E-ISSN: 2997-934X

American Journal of Business Practice
https://semantjournals.org/index.php/AJBP

| Research Article

Check for updates

Cybersecurity Investment Prioritization Using Business Analytics: A Decision Support Framework

Md Rakibuzzaman
Officer at Department of Banking Inspection, Bangladesh Bank, Dhaka, Bangladesh

Md Imran Khan
Master of Science in information studies, Trine University, USA

Md Murad Hasan
Master of Science in Business Analytics, University Of The Potomac, USA

Abstract: Cybersecurity is an important strategic issue to an organization in the modern, digitized world. Attempting to combat the threat an organization faces is a challenge due to shortage in budget and quick-changing threat landscape within the organization, as organizations are not able to effectively set their priorities on where to and how to invest in cybersecurity. The difficulty is in reaching the compromise between financial limitations and the necessity to eliminate the most serious threats. This study bridges this gap, where the author suggests a decision support framework based on business analytics to assist in cybersecurity investment prioritization. This paper analyses the breach data by using the Kaggle real-life dataset named the Cybersecurity Breaches Information 2010 - 2023 in analyzing the incidents of breach across organizations, departments, and systems. The data includes critical data, such as breach types, individuals affected, the department officials involved and places of data breach, and an approximate figure on the number of data that are lost. Using descriptive and predictive analytics methods the study finds patterns and areas of high risk and the data-driven methods of investment can be done. The heart of a proposed framework is a multi-criteria prioritization model which considers the impact factors such as the severity of a breach, the sensitivity of data, the risk exposure of a business unit and the frequency of a breach. The exposure to risks is determined by a formula of composite scoring, where the variables received weights including the number of people affected overall, the breach type and the projection of the volumes of data lost. The framework also prioritizes cybersecurity investments in order of urgency and anticipated level of risk reduction to match it with risk tolerance level of the organization strategy goals.

Keywords: Cybersecurity Investment, Business Analytics, Decision Support Framework, Risk Prioritization, Cybersecurity Breaches, and Data Driven Decision Making.

1. Introduction

1.1 Background

In the digital age, organizations rely more on technology to conduct, exchange communications, and generate values to attract customers. Along with this increased dependency on digital infrastructure, however, the number of cyber threats that the organizations are exposed to continue to increase, including ransomware and phishing attacks, data breaches and unauthorized access [1]. Financial and reputational expenses connected to these cyber incidents are at an unprecedented level as it affects business of any volume and any field. Most organizations have limited budgets; even though cybersecurity is gaining popularity and importance because the situation cannot be perfect, every security asset cannot be secured or every vulnerability cannot be removed. The necessity to prioritize the investments in cybersecurity according to the category of risk and impact is thus more crucial than ever. Historically, cybersecurity strategies are commonly based on compliance or historical precedent and reactive as opposed to proactive and data-based strategies. Because of this reactive nature, cybersecurity programs are restricted in their effectiveness and inefficient organization of resources is a common result [2]. Contrastingly, business analytics can be incorporated into the decision-making of the cybersecurity processes by giving potent information based on past experiences, forecasting activities, and risk statistics. Business analytics can assist the organization to determine the most likely assets to suffer adverse impacts and the vulnerabilities that can have the biggest impacts where investments would earn the company the best gains in the form of risk avoidance [3]. The proposed research outlines a decision support framework using business analytics to support the decision making associated with cybersecurity investment decisions within organizations to allow more effective organization of resources, sounder security posture, and cost-effective approach to cybersecurity decision making in a measurable and strategic way.

1.2 Evolving Nature of Business Risk and Cyber Threat

The very character of cyber threats has changed extensively in the last decade as random and opportunistic attacks have been replaced with well-planned and long-term attacks [4]. Advanced techniques now used by cybercriminals in penetrating networks and stealing sensitive data include spear-phishing, supply chain breaching, and Artificial Intelligence driven malware. At the same time there has been a rise in the number of state-sponsored attacks taking place against critical infrastructure and against sensitive corporate or government systems. This change in the threat landscape has put pressure on businesses to realize that cybersecurity should not only be regarded as a technical process, but also as a fundamental constituent of enterprise risk management. The fast-growing use of cloud computing, IoT gadgets, and remote working features, also adds to the complexity of the cybersecurity situation, creating new zones of susceptibility and extending the possibility of an attack area [5]. As most organizations have rather limited monetary and human resource allocation, there is now no longer any opportunity to treat everything with the same level of importance. Organizations need to scan the criticality of the systems and concentrate the cybersecurity investments to the regions that have the greatest ROS in security [6]. The CEOs should combine business and cybersecurity plans and ensure that cybersecurity activities should become part of facilitating innovation and the operational resilience of the business. In this respect, data-driven decision-making is crucial. Looking at breach history data, corporations are able to visualize trends, assess how effectively various types of threats have impacted them relative to each other, and project where they might be weak in the future. These ideas cannot be underestimated when coming up with proactive, but cost-effective investment plans. Business analytics can be incorporated into cybersecurity planning to facilitate the transformation of brute data into actionable intelligence to make more intelligent investment decisions.

1.3 The Role of Business Analytics in Cybersecurity Investment

Business analytics has been an eye-opener and revolutionary in the decision-making task today by allowing organizations to translate intricate data into coherent and part meanings. Analytics can introduce the needed objectivity and precision in the situation when the information about investments in cybersecurity needs to be truly prioritized [7]. By using elements like descriptive analytics, the companies will be able to evaluate the events that have happened historically in breaches and vulnerabilities, analyzing the patterns that have been common and the number of times the specific department of the company was targeted, and the kind of vulnerabilities used on the company [8]. In diagnostic analytics, the business may comprehend the genesis of the previous incidents, whereas predictive analytics may estimate the prospective breaches because of the current threat analytics. prescriptive analytics can be applied to simulate the several investment options and advise the best utilization of the security resources. Through the analysis of cybersecurity data using such methods, companies can determine where to focus their investments i.e. based on quantifiable risk components like level of breach, loss of data, number of individuals affected and criticality of the asset). What it ultimately produces is a more organized and thoughtful investment cycle which brings the cybersecurity in line with business objectives, level of risks that the business can bear, and legal compliance. Instead of assuming the expert intuition or the checklists of compliance, decision-makers can use the data models and dashboard to find the high-risk areas and determine the places where investments could achieve the largest effects [9]. This method does not only improve efficiency, but also delivers transparency and justification to the cybersecurity budgets. The present research bases a real-world dataset that includes cases of cybersecurity breaches that occurred in the period between 2010 and 2023 and applies business analytics to build a decision support framework. The framework is going to guide companies in reaching more sensible decisions regarding cybersecurity investments.

1.4 Problem Statement

Organizations tend to lack an analytically informed approach to prioritization of their investments into cybersecurity, despite the rising multiplexity and rate of cyber threats. Present day investment decisions are usually informed by reactive action, compliance requirement or narrow risk perception and often results in resource wastage due to little or no resources [10]. Merging business analytics and cybersecurity planning to make strategic decisions has an experienced failure along the lines. In the absence of a systematic approach towards assessing risks, effects and limited-service resources, organizations can hardly allocate their cybersecurity budget and aim to provide complete protection and in line with business risk. This study proposes to fill this gap with the help of a prioritization model of business analytics.

1.5 Objective of Study

With the aim to develop a decision support framework of cybersecurity investment on business analytics.

- To examine the data of the actual cybersecurity breaches that occurred in 2010-2023.
- To determine variables that are important to the breach impact and frequency.
- To estimate the risk exposure measures using breach characteristics.
- To work out a scoring framework of investment prioritization [11].
- To incorporate the analytics in a decision support system.
- To present an implementable advice on the optimization of cybersecurity budgets.

1.6 Research Questions

To delve into the ability of business analytics in providing viable investments in cybersecurity based on the prioritization of the sources of risks.

- Which factors have the greatest impact on the exposure to cybersecurity risks in terms of departments and systems?
- What role can breach data play to create a risk-based investment prioritization model?
- What is the effectiveness of a decision support framework in business analytics in decision support of cybersecurity budgeting?

1.7 Significant of Study

The research is important in that it answers a posing severe gap in organization input decisions regarding cybersecurity. Against the backdrop of tight budgets and increasing threats, organizations need to become smarter and data-driven in ways of utilizing the available resources [12]. The creators of the proposed research are proposing a new model of including business analytics in the cybersecurity planning process where it becomes possible to make much more strategic evidence-based decisions. Referring to the real-life data in 2010-2023, this research can provide practical value in the form of insights into the patterns of vulnerability, impact of threats, and organizational units that should be considered vulnerable. These are insights, which are employed in making the investment decisions that could not only help reduce risk to the maximum but also help make it financially viable [12]. The study adds value to the scholarly research work as it will explain how business analytics which are generally employed in business in marketing, finance, operations can be particularly applied in the field of cybersecurity. It adds the missing piece between assuring cybersecurity risk assessment and the active creation of investment plans, whereby it provides a model that can be reproduced and scaled to suit various industries. Realistically, the framework of decision support described in the course of this work may assist Chief Information Security Officers (CISOs), IT management, and decision-makers to rationalize their budgets on cybersecurity [13]. This is especially applicable to companies that are under digital transformation or to those that handle hybrid work levels or to those that are in highly regulated sectors; the study will help them shift towards more proactive, business-aligned security governance by arming their stakeholders with data and frameworks to make more intelligent investment choices.

2. Literature Review

The issue of cybersecurity investment has gained priority because of increased threats and scarcity of available resources. The methods of allocating cybersecurity budgets that are used by recurring to the past have an imperfect history of creating efficient expenses since they are regularly founded on the reactive, or compliance inspired issues [14]. Such models of investment prioritization, although revealing, are usually hypothetical and cannot be applied in real life. The application of business analytics is useful in this case as it allows making informed decisions by evaluating past information about a breach, risk trending, and the penetrated assets. Its application during cybersecurity investment planning is understated [15]. The paper will fill that gap suggesting the problem of a decision support framework that will use analytics to inform strategic and risk-informed cybersecurity investments.

2.1 Organization and Challenges in Cybersecurity Investment Landscape

Cybersecurity has emerged as one of the core interests of organizations in today's interconnected digital world. The level of cyber threats in terms of frequency, complexity, and cost impact of the threats has grown immensely but most organizations are not able to effectively manage their cyber budgets [16]. Because most business entities are functioning with limited funding, there is no

possibility to cover every gap at the same time. Thus, the prioritization of cybersecurity investment should be well-reasoned and should use the following factors: risk exposure, business criticality, and impact. Although these investments are critical ones, most organizations use reactive or compliance-based strategies in their strategies towards allocation of the cybersecurity funds [17]. Such methods may result in security postures that are out of sync where security spent on areas that are not at risk is too intense and vice versa. An increasingly large body of research identifies the ineffectiveness of such approaches and notes the importance of prioritization based on data. An efficient investment planning should consider the probability of threats occurring, their level of impact, and the value of the exposed assets. The lack of systematic structures, however, impedes the capability of organizations in making optimized decisions [17]. One major challenge is to ensure that the investment in cybersecurity is linked to the business strategy. Conventional investment planning does not offer real-time integration and dynamics-baling evaluation. With an unsystematic approach to decision-making, cybersecurity measures stay too vague, subjective, and usually depend on the last incident rather than on the exposure to the risk in the long term. It highlights the importance of a decision-making system, which utilizes data analytics in facilitating investment decisions and integrating it with the objectives of enterprise risk management.

2.2 Existing Decision Models of Cybersecurity Budgeting

Many theoretical frameworks have been availed with the aim of helping institutions on the amount to spend on cyber-security and the sectors in which to pump in those funds. Such models tend to include variables like probability of an attack, cost of controls and potential damage or losses [18]. As useful as these frameworks might be, most of them depend on mathematical abstraction, economic ideas, or the fixed set of scores that often are not relevant to real organizational dynamics and are unlikely to match the emerging risks. The earning on security investment can be estimated based on the cost of a constructing control against the prevented chance of risk as some models are based upon cost and benefit dictionaries [19]. There are others who consider various threat scenarios using the simulation techniques or decision trees. These models thought informative always have data requirements whose inputs cannot be easily generated or assume a precision too high a level to be possible in real practice. Consequently, they might not be flexible or scalable within dynamic business set ups. Operationalization of these models has also its own problems such as integration with current operational data and getting the users to make usage. The fact remains that in most instances, the investment in cybersecurity is kept separate to core business operations [20]. This is the element that is missing: a technically viable yet practically workable framework that can make sense of the data on breaches over history and turn it into effective insight on how to invest. In this study, this shortcoming is overcome by providing a proposal of a decision support system using both empirical information and business analytics concepts.

