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*—Security breaches persist in outpacing state-of-the-art preventive measures. Consequently, organizations must employ quantitative measures that offer greater efficiency in assessing the impact of cyberattacks. This paper introduces the TSS Model as a proposed framework for enhancing quantitative cost efficiency in evaluating the repercussions 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, 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[20]. 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[15]. 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[21]. 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 [18]. 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, 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[22].

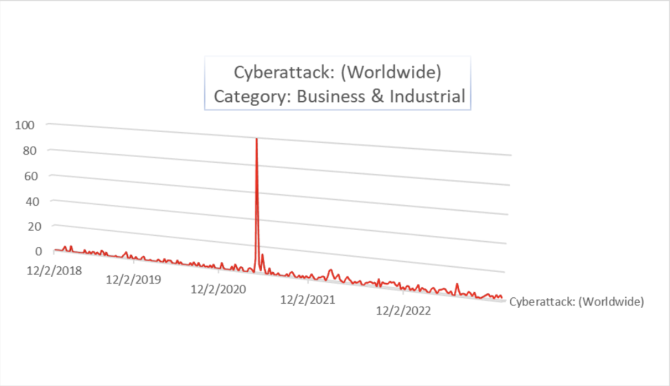


Fig. 1. Data Breaches over the years in Business and Industrial landscape

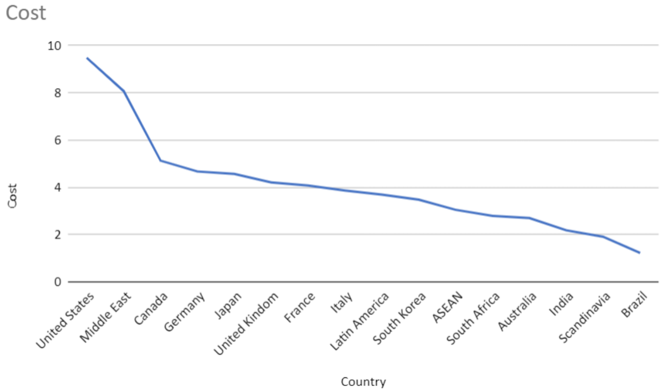


Fig. 2. Data Breaches over the world in various Countries

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 [23]. 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 [17]. 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 [12] and [13], 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.

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[15]. 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.

B. 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].

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

C. 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[16]. The enclave model is parameterized by outputs from testbed experiments and simulation runs are executed on this model to inform the network model[6].

IV. Proposed Model

TSS model builds on the existing model to calculate the quantitative impact of a security breach by calculating the impact of the following factors: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).

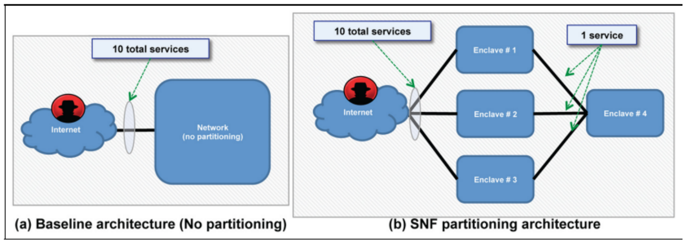


Fig. 3. Enclave model in SNF's network partitioning architecture

A. 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.

Factors to consider for Data Impact:

a. Total Cost per Record (TCPR): The amount of data exposed or stolen during the breach.

b. Data sensitivity (S): This is a measure of the importance of the data in terms of its confidentiality, integrity, and availability.

We assigned a weight to the data based on sensitivity on a scale of 0 to 1 using the ISO 27001 information classification standard [11].

TABLE I
DATA SENSITIVITY METRIC

Classification	Sensitivity	Multiplication metrics
Restricted	Critical	0.95
Confidential	High	0.90
Internal	Medium	0.87
Public	Low	0.55

$$DI = TCPR * S$$

B. Operational Impact (OI)

Operational impact looks at how the breach affects the day-to-day operations of an organization. It might involve disruptions, process changes, or efficiency improvements.

Operational impact is measured by multiplying the downtime of a service by the cost associated with restoring the service.

$$OI = T * R$$

To restore IT services and components quickly in the event of a failure, we look at the time to repair, which depends upon whether a component is repairable or not.

