treatment of risk by integrating ISO 27005 and NIST 800-30 to determine how to mitigate, transfer, accept or avoid risk.

Cyber risk treatment options

1. Risk mitigation: reduce the likelihood or impact

- Implement air-gapped protected immutable backups, with an investment of $1 million.
- Improve segmentation of critical banking systems, with an investment of $1.5 million.
- Improve ransomware detection and response technologies and tools, with an investment of $500,000.
- **Estimated risk reduction:** 60% vulnerability drop from 0.40 to 0.16.

2. Risk transfer: cyber security strategy

- Cyber insurance coverage with a $10 million policy, covering downtime or downtime, recovery costs and legal fees.
- Annual premium: $2 million.

3. Residual risk analysis

After mitigation, reassess and recalculate vulnerability.

- **New LEF = 6 × 0.16 = 0.96 (reduced from 2.4 events/year)**
- **New ALE = 0.96 × 11,800,000 = 11,328,000 (reduced from $28.3 million/year)**
- **Risk reduction = 60%.**

4. Decision making and business justification to C-suite and corporate governance

ROI on cybersecurity investment

- **Required investment (mitigation measures) = $3 million**
- **Expected reduction in annual losses = $28.3 million - $11, 3 million = $17 million.**
- **ROI = (Savings - Investment) / Investment**

- **ROI = ($17 million - 3 million) / $3 million = 466%**

Rationale for cybersecurity

- Cyber insurance policy ($10 million coverage) reduces financial exposure.
- After cyber security, maximum annual out-of-pocket loss is $1.3 million instead of $11.3 million.

Recomendation

- Invest $3 million in cyber security enhancements, **backups, segmentation, and endpoint.**
- Acquire a $10 million cyber insurance policy to cover residual risk.
- Annually monitor and improve risk modeling using NIST methodology and adjust risk quantification inputs.
- Keep corporate governance and C-level bodies (CEO, CFO, CISO, etc.) informed of cyber risk metrics to align with business strategy and regulatory compliance.

Assessment

Through this FAIR-based approach quantification analysis, integrating principles from ISO 27005 and NIST 800-30, provides a data-driven approach to cyber risk decision making, while enabling:

- The prioritization of cyber security investments based on financial impact.
- Reducing cyber exposure through targeted cyber defense controls and capabilities.
- Leveraging cyber security as a mechanism for risk transfer and agility.
- Ensure that cyber strategies are aligned with business objectives and regulatory requirements.

Annex

Considered analysis:

Additional Quantification Metrics

Mean Time to Detection (MTTD) and Mean Time to Response (MTTR) are essential to measure the effectiveness of cyber incident detection and response capabilities.

Current MTTD

- Industry average for ransomware cyberattacks: 24 hours.
- With SIEM and threat intelligence enhancements: 6 hours.
- MTTD before investment: 24 hours.
- MTTD after investment: 6 hours

Current MTTR

- Includes time to isolate affected systems, investigate, and execute response plans.
- Without advanced detection and response: 36 hours.
- With enhanced SOC and automated response: 12 hours.
- MTTR before investment: 36 hours.
- MTTR after investment: 12 hours

Impact on risk reduction, as faster detection and response can reduce the magnitude of losses by minimizing operational downtime and data exposure.

Return on cyber security investment (ROI)

The cyber security ROI is calculated as follows:

$$ROI = \frac{\textbf{Annual Loss Reduction} - \textbf{Investment Cost}}{\textbf{Investments Cost}} \times 100\%$$

- Investment in new cyber security controls (backups, segmentation, endpoint), $3 million.
- Annual loss reduction (from CRQ calculation): $17 million.

Calculation of cyber ROI:

$$ROI = \frac{17\ \text{M} - 3\ \text{M}}{3\ \text{M}} \times 100\% = 466\%$$

This ROI of 466% tells us that investment in cyber security is highly justified and provides significant financial benefits.

Risk reduction impact: Where faster detection and response can reduce the magnitude of losses by minimizing operational downtime and data exposure.

Recovery Point Objective (RPO)

Considering that it is the maximum tolerable period in which a data loss can occur.