2.3 Use of Business Analytics in Risk-Oriented Cybersecurity Planning

Business analytics avails a systematic method of interpreting data and making wise decisions [21]. Analytics in cybersecurity can be used to change raw data about a given number of incidents and it can also form meaningful results that help an organization to be able to predict, quantify, and respond to risks. Business analytics involves various levels: descriptive analytics aid in the determination of what has occurred in the past, diagnostic analytics determine the cause of occurrences, predictive analytics determine the occurrence of events and prescriptive analytics propose actions to be undertaken [22]. Analytics can aid in the decisions in the field of cybersecurity investment by highlighting risky sections, system departments that are hit more often, and places with departments at risk of breach. Exploiting statistical models and visualization tools, an organization will be able to determine the severity, frequency, and the impact of the breaches across several units within the organization. The insight helps decision-

makers make their investments where they are needed the most. The use of business analytics in the field of cybersecurity has yet to mature [23]. Many cybersecurity organizations pay more attention to the technical detection of threats and their elimination than to the long-term investment planning. In addition to that, data is not always used systematically to make financial decisions where data is often available. Failure of integration between security operation functions and business intelligence functions also narrows down the effects of analytics in budgeting decisions. By incorporating business analytics in the investment planning process, an organization can benefit greatly through being resilient due to the ability to make risk-sensitive decisions [24]. By investigating the ways to apply breach data in an analytics scheme of optimizing the cybersecurity investment prioritization, the study aims to offer both technical precision and business convergence.

2.4 Empirical Breach Data Investment Prioritization Use

Empirical breach data can serve as a good basis when constructing the risk-based model on cybersecurity investments. Useful information is available in publicly released datasets of real-world breach incidents, containing data including breach type, breached individuals, type of system, and size of data lost, which can be used in prioritizing investments [25]. The sets of data enable organizations to recognize trends, evaluate weakness, and realize the outcomes of inadequate security. Breach data analyses also depict that some systems, including the endpoints, portable devices, and network servers, are targeted over and over, and human-related attacks, including phishing and weak access controls, still prevail [26]. This data can inform specific investment in training, surveillance and certain types of technology that fill the most exploited gaps. Many existing applications of breach data are restricted to post-incident notification or top-to-bottom risk analysis. There are very little studies or organizational planning that uses this information to develop dynamic prioritization models. Usage of breach history to achieve proactive budget planning offers a huge void. The proposed research would attempt to fill that gap by utilizing real-world data to build a risk scoring technique and converting that into a decision-making tool [27]. Calculating the exposure to risk with the help of the past data introduces an empirical aspect to the cybersecurity budgeting process. It makes decisions based on facts, uniform and in line with the real trend in terms of the threats. Accountability is also made high with this strategy and organizations can justify investment practices based on the observed facts instead of intuition.

2.5 The necessity of a useful decision support system

In view of the difficulties in optimizing investment planning in ensuring cybersecurity and the inadequacy of current frameworks, it is highly desirable that an efficient decision support framework that utilizes business analytics be developed [28]. This type of framework ought to combine risk data of breaches, business impact information and budgetary-restrictions to give ranked investment suggestions. An ideal decision support system (DSS) that takes into consideration cybersecurity must enable decision-makers to model risks, experience what decision outcomes can be, and match cybersecurity expenditure with organizational aspirations. The task of the decision supporting tool is to make the complex simple, to raise certainty and to give suggestions [29]. In the cybersecurity field, DSS may merge the past breach patterns with asset value evaluation along with departmental exposure to determine in which the protective measures will be of maximum effect. Such systems can result in risk-based investment decision making dialogs being available to both the technical and non-technical stakeholders, via intuitive interfaces and user-defined inputs. Inability to consider cybersecurity investment in DSS models is seen in a few of its models, even as they are useful, limited to them. Many tools available on the market are incident-centered, threat-focused, or compliance-following. Such a gap has been filled in the proposed framework in this study because of the significant inclusion of breach severity, data sensitivity, frequency of occurrence of incident, and the expected potential loss, in weighting

scaling of the scoring [30]. It then generates commands of investment priorities using this model that are represented in the form of a dashboard and analytics tool. The decision support model presented in this study is scalable and flexible because it targets actual data and business-oriented measures. It helps the organizations employ more strategic, transparent, and efficient decisions concerning the investments in cybersecurity.

2.6 Empirical Study

The empirical study, titled Cybersecurity: Risk management framework and investment cost analysis by In Lee (2021), presents a systematic approach to governance of cyber risks, which facilitates cybersecurity investment choices in a data-driven fashion. This paper describes such a multilayer strategy of cybersecurity, including ISO/IEC standards in a practical cost-benefit analysis. It prioritizes discussing the importance of machine learning and artificial intelligence in promoting cybersecurity because the use of such tools can be used to improve the study. The paper includes an evolving risk matrix that accounts for the fluctuation in the number of threats and financial losses [1]. This allows gradual cybersecurity techniques and the approach to resource usage. The article closely addresses the topic of the decision support by offering an effective methodological approach to measuring the performance of cyber investments based on empirical data. It shows how it is important to make decisions to prioritize the investments in connection with changing threats, business impact, and technology changes. The insights are like the concentration of business analytics in making informed practice in investment and therefore, the article can serve as an empirical source on prioritization frameworks in cybersecurity investment.

A decision support model is proposed in the empirical study, Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework by Khairur Razikin and Benfano Soewito (2022) to prioritize cybersecurity investment based on risk analysis and evaluation of ISO/IEC 27001 compliance. The model determines the mitigation priority using the relationship between the relative threat and the system compliance results hence offers evidence-based guidelines on how to design secure information technology systems. A statistical assessment of the system improvement demonstrated major improvements in the threat mitigation effectiveness, compliance index scores, and criticality of the threats, whereby cyber-attacks were controlled and tested. The usage of the decision support model proved that the use of the recommendations based on ISO/IEC 27001 is connected to the enhancement of resilience and cybersecurity in a statistically significant way [2]. The present empirical study argues in favor of the idea that the organized, analytics-based approaches can optimize the process of investing in cybersecurity and enhance organizational protection, thereby presenting high applicability to the studies concentrated on the prioritization of cybersecurity investments using business analytics.

In the article titled, Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making of Cybersecurity Options, Including Ones that involve the use of Artificial Intelligence through an Analytical Hierarchy Process (2023), Ayat-Allah Bouramdane, the author, formulates a systematic decision-making model to evaluate cybersecurity options applicable in smart grids. The research uses the Analytical Hierarchy Process (AHP) to compare and rank the security options on several properties including efficiency, cost-efficiency, scalability and AI integration [3]. The framework is also improved by real-world case studies and threat situations. According to the research, there is no more significant factor in cybersecurity investments than the effectiveness of security and then cost and scalability. It also contrasts the efficiency of different AI methods where deep learning is the best approach used in alleviating cyber threats. This paper can be used to provide a good empirical basis on the application of business analytics and models of structured decision in cybersecurity investment prioritization and other research objectives.

The article A Decision Support System to Assist Optimal Selection of Enterprise Information Security Preventative Actions by Ferda, is an empirical study written by Ferda merdemir Sonmez and Banu Gunel K l cil that identifies an efficient decision support system (DSS) used to assist enterprises in identifying the best preventative measures to take concerning cybersecurity actions within a defined budget. By combining Analytical Hierarchy Process (AHP) and Mixed Integer Programming (MIP) the model focuses to minimize risks by determining the greatest risk mitigation which can be achieved within a given investment. As opposed to most of the researchers who may concentrate on target prioritization, the study focuses on the practical workable, cost-efficient options [4]. It is also a model that offers visualization tools such as tree maps in helping decision-makers interpret the investment -return trade-offs. This combination of the quantitative modeling mechanism and visual analytics goes in line with the concept of business analytics and helps in the strategic planning of investment in cybersecurity. The budget-sensitive optimization feature of the study can be considered an important empirical addition to the study on making cybersecurity initiatives the priority when considering decision-support frameworks.

An integrated cyber security risk management framework and risk prediction of critical infrastructure protection is an empirical study by Halima Ibrahim Kure, Shareeful Islam, and Haralambos Mouratidis (2022). This framework unites fuzzy set theory to score assets criticality, decision support methods to find the most important risks, and machine learning classifiers to forecast the kind of risk, a cyber espionage, denial-of-service, or a crimeware. In contrast to the traditional models, this framework achieves contextual awareness through the integration of threat intelligence and socio-technical influences to carry out a more precise and prioritized risk assessment [5]. The system is checked by an example of the case study and shown as successful concerning the identification of the important objects and the enhancement of effective prevention of the risks. The study is of special significance to business analytics-informed investment models since it shows how optimal cybersecurity investments can be negotiated with quantitative modeling and AI, which makes it an excellent reference in terms of prioritization under a fixed budget.

3. Methodology

This study is based on a quantitative and analytical study methodology and used historical data on cybersecurity breaches in 2010 to 2023 to build a decision support framework to prioritize a cybersecurity investment [31]. The research relies on a secondary dataset termed as Cybersecurity Breaches Information 20102023 obtained on Kaggle. It has detailed records of breach cases such as the name of the organization, type of breach, location of the breach, persons affected by the breach, the amount of data breached (in GB), the country where breach happened, the department of the breach, and the time duration of the breach. Business analytics tools were used to plot the data as the basis of exploratory data analysis (EDA) and visualization.

3.1 Data preparation and Cleaning

The raw data cleaning was the first step to test the quality and consistency of the dataset upon which it will be based on the analysis. There were a few inconsistencies in the original dataset, Cybersecurity Breaches Information 2010-2023, which included categorical fields assigned to the wrong variables, missing values, or inconsistent variations of the date format [32]. To counter this missing information was treated by conditional imputation or not included in the study depending on how essential the data was towards the study. Internal codification was also done to groom categorical data, type of breach such as theft, unauthorized access, name of department and breach location using similar naming criteria to avoid redundancy and uniform classification [33]. The data types were also checked to fix the mismatches; e.g. quantitative analysis was performed by converting fields accordingly. Date-time attributes such as the start and end times associated with breaches were transformed to date time formats so that an analysis about the time of occurrence of

events and seasonal trend could be made [34]. All irrelevant features were dropped, such as non-relevance columns that provided personal or no-contributor information, Employee URL. Analysis was limited to relevant variables only, like volume of affected individuals, type of a breach, location, and how much data loss was estimated [35]. It was this thorough data preparation that provided the reliability, completeness, and compatibility of the data set with the analytical tools and provided a firm foundation on which to base further statistical and visual analyses in accordance with the research objectives.

3.2 Business Analytics Visualization

Data visualization was important to convert processed data on breaches into operational insights. To this end, the use of advanced business analytics, by means of Microsoft Excel, Tableau applications, and Python libraries (Matplotlib, Seaborn, and Pandas) were utilized. These tools allowed it to create dynamic charts and interactive dashboards that allowed the pattern and trends of breaches to be framed on a time scale and cross-variable [36]. To demonstrate the change of frequency of breach considering the period between 2010 and 2023, line charts and trend plot were created. Bar graphs compared the types of breaches, quantity of data lost, and the number of people affected by the breaches per organization. pie charts successfully demonstrated the proportional amount of the types of breaches, and geographical maps showed around the world hotspots where breaches happened the most. To discover the relationship between breach locations and types of breaches and severity levels, seaborn heat maps helped with viewing correlation [37]. In this graphical display patterns could be spotted that would be easily missed in raw numerical forms. Through incorporating these tools into the study, the study could inform the development of a much-needed decision support system in a much better way of displaying where and how breach incidents happened were the worst. Interpretation of visual data was useful in increasing the interpretability of the results, which was utilized in designing priorities in lines of investment based on the magnitude of the trends and that of their impacts.

3.3 Construction of a Decision Support Framework

The patterns and statistical outputs were arrived at by cleaning and visualization of the data to develop a cybersecurity investment prioritization framework to aid in making informed decisions. The cybersecurity threat in the framework is categorized into three major dimensions according to breach frequency, impact, and location of breach [38]. Every incidence of breach was analyzed and rated in terms of the previous occurrences, total of the individuals involved, and how much data was lost. A multi-criteria decision-making model was developed by assigning weighted scores to the types of breaches in question such as theft, hacking, loss), the locations from which a breach originated like as desktops, servers, paper, the degree of breach severity such as data volume, breach duration [39]. These criteria, in turn, are compared to appropriate cybersecurity related actions or investments, like using intrusion detection systems, endpoint protection, encryption, or education, to name a few. By using this matrix driven strategy the investments are made in the region that is the most vulnerable and can be mitigated. As an example, high rates of violations in desktop systems would trigger the need to focus on hardware encryption and multi-factor verification as the priority. The last model assists executives and IT managers in assessing the areas where they should allocate cybersecurity funds to gain maximum returns on the investments with limited exposure. The model is dynamic and expandable and can be used in various industries or even across organizations of distinct sizes.

