QBER™

QUANTIFIED BUSINESS EXPOSURE TO RISKS

CYBER RISK QUANTIFICATION MODEL DESIGNED BY ZERON

CHAPTER 1

Introduction

In today's digital landscape, organizations face unprecedented cyber threats that can compromise their data, operations, and reputation. Cyber risk quantification has emerged as a critical tool for organizations to assess and manage their exposure to these threats effectively.

Significance of Cyber Risk Quantification:

Cyber risk quantification enables organizations to systematically evaluate and prioritize cybersecurity investments based on data-driven insights. By quantifying cyber risks, organizations can better understand the potential impact of cyber threats on their business operations, finances, and reputation, empowering them to make informed decisions about risk mitigation strategies.

Evolution of Cyber Risk Quantification:

The concept of cyber risk quantification has evolved over time in response to the growing complexity and sophistication of cyber threats. From simple risk assessments to advanced quantitative models, organizations have embraced various approaches to quantify cyber risks effectively.

Principles of Cyber Risk Quantification:

At its core, cyber risk quantification is guided by several fundamental principles that underpin its effectiveness. These principles include risk transparency, data-driven decision-making, and continuous improvement. By adhering to these principles, organizations can establish a robust framework for assessing and managing cyber risks proactively.

CHAPTER 2

Limitation of Existing Models

While traditional approaches to cyber risk quantification have made significant contributions to cybersecurity, they are not without their limitations. This chapter explores the shortcomings of existing models, such as the FAIR (Factor Analysis of Information Risk) model, and discusses the implications of these limitations for organizations.

Static Risk Assessments:

One of the primary limitations of traditional models is their reliance on static risk assessments that fail to account for the dynamic nature of cyber threats. Static risk assessments provide a snapshot of risk at a particular point in time, making them ill-suited to address the constantly evolving threat landscape.

Subjectivity and Simplification:

Traditional models often suffer from subjectivity and oversimplification, leading to inaccuracies and inconsistencies in risk assessments. These models rely on subjective inputs and simplified risk calculations, which can undermine their reliability and effectiveness in providing accurate risk assessments.

Inability to Capture Emerging Threats:

Moreover, traditional models struggle to capture emerging threats, vulnerabilities, and attack vectors, limiting their ability to provide timely and actionable insights to organizations. As cyber threats continue to evolve in complexity and sophistication, traditional models may become increasingly obsolete in addressing these emerging challenges.

CHAPTER 3

Quantified Business Exposure to Risks [QBER]

In response to the limitations of existing models, the Quantified Business Exposure to Risk (QBER) model offers a novel approach to cyber risk quantification that addresses these challenges. This chapter provides an in-depth exploration of the QBER model, highlighting its key features and functionalities.

Integration of Threat Intelligence:

At the core of the QBER model lies its integration of threat intelligence, economic models, and automated risk analysis techniques. By leveraging threat intelligence sources, the QBER model can identify emerging threats and vulnerabilities, providing organizations with timely and actionable insights into their cyber risk exposure.

Dynamic Risk Assessments:

Unlike traditional models, the QBER model offers dynamic risk assessments that adapt to the evolving threat landscape in real-time. By continuously monitoring cyber threats and vulnerabilities, the QBER model can provide organizations with up-to-date risk assessments that reflect the current state of their cybersecurity posture.

Data-Driven Decision-Making:

The QBER model enables data-driven decision-making by leveraging advanced analytics and mathematical simulations to quantify cyber risks. By providing organizations with actionable insights based on empirical data, the QBER model empowers stakeholders to make informed decisions about risk mitigation strategies.

CHAPTER 4

Parameters passed in QBER

Industry Sector

The sector in which the organization operates, influencing the types and levels of cyber threats faced.

Market Cap or Revenue

The financial size of the company, indicating its attractiveness as a target for cyber attacks.

Workforce

The size of the workforce, affecting the organization's attack surface and security requirements.

Security Solutions

The variety and effectiveness of cybersecurity solutions deployed, impacting the organization's overall security posture.