For repairable assets, we look at two different values

a. Mean Time Between Failures (MTBF): The average time gap between failures of a repairable component is simply the average amount of time that passes between failures of a repairable asset.

$$MTBF = TotalOperatingTime/NumberofFailures$$

b. Mean Time to Repair (MTTR): The average time required to return a repairable component to service it is the amount of time that an asset will be out of service for repair for each time that it fails.

$$MTTR = TotalRepairTime/totalnumberofFailures$$

For non-repairable assets, the most important metric is The Mean Time To Failure (MTTF): The average time a non-repairable component will last. Half of the assets of that type will fail before the MTTF, and half will last longer than the MTTF. To calculate MTTF, we divide the total number of hours of operation by the total number of assets in use.

$$MTTF = Totalhoursofoperation/Totalassetsinuse$$

Substituting eqn 2 and 3 in 1 we have

$$NRS = MTTF * CAR$$

$$RS = MTBF + MTTR * CAR$$

C. 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.

Factors to consider for Reputational Impact: We identified five key factors of influence in calculating the reputational impact of a breach and assigned multiplication metrics.

TABLE II
REPUTATIONAL IMPACT

Stakeholder	Multiplication metrics
Consumer	1.91
Investor	1.25
Employee	0.71
Regulator	1.21
Media Coverage	1.45

D. Regulatory and Legal Impact (RL)

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.

Fines and penalties (P): Legal and regulatory fines and penalties imposed on the organization.

Legal costs (L): Expenses associated with lawsuits and legal actions.

$$RegulatoryandLegalImpact(RL) = P + L$$

E. Supply Chain Impact (SI)

Supply chain impact evaluates how the event affects the supply chain, including disruptions in the production and distribution of goods or services.

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): This measures how the breach affects the organization's ability to meet customer demands.

$$SC = SI + CI$$

F. 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.

Factors to consider for Employee and Stakeholder Impact a. Employee morale (EM): The effect on the well-being and morale of the organization's employees.

b. Impact on stakeholders (ST): The impact on investors, partners, and other stakeholders.

$$ES = EM + ST$$

G. 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

Factors to consider for Long-Term Consequences:

a. Ongoing security costs (OS): The additional security investments required to prevent future breaches. b. Loss of competitive advantage (CA): The long-term impact on the organization's market position.

$$LC = OS + CA$$

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

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. Experiment and Result

We analyzed the Ponemon cost of a data breach 2023 report to generate the dataset used in our experiment and we assumed constant values within a considerable range to prove the validity of our model.

A. Cost of Data Breach Per Record

The cost of a breach per record refers to the financial loss incurred for each piece of compromised or stolen data during a security breach. This metric is crucial for organizations to understand the potential financial liabilities associated with data breaches and to assess the overall impact on their operations[7].

The Ponemon Cost of a Data Breach report is often used as a reference for analyzing the cost of a breach per record. This report provides valuable insights into the financial repercussions of data breaches, including the average cost per record across different industries and geographical locations

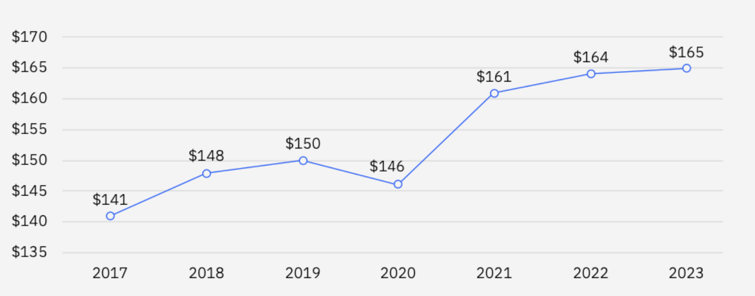


Fig. 4. Cost Per Record of Data breach extract from Ponenom

B. Cost of Data Breach Per Country

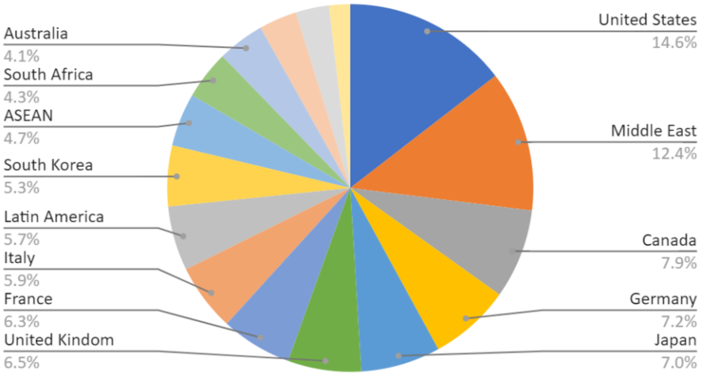


Fig. 5. Cost of Data breach on various Countries

According to a 2023 cost of a data breach analysis by IBM and the Ponemon Institute, the average cost of a data breach has increased to a new high of US$ 4.45 million, up 2% from US$ 4.35 million in 2022[8].