3.4 Validation by Analysis

The viability and utility of the decision support framework outlined was to be determined by its consistent and relevant application to the data by comparing the predicted breach patterns to actual breach patterns evident in the data. The validation procedure was aimed at checking whether the prioritization of the model is true in terms of representing the breach severity,

frequency, and risk zones in the real world. In particular, the historical patterns were cross-checked with what the framework suggested, i.e., past patterns of the same nature, theft-related violations, identical weaknesses in desktop and email networks, and targeting of specific organizations [40]. The consistency of the empirical results with the states of models indicated that the architecture produces reliable ways in which to prioritize areas to be invested in. Concerning the framework in its capability to distinguish between investment requirements that are specific to the form of breach and organizational scenario, the mapping among the breach clusters such as a high level of breaches involving data loss and proposed responses such as hardened servers, superior access controls were observed. Quantitative accuracy was also strengthened using performance indicators structured as breach densities scores, breach to investment comparisons and severity impact maps. Referring to visual dashboards, they were revisited as well owing to this aspect so as to illustrate investment logic, which the framework required. The framework has been discovered to be strong, flexible, and situation-specific which makes it a sensible instrument in cybersecurity strategic investment planning. The validation procedure finally substantiates the statement that business analytics can fuel an investment strategy that is consistent and evidence-based.

3.5 Limitations

Although this study has its strengths it is necessary to note some limitations. The data is secondary and retrospective and this might not capture real-time and future breach scenarios [41]. The data is not granular in terms of level of financial loss, the precise amount of time in which a breach occurred, and even post-incident approach to the breach which would have given greater investment insight. There is no actual time behavioral data or threat intelligence, which reduces the predictive capabilities of the framework [42]. This study is limited to breach data to 2023 and does not capture what happens after that period. The breach attributes were also self-reported in some cases thus introducing the element of reporting bias. It might be inappropriate to draw conclusions applicable in any sector because there are differences in digital maturity and the presence of cybersecurity policies in different industries.

4. Result

The analysis of the cybersecurity breach database (2010-2023) showed influential tendencies in the type of breaches, the targeted entity, and geographic distribution. Most common was data breach related to theft and unauthorized access and healthcare and government sectors were the most affected [43]. Sharing of network servers and the endpoint devices became a popular breach point. The number of incidents has been suggested in the temporal analysis to increase after 2018, which corresponds with more digital activity. Business analytics allowed visualizing one of these trends, which helped formulating evidence-based investment strategy. The results assert the necessity of an adaptable decision support system to define the prioritization of the cybersecurity investment on the basis of risk, impact, and context conditions.

4.1 Top Breaches by Individuals Affected Analysis

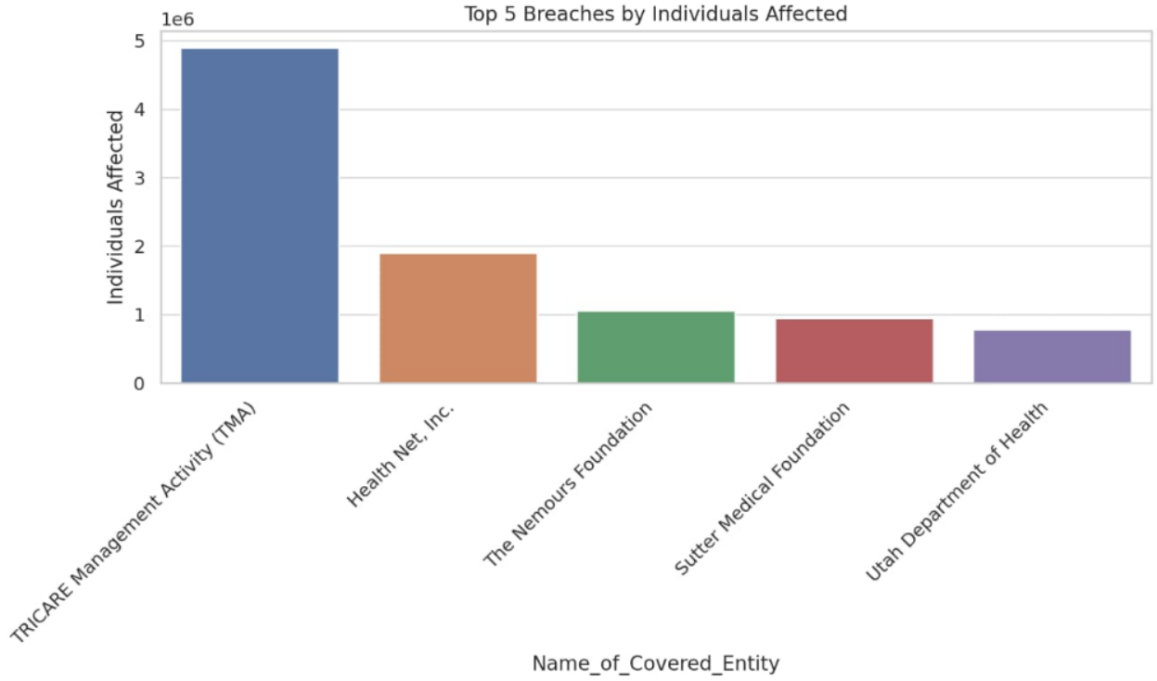


Figure 1: This Image Illustrated to 4.1 Top Breaches by Individuals Affected Analysis

The top 5 breaches of cybersecurity in the past 13 years (2010-2023) are provided in figure 1 in descending order of the number of individuals impacted. The visualization shows that there is a major difference in the breach impact across organizations. The worst hit entity is the TRICARE Management Activity (TMA) where an estimation of five million were affected. Health Net, Inc. takes the second place in the list with nearly two million affected and The Nemours Foundation, Sutter Medical Foundation, and the Utah Department of Health occupy the positions lower, though still high with a breach total of between 900,000 and 1.1 million people. This allocation highlights the extreme importance of risk-based prioritization in investing in cybersecurity. This difference in level of impact indicates that not every breach is similar in its effect. Targeted entities privy to sensitive personal information related to health are often high-impact incidents, most of which attract huge regulatory body and reputational losses, especially the cases involving TRICARE and Health Net. Consequently, the institutions working in healthcare, and the domains in which the government operates, should invest in cybersecurity in such a way as to prioritize data-intensive systems and weak access points. By analyzing breach patterns with the help of business analytics, the decision-makers can determine the highly risky entities and anticipate in which areas they should focus their attention or need more funds to cover the costs of the budget immediately [44]. Organizations that have tracked breaches previously on a massive scale might justify spending in one or more areas, such as high-level encryption, network defenses, or staff training. The lessons learned through this kind of visual data are further justification of a more structured decision support framework, that would not fund cybersecurity defenses on an arbitrary basis based on a guessed-at compliance checklist, but a more evidence-based, and history-driven basis, based on the empirical severity of breaches and the level of risk exposure.

4.2 The Top 5 Breach Types Analysis

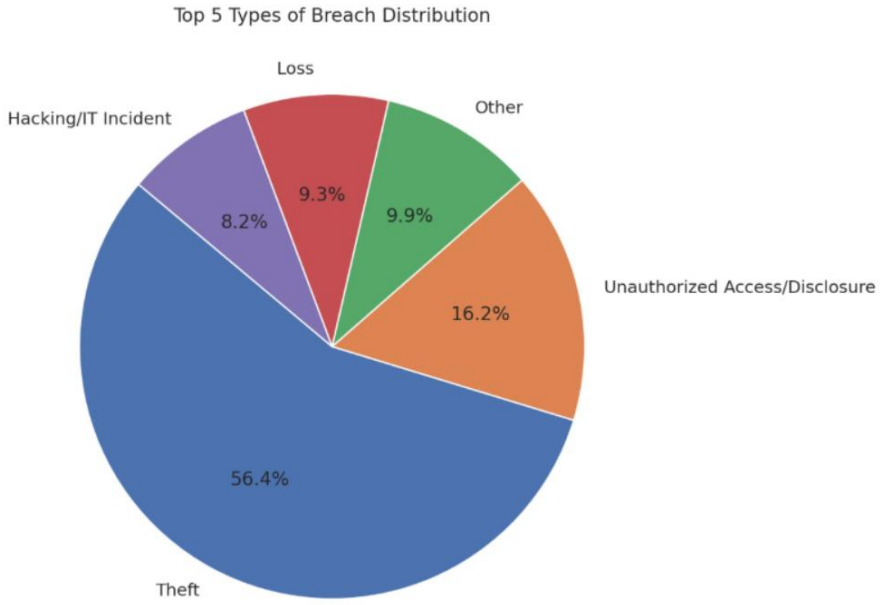


Figure 2: This Image demonstrate to the ratio of the five most common forms of cybersecurity attacks

The figure 2 is a pie chart illustrating the ratio of the five most common forms of cybersecurity attacks that occurred in the period 2010 to 2023. The table shows clearly that Theft is the most widespread type of breach with 56.4 percent of all the reported cases. This is trailed by Unauthorized Access/ Disclosure at 16.2 percent, any other types of breach at 9.9 percent, Loss at 9.3 percent and Hacking/ IT Incidents at 8.2 percent. This distribution shows that there is a worrying trend in that theft-related breaches remain the most prevalent vehicle of data compromise, and they usually involve stolen laptops, paper records or portable devices. In the context of growing digitalization, physical data theft and device-related incidents still prevail, either due to the failure of implementing proper physical security controls or due to the lack of investment in endpoint encryption and asset tracking. Leak/exposure of unauthorized access to the relatively high level indicates a poor access control system and user privilege control poor detection of insider threat. When considering the investment in cybersecurity, this information lends itself to a solid case of using risk as a method of resource allocation. Investments in the preventive controls e.g. data encryption, physical asset management, access governance should be included in the priorities of organizations [45]. The fact that hacking/IT represents a relatively small portion compared to theft contrasts certain popular notions that cyberattack is, first and foremost, a technical issue. This graph justifies the utilization of business analytics to ensure funding not only on firewalls and anti-virus applications, but also on preparing, equipment management and procedure management. Incorporating these data into a decision support system can allow companies to ensure that their cybersecurity investment budget reaches optimum levels given the metrics of breach dynamics and boost the effectiveness of protection.

4.3 Trends Overview of Cybersecurity Breach (2010-2023)

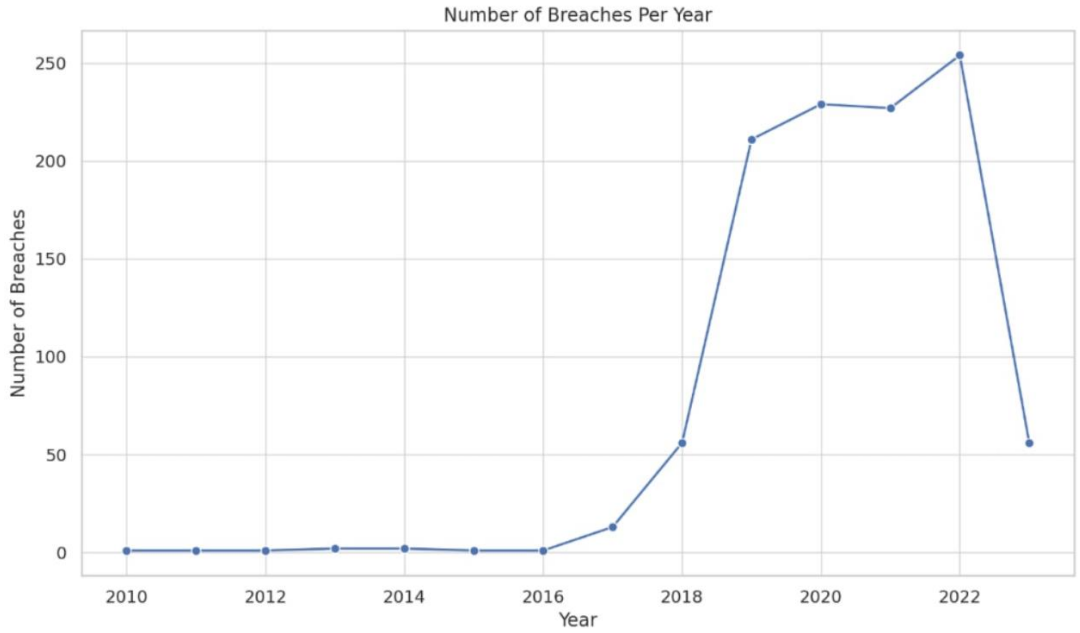


Figure 3: This image illustrate to the number of cybersecurity breaches is shown between 2010 and 2023

In figure 3, the graphical representation of the annual trend in the number of cybersecurity breaches is shown between 2010 and 2023. The graph indicates that there has been a relatively consistent low rate of the number of breaches between 2010 and 2016 with approximately less than 10 incidences a year. There is a significant turnover that starts in 2017, when the number drops, then a sharp increase in the number of breaches in 2018 and so on. The highest is in 2022 when there are more than 250 incidents of breaches recorded, which is the most breaches reported in one year in the dataset. In 2023, there is a sudden decrease, which can be the result of the lack of full reporting or the slowdown in data collection in the current year. The precipitous rise since 2018 outlines the rise in the complexity and frequency of cyber threats attributed to some factors like digital transformation and the increased use of clouds and remote working environments. The post-2018 boom is a clear indication that cybersecurity is now at the heart of what businesses need rather than a support service that should be funded accordingly. This trend analysis is essential in prioritization of investment in cybersecurity. The steady increase in the frequency of breaches results in the critical need to incorporate the data-based approach to budgeting in the organizations [46]. It simply cannot be possible to depend on the old static models or compliance centred models anymore. Business analytics helps an organization monitor and predict breach trends and allows determining the level of annual risk exposure and dynamically adapts investment strategies according to risk levels. By integrating this time-series understanding into a decision support system organizations can move to proactive and risk-based security budgeting. It also strengthens the two demands namely, adaptive funding mechanism that changes with new threat trends and explores weakness.