Line of Business

The diversity of business units and operations, each presenting unique cyber risk profiles.

Locations

The geographic spread of the company's operations, influencing regulatory compliance and exposure to regional threats.

Regulations

The regulatory frameworks applicable to the organization, dictating compliance requirements and security standards.

CHAPTER 5

Practical Implementation of QBER

Implementing the QBER model requires a systematic approach that encompasses data collection, risk assessment, and decision-making.

Data Collection:

The first step in implementing the QBER model is to collect comprehensive and accurate data about the organization's business units, assets, and operations. This may involve gathering data from internal sources, such as databases and network logs, as well as external sources, such as threat intelligence feeds and industry benchmarks.

Risk Assessment Methodologies:

Once the data has been collected, the next step is to assess cyber risks using the methodologies and techniques provided by the QBER model. This may involve conducting threat assessments, vulnerability scans, and scenario analysis to identify potential risks and their potential impacts on the organization.

Decision-Making Frameworks:

Finally, organizations must use the insights generated by the QBER model to inform decision-making and resource allocation. This may involve prioritizing risk mitigation strategies, allocating cybersecurity budgets, and implementing security controls to reduce the organization's exposure to cyber threats.

CHAPTER 5.1

Practical Implementation of QBER

Mathematical Calculations

Risk Assessment Score (RAS):

The Risk Assessment Score (RAS) is computed based on the aggregation of risk factors associated with each identified threat. The formula for calculating RAS is as follows

$$\text{RAS} = \sum_{i=1}^{n}(W_i \times I_i)'$$

Where, RAS = Risk Assessment Score, W_i = Weight assigned to the I_i^{th} risk factor and I_i = impact of I_i^{th} risk factor

The RAS provides a quantitative measure of the overall cyber risk exposure faced by the organization, considering both the likelihood and potential impact of cyber threats.

Cost-Benefit Analysis (CBA):

Cost-benefit analysis (CBA) is a fundamental component of the decision-making process in cyber risk management. It involves comparing the costs associated with implementing security controls against the potential benefits of reducing cyber risk. The formula for conducting a cost-benefit analysis is as follows

$$\text{CBA = Benfits - Costs}$$

Where, CBA = Cost Benefit Analysis, Benefits = Potentials benefits from implementinf security controls,
and Cost = Costs associated with implementing security controls

Return on Security Investment (ROSI):

Return on Security Investment (ROSI) is a metric used to evaluate the effectiveness of cybersecurity investments in mitigating cyber risk. It is calculated by comparing the expected reduction in potential financial losses (Benefits) against the costs associated with implementing security controls (Costs). The formula for calculating ROSI is as follows

$$\text{ROSI = CBA/Costs}$$

ROSI provides organizations with a quantitative measure of the cost-effectiveness of their cybersecurity investments, enabling them to prioritize resource allocation and risk mitigation strategies effectively.

CHAPTER 6

Gordon Loeb Model with QBER

Integration of Economic Models:

