Quantitative measurement of the impact of security breaches

Oluwatosin Falebita
Computer Science
Colorado state University
oluwatosin.falebita@colostate.edu

Srivarshini Ksheerasagar
Computer Science
Colorado state University
varsh@colostate.edu

Sarthak Bharadwaj
Computer Science
Colorado state University
sarthak7@colostate.edu

***Abstract*—To recognize, better comprehend, and investigate more efficient mitigation techniques for the dangers and expenses associated with cyberattacks. Techniques to create methods that calculate the likelihood of a security breach, which may be used to evaluate risk and create a variety of measures. Introducing TSS Model that properly evaluates the impact of Security breaches.**

***Index Terms*—cyberSecurity, cyber breaches, TSS Model**

I. Introduction

The absence of established techniques for evaluating the quantitative impact of losses brought on by security breaches is a major problem in the field of cybersecurity. Overestimations have resulted from this shortcoming, which can be especially harmful when businesses try to put security procedures in place to reduce possible losses. As a result, without precise projections of possible financial losses, businesses might not be able to maximize their information security expenditures.

Our area of research is focused on developing new metrics for measuring the impact of cyber breaches. Traditional metrics, such as the number of records breached or the amount of money stolen, are often inadequate for capturing the full impact of a breach. For example, a breach that exposes sensitive customer data may damage a company's reputation and lead to lost sales, even if no money is stolen.

A formal quantitative model and a methodical approach based on the concept of cyber value at risk of records and other considerations must be used to estimate the overall cost. Because crucial factors in determining the danger of data breaches are ignored, current approaches for estimating the cost of security breaches are ineffective.

We are creating new measures that account for the whole spectrum of effects from a security breach, such as the cost of fixing the breach and the cost of missed sales and productivity. Research is also being done to provide techniques for calculating the likelihood of a breach. Utilizing this data will enable the assessment of risk and the creation of more potent mitigation plans. Researchers are estimating the likelihood of a breach using a range of techniques, such as:

- Examining surveys of existing models used in measuring the impact of cyber breaches.
- Propose the TSS model to estimate the impact of cyber breaches.

We tried to introduce a Model that addresses all the issues mentioned above to estimate the impact of cyber breaches called the TSS Model that considered various factors such as- costs, financial impact, downtime, Customer Trust and reputation impact, fine on Penalties, etc.

II. Literature Review

In this section, we explore core principles that are essential for developing a thorough understanding of previous studies on evaluating the consequences of security breaches. In this study, we delve into the complexities of risk management in the context of corporate cybersecurity, aiming to provide a comprehensive understanding of the various factors involved in measuring the impact of security breach. Subsequently, we present a complete analysis of the predominant standard model utilized for assessing the financial implications of security breaches, so facilitating a thorough comprehension of the traditional methodologies applied for quantifying the costs involved. In order to deepen our comprehension of the topic, we then explore the notion of Cyber Value at Risk, emphasizing its importance and pertinence within the domain of cybersecurity.

A. Risk and impact of Security breach

Risk, frequently expressed as the product of the impact and the probability of occurrence [1], is a widely used term to denote the potential for loss and injury. Unpredictability is an inherent characteristic of risk, which presents a formidable obstacle in accurately forecasting the precise consequence. The degrees of variation in the implications of risk are contingent upon the context and extent of the discourse. Efficiently managing the complex challenges presented by cyber threats in the domain of cybersecurity, which intersects with corporate operations, requires a fundamental comprehension of risk. This necessitates the assessment of the probable outcomes and their potential repercussions, all within the context of risk management as a whole. The management of risk encompasses several strategies such as mitigation, reduction, ignoring, transfer, and acceptance, particularly when supported by sound economic rationale. One of the foremost challenges confronting firms in the modern era is the susceptibility to security breaches, which engenders a range of tangible and intangible expenses capable of profoundly disrupting the entirety of a company's operations. In relation to the varying expenses associated with cyberattacks, it was observed that Multinational Enterprises

(MNEs) incurred an average cost of US$ 1.09 million for data breaches in 2020, which represented a decrease from the US$ 1.41 million incurred in 2019. Conversely, Small and Medium Enterprises (SMEs) experienced an average cost of US$ 101,000 for such incidents in 2020, as opposed to the US$ 108,000 incurred in 2019 [3]. In addition to the financial implications of cyberattacks, there exist various costs associated with penalties levied by governmental bodies and other entities on non-compliant enterprises in relation to cybersecurity rules. From July 2017 to November 2022, it was observed that the implementation of the General Data Protection Regulation (GDPR) in Europe led to the imposition of 837 fines, amounting to a cumulative sum of C 1.2 billion in penalties. The predominant form of violation seen was the lack of enough legal grounds for data processing, resulting in 209 penalties. Additionally, there were 179 instances where insufficient technological and organizational measures were implemented to safeguard information security. Furthermore, 128 fines were imposed for non-adherence to general rules governing data processing.