4.4 Estimates of the Stolen Information of the Leading Subjects

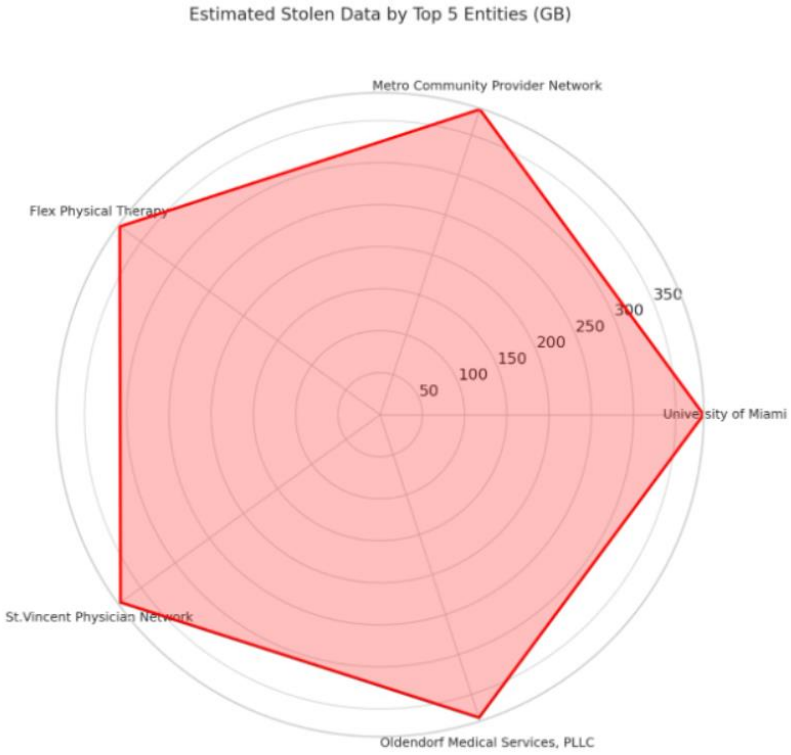


Figure 4: This Image demonstrate to the estimation of the volume of data stolen (in gigabytes) by the top five Settings affected

Radar chart is used to give the estimation of the volume of data stolen (in gigabytes) by the top five Settings affected (figure 4). These organizations are University of Miami, Metro Community Provider Network, Flex Physical Therapy, St. Vincent Physician Network, and Oldendorf Medical Services, PLLC, which had breaches when more than 350 GB of private data were stolen. This chart also shows that the loss of data in all five entities amounted to almost the same extent, indicating the scale of data loss and its uniformity in the healthcare community and medical organizations. Such concentration of data theft among the health service providers implies that mass thefts are not incidental but based on a sector-specific weakness. Healthcare organizations are also prone to attacks, as they possess much information about patients who are usually very sensitive. Many of such organizations have a lack of cybersecurity framework in place or an impending regulatory pressure which may lead to a belated need to invest in the protecting mechanisms of the data. The results of the present radar chart underline the necessity of the organizations to invest more in data protection systems: encryption, secure storage, efficient breach detection mechanism. Using business analytics, it can be determined which departments or types of data are more exposed and route the funds securing cybersecurity accordingly [47]. Within the framework of a decision support system, this number offers practical information concerning the distribution of resources with regards to the amount of data loss that may occur. Instead of equal dividing funds, companies are able to spend more on defense of systems that handle high-value and large-scale data resources on a weighted risk basis approach. This enhances the value of empirical breach data in obtaining accurate and data-driven cybersecurity budgeting

4.5 Impact Analysis Country-Wise of People Affected with Breaches

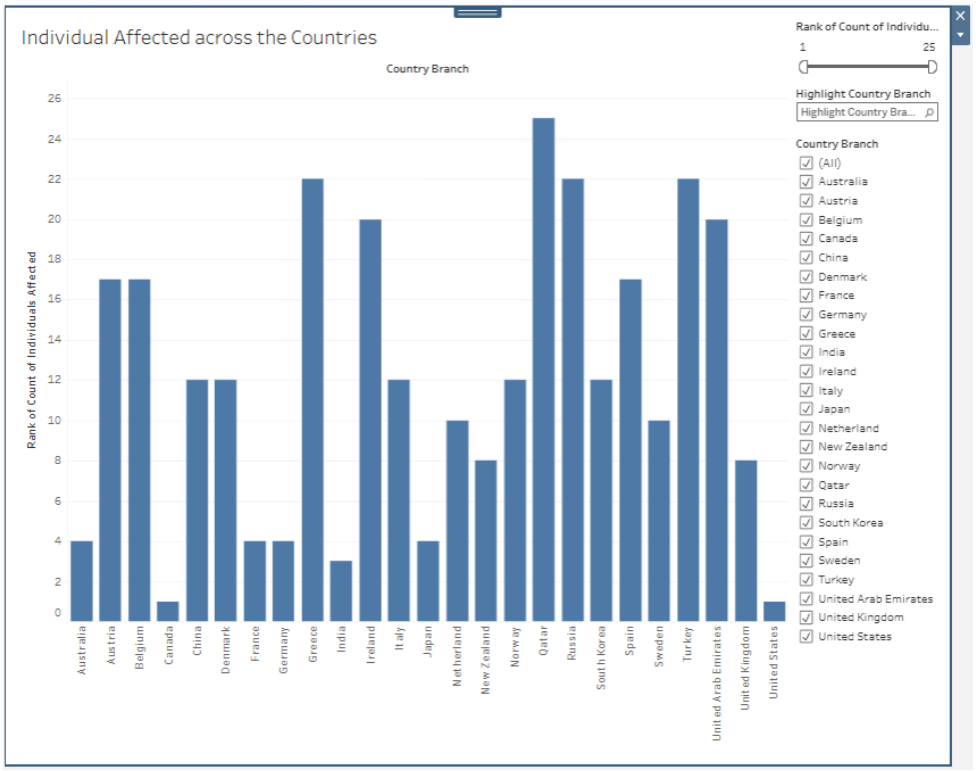


Figure 5: This Image display on Country-Wise of People Affected with Breaches

Figure 5 shows the ranking of the countries depending on the quantum of the number of people who have suffered the impact of cybersecurity breaches in the international branches. The statistics point out that Qatar, New Zealand, Spain, and the United Arab Emirates also indicate the greatest impact with more than 20 cases touching upon a great number of people. India, and Sweden are some other countries that are largely affected whereas France, Germany, and United Kingdom among others record a smaller number affected. This geographical variation means that cybersecurity threats do not distribute equally and instead their concentration in specific regions with higher risks- probably because there is inequality in law enforcement, advancement in digital development and organizational adoption of cybersecurity measures. As an example, a more vulnerable country when it comes to exposure to data breaches due to extensive but less established governance or infrastructure such as the cases of Qatar or New Zealand will be characterized by the fast digital adoption rate. This international imbalance is quite relevant when it comes to the prioritizing of investment. Multinational companies should also finance cybersecurity in relation to regional threats exposure besides the internal value of the company assets [48]. Business analytics technology can be used to plot breach hotspots on a geographical map that can inform the leadership to adopt investment strategies that are specific to risks in a given area. This understanding is in favor of producing a dynamic decision support framework that takes into consideration historical breach severity, geographical breach density. Instead of adopting an equalized approach to all the branches, the resources should follow contextual realities-the more exposed a country is, the more investments per unit of security technology, staff education and compliance checks should be. This strengthens the idea that cybersecurity investment cannot be arbitrary, it has to be evidence-based, can follow a risk concentration, or remain anchored to an analytic framework based on historical facts.

4.6 Geographical Analysis of Predicted Stolen Data

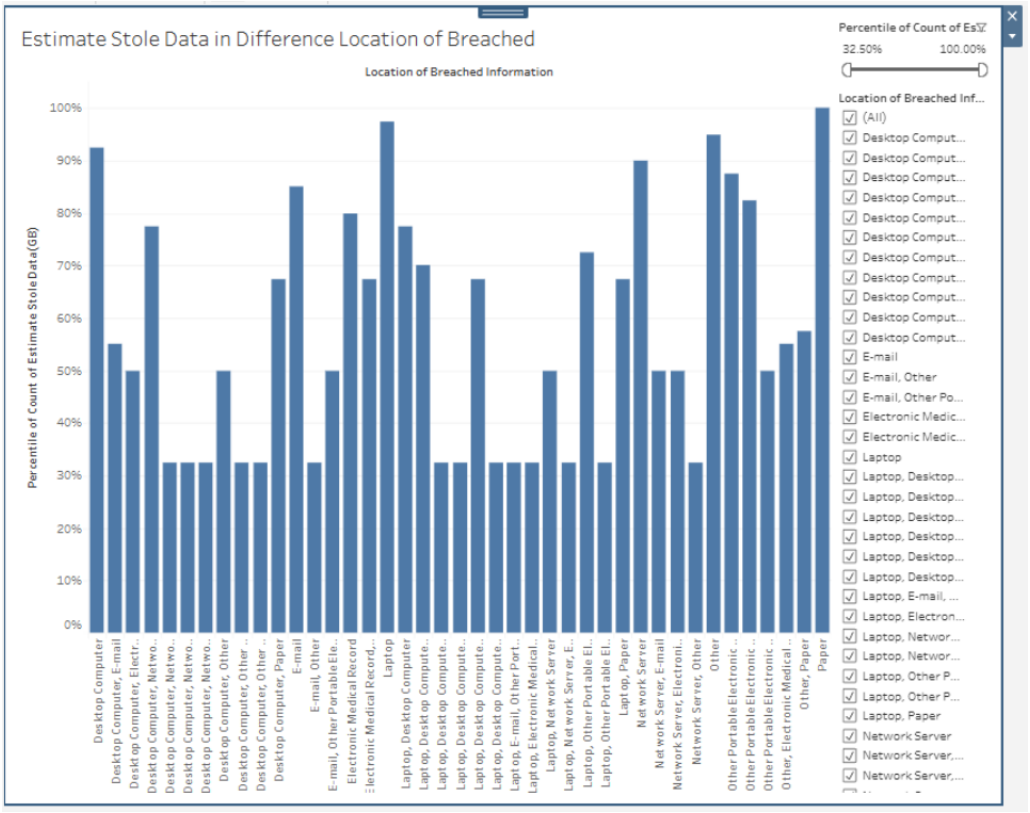


Figure 6: This Image shows the percentage distribution of estimated stolen data (in gigabyte) at different locations of the breached information

Figure 6 is a bar chart concerning the percentage distribution of estimated stolen data (in gigabyte) at different locations of the breached information. The statistics cite network servers, laptops, email systems, desktop computers and other portable electronic devices as the most vulnerable point of access and storage of data in cases of breaches. Locations like Laptop, Network Server, Paper and Email, Others also portray high volumes of breaches with some breaches passing the 90-percentile mark of the estimated sealed data. The graph indicates that network servers, and multi-location set-up (e.g. laptop desktop) are high-expenditure areas which will lead to large data losses. However, on the other hand, single insolation such as paper records or single desktops exhibits a data exposure that is relatively much lower than other fractions yet stands notable in cases of combined breach points. This observation is very critical to cyber security investment planning. Through business analytics, companies can set priorities of where to fund their effort by knowing which assets and infrastructures are at high-level exposure breach points. To provide an example, better server protection, secure remote access policy, encrypted laptops storage, and endpoint detection systems must be about higher investment priority [48]. This discussion justifies the introduction of a decision support model, which focuses on risk profiling on locations. Rather than utilizing generalized forms of cybersecurity to all systems, companies can be more targeted when it comes to budget allocation and funnel that money toward items and entry points traditionally shown to lead to larger amounts of data loss. This number further reinstates the idea that the location of breaches is an essential input variable in the context of investment setting priorities and mercies on-going analytic observation to support the constant improvement of security strategy.