Numerous cost variables are considered in the Ponemon Institute and IBM Security research, including loss of brand equity, customer turnover, legal, regulatory, and technical efforts, as well as a drain on employee productivity.

C. Cost of Data Breach Per Sector

As displayed above, through our observations, the healthcare sector experienced the largest average cost of a data breach between March 2022 and March 2023, coming in at

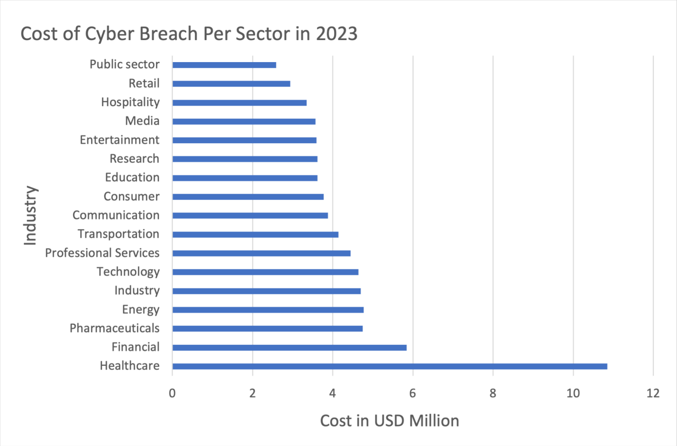


Fig. 6. Cost Per Record of Data breach extract from Ponenom

about 11 million US dollars. Second place went to the financial industry, with an average of 5.9 million USD per breach[9].

According to the cost-analysis-of-healthcare-sector-data-breaches, Generally speaking, they categorized types of costs associated with breaches: direct costs and indirect costs[10]. As per a study organization, the direct expenses consist of hiring forensic specialists, contracting out helpline assistance, and offering complimentary credit monitoring subscriptions and savings on subsequent items and services.

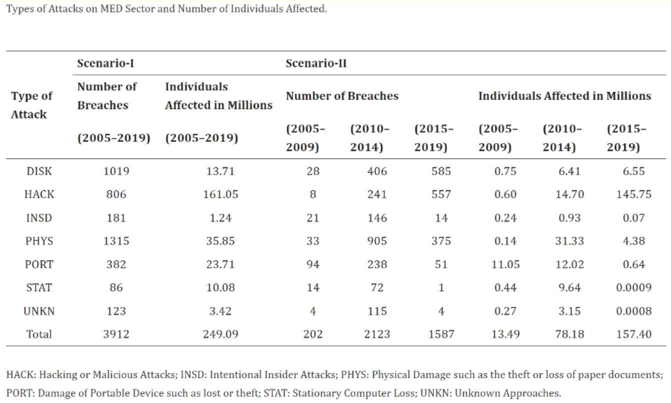
TABLE III
COST OF INDUSTRY DATA BREACH PER USD IN MILLIONS

Industry	Cost
Healthcare	10.85
Financial	5.84
Pharmaceuticals	4.75
Energy	4.77
Industry	4.7
Technology	4.64
Professional Services	4.44
Transportation	4.14
Communication	3.88
Consumer	3.77
Education	3.62
Research	3.62
Entertainment	3.59
Media	3.57
Hospitality	3.35
Retail	2.94
Public sector	2.59

D. *Observing the Health Care sector*

According to the cost-analysis-of-healthcare-sector-data-breaches, Generally speaking, they categorized types of costs associated with breaches: direct costs and indirect costs. As per a study organization, the direct expenses consist of hiring forensic specialists, contracting out helpline assistance, and offering complimentary credit monitoring subscriptions and savings on subsequent items and services. Internal inquiries and correspondence are examples of indirect expenses, along with the estimated cost of client loss as a result of employee turnover or lower customer acquisition rates[10]. The total cost of an organization's direct and indirect expenses is used to determine the cost of a data breach. Entities in the healthcare and public health (HPH) sector must deal with the expense of recovery, legal action, and the negative effects on their reputation from losing clients and patients.