B. Surveys of existing models used in measuring the impact of cyber breaches

In our studies of various papers as well as articles, there was one such article that allowed researchers to evaluate the impact of a security breach on a company's stock returns by comparing the returns following the breach to the returns before the breach.[2] The article aims to investigate the likelihood of a shift in investor's evaluations of the costs of information security breaches and to assist resolve the conflicting data regarding the impact of breaches on enterprise's stock market returns. The fundamental one-factor CAPM market model Numerous accounting, economics, and finance research have made considerable use of the one-factor CAPM model. The one-factor market model has also served as the foundational technique for the information security breach. Apparently, what has been observed is that, Investors seemed to have estimated the costs of breaches that happened after 9/11—including potential future revenue losses—to be lower than the costs of breaches that happened before 9/11. These results provide fresh insight into the conflicting findings of past research and highlight significant questions for further investigation. As mentioned in the paper, Some earlier research has treated security breaches as a general (i.e., all-encompassing) category, without making a distinction between the various types of breaches. However, the paper contradicted its own statement explaining the commonly used categories that categorizes information security breaches: information availability breaches (i.e., breaches that prevent authorized users of information from having timely access to such information, including breaches commonly referred to as "denial of service" [DOS]); information confidentiality breaches (i.e., breaches that allow unauthorized users access to confidential information); and information integrity breaches (i.e., breaches that deface websites). Undoubtedly, a few data security breaches fall into more than one of the aforementioned categories. When considered collectively,

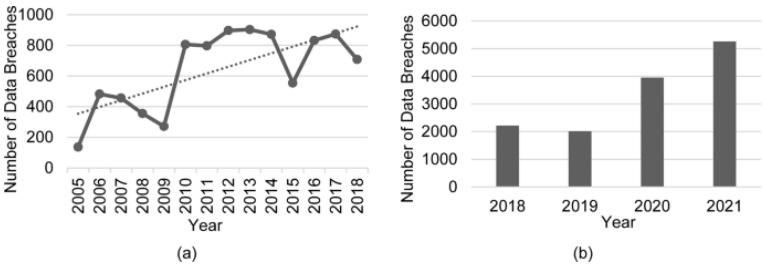

Fig. 1. Data Breaches over the years

the current study's findings indicate that the average cost of information security breaches has decreased recently. This means that rather than seeing information security breaches as a potentially major threat to a company's ability to survive economically, investors now seem to be more inclined to regard them as a business "nuisance" or just another ongoing operating expense.

There is cause for grave concern over investors' seeming change of perspective on breaches of information security. Corporate executives are likely to interpret security breaches as a signal from investors to maintain current levels of information security investment in their companies, or at the very least, not raise them considerably, if they believe that security breaches are more of a bother than a potentially catastrophic economic threat to their survival. Such a viewpoint is misplaced given that an unanticipated significant breach—the so-called "black swan"—has the ability to jeopardize a firm's ability to survive.

Malaiya et.al develops a comprehensive, formal model that estimates the two components of security risks: breach cost and the likelihood of a data breach within 12 months using combination of formulars that evaluates costs such investigation costs, Crisis management cost per record(CMCPR), Regulatory and Industry Sanctions Cost(SCPR), Class Action Lawsuit Cost per Record(CALCPR), Computation of Data Breach Cost(CDBC), and Security Costs Regardless of Data Breach(SCRDB)[3].

The final formula is as follows-

$$P_i = F_C * F_{BDM} * F_I * F_{BC} * F_E * F_P * \alpha e^{(-\beta x)}$$

III. Methodology

Our proposed methodology seeks to develop a comprehensive model that provides a quantitative measurement of the impact of security breaches. Security breaches can significantly affect an organization's ability to maintain business continuity. In this endeavor, we have taken into account a wide spectrum of potential impacts arising from security breaches and have formulated the Total Security Impact (TSS) model to precisely quantify the cumulative impact of such breaches.