4.7 Effect Differences by Types of Breach

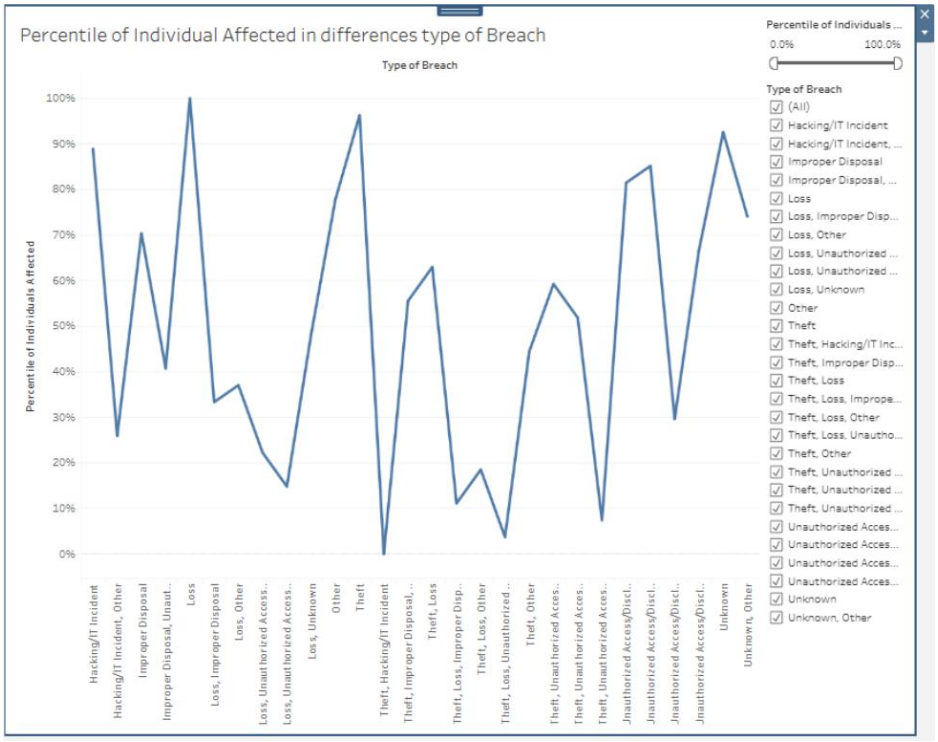


Figure 7: This Image display on the percentile distribution of people attacked by data breaches of various categories

Figure 7 shows the percentile distribution of people attacked by data breaches of various categories. In the line graph, it is possible to observe the consistency of the influence of the specific types of breaches (Theft, Unauthorised Access/Disclosure, and Hacking/IT Incidents) on the larger percentage of individuals. It is important to note that one notable pattern is the high spike in breach combinations such as Unauthorized Access & Theft and Hacking/IT Incident and Other with percentiles of 80-almost 100 and therefore, their disproportionate effect. Conversely, there are categories such as Improper Disposal, Loss & Unknown, and some combinations of Other which are of relatively lower percentiles, implying less personal impact as a result. This allocation focuses on the point that not all breaches pose equal threat to individuals. Decision-support and investment strategy as far as decision-support and investment strategy is concerned, this data is very valuable. It enables cybersecurity leaders to sort the categories of breaches based on the damage that they caused historically and reduce mitigation efforts as such. To cite an example, one can invest extensively in intrusion detection systems, endpoint security, and data encryption to fight theft-related and hacking-associated break-ins well, as these are the forms of breaches that are most likely to result in massive data exposure. such a chart allows a sophisticated, data-driven investment strategy to consider not the frequency, but the severity of breaches in terms of human resource implications. The framework of a decision support, based on this insight, would calculate weighted risk metrics of breach types and then allocate costly resources to breach types with the greatest individual exposure potential in an optimal manner. Figure 7 reiterates how business analytics are helpful in revealing the patterns of breaches and in aligning the money used in cybersecurity with the actual data showing its impact, and in pursuing wiser, risk-appropriate protection.

4.8 Geographic Representation of Estimated Stole Statistics

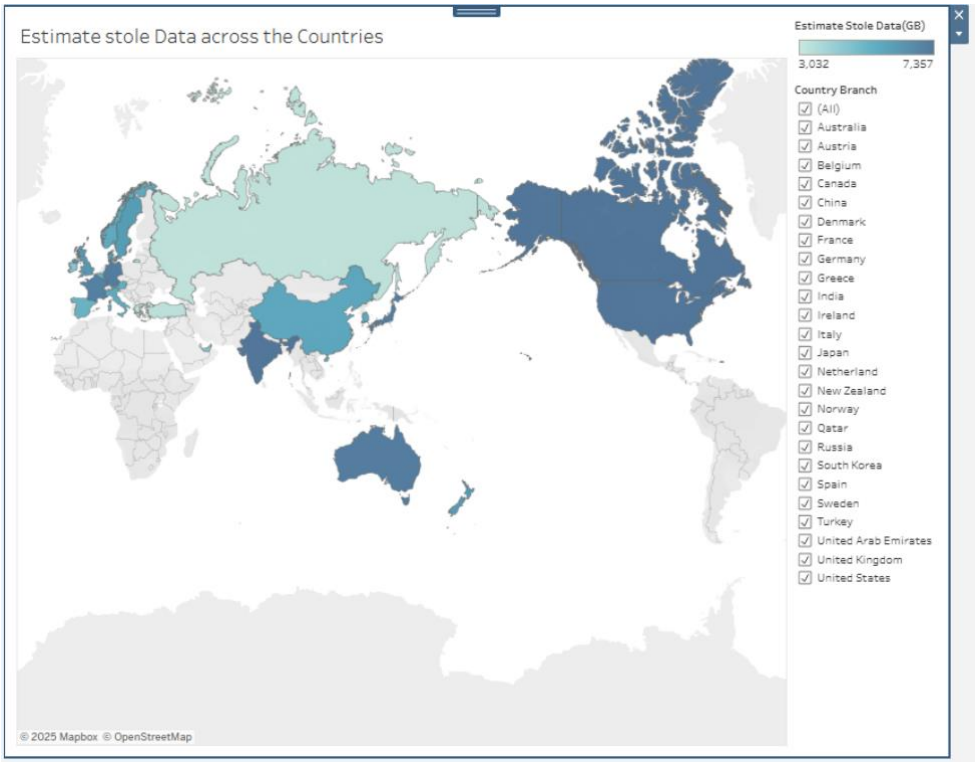


Figure 8: This Image represent to the estimated volume of data stolen (in gigabytes) in different countries in 2010-2023

In figure 8, visualization of a global map is presented, which shows the estimated volume of data stolen (in gigabytes) in different countries in 2010-2023. The magnitude of data breaches according to country is described in color gradient with darker colored countries having higher data breach numbers. The United States, Canada, India, Australia, and some of the European countries are the most notable, where the greatest losses are reported. The same may be linked to the spatial concentration of digital infrastructure including sensitive databases of the government and private sectors and stricter breach reporting laws within these markets. This geographic pattern is essential to strategic planning in investing in cybersecurity. Nations experiencing high breach rates must place prime importance on cybersecurity funding and the modernization of technology and how risk can be countered. Using such a map as a part of a decision support system, an organization or government can also conduct regional risk analysis to distribute resources efficiently. As an example, whenever a certain area like North America shows a constant data loss, entities in this region can invest more in intrusion detection systems, cloud security, and data loss prevention systems than other areas that are not at a high risk of losing data. Figure 8 assists in making business-based reasoning on investments in region-specific apps of cybersecurity investments. The decision-makers can use the weighted investment portfolio instead of using the same global budget- investing where breach history and data exposure are the worst. This is consistent with your research objective which is placed to optimize cybersecurity investments using data-based intelligence [49]. This number enables stakeholders to combine geographic intelligence and cybersecurity key performance indicators to improve investment plans according to the real effects of breaches on the global map.

4.9 Trend of Individual Impact Since Breach Onset Analysis

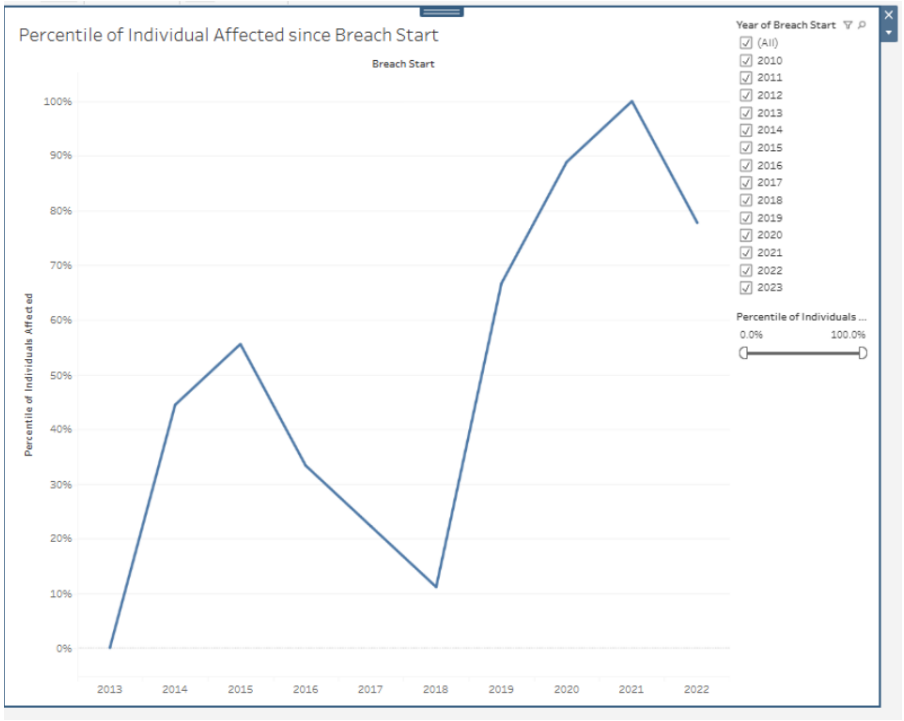
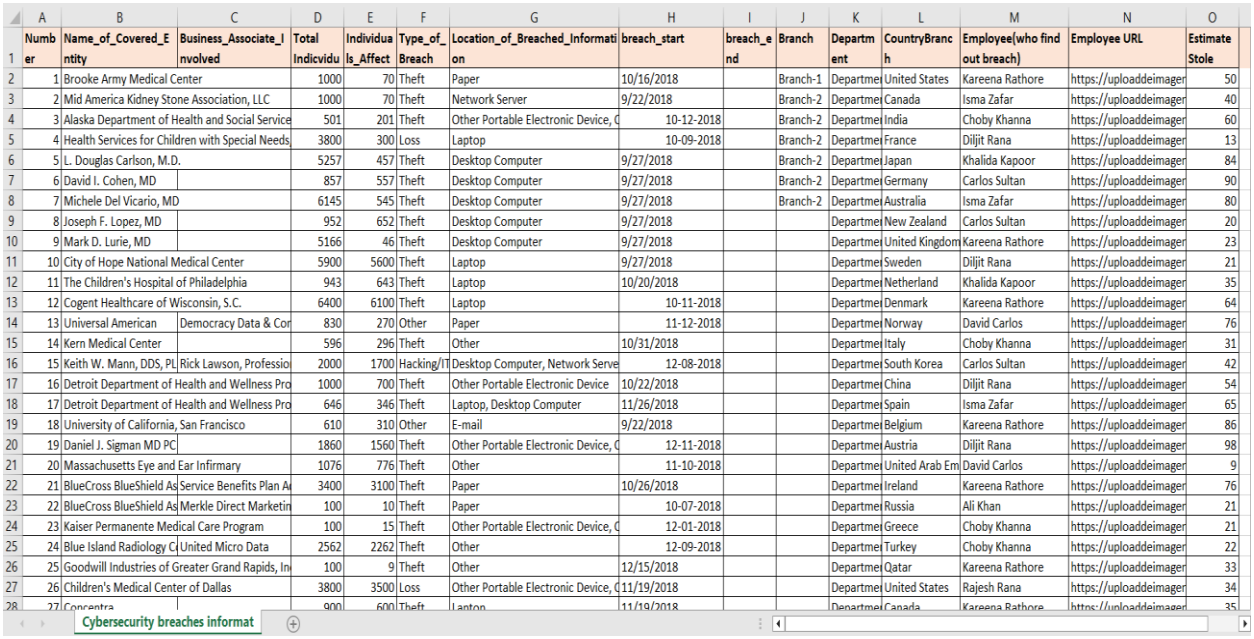


Figure 9: This figure displays percentile representation of individual affected since the beginning of reported data breaches in 2013 to 2023

Figure 9 shows the percentile distribution of the number of affected people since the time of the first reported cases of data breaches in 2013-2023. The graph indicates a great variability in the depth and the scope of cybersecurity incidents as time passed. Its sudden increase in 2013-2015 can be described as the premature boom of impactful breaches that was possible because of the lack of preparedness in the period of massive digitalization. But a declining trend occurs in the years after, which indicates that in 2016-2018 security measures were temporarily improved or underreported. The most striking is the sharp increase after 2018 with the maximum in 2021, when the percentile of the affected population is close to 100%. This threatening increase is the indicator of the rising complexity of hacking efforts and their expanded nature, particularly the pandemic, when work-at-home offices, cloud migration, and growing online dependencies created new bald spots. A little decline in 2022, although significant, indicates that some organizations implement countermeasures. This temporal trend is crucial when managing business analytics since it involves prioritizing on cybersecurity investments. The decision-makers can associate the peak breach impact year with IT policy adjustments, new threats, or cyber hygiene weakness. The post-2018 surge is an SOS signal that the endpoint security is not as high as it should be, that the breach detection capabilities are lacking, and that security awareness initiatives should be upgraded. Following the decision support framework suggested in the present paper, such temporal analysis allows forecasting of risks and optimization of resources. This can be used to enable organizations to determine how their budgets towards cybersecurity should be prioritized in a manner that can make it a proactive defense rather than a reactive one by aligning it with times when the impact of breaches have affected them the most [50]. The illustration clearly goes to underline the fact that security investments on cybersecurity should not be stagnant but rather they should dynamically change with trends of breach as time goes by.