- **Current RPO:** 24 hours (daily backups).
- **After investment (cloud and immutable backups):** 1 hour.

Reducing the RPO minimizes data loss, which is critical for financial transactions.

Recovery Time Objective (RTO)

Taking into account that this is the maximum time computer systems can be down before causing unacceptable damage.

- **Current RTO:** 48 hours (manual recovery and obsolete backups).
- **After investment (automated failover and recovery plan enhancements):** 8 hours.

Here a lower RTO ensures that business operations resume more quickly, reducing financial and reputational impact.

Work Recovery Time (WRT)

Considering that this is the additional time required after restoring IT systems to fully resume business operations.

- **Current WRT:** 12 hours (manual verification processes).
- **Optimized WRT:** 4 hours (automated validation and pre-tested recovery procedures).

Maximum tolerable downtime (MTD)

Taking into account that it is the maximum total downtime that a company can withstand before irreversible damage occurs.

- Business risk analysis indicates that the online banking system has a maximum tolerable downtime of 72 hours.
- Current recovery process (RTO + WRT): 60 hours.
- Optimized process (RTO + WRT): 12 hours, well below the MTD threshold.

It should be noted that it is confirmed that the improvements in RTO and WRT are in line with the business continuity objectives that include the cyber risk quantification metrics. We can see their influence.

Variable	Influence	Impact
Shorter MTTD and MTTR	Faster threat containment	Reduced exposure to cyber risk
Lower RPO	Minimizes data loss	Reduces financial and operational impact
Lower RTO & WRT	Faster system recovery	Reduces business interruption costs
MTD alignment	Ensures resilience	Prevents catastrophic business failure
High cyber ROI	Justifies cyver security investment	Improves decisión making

Financial modeling approach

1. Monte Carlo Simulation for loss estimation

I seek to model the financial impact through Monte Carlo simulations taking into account various risk factors, such as downtime, data loss, regulatory penalties, and reputational damage.

Assumptions and input variables:

- **Operational downtime:** estimated between 12 and 72 hours (triangular distribution, Mode = 24 hours).
- **Regulatory fines (GDPR, NIS2, DORA, SEC):** between $5 million and $50 million (normal distribution, mean = $25 million, SD = $10 million).
- **Probability of ransom payment:** 30% probability of payment, with ransom demands between $2 million and $10 million (uniform distribution).
- **Lost business revenue per hour:** between $1 million and $5 million (log-normal distribution, mean = $2.5 million).
- **Incident response and recovery costs:** between $3 million and $15 million (exponential distribution, mean = $7 million)

Upon applying the 10,000 Monte Carlo iterations, the expected financial loss ranges from $20 million to $150 million, with a 95% confidence interval of $45 million to $85 million.

2. Bayesian analysis for updating the probability of risk

Given prior incident data, Bayesian inference updates the probability of ransomware recurrence:

A priori probability:

- **Historical frequency of ransomware in financial institutions:** 10% per year

New data input:

- **Increase in attacks across the sector (+20% y/y).**
- Threat-specific information indicating that ransomware groups are being targeted.

Bayesian update application:

$$P(A|B) = \frac{\mathbf{P}\,(\mathbf{B}|\mathbf{A}) \cdot \mathbf{P}\,(\mathbf{A})}{P(B)}$$

- **Updated probability of ransomware:** 16% annually.
- **Adjusted annualized loss expectation (ALE):**

$$ALE = SLE\ x\ ARO$$

Where SLE (Single Loss Expectancy) = $65 M (from Monte Carlo)

ARO (annual rate of occurrence) = 0.16

ALE updated = $10.4 million per year

3. Key performance indicators (KPI)

Metric	Pre-Investment	Post-Investment (With Cybersecurity Enhancements)
Mean Time to Detect (MTTD)	24 hours	6 hours
Mean Time to Respond (MTTR)	36 hours	12 hours
Recovery Point Objective (RPO)	24 hours	1 hour
Recovery Time Objective (RTO)	48 hours	8 hours
Work Recovery Time (WRT)	12 hours	4 hours

4. Risk treatment and cost-benefit analysis

The financial institution considers the following strategies to mitigate ransomware risks:

Mitigation Strategy	Implementation Cost	Estimated Loss Reduction	Cyber ROI
AI-based Threat Detection	$3M	$17M	466%
Immutable Backups	$5M	$25M	400%
SOC Expansion	$10M	$35M	250%

Justification:

Investing $18 million in combined cyber security improvements results in an expected loss reduction of $77 million, demonstrating high ROI and strategic resilience.