According to a 2018 study, the average overall cost of a data breach in the US across all businesses was $7.91 million. At $233.5 per person, the US also has the highest per capita expenditures. Additionally, from 2017 to 2018, both of these costs rose in the US as a result of various factors, including the preference for quick victim notifications over thorough and comprehensive protected health information, which is prohibited in this part and compromises the security and privacy of that information. An associate possesses a sincere conviction that the individual to whom the material was disclosed was not authorized and could not have plausibly kept such data. People may be subject to a variety of financial fines in addition to the shame of having their personal information compromised[11].



Types of Attacks on MED Sector and Number of Individuals Affected.

Type of Attack	Scenario-I		Scenario-II					
	Number of Breaches	Individuals Affected in Millions	Number of Breaches			Individuals Affected in Millions		
	(2005–2019)	(2005–2019)	(2005–2009)	(2010–2014)	(2015–2019)	(2005–2009)	(2010–2014)	(2015–2019)
DISK	1019	13.71	28	406	585	0.75	6.41	6.55
HACK	806	161.05	8	241	557	0.60	14.70	145.75
INSD	181	1.24	21	146	14	0.24	0.93	0.07
PHYS	1315	35.85	33	905	375	0.14	31.33	4.38
PORT	382	23.71	94	238	51	11.05	12.02	0.64
STAT	86	10.08	14	72	1	0.44	9.64	0.0009
UNKN	123	3.42	4	115	4	0.27	3.15	0.0008
Total	3912	249.09	202	2123	1587	13.49	78.18	157.40

HACK: Hacking or Malicious Attacks; INSD: Intentional Insider Attacks; PHYS: Physical Damage such as the theft or loss of paper documents; PORT: Damage of Portable Device such as lost or theft; STAT: Stationary Computer Loss; UNKN: Unknown Approaches.

Fig. 7. Cost of Data breach on various Countries

E. *Model Evaluation*

To access and test the TSS model proposed, we acquired data from IBM Cost of a Data Breach Report 2023 [24] and various internet sources and to calculate the accuracy, compared with the model that Malaiya at el created. Through this TSS model we not only calculate the impact of a security breach, we also try to calculate the probability of breaches that will happen within 12 months.

We took the common attributes that would affect the face of an organization no matter the fields they are in and grouped the attributes for the TSS model.

These attributes are common in every and all organizations no matter the field they flourish in. Sectors such as Hospitality, retail, educational, entertainment or research..etc., all of them will be concerned about the attributes mentioned above in case of a breach. To test our model, we came collected numbers from various sources

To access and test the TSS model proposed, we acquired data from various internet sources that gives any information on the said attributes and to calculate the accuracy, compared with the model that Malaiya at el created[14].

To calculate the impact of each parameter, the data sensitivity metrics depending on the type of attributes considered(For example for Data impact confidential metrics has been considered as loss of data meaning loss of confidentiality) has been multiplied with the actual Data impact value acquired from sources. Each parameter value is calculated in the same way and after acquiring the value that the TSS model generates, it is being compared with the Malaiya et al's equation on probability of breaches. If it is accurate that means the TSS model's attributes were the right one to be considered. If not the attributes are to be changed and the sensitivity matrix values are to be replaced as well.

For an example we wanted to try the attributes related to the Health care sector as Data breaches are said to have a major effect on the targeted healthcare institution as well as the specific victims.

Here are the numbers for the Health care Industry from gathering all the reports.

TABLE IV
COST OF INDUSTRY DATA BREACH PER USD IN MILLIONS

Impact Type − value × Data sensitivity metrics	Vale
Data Impact 300 × 10^9× 0.90	27 × 10^{10}
Operational impact 0.64 × 10^6× 0.87	556800
Reputational impact 0.07 × 10^6× 0.55	38500
Regulatory and legal impact 145.75 × 10^6× 0.90	131.175 × 10^6
Supply chain impact 4.34 × 10^6× 0.87	377.58 × 10^4
Employee and stakeholder impact 0.09 × 10^4× 0.87	783
Long term consequences 0.08 × 10^4× 0.55	440

$$TSS = 27 \times 10^{10} + 556.8 \times 10^3 + 385 \times 10^3 + 131.175 \times 10^6 + 377.58\ \times 10^4 + 0.783 \times 10^3 + 0.440 \times 10^3$$

VI. CONCLUSION

We have formulated a model aimed at quantifying the impact of cybersecurity breaches, distinguishing our approach from the work by Malaiya et al., who focused on estimating the probability of a data breach occurring within an organization over the upcoming 12 months. Our model provides more accurate metrics for calculating the impact of security breaches by considering the long-term consequences of a security breach.