Business continuity, as defined in , revolves around minimizing resource costs on which various organizational processes rely, while simultaneously maximizing their returns. It is a fundamental goal for organizations aiming to ensure the seamless flow of their operations. However, the quantification

of security breach impacts goes beyond mere cost considerations; it's about managing and mitigating the consequences of security incidents that pose threats to the very survival of organizations, emanating from both internal and external sources.

Our novel approach combines these two critical concepts, leading to the development of the- "TSS dynamic cost model". This model enables organizations to quantify the impact of security incidents in terms of resource allocation required to respond to the changes triggered by a security breach. Furthermore, it takes into account the associated costs stemming from the effects of these changes.

One critical issue in the field of cybersecurity is the lack of standardized methods for assessing the quantitative impact of damages caused by security breaches. This deficiency has led to the occurrence of overestimations, which can be particularly detrimental when organizations attempt to implement security controls to minimize potential losses. Consequently, organizations may not be fully equipped to optimize their investments in information security due to the absence of accurate estimates concerning potential financial losses.

The development of the TSS dynamic cost model addresses these concerns by offering a structured framework for quantifying the impact of security breaches. This model provides organizations with a means to assess the direct and indirect costs associated with breaches, which can be invaluable for budget allocation and resource management. By quantifying the impact, organizations gain a better understanding of the financial consequences and can make more informed decisions about the allocation of resources and investments in security controls.

The TSS model integrates the financial impact, data impact, operational impact, Reputational impact

A. Measuring the Impact of Security Breach

A "breach" refers to a significant security incident in which control over data is compromised or lost, resulting in unauthorized disclosure, acquisition, or access to sensitive information. This can encompass scenarios where someone who is not an authorized user gains access to, or potentially could access, personally identifiable information (PII), or when an authorized user accesses PII for purposes not sanctioned or authorized.[4]

An occurrence of a security can lead to-

- Loss of Control: The occurrence of a breach can result in a situation where an organization or entity loses control over its data. This can occur due to a variety of reasons, such as a cyberattack, insider threat, or technical vulnerabilities.
- Compromise: Data compromise refers to the situation where there is a risk to the availability, confidentiality, or integrity of the information. Data that has been compromised is susceptible to unwanted access or modification.
- Unauthorized Disclosure: This is when private information is accidentally and unintentionally made public. There may have been a breach that resulted in the disclosure, which frequently raises security and privacy issues.
- Unauthorized Acquisition: Acquisition is the term used to describe the unapproved acquisition of data.

IV. Modifications

- Factors to consider for Financial Impact:
  Direct costs (D)- Expenses related to breach detection, containment, recovery, and legal and regulatory compliance. Indirect costs (I)- Loss of revenue, damage to brand reputation, and long-term customer churn. Formula for Financial Impact (F):- F = D + I
- Factors to consider for Data Impact:
  Volume of data compromised (V)- The amount of data exposed or stolen during the breach. Data sensitivity (S)- The importance of the data in terms of its confidentiality, integrity, and availability. Formula for Data Impact (D):- D = V * S
- Factors to consider for Operational Impact:
  Factors to consider: Downtime (T)- The duration of operational disruption caused by the breach. Recovery and remediation costs (R)- Costs associated with restoring systems and services. Formula for Operational Impact (O):- O = T * R
- Factors to consider for Reputational Impact:
  Customer trust impact (C)- The degree to which customer trust and loyalty are affected. Media coverage (M)- The extent and tone of media coverage related to the breach. Formula for Reputational Impact (R):- R = C + M
- Factors to consider for Regulatory and Legal Impact:
  Fines and penalties (P)- Legal and regulatory fines and penalties imposed on the organization. Legal costs (L)- Expenses associated with lawsuits and legal actions. Formula for Regulatory and Legal Impact (RL):- RL = P + L
- Factors to consider for Supply Chain Impact:
  Impact on suppliers (SI)- The effect of the breach on suppliers and their ability to deliver goods or services. Impact on customers (CI)- How the breach affects the organization's ability to meet customer demands. Formula for Supply Chain Impact (SC):- SC = SI + CI
- Factors to consider for Employee and Stakeholder Impact:
  Employee morale (EM)- The effect on the well-being and morale of the organization's employees. Impact on stakeholders (ST)- The impact on investors, partners, and other stakeholders. Formula for Employee and Stakeholder Impact (ES):- ES = EM + ST
- Factors to consider for Long-Term Consequences:
  Ongoing security costs (OS)- The additional security investments required to prevent future breaches. Loss of competitive advantage (CA)- The long-term impact on the organization's market position. Formula for Long-Term Consequences (LC):- LC = OS + CA