Strategic implications and ERM integration

Integrating Monte Carlo and Bayesian analysis into your Enterprise Risk Management (ERM) framework,

- Aligns cyber risk with financial, credit, and liquidity risks.

- Improves regulatory compliance with GDPR, NIS2, DORA, and SEC cyber risk quantification mandates.
- Improves management-level decision making using data-driven risk analytics.

Heat map

We define each type of risk to visualize the current, inherent, and residual risk in a heat map:

- **Inherent risk:** The level of risk before any controls or mitigation measures are applied.
- **Current risk:** The level of risk with existing security controls, but before further treatment of the risk.
- **Residual risk:** The risk remaining after implementing cyber security enhancements.

INHERENT RISK					
Probability	IMPACT				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost definite					1
Probable					
Possible					
Improbable					
Rare					

Extreme Risks	1
High Risks	0
Moderate risks	0
Low Risks	0
TOTAL RISKS	1

1 **Risk Scenario ID**

CURRENT RISK					
Probability	IMPACT				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost definite					
Probable				1	
Possible					
Improbable					
Rare					

Extreme Risks	0
High Risks	1
Moderate risks	0
Low Risks	0
TOTAL RISKS	1

1 **Risk Scenario ID**

RESIDUAL RISK					
Probability	IMPACT				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost definite					
Probable					
Possible					
Improbable			1		
Rare					

Extreme Risks	0
High Risks	0
Moderate risks	1
Low Risks	0
TOTAL RISKS	1

1 **Risk Scenario ID**

Heat map interpretation

Risk Level	Probability	Impact	Level
Inherent Risk (Prior Controls)	Almost certain (80%)	Catastrophic ($100M+)	Extreme
Current risk (with existing security)	Probable (60%)	Major ($50M-$80M)	High
Residual risk (After AI-based detection, backups, SOC expansión)	Improbable (30%)	Moderate ($20M-$40M)	Moderate

I now return to assess the return on investment (ROI) calculation of cyber security controls by applying a financial modeling approach.

- The Bank invests $2.5 million in cyber security controls, including:
- AI-based threat detection
- Advanced firewalls
- Employee training
- Incident response enhancements

Prior to implementing these controls, the **estimated annual loss expectation (ALE)** from cyber incidents was $6 million.

After implementing the controls, the new estimated ALE is $2 million, a risk reduction of $4 million.

ROI Calculation

$$ROI = \frac{\text{Risk Reduction} - \text{Cost of Controls}}{\text{Cost of Control}} \times 100\%$$

$$ROI = \frac{(6\ \text{M} - 2\text{M}) - 2,5\ \text{M}}{2,5\ \text{M}} \times 100\%$$

$$ROI = \frac{(4\ \text{M} - 2,5\ \text{M})}{2,5\ \text{M}} \times 100\%$$

$$ROI = \frac{1,5\ \text{M}}{2,5\ \text{M}} \times 100\%$$

$$ROI = 60\ \%$$

Here we see that the investment in cyber security has a 60% ROI, which means that every dollar spent generates $1.60 in value by reducing cyber security-related losses.

Meaning that the bank in turn avoids an annual loss of $4 million by spending $2.5 million, which justifies the investment.

Monte Carlo simulation for cyber risk ROI

After running 10,000 simulations, the cyber security ROI is:

- **Median ROI:** ~59.5% (Aligns with our manual calculation).
- **10th percentile (Worst case):** ~2.7% (Lower than expected risk reduction).
- **90th percentile (Best case):** ~117.6% (Significant reduction in cyber losses).

Valuation

- Investment in cyber security consistently delivers a positive ROI in most scenarios.
- In the worst case, the ROI remains slightly positive, meaning that the investment does not generate financial losses.
- In the best case, the ROI more than doubles the initial investment.