VII. LIMITATION AND FUTURE WORK

Our research was constrained to evaluating the overall impact of a cybersecurity breach within the healthcare sector. We specifically omitted the analysis of breach probability, as this aspect has already been addressed by Malaiya et al [3]. To enhance the breadth and depth of our investigation, we aim to advance our research by incorporating both the TSS Model and the probability data breach model introduced by Malaiya et al. This integration is anticipated to yield a more comprehensive and robust set of metrics for effectively calculating security risk in the context of cybersecurity breaches. By combining these models, we aspire to offer a more nuanced and holistic perspective on the security landscape, providing valuable insights for mitigating potential risks and fortifying cybersecurity measures within the healthcare domain.

VIII. 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/.

[11] "ISO/IEC 27001:2022," ISO, Feb. 02, 2023. https://www.iso.org/standard/27001

[12] Rok Bojanc, Borka Jerman-Blaˇziˇc, Metka Tekavˇciˇc, Managing the investment in information security technology by use of a quantitative modeling, Information Processing Management, Volume 48, Issue 6, 2012, Pages 1031-1052, ISSN 0306-4573.

[13] Sandip C. Patel, James H. Graham, Patricia A.S. Ralston, Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements, International Journal of Information Management, Volume 28, Issue 6, 2008, Pages 483-491, ISSN 0268-4012

[14] A. M. Algarni and Y. K. Malaiya, "A consolidated approach for estimation of data security breach costs," 2016 2nd International Conference on Information Management

(ICIM), London, UK, 2016, pp. 26-39, doi: 10.1109/INFOMAN.2016.7477530.

[15] R. Lanotte, M. Merro, A. Munteanu and S. Tini, ”Formal Impact Metrics for Cyber-physical Attacks,” 2021 IEEE 34th Computer Security Foundations Symposium (CSF), Dubrovnik, Croatia, 2021, pp. 1-16, doi: 10.1109/CSF51468.2021.00040.

[16] V. Vijayaraghavan and S. Paul, ”iMeasure Security (iMS): A Novel Framework for Security Quantification,” 2009 First International Conference on Networks Communications, Chennai, India, 2009, pp. 414-421, doi: 10.1109/NetCoM.2009.77.

[17] Martin, C., Kadry, A. and Abu-Shady, G., 2014, July. Quantifying the financial impact of it security breaches on business processes. In 2014 Twelfth Annual International Conference on Privacy, Security and Trust (pp. 149-155). IEEE.

[18] Carfora, M.F. and Orlando, A., 2019, June. Quantile-based risk measures in cyber security. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-4). IEEE.

[19] L. E. Kincaid, P”rinted Wiring Board Cleaner Technologies Substitutes Assessment: Making Holes Conductive”, 1997.

[20] M. Ko and C. Dorantes, The impact of information security breaches on financial performance of the breached firms: an empirical investigation”, in Journal of Information Technology Management, vol. 17, no. 2, pp. 13-22, 2006.

[21] S.J. Mason, R.R. Hill, L. Mönch, O. Rose, T. Jefferson, and J.W. Fowler, “Towards a flexible approach for business process modeling and simulation environment”. In Proceedings of the 2008 Winter Simulation Conference, Miami, FL., USA, 2008

[22] R.J. Paul, V. Hlupic, and G. Giaglis, “Simulation modeling of business processes”, in Proceedings of the 3rd UK Academy of Information Systems Conference, Oxford, UK, pp. 311-320, 1998.

[23] T. K. T. G. D. Pekos, “Analysing and determining return on investment for information security”. In Proceedings of International Conference on Applied Economics, p. 879, 2008.

[24]“IBM: Cost of a Data Breach Report,” Computer Fraud Security, vol. 2023, no. 8, pp. 4–4, Jan. 2023, doi: 10.1016/s1361-3723(21)00082-8.