5. Dataset

5.1 Screenshot of Dataset



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Number	Name_of_Covered_Entity	Business_Associate_Involved	Total Indicvidu	Individuals_Affect	Type_of_Breach	Location_of_Breached_Information	breach_start	breach_end	Branch	Department	CountryBranch	Employee(who find out breach)	Employee URL	Estimate Stole
2	1	Brooke Army Medical Center		1000	70	Theft	Paper	10/16/2018		Branch-1	Departmei	United States	Kareena Rathore	https://uploaddeimager	50
3	2	Mid America Kidney Stone Association, LLC		1000	70	Theft	Network Server	9/22/2018		Branch-2	Departmei	Canada	Isma Zafar	https://uploaddeimager	40
4	3	Alaska Department of Health and Social Service		501	201	Theft	Other Portable Electronic Device, C	10-12-2018		Branch-2	Departmei	India	Choby Khanna	https://uploaddeimager	60
5	4	Health Services for Children with Special Needs		3800	300	Loss	Laptop	10-09-2018		Branch-2	Departmei	France	Diljit Rana	https://uploaddeimager	13
6	5	L. Douglas Carlson, M.D.		5257	457	Theft	Desktop Computer	9/27/2018		Branch-2	Departmei	Japan	Khalida Kapoor	https://uploaddeimager	84
7	6	David I. Cohen, MD		857	557	Theft	Desktop Computer	9/27/2018		Branch-2	Departmei	Germany	Carlos Sultan	https://uploaddeimager	90
8	7	Michele Del Vicario, MD		6145	545	Theft	Desktop Computer	9/27/2018		Branch-2	Departmei	Australia	Isma Zafar	https://uploaddeimager	80
9	8	Joseph F. Lopez, MD		952	652	Theft	Desktop Computer	9/27/2018			Departmei	New Zealand	Carlos Sultan	https://uploaddeimager	20
10	9	Mark D. Lurie, MD		5166	46	Theft	Desktop Computer	9/27/2018			Departmei	United Kingdom	Kareena Rathore	https://uploaddeimager	23
11	10	City of Hope National Medical Center		5900	5600	Theft	Laptop	9/27/2018			Departmei	Sweden	Diljit Rana	https://uploaddeimager	21
12	11	The Children's Hospital of Philadelphia		943	643	Theft	Laptop	10/20/2018			Departmei	Netherland	Khalida Kapoor	https://uploaddeimager	35
13	12	Cogent Healthcare of Wisconsin, S.C.		6400	6100	Theft	Laptop	10-11-2018			Departmei	Denmark	Kareena Rathore	https://uploaddeimager	64
14	13	Universal American	Democracy Data & Cor	830	270	Other	Paper	11-12-2018			Departmei	Norway	David Carlos	https://uploaddeimager	76
15	14	Kern Medical Center		596	296	Theft	Other	10/31/2018			Departmei	Italy	Choby Khanna	https://uploaddeimager	31
16	15	Keith W. Mann, DDS, PL	Rick Lawson, Professio	2000	1700	Hacking/IT	Desktop Computer, Network Serve	12-08-2018			Departmei	South Korea	Carlos Sultan	https://uploaddeimager	42
17	16	Detroit Department of Health and Wellness Pro		1000	700	Theft	Other Portable Electronic Device	10/22/2018			Departmei	China	Diljit Rana	https://uploaddeimager	54
18	17	Detroit Department of Health and Wellness Pro		646	346	Theft	Laptop, Desktop Computer	11/26/2018			Departmei	Spain	Isma Zafar	https://uploaddeimager	65
19	18	University of California, San Francisco		610	310	Other	E-mail	9/22/2018			Departmei	Belgium	Kareena Rathore	https://uploaddeimager	86
20	19	Daniel J. Sigman MD PC		1860	1560	Theft	Other Portable Electronic Device, C	12-11-2018			Departmei	Austria	Diljit Rana	https://uploaddeimager	98
21	20	Massachusetts Eye and Ear Infirmary		1076	776	Theft	Other	11-10-2018			Departmei	United Arab Em	David Carlos	https://uploaddeimager	9
22	21	BlueCross BlueShield As	Service Benefits Plan Ac	3400	3100	Theft	Paper	10/26/2018			Departmei	Ireland	Kareena Rathore	https://uploaddeimager	76
23	22	BlueCross BlueShield As	Merkle Direct Marketin	100	10	Theft	Paper	10-07-2018			Departmei	Russia	Ali Khan	https://uploaddeimager	21
24	23	Kaiser Permanente Medical Care Program		100	15	Theft	Other Portable Electronic Device, C	12-01-2018			Departmei	Greece	Choby Khanna	https://uploaddeimager	21
25	24	Blue Island Radiology C	United Micro Data	2562	2262	Theft	Other	12-09-2018			Departmei	Turkey	Choby Khanna	https://uploaddeimager	22
26	25	Goodwill Industries of Greater Grand Rapids, In		100	9	Theft	Other	12/15/2018			Departmei	Qatar	Kareena Rathore	https://uploaddeimager	33
27	26	Children's Medical Center of Dallas		3800	3500	Loss	Other Portable Electronic Device, C	11/19/2018			Departmei	United States	Rajesh Rana	https://uploaddeimager	34
28	27	Concentra		900	600	Theft	Laptop	11/19/2018			Departmei	Canada	Kareena Rathore	https://uploaddeimager	35

Cybersecurity breaches informat

5.2 Dataset Overview

The dataset that the research is based on is the Cybersecurity Breaches Information 2010-2023 data set provided by the government that is used to analyses the past history of cybersecurity breaches, be helpful in forming data-driven investment prioritization strategies. It has elaborated theoretical data of more than 1,050 cybersecurity violations cases between 2010 and 2023 involving different institutions and sectors. The data consists of an individual breach case per row with a vast number of attributes, which includes the name of the affected organization, a presence/absence of business association, the total number of individuals affected, the nature of the breach, the location of the breach, the estimated number of gigabytes of stolen data, the date of the start and end of the breach, a cross between the branch and department-level, and branch details country-wise. Such weight and information abundance allow multi-dimensional breach patterns analysis providing quantitative and non-categorical vision of the cybersecurity field during the last ten years [64]. The use of the breach types also allows determining the types of threats by their nature and impact such as theft, hacking/IT incidents, unauthorized access, and data loss. Time dimension of the data set permits the analogy of the changes in cyber threats over time to show patterns in maximum cases like the increased incidents since 2018. The Location_of_Breached_Information variable identifies the popular areas of exposure of keys such as laptop computer, desktop computer, paper records and network server which are essential in defining the specific security investments. The estimate of the amount of lost data (in GB) further measures the severity of breach, which improves risk assessment. Having structured and labeled fields, the dataset is quite decent to work with business analytics tools (Tableau, Excel, Python), and to visualize the information and create frameworks it is highly eligible. using the organizational metadata e.g., department and branch classification, the dataset can be used to do segmentation analysis that allows doing industry-specific investment decision-making. Its usability rank and licensing released on the open Apache 2.0 license guarantee optimum transparency, reproducibility, and ethicality. This dataset has rich, real-life evidence that suits the research goal of creating a decision support system to prioritize cybersecurity investments on an objective measure of exposure to loss of sensitivity, frequency of breach, and impact on sensitive data.

6. Proposed Framework

6.1 Cybersecurity Investment Prioritization Framework

The main contribution of this study is the development of a multi-phase decision-making framework that assists companies to focus on what they need to invest in cybersecurity based on past breach history and business analytics. The framework was formulated in such a way that it can convert raw data on incidents into strategic investment advice through the integration of several aspects of risk such as frequent breaches, severity of the impact, quantity of data that is lost due to a breach and the vulnerability points in a system [51]. This framework starts with data inputs based on the two-variate variables of the dataset named the Cybersecurity Breaches Information 20102023 that entailed variables like the type and nature of the breach, the number of people affected, the location place where the breach happened, and the estimated amount of data stolen in GBs. These inputs are run through an analytical model that gives them a weighted risk score using parameters of breach recurrence, potential harm, and infrastructure criticality. Every incident is classified and rated to establish its rate of risk exposure, and this is plotted in the line of already set categories of investment such as endpoint security, network infrastructure, access control or data encryption. As tools, the framework will utilize business analytics such as Tableau and Python in visualizing the concentration of risks and establishing risk priority among threats. This leads to an organized matrix of investments which directs decision-makers where to focus the little security funds to have high returns. An example would be that, in case a trend is identified about network servers' data breaches in a healthcare organization, the framework would first focus on investing in intrusion detection systems and encrypting at server side in the sector. This process will enable companies to reduce risk proactively because it will concentrate on areas that have been weak historically instead of depending on ad-hoc or reactive expenditures [52]. In addition, the framework is flexibly structured and scalable allowing implementation to be applied in various fields and various companies of diverse scales. It can also be used as a dynamic model; hence it can incorporate real-time data update investment recommendations whenever new threats appear. In the end, this decision-making structure will enable security and executive personnel to make well-informed, data-determined investment decisions that consider cybersecurity strategy and priorities relative to actual risk exposure and company priorities.

7. Discussion and Analysis

7.1 Analysis of Investment Strategy based on Cybersecurity Breach Trends

The evaluated data indicate a very strong increase of cybersecurity attacks, especially since the year 2018. The trend shows a sharp increase with the highest number leveling to 2022, as illustrated in figure 3 as the number of breaches per year. The fact that the threat landscape has been on the increase indicates organizations have to respond strategically [53]. The steep growth in cases can be attributed to the sophistication of attackers the online growth of businesses. Business analytics helps in detecting trends, e.g. breaches concentration in a particular year or industry and the decision-makers knowing where to invest based on past and future trends. As an illustration, using a data-driven approach would focus on the improvement of security infrastructures in the industries that continuously demonstrate high volumes of breaches [53]. The pattern of breach frequency changing in time reveals that dynamic investment schemes are required that will adjust to variations in the intensity of threats. Instead of an inflexible annual cybersecurity budget, absolutely it is not possible to have a static annual budget but rather dynamic financial planning models based on real-time analytics [54]. Business intelligence tools may assist the simulation of breach scenarios and predicting ROI of various cybersecurity solutions. Incorporation of breach frequency analysis in strategy planning will enable proactive approach as opposed to reactive to the funding of cybersecurity. Such trend data supports the argument that security budgets still need to be redirected to accommodate new types of threats, which enhances resilience and reduces the overall damage.

