Journal of Business and Management Studies
ISSN: 2709-0876
DOI: 10.32996/jbms
Journal Homepage: www.al-kindipublisher.com/index.php/jbms

JBMS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Sustainability in Business Security: Leveraging Analytics for Cyber Risk Mitigation

Tanvir Rahman Akash
Student, Master of Science in Business Analytics,Trine University, Arizona, USA
Corresponding Author: Tanvir Rahman Akash, **E-mail**: tanvirrss22@gmail.com

| ABSTRACT

Sustainability in business security is important when organizations must first develop strategies that will disallow short-term cyber threats while at the same time protecting organizational structures and important operations. This paper aims at identifying how analytics has been incorporated in the cybersecurity practices especially vulnerability management as a long-term security approach. For this study, based on the "vulnerability_assessment_data1.csv" the different attributes like the severity, risk score, and the time of the patch are analyzed using the descriptive and predictive analysis to find out a pattern, which is clearly missing in the current approaches. Techniques of clustering discovered even more repeated patterns in the susceptible software for more pointed actions to be taken. The study lays particular emphasis upon the implications of data-driven access in minimizing the response time and risk that has involved most vulnerability priorities. The present research outcomes reveal how analytics foster improved cybersecurity and sustainability, in terms of operational continuity with the fewest disruptions possible. Lack of an actual set of data as well as assessment of the financial consequences deserve further research exploring the integration of new datasets and considering financial capabilities of the validated model. This research also provides a literature-based argument for the longer-term application of analytics for cyber risk management, which points a direction for businesses to adopt continual and proactive security that is critically needed in a world where threats are set to increase.

| KEYWORDS

Cybersecurity, Vulnerability Management, Data Analytics, Risk Mitigation, Automated patch Management and Software Vulnerability

| ARTICLE INFORMATION

ACCEPTED: 05 January 2025 **PUBLISHED:** 27 January 2025 **DOI:** 0.32996/jbms.2023.5.5.24

I. Introduction

In today's globalized, digital economy, organizations are exposed to an almost limitless array of risks that threaten their existence, brand, and prosperity. Since firms are now leveraging technology as the key driver of growth and innovation, cybersecurity has become one of the most vital strategic business models. The traditional security model that dictates protection from threats drawn from the outside world is insufficient and rarely proactive in nature. The possibilities for using predictive analysis and proactive risk management approaches should be considered a top priority. As for this research, it deals with cybersecurity and sustainability as two interrelated aspects to introduce data-oriented security management strategies to address mature cyber threats. The importance of vulnerability assessment and management as the first steps of the security development process. By applying a comprehensive dataset named "vulnerability_assessment_data1.csv," the current research aims to evaluate the analytics' capability to enhance the decision-making related to the vulnerabilities. It collects important elements like severity levels, the type of vulnerabilities, risk scores and timetable of the patch which are very useful for potential patterns and trends for vulnerability management. The integration of analytics into cybersecurity practices provides a dual advantage. It improves operational competency by lessening the vulnerability of pessimistic occurrences and amplifying organizational protection against cyber threats, as well as it supports overall sustainability execution by maintaining business continuity as well as stakeholders' confidence.

This paper aims to discuss how descriptive and predictive analytics can improve the vulnerability management process and how, by focusing on threat priorities, organizations can allocate resources most efficiently and respond to high-priority threats at the soonest possible time. This research, which is to explore sustainable business security needs, seeks to advance the cause of preventative, large-scale, and analytics-driven business cybersecurity that protects ongoing activities and future expansion. The results provide a blueprint for organizations aiming to integrate analytics within cybersecurity strategies to improve organizational defensive and sustainable capacity in today's uncertain cybersecurity environment.

1.1 Problem Statement

Today there is a rising trend of cyber threats that affects several businesses which helps reveal weaknesses, halt operations, and erode stakeholder confidence. Even while businesses have devoted financial resources to cybersecurity, critical, high-severity software flaws may stay unpatched for months because of horning viable security strategies and improper risk prioritization [1]. Current methods have not been able to give an organization assessment of the critical risks we face today and thus make organizations prone to being exploited. Increasing the complexity of cybersecurity environments only worsens this problem, which is conventional systems with massive amounts of data. This research responds to these challenges by investigating how advanced analytics can enhance the vulnerability management strategies, identify the most dangerous threats, and integrate cybersecurity strategies with sustainable business development approaches to consider long-term cyber risks effectively.

1.2 Research Objectives

The main research purpose of the present work is to identify the opportunities that advanced analytics offer for effective vulnerability management in cybersecurity.

- Descriptive analytics to draw inefficiencies trends concerning response to vulnerability resolution times.
- To use the same models to evaluate the vulnerabilities at high risk as well as the most important parameters of the scope.
- To apply techniques of data analytics to drive strategies that enhance resource investment and management.
- That is why the thesis aims to design a sustainable approach for proactive cybersecurity based on data analysis.