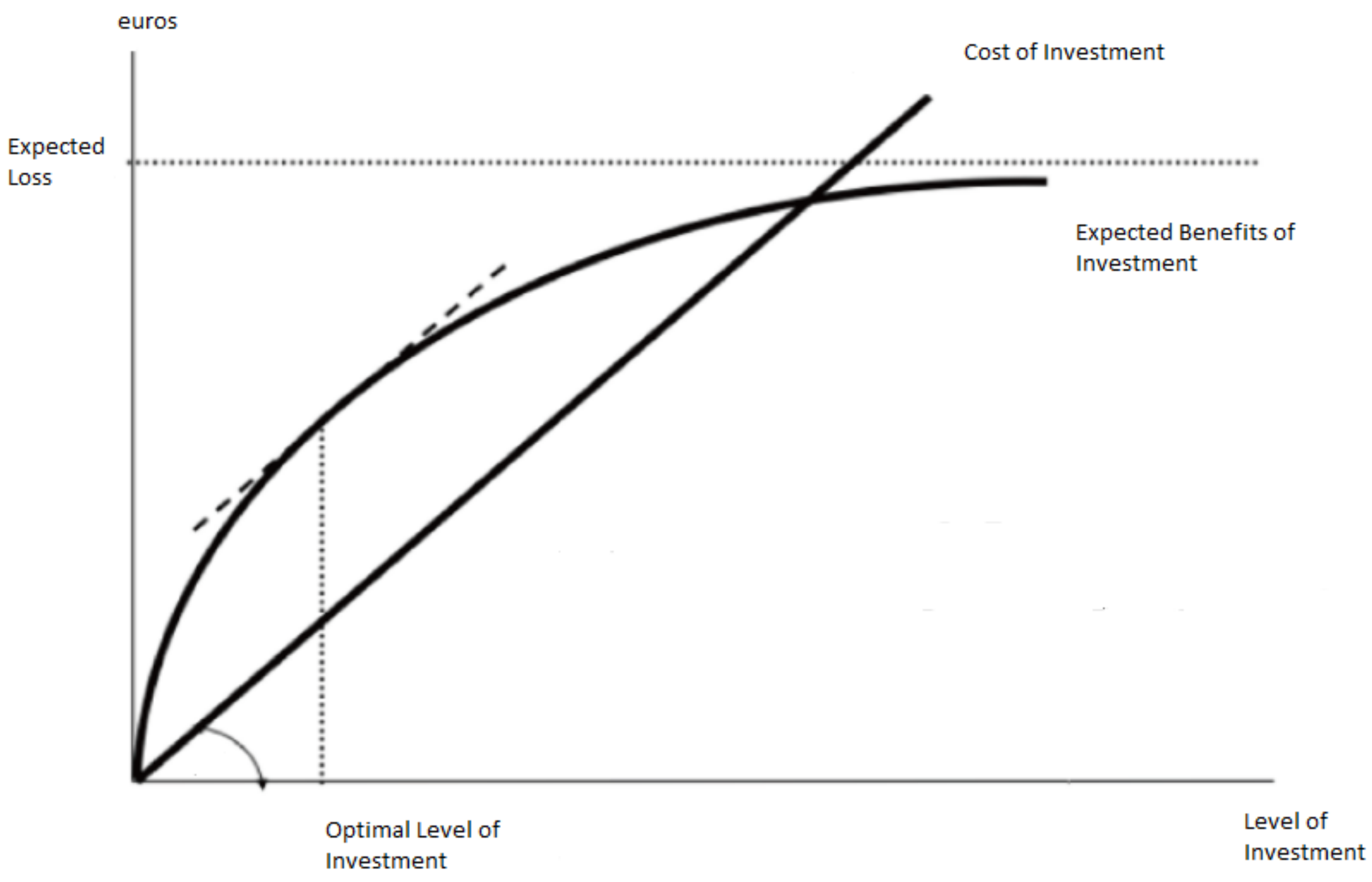
The basic components of the Gordon-Loeb model are as follows:

- Data (information) sets of organizations that are vulnerable to cyber-attacks. This vulnerability, denoted as v (0 ≤ v ≤ 1), represents the probability that a breach to a specific information set will occur under current conditions.

- If an information set is breached, the value of the information set represents the potential loss (i.e., the cost of the breach) and can be expressed as a monetary value, denoted as L. Thus, vL is the expected loss from a cyber breach prior to an investment in additional cybersecurity activities.

- An investment in cybersecurity, denoted as z, will reduce v based on the productivity of the cybersecurity investment. The productivity of investment is what the Gordon-Loeb model refers to as the security breach probability function.

Gordon and **Loeb** were able to show that, for two broad classes of security breach probability functions, the optimal level of investment in information security, z*, would not exceed roughly 37% of the expected loss from a security breach. More specifically: z* (v) ≤ (1/e) vL.



Decision-Making Frameworks:

Moreover, the integration of the Gordon-Loeb method with the QBER model enables organizations to develop robust decision-making frameworks that consider both technical and economic factors. By incorporating economic considerations into the risk assessment process, organizations can make more informed decisions about resource allocation and risk mitigation strategies.