7.2 Evaluating the Sphere of Breaches Influence

The frequency of cybersecurity breaches is not the only factor contributing to its severity since the number of those affected and the amount of data compromised is also important [54]. The figures 1 and 9 demonstrate the staggering scale of certain breaches where thousands and millions of people have been affected and losses of data have been recorded in terabytes. The increased number of people affected since 2019 is an indicator of the growth of sensitive footprints of data in the digital environment. In Figure 1, the breach of TRICARE Management Activity and Health Net, Inc. impacted multiple million people, which is a prime indicator of the disastrous possibilities of uncontrolled vulnerabilities. Figure 4 that demonstrates stolen data volumes by leading entities proves that breaches are not confined in volume, but count various institutions in healthcare industry, education, and governmental employment. This information shows that there is an urgent need to categorize cyber threats beyond the numbers but into business terms like the quantity of data records that were lost and the business functions affected. To decision-makers, this level of data usefulness assists them to know which assets need the most attention in terms of security [55]. Business analytics has the capability to measure breaches impact between departments, making organizations prioritize valuable digital assets. As an example, industries handling sensitive personal health information or monetary data would need to invest more in data loss prevention applications. The combination of breach impact and data value makes the decision more complex because one must approach the defense in layers, based on analytics of prioritizing which breach vectors are most damaging.

7.3 Utilizing the Business Analytics to Inform Strategic Cybersecurity Decisions

Business analytics play the role of enabling interpretation of raw cyber incident data to useful information. Through dashboards, correlation matrices and predictive models, organizations will be able to understand and comprehend various data sets and use them to make cybersecurity investment decisions [56]. As an example, in Figure 2 and Figure 6, it can be seen how the breaches type and location are distributed, with the most significant weight belonging to the vectors of theft, unauthorized access, and desktop vulnerability. Analytics also allows the recognition of these lofty risk breach modes and correlates them with certain system vulnerability or shortcomings in procedures. Thus, decision-makers will be able to focus their budget on sections like end-point protection, access control or the training of its employees. In addition, radar charts displayed in Figure 4 can be applied to represent multidimensional breach measures across institutions and aid comparative risk assessment. Scenario modeling and simulation are tools that help to predict the loss rate when the amount of money is invested in different levels; and this can be facilitated through business analytics [57]. Such a method allows maximizing the expenditures by making them aimed at the maximum reduction of impact. And, with the incorporation of machine learning models, organizations would be able to identify anomalies in real-time, which would also increase the capabilities of breach response. Predictive analytics enables leaders to determine the future attack surfaces, rather than basing the decisions on past data. Such a proactive model will make sound cybersecurity decisions, not intuitive guesses but decisions made based on mathematical trends [58]. Business analytics shifts the management of cybersecurity trends into a proactive aspect since business investments are always made in accordance with the changing risk situations.

7.4 Ranking investments in Cybersecurity according to risks and exposure

The necessity to have evidence-based investments in cybersecurity in order of severity of breaches and geographic issues is one of the focal points in the research. Figure 5 and Figure 8 have a strong variance in the breach impact among countries [59]. The most common rates and volumes of breached information emerge in the United States, Canada, and some countries located in Europe and Asia. These observations enable global institutions to adjust their investment plans, based on local threat settings. As an illustration, a multinational company might need to spend

more of its budget on data centers in the territories with the high-security risks and keep the minimum provisions there. Figure 7 proves the heterogeneity of the form of breaches in severity, strengthening the fact that not every cyber issue is equally devastating. This variance in risk exposure highlights the need to implement a layered model of investment where the most high-risk breach types like theft and unauthorized access are ranked first and given better security measures. Business analytical tools, such as heat maps and percentile distribution charts help in plotting exposure areas and risk classification. Such observations can flow into a cybersecurity investment matrix where investment in risk funds gets commensurate with allocated spending on the risk. Incorporating business analytics into the preferences of the prioritized framework also means that priority is guaranteed to the systems that are most at risk of affecting large impacts. They also provide executive stakeholders with quantitative grounds to approve cybersecurity budgets and they change the perception of being viewed as cost centers into being regarded as risk reduction assets. Exposure to investment needs can be charted clearly by the organizations, through which a defensible and transparent cybersecurity budget strategy can be developed by the organization.

7.5 Integration of Findings and Strategic Planning in Informing a Decision

Business analytics can add a rigorous, framework-based system of dealing with rising digital threats when they are incorporated into the investment decision-making process in cybersecurity. The visual evidence discussed in Figures 1 through 9 all allude to the multidimensionality of cyber breaches, including everything beginning at the level of individuals and ending at the level of national data exposure. This information will be valuable because it will help us make a rational decision-making process, i.e. investment should be based on facts not organizational hypotheses [60]. Business analytics offers means to perform post mortems of the activity performed, keep track of the weaknesses in place and predict their drawbacks in the future. These abilities enable cybersecurity leaders to build dynamic defense strategies that are data driven. To further optimize the strategic decisions, the analytics can also be combined with key performance indicators (KPIs), which can then be used to assess the success or failure of investments in the future. Cross-functional insights-based on breach type analysis to geographic trends can be used to enable the creation of cross-functional security policies that address both technical and organizational levels. This corresponds to the larger idea of cybersecurity as a cross-departmental issue. This paper supports the view that cybersecurity is no longer solely a technical cost to be incurred but a strategic investment to be made. Through the years, business analytics forms the backbone of decision-makers having the capacity to defend budgets, align resources, and develop resilient organizations that are ready to meet the future digital landscape.

7.6 Ethical Considerations

This study provides a high level of adherence to the ethical norms of research because it only uses publicly available secondary data that is anonymized. There was no use or transfer of personally identifiable information (PII) The information was not any sensitive organizational records. Ethical integrity in the process of preparation and analysis of data was followed by not doing a data influence or selective reporting [61]. All the visualizations and interpretations were carried out unbiasedly to prevent the falsity of the severity of breaches or risk to an organization. The decision support model proposed will aid ethical cybersecurity investments which should focus on risk disincentives and mitigation instead of punitive measures. The fact that the data will be misused was also considered, and the findings were presented in such a way that promotes a positive change of the cybersecurity posture but not a stigmatization of any entity. Careful and honest exchange of scholarly information the study complies with data use regulations and citation policies, thus allowing impartial and transparent research [68]. How the proposed study will contribute to building cybersecurity resilience in sectors (ethically and equitably) is that the

study will facilitate intelligent decision-making with the aid of business analytics to drive cybersecurity resilience in the sectors.

8. Future Work

Although this study presents a business analytical framework on how to prioritize investments in cybersecurity based on data, a lot of opportunities can be explored and improved in the future [62]. The argument holds that one of the promising areas is to combine real-time threat intelligence streams and AI-based anomaly detection into the decision support framework, which makes it more dynamic and responsive to decide on investing assets. Predictive modeling with machine learning algorithms to provide the likelihoods of breaches occurring based on the organizational behavior, the maturity of the digital infrastructure, and the level of threats in the region can also be implemented in the future. expanding the framework to cover industry-specific benchmarks, e.g. specific to healthcare, finance, or government sectors, may have the additional benefit of making the investment suggestions more applicable and more accurate. The other front to be considered is creating a risk-scoring engine which continually calculates the return on security investment (ROSI) as it matches the spent on the mitigation of risks in the long run. This would be facilitated by means of longitudinal data and constant performance analytics. Also, the future studies might be aimed to test the human factor in cybersecurity, correlating it with the behavioral analytics to detect the insider threats and to determine the practical results of the training programs among the employees [63]. The existing dataset might be further expanded in terms of the more detailed breach data, including the duration of the breach, the time to identify it, and the cost of a single breach, which would allow gaining insights into the most troublesome vulnerabilities. With the addition of the privacy rules and frameworks, including such standards as GDPR and HIPAA, to the investment model, it would provide enhanced usefulness to the global organizations. Finally, further developing the interactive dashboard or a tool that would automate the prioritization process is the future work where executives and IT managers may simulate different investment scenarios and get real-time recommendations. With the support of the flux of technologies and trans-disciplinary data, the proposed decision support framework can transform into an intelligent, powerful cybersecurity investment platform that makes organizations make smarter, faster, and cheaper decisions in a growing technological complex threat environment.

9. Conclusion

This study has demonstrated the efficient and detailed approach of making the investment priority in the domain of cybersecurity via the integration of the decision support framework based on business analytics. The analysis of the breach data of the period between 2010 and 2023 provided strategic information on the rate of breach, breach intensity, categories, sectors, and geographical areas of attacks, which cumulatively assisted in the direction of the cybersecurity investments that require the most immediate action. The research concluded that theft and unauthorized access has been the most prevalent types of breach with network servers, desktops and endpoint devices being the most common target. To identify the essential vulnerabilities and trends that could go unnoticed in classical analysis, visualizations were created with the help of Tableau, Excel, and Python libraries. The structured system of breach-based categorization and ranking of investment needs provided by the proposed framework will give the organizations an effective strategic instrument to ensure that their resources on cybersecurity are spent on genuine risk exposure. It is especially critical at the time when cyber threats like never before are increasing, budgets are tight, and decision-makers need the right, evidence-based answers. This study notes that it is necessary to make plans proactive by moving beyond reactive security to planning based on analytical insights. Although the study itself admits several limitations in not having financial impact data and not having real time threats feeds, it shows that a historical relationship between breach types can nonetheless provide a powerful base in which investments might be modeled. By incorporating business analytics into cybersecurity planning, not only does this make decisions

made in cybersecurity more excellent in quality but it also increases stakeholders' understanding of why they should allocate cybersecurity budgets by demonstrating clear reductions to risks by making decisions. Besides, this study will provide the framework in which predictive models based on AI, real-time data streams, and other industry-specific customization could be used to narrow the decision-making process in future studies. Finally, the results support the major hypothesis that the increased investment in cybersecurity must be more targeted with the analytical inputs as it becomes more efficient and effective. Through this framework, organizations can develop a robust digital defense position, making the most out of available resources and continuously protecting the assets that matter with the ongoing threats.

10. References:

1. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.

   https://www.sciencedirect.com/science/article/abs/pii/S0007681321000240

2. Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal, 23(3), 383-404.

   https://www.sciencedirect.com/science/article/pii/S1110866522000226

3. Bouramdane, A. A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. Journal of Cybersecurity and Privacy, 3(4), 662-705.

   https://www.mdpi.com/2624-800X/3/4/31

4. Sönmez, F. Ö., & Kılıç, B. G. (2020). A decision support system for optimal selection of enterprise information security preventative actions. IEEE Transactions on Network and Service Management, 18(3), 3260-3279.

   https://ieeexplore.ieee.org/abstract/document/9295382

5. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Computing and Applications, 34(18), 15241-15271.

   https://link.springer.com/article/10.1007/s00521-022-06959-2

6. Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. Information & Computer Security, 28(4), 591-625.

   https://www.emerald.com/insight/content/doi/10.1108/ics-11-2018-0131/full/html

7. Shaqiri, B. (2023). A System for Cost-Efficient Cybersecurity Planning, Compliance, and Investment Prioritization (Master's thesis, University of Zurich).

   https://www.zora.uzh.ch/id/eprint/255737/

8. Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. Risk Analysis, 40(1), 183-199.

   https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.12891

9. van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. Computers & Security, 113, 102535.

https://www.sciencedirect.com/science/article/abs/pii/S016740482100359X

10. Sönmez, F. Ö., & Kılıç, B. G. (2020). A decision support system for optimal selection of enterprise information security preventative actions. IEEE Transactions on Network and Service Management, 18(3), 3260-3279.

    https://ieeexplore.ieee.org/abstract/document/9295382

11. Abushark, Y. B., Khan, A. I., Alsolami, F., Almalawi, A., Alam, M. M., Agrawal, A., ... & Khan, R. A. (2022). Cyber security analysis and evaluation for intrusion detection systems. Comput. Mater. Contin, 72(1), 1765-1783.

    https://www.academia.edu/download/102439430/pdf.pdf

12. Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580.

    https://www.sciencedirect.com/science/article/abs/pii/S0167923621000907

13. Franco, M. F., Lacerda, F. M., & Stiller, B. (2022). A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises. Revista de Gestão e Projetos, 13(3), 10-37.

    https://uninove.emnuvens.com.br/gep/article/view/23083

14. Nwaimo, C. S., Adewumi, A., & Ajiga, D. (2022). Advanced data analytics and business intelligence: Building resilience in risk management. International Journal of Scientific Research and Applications, 6(2), 121.

    https://www.researchgate.net/profile/Adetumi-Adewumi/publication/388493052_Advanced_data_analytics_and_business_intelligence_Building_resilience_in_risk_management/links/67620d46af28fb680fc087d7/Advanced-data-analytics-and-business-intelligence-Building-resilience-in-risk-management.pdf

15. Quang, L. V., Duc, T. H., Debnath, N. C., & Long, N. N. (2023). Managing Risks in the Adoption of Cybersecurity Technology in Manufacturing Enterprises: Identification and Assessment. International Journal for Computers & Their Applications, 30(4).

    https://openurl.ebsco.com/EPDB%3Agcd%3A7%3A1495671/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A174858376&crl=c&link_origin=scholar.google.com