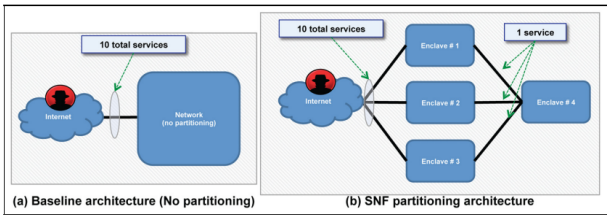

Fig. 2. Enclave model in SNF's network partitioning architecture

A. Existing Model

Considering all the above factors, we searched for sources that addressed all of the issues and considered all of the factors for evaluating a proper security breach impact and then came across the "risk-adjusted ROSI" (RaROSI), which takes into account the worst cases. The idea is to consider the difference between the expected loss without the mitigation effect of the investment E[L] and the worst case loss, at a given confidence level 'alpha', mitigated by the investment[5].

$$RaROSI_{\alpha} = \frac{\delta U[L] - I_0}{I_0}$$

B. Enclave Model

The enclave model seeks to characterize the dynamics of attack and defense, at the device level, within a single enclave . The model aims to capture the threat model of an attacker who penetrates the enclave by compromising a single enclave device and attempts to spread to other enclave devices. The model uses an epidemic model to capture device-to-device infection spreading within an enclave. The enclave model is parameterized by outputs from testbed experiments and simulation runs are executed on this model to inform the network model[6].

C. Proposed Model

TSS Model = Financial Impact (FI) + Data Impact (DI) + Operational Impact (OI) + Reputational Impact (RI) + Regulatory and Legal Impact (RL) + Supply Chain Impact (SC) + Employee and Stakeholder Impact (ES) + Long-Term Consequences (LC)

$$TSS = FI + DI + OI + RI + RL + SC + ES + LC$$

The formula that we came up represents a way to assess and quantify the overall impact of a security breach on all the possible dimentions. The formula is essentially an attempt to provide a comprehensive assessment of the impact of a given breach by breaking it down into different dimensions. By considering each of these dimensions and quantifying their impact, you can gain a more holistic view of the consequences of a particular event or decision.

The formula you've provided represents a way to assess and quantify the overall impact of a particular event, decision, or situation, which can have multiple dimensions or aspects. Let me break down the components of the formula:

Financial Impact (FI): This part of the formula considers the financial consequences or effects of the event or situation. It could involve gains or losses, increased or decreased revenue, and any other financial implications.

Data Impact (DI): Data impact assesses the effect on data-related aspects. This can include data breaches, data loss, data quality issues, and any other data-related consequences.

Operational Impact (OI): Operational impact looks at how the event affects the day-to-day operations of an organization. It might involve disruptions, process changes, or efficiency improvements.

Reputational Impact (RI): Reputational impact considers how the event affects the organization's image, brand, and reputation. Positive events can enhance reputation, while negative events can damage it.

Regulatory and Legal Impact (RL): This component assesses the impact of the event on compliance with laws and regulations. It includes legal consequences, fines, and any regulatory actions.

Supply Chain Impact (SC): Supply chain impact evaluates how the event affects the supply chain, including disruptions in the production and distribution of goods or services.

Employee and Stakeholder Impact (ES): This part looks at how the event affects employees and stakeholders. It might include their well-being, satisfaction, and any changes in their relationship with the organization.

Long-Term Consequences (LC): Long-term consequences consider the lasting effects of the event, decision, or situation. This can include long-term financial implications, changes in market position, or ongoing reputation effects.

These notations depict several aspects of a situation whose calculations are showed in the "Modifications" section.

The formula is essentially an attempt to provide a comprehensive assessment of the impact of a given situation by breaking it down into different dimensions. By considering each of these dimensions and quantifying their impact, you can gain a more holistic view of the consequences of a particular event or decision.