CHAPTER 6.1

Gordon Loeb Model with QBER

Mathematical Calculations

Expected Loss (EL)

The Expected Loss (EL) represents the anticipated financial loss resulting from potential cyber threats. It is calculated as the product of the Annualized Rate of Occurrence (ARO) of the threat and the Single Loss Expectancy (SLE) associated with the threat. The formula for calculating EL is as follows

$$\text{EL} = \text{ARO X SLE}$$

Where, EL = Expected Loss, ARO = Annualised Rate of Occurrence [data taken from Threat Intel in real time], and
SLE = Single Loss Expectancy [data taken from Financial Threat Intel]

Optimal Security Investments (OSI)

QBER determines the Optimal Security Investment (OSI) by comparing the expected reduction in potential financial losses resulting from the implementation of security controls against the baseline expected loss, considering LOB-specific risk factors. The formula for calculating OSI with LOB considerations is as follows

$$OSI_{\text{Total}} = \sum_{i=1}^{n} OSI_{\text{LOB}_i}$$

Where, $\text{OSI}_{\text{Total}}$ = Total Optimal Security Investments, n = Number of Line of Business (LOBs),
OSI_{LOBi} = Optimal Security Investment for the i^{th} Line of Business

Risk Mitigation Factor

QBER calculates the Risk Mitigation Factor (RMF) by comparing the expected reduction in potential financial losses resulting from the implementation of security controls against the baseline expected loss. In addition to technical factors, QBER incorporates LOB considerations into the calculation of RMF to account for the unique risk profiles of different business units

$$RMF_{\text{LOB}} = \frac{(EL_{\text{LOB}} - EL_{\text{LOB}_{\text{new}}})}{EL_{\text{LOB}}} \times 100\,\%$$