16. Alahmari, A. A., & Duncan, R. A. (2021, November). Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs. In 2021 IEEE International Conference on Computing (ICOCO) (pp. 115-121). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9673554

17. Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. Technological Sustainability, 2(4), 372-387.

    https://www.emerald.com/insight/content/doi/10.1108/techs-05-2023-0022/full/html

18. Kim, S. (2022). Critical success factors evaluation by multi-criteria decision-making: a strategic information system planning and strategy-as-practice perspective. Information, 13(6), 270.

    https://www.mdpi.com/2078-2489/13/6/270

19. Judijanto, L., Hindarto, D., & Wahjono, S. I. (2023). Edge of enterprise architecture in addressing cyber security threats and business risks. International Journal Software Engineering and Computer Science (IJSECS), 3(3), 386-396.

https://journal.lembagakita.org/ijsecs/article/view/1816

20. Shreeve, B., Gralha, C., Rashid, A., Araújo, J., & Goulão, M. (2023). Making sense of the unknown: How managers make cyber security decisions. ACM Transactions on Software Engineering and Methodology, 32(4), 1-33.

https://dl.acm.org/doi/full/10.1145/3548682

21. Bokan, B., & Santos, J. (2022, April). Threat modeling for enterprise cybersecurity architecture. In 2022 Systems and Information Engineering Design Symposium (SIEDS) (pp. 25-30). IEEE.

https://ieeexplore.ieee.org/abstract/document/9799322

22. Shreeve, B., Hallett, J., Edwards, M., Ramokapane, K. M., Atkins, R., & Rashid, A. (2020). The best laid plans or lack thereof: Security decision-making of different stakeholder groups. IEEE Transactions on Software Engineering, 48(5), 1515-1528.

https://ieeexplore.ieee.org/abstract/document/9195777

23. Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M. H. A., Hitchens, M., & Ryan, M. (2023). Modelling the ethical priorities influencing decision-making in cybersecurity contexts. Organizational Cybersecurity Journal: Practice, Process and People, 3(2), 127-149.

https://www.emerald.com/insight/content/doi/10.1108/ocj-09-2022-0015/full/html

24. Pigola, A. (2023). Developing and investing in dynamic capabilities into business to enhance cybersecurity intelligence.

https://bibliotecatede.uninove.br/handle/tede/3279

25. Zadeh, A., Lavine, B., Zolbanin, H., & Hopkins, D. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. Decision Analytics Journal, 9, 100328.

https://www.sciencedirect.com/science/article/pii/S2772662223001686

26. Vakili, S. V., Ölçer, A. I., & Schönborn, A. (2021). Identification of shipyard priorities in a multi-criteria decision-making environment through a Transdisciplinary energy management framework: a real case study for a Turkish shipyard. Journal of Marine Science and Engineering, 9(10), 1132.

https://www.mdpi.com/2077-1312/9/10/1132

27. Moreira, F. R., Da Silva Filho, D. A., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2021). Evaluating the performance of NIST's framework cybersecurity controls through a constructivist multicriteria methodology. Ieee Access, 9, 129605-129618.

https://ieeexplore.ieee.org/abstract/document/9540950

28. Balogun, E. D., Ogunsola, K. O., & Samuel, A. D. E. B. A. N. J. I. (2021). A cloud-based data warehousing framework for real-time business intelligence and decision-making optimization. International Journal of Business Intelligence Frameworks, 6(4), 121-134.

https://www.researchgate.net/profile/Emmanuel-Balogun-11/publication/390137583_A_Cloud-Based_Data_Warehousing_Framework_for_Real-

_Time_Business_Intelligence_and_Decision-Making_Optimization/links/67e1d979e62c604a0d11d86f/A-Cloud-Based-Data-Warehousing-Framework-for-Real-Time-Business-Intelligence-and-Decision-Making-Optimization.pdf

29. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.

    https://www.sciencedirect.com/science/article/pii/S1566253523001136

30. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

    https://www.mdpi.com/1424-8220/23/15/6666

31. Liu, C. W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. Journal of Management Information Systems, 37(3), 758-787.

    https://www.tandfonline.com/doi/abs/10.1080/07421222.2020.1790190

32. Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., & Komárková, J. (2022). CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. Computers & Security, 115, 102609.

    https://www.sciencedirect.com/science/article/abs/pii/S0167404822000086

33. Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108.

    https://dergipark.org.tr/en/pub/rjbm/issue/80308/1372698

34. Tagarev, T. (2020). Towards the design of a collaborative cybersecurity networked organisation: identification and prioritisation of governance needs and objectives. Future Internet, 12(4), 62.

    https://www.mdpi.com/1999-5903/12/4/62

35. Puttaraju, K. H. (2023). Augmenting classical strategic tools with artificial intelligence: A systematic review of enhanced decision-making methodologies. International Journal of Science and Research(IJSR), 12(11), 2242-2247.

    https://www.researchgate.net/profile/Karthik-Hosavaranchi-Puttaraju-3/publication/388879047_Augmenting_Classical_Strategic_Tools_with_Artificial_Intelligence_A_Systematic_Review_of_Enhanced_Decision-Making_Methodologies/links/6832ec1bd1054b0207f315b0/Augmenting-Classical-Strategic-Tools-with-Artificial-Intelligence-A-Systematic-Review-of-Enhanced-Decision-Making-Methodologies.pdf

36. Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. Risk Analysis, 43(10), 2082-2098.

    https://onlinelibrary.wiley.com/doi/full/10.1111/risa.14092

37. Nisioti, A., Loukas, G., Laszka, A., & Panaousis, E. (2021). Data-driven decision support for optimizing cyber forensic investigations. IEEE Transactions on Information Forensics and Security, 16, 2397-2412.

https://ieeexplore.ieee.org/abstract/document/9339971

38. Ahmed, S., Ahmed, I., Kamruzzaman, M., & Saha, R. (2022). Cybersecurity Challenges in IT Infrastructure and Data Management: A Comprehensive Review of Threats, Mitigation Strategies, and Future Trend. Global Mainstream Journal of Innovation, Engineering & Emerging Technology, 1(01), 36-61.

    https://www.researchgate.net/publication/391566074_Cybersecurity_Challenges_In_IT_Infrastructure_And_Data_Management_A_Comprehensive_Review_Of_Threats_Mitigation_Strategies_And_Future_Trend

39. Shukla, M., Sarmah, S. P., & Tiwari, M. K. (2023). A multi-objective framework for the identification and optimisation of factors affecting cybersecurity in the Industry 4.0 supply chain. International Journal of Production Research, 61(15), 5266-5281.

    https://www.tandfonline.com/doi/abs/10.1080/00207543.2022.2100840

40. Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber risk assessment and optimization: A small business case study. IEEE Access, 11, 44467-44481.

    https://ieeexplore.ieee.org/abstract/document/10114920

41. Aliahmadi, A., & Nozari, H. (2023, January). Evaluation of security metrics in AIoT and blockchain-based supply chain by Neutrosophic decision-making method. In Supply chain forum: an international journal (Vol. 24, No. 1, pp. 31-42). Taylor & Francis.

    https://www.tandfonline.com/doi/abs/10.1080/16258312.2022.2101898

42. Ejiofor, O. E. (2023). A comprehensive framework for strengthening USA financial cybersecurity: integrating machine learning and AI in fraud detection systems. European Journal of Computer Science and Information Technology, 11(6), 62-83.

    https://www.researchgate.net/profile/Oluwabusayo-Bello/publication/381548436_A_Comprehensive_Framework_for_Strengthening_USA_Financial_Cybersecurity_Integrating_Machine_Learning_and_AI_in_Fraud_Detection_Systems/links/667360e81846ca33b83e1d36/A-Comprehensive-Framework-for-Strengthening-USA-Financial-Cybersecurity-Integrating-Machine-Learning-and-AI-in-Fraud-Detection-Systems.pdf

43. Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.

    https://www.mdpi.com/2071-1050/15/18/13369

44. Ferreira, L., Silva, D. C., & Itzazelaia, M. U. (2023). Recommender systems in cybersecurity. Knowledge and information systems, 65(12), 5523-5559.

    https://link.springer.com/article/10.1007/s10115-023-01906-6

45. Akella, N., & Yogi, M. K. (2022). Correlating Decision Theory with Cyber Threat Intelligence: Novel Perspectives.

    https://www.researchgate.net/profile/Neha-Akella/publication/374976771_Correlating_Decision_Theory_with_Cyber_Threat_Intelligence_Novel_Perspectives/links/653a19401d6e8a70704e791b/Correlating-Decision-Theory-with-Cyber-Threat-Intelligence-Novel-Perspectives.pdf

46. Sumrit, D. (2021). Prioritization of policy initiatives to overcome Industry 4.0 transformation barriers based on a Pythagorean fuzzy multi-criteria decision making approach. Cogent Engineering, 8(1), 1979712.

https://www.tandfonline.com/doi/full/10.1080/23311916.2021.1979712

47. Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132, 103352.

    https://www.sciencedirect.com/science/article/pii/S0167404823002626

48. Rios Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & G. Rasines, D. (2021). An adversarial risk analysis framework for cybersecurity. Risk Analysis, 41(1), 16-36.

    https://onlinelibrary.wiley.com/doi/full/10.1111/risa.13331

49. Kumar, D., Singh, R. K., Mishra, R., & Daim, T. U. (2023). Roadmap for integrating blockchain with Internet of Things (IoT) for sustainable and secured operations in logistics and supply chains: Decision making framework with case illustration. Technological Forecasting and Social Change, 196, 122837.

    https://www.sciencedirect.com/science/article/abs/pii/S004016252300522X

50. Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974.

    https://www.sciencedirect.com/science/article/pii/S0167404822003662

51. Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEe Access, 10, 85701-85719.

    https://ieeexplore.ieee.org/abstract/document/9853515

52. Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. Annals of Data Science, 10(6), 1473-1498.

    https://link.springer.com/article/10.1007/s40745-022-00444-2

53. Rodriguez-Garcia, P., Li, Y., Lopez-Lopez, D., & Juan, A. A. (2023). Strategic decision making in smart home ecosystems: A review on the use of artificial intelligence and Internet of things. Internet of Things, 22, 100772.

    https://www.sciencedirect.com/science/article/pii/S2542660523000951

54. Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial Management & Data Systems, 121(3), 613-636.

    https://www.emerald.com/insight/content/doi/10.1108/imds-08-2020-0462/full/html

55. Kang, Y. (2023). Development of large-scale farming based on explainable machine learning for a sustainable rural economy: the case of cyber risk analysis to prevent costly data breaches. Applied Artificial Intelligence, 37(1), 2223862.

    https://www.tandfonline.com/doi/full/10.1080/08839514.2023.2223862

56. Priya, N. (2022). Cybersecurity considerations for industrial IoT in critical infrastructure sector. International Journal of Computer and Organization Trends, 12(1), 27-36.

    https://www.researchgate.net/profile/Neha-Priya-4/publication/360617087_Cybersecurity_Considerations_for_Industrial_IoT_in_Critical_Infr

astructure_Sector/links/6298678ba3fe3e3df8558643/Cybersecurity-Considerations-for-Industrial-IoT-in-Critical-Infrastructure-Sector.pdf

57. Dasawat, S. S., & Sharma, S. (2023, May). Cyber security integration with smart new age sustainable startup business, risk management, automation and scaling system for entrepreneurs: an artificial intelligence approach. In 2023 7th international conference on intelligent computing and control systems (ICICCS) (pp. 1357-1363). IEEE.

    https://ieeexplore.ieee.org/abstract/document/10142779

58. AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. Electronics, 12(17), 3629.

    https://www.mdpi.com/2079-9292/12/17/3629

59. Eilts, D. (2020). An empirical assessment of cybersecurity readiness and resilience in small businesses.

    https://core.ac.uk/download/pdf/304334147.pdf

60. Singh, S., Rajest, S. S., Hadoussa, S., Obaid, A. J., & Regin, R. (Eds.). (2023). Data-driven decision making for long-term business success. IGI Global.

61. Kayode-Ajala, O. (2023). Applications of Cyber Threat Intelligence (CTI) in financial institutions and challenges in its adoption. Applied Research in Artificial Intelligence and Cloud Computing, 6(8), 1-21.

    https://core.ac.uk/download/pdf/588488097.pdf

62. Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., & van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), 100014.

    https://www.sciencedirect.com/science/article/pii/S2666954421000132

63. Muhammad, A., Siddique, A., Mubasher, M., Aldweesh, A., & Naveed, Q. N. (2023). Prioritizing non-functional requirements in agile process using multi criteria decision making analysis. IEEE Access, 11, 24631-24654.

    https://ieeexplore.ieee.org/abstract/document/10061380

64. Dataset Link: https://www.kaggle.com/datasets/sumanth3112/hello-world