The total "TSS" score is the sum of these individual impacts, giving you an overall assessment of the situation that takes into account its multifaceted nature. This can be a useful tool for decision-making, risk assessment, and impact analysis in various contexts, such as business, project management, and crisis management.

V. Questions our Research Answered

Research Question 1- While adressing about an an Economic Approach to Estimating Cyberattacks Costs using Data from Industry Reports, the author stated that current approaches fail to provide individualized and quantitative monetary estimations of cybersecurity impacts[8].

Answer- The Real Cyber Value at Risk (RCVaR) concept is proposed by the author. This study examines cybersecurity data derived from publicly available sources and integrates it with economic methodologies to forecast the expenses and corresponding variations (i.e., risks) connected with cyberattacks

against corporations. The RCVaR (Robust Conditional Value at Risk) framework is grounded in sound economic methodologies, including real-world data rather than relying solely on probability estimations. Firstly, it introduces a methodology for extracting and statistically analyzing cybersecurity-related information from industry reports. Secondly, it proposes a model that utilizes real-world business information and security measures to estimate the potential costs of cyberattacks in advance. Thirdly, it computes the Cyber Value at Risk (CVaR) by utilizing quantitative data from security reports, which is a departure from traditional approaches that rely on probability estimations to quantify deviations from expected cost values. Lastly, the article introduces a user-friendly web-based tool for cost and risk analysis, which employs the RCVaR methodology.

Research Question-2 How does the modularized hierarchical simulation framework[6] work in modeling a complete cyber system?

Answer- The modularized hierarchical simulation framework allows the model to incorporate data from testbed experiments, reduces implementation effort by dividing the simulation model into multiple components, and supports quicker simulation execution times due to reduced complexity at the larger scale network model .This structure provides a flexible and re-usable simulation framework, allowing different versions of one component model to be substituted into the framework without changing the underlying implementation of other component models, and a component model may be used as part of multiple complete simulation models with potentially little or no modification.

VI. Contributions

Tosin- Summary of work- After researching about cyber security on various levels, came up with the factors effecting the measurement of security breaches Challenges faced: There were too many factors that effected the precise calculation of impact of security breaches, therefore we categorized the main factors that helped in coming up with the model. Meanwhile, we could not find any publicly available data to test the model as at the moment of writing the report.

Srivarshini- Summary of work- Researched about the impact of security breaches exspecially in stock markets and observed that there was a negative impact of breaches on the stock market. Had to research about what factors actually is being effected but the security breach and collectively decided on what parameters to be used. Challenges faced- Had to go through several years of reports of all news.

Sarthak - Summary of work- Compile a list of relevant papers and gave a summary of each which was used in part literature review

VII. References

[1] S. Kaplan and B. J. Garrick, “On The Quantitative Definition of Risk,” Risk Analysis, vol. 1, no. 1, pp. 11–27, 1981

[2] Gordon, Lawrence A., Loeb, Martin P., and Zhou, Lei. ‘The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?’ 1 Jan. 2011:33–56.

[3] Algarni, Abdullah M., Vijey Thayananthan, and Yashwant K. Malaiya. ”Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems.” Applied Sciences 11.8 (2021): 3678.

[4] Ko, M. and Dorantes, C., 2006. The impact of information security breaches on financial performance of the breached firms: an empirical investigation. Journal of Information Technology Management, 17(2), pp.13-22.

[5] Kim, Sanghee, and Seongjoo Song. ”Cyber risk measurement via loss distribution approach and GARCH model.” Communications for

[6] Statistical Applications and Methods 30.1 (2023): 75-94. Quantifying the mission impact of network-level cyber defensive mitigations Neal Wagner, Cem Sx Sxahin, Michael Winterrose, James Riordan, Diana Hanson, Jaime Pen˜a and William W Streilein

[7] Franco, Muriel Figueredo, et al. ”RCVaR: an Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports.” arXiv preprint arXiv:2307.11140 (2023).

[8] Orlando, Albina. ”Cyber risk quantification: Investigating the role of cyber value at risk.” Risks 9.10 (2021): 18

[9] Carfora, Maria Francesca, and Albina Orlando. ”Quantile based risk measures in cyber security.” 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2019.

[10] H. Aver, “Cybersecurity Economics,” September 2020, Available at https://www.kaspersky.com/blog/it-security-economics-2020-main/ 37205/.