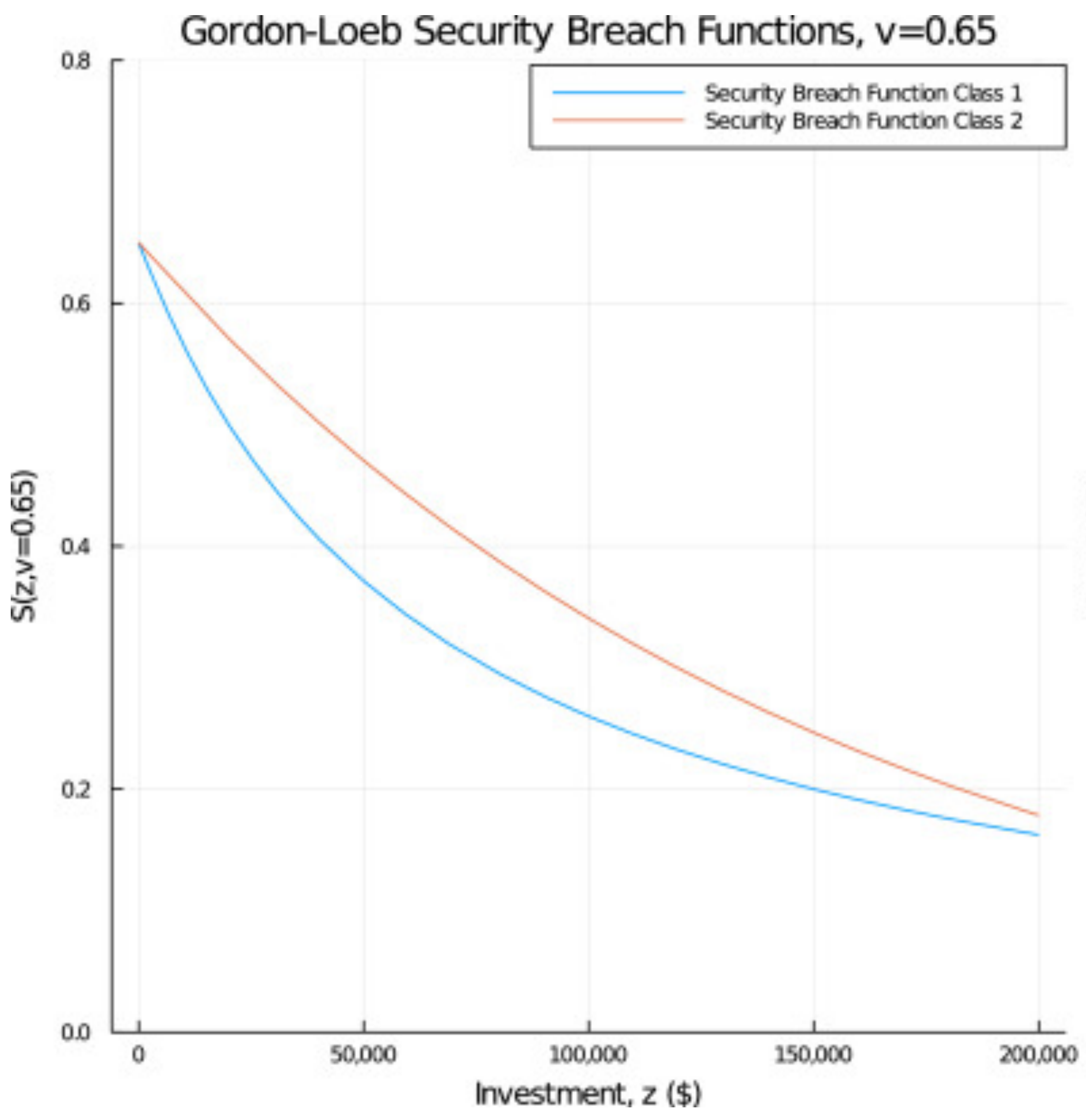
CHAPTER 7

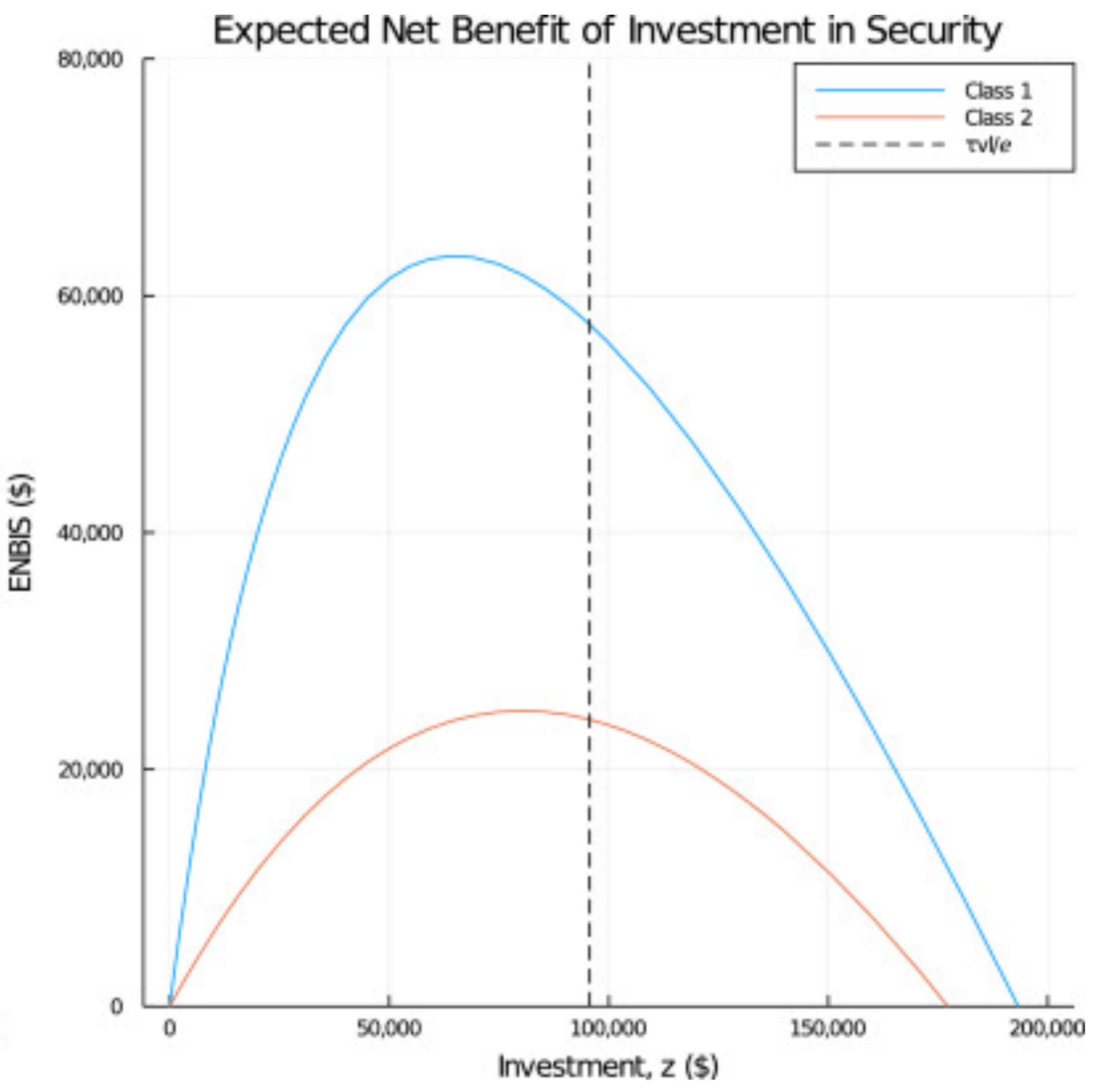
Real Cyber Value at Risk with QBER

The Real Cyber Value at Risk (Real CVaR) represents the potential financial loss an organization faces due to cyber threats, considering both the probability of occurrence and the magnitude of impact. Unlike traditional approaches that rely solely on generic models, the Real CVaR takes into account organization-specific factors to provide a more accurate estimation of cyber risk.

To calculate the Real CVaR, QBER integrates the Gordon-Loeb equation with organization-specific factors, namely Expected Loss (EL), Optimal Security Investment (OSI), and Risk Mitigation Factor (RMF) for each Line of Business (LOB). This integration allows us to tailor the cyber risk assessment to the unique characteristics and risk appetite of the organization.

$$Real\ CVaR = \sum_{i=1}^{n} (EL_{\mathrm{LOB}_i} - (OSI_{\mathrm{LOB}_i} \times RMF_{\mathrm{LOB}_i}))$$





Where

EL = Expected Loss

OSI = Optimal Security Investment

RMF = Risk Mitigation Factor

LOB = Line of Business

n = No of LOBs

Comparison with other Industry Models

Feature	QBER	FAIR	OCTAVE
Granularity	Provides fine-grained analysis by considering business units and segments for accurate risk assessment.	Generally lacks granularity, typically focuses on high-level risk factors without detailed segmentation.	Typically focuses on organizational-level risks without detailed segmentation of business units.
Integration of Threat Intelligence	Integrates threat intelligence from OSINT and industry reports, enhancing the accuracy of risk analysis.	Does not emphasize integration of external threat intelligence sources as a primary feature.	Does not emphasize integration of external threat intelligence sources as a primary feature.
Dynamic Risk Assessment	Dynamically assesses security control effectiveness and adapts to changes in the cybersecurity landscape.	May lack dynamic adaptability, often requiring manual updates to reflect changes in the threat landscape.	May lack dynamic adaptability, often requiring manual updates to reflect changes in the threat landscape.
Cost-Benefit Analysis	Incorporates a modified Return on Security Investment (ROSI) model for cost-effective security investments, providing actionable recommendations based on cost-benefit analysis.	May lack a comprehensive cost-benefit analysis framework for evaluating security investments.	May lack a comprehensive cost-benefit analysis framework for evaluating security investments.

Thank
You

ZERON

www.zeron.one | info@zeron.one

409 ATL Corporate Park, Saki Vihar Road, Powai,
Mumbai, Maharastra 400072

Teamcognito products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. Teamcognito does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding Teamcognito's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.