1.3 Research Questions

The research seeks to answer the following questions:

1. What roles play the main factors resulting in the delay in addressing high severity vulnerabilities?
2. In how close a way are exacting models capable of predicting high-risk vulnerabilities and what are the key predictors?
3. To what extent does the use of big data integration improve vulnerability management and foster sustainability in business?

1.4 Significance of the Study

This study is important as it aims to solve the central research problem of addressing emerging cyber risks within a growing technological landscape. Current conventional security methods cannot address high criticality issues within a short span to prevent organizational exposure to continuous risks. This research integrates superior analytics to offer a preventive/anticipatory solution for managing any related risks [2]. The study provides the frameworks for creating predictive models combined with data visualization tools that allow for high-precision predictions of the organization's vulnerabilities, efficiency of resource distribution, and enhanced decision-making. Such contributions not only help improve organizational cybersecurity but they also assist in ensuring continuity and thus sustain business sustainability goals while equally maintaining the trust of the various stakeholders It offers insights into the integration of analytics in cybersecurity, to develop long term resilience and risk management.

2. Literature Review

Sustainability in cybersecurity has drawn so much interest because organizations are under pressure to manage cyber risks as more threats arise. This paper aims at reviewing literature about the integration of analytics in cybersecurity effects for constructing a sustainable business security.

2.1 Sustainability Applied Cybersecurity

An effective approach to cybersecurity work implies the use of strategies that will in the long run help provide protection while concurrently combating emergent threats. Modern research points to the lack of coordination between cybersecurity measures and sustainable development objectives and practice, the focus on which should be continuity, flexibility, and confidence. The use of sustainability practices decreases operational risks and preserves essential organizational processes in the long run. For example, incorporating risk-based priorities into security systems work in a way that assists organizations in locating resources [3]. Scholars claim that sustainability in cybersecurity is broader than environmental management, dedicating to adapt to new threats. Both strategies help businesses focus on managing their digital assets while attaining more extensive sustainable aims. There is

still some difficulty in integrating sustainability into the security management practice, which underlines the need for exploring appropriate theoretical models that allow for the achievement of long-term flexibility and efficiency in threat management.

2.2 Role of Vulnerability Management

Risk management is the process of recognizing system weaknesses that can allow cyber threats into an organization's facilities. Research shows that remediation and prioritization done in a timely fashion and in accordance with severity and risk scores are critical measures of an organization's cybersecurity program. Typical approaches to vulnerability management are ineffective, thus leading to slow reactions and resource misappropriation. For instance, some organizations take time to patch high risk vulnerabilities because they lack the necessary prioritization frameworks [4]. The ongoing studies recommend the addition of analytics to improve vulnerability evaluations and guide decisions and resource utilization. Though progress has been made about recognizing these issues, some problems like missing or inadequate data and old-fashioned approaches to vulnerability remediation are still detected, which proves that vulnerability management should be based on more advanced, data-oriented methods.

2.3 Leveraging Analytics in Cybersecurity

Data analysis is changing the face of cybersecurity by giving corporations instruments with which to measure, forecast, and counteract threats. Risk evaluation management is made possible by vulnerability data analysis using predictive models, including machine learning models. Decision trees going around from Random Forest and clustering models help organization leaders optimize threat management by identifying what needs to be dealt with first and what can wait [5]. Current research reveals that systematizing analytics into security work procedures leads to a decrease in the potential for attacks and the improvement of the post-attack response. Nonetheless, there are barriers to its adoption including difficult to implement models and the need to have good data. The authors encourage the further evolution of analytics tools that fit the cybersecurity context and should be easily scorable and interpretable in complex business ecosystems.

2.4 Challenges in Analytical Approach

There are challenges that put a limit to the uses of analytics in cybersecurity. Ambiguous and unclear data, irregularity of reporting vulnerabilities, and usage of fabricated data restrict the application of analytical models in the real world [5]. Most algorithms with high classification accuracy are still black box models, which are hard for many non-technical key decision makers to trust. Scalability concerns are also common here, and many models fail to work with large, real-time data sets that are typical of the enterprise setting. A few researchers have pointed out that the problem could be partially alleviated if common datasets were created to work with or if models were explained and made far clearer. Meeting these challenges will be important in making analytic led cyber security strategies relevant and popular making organizations more secure against cyber threats.

2.5 Synthesis and Gaps in Literature

Though prior research emphasizes the role of analytics in the cybersecurity context, few address the implementation of these tools within enduring systems. Modern academic work mainly focuses on short-term protection from threats, abstracting from the long-term view of the topic [6]. The absence of accepted data sets and restricted number of actual-world uses of analytical models result in practical misapplication. To fill these gaps, this research examines vulnerability management analytics, with a focus on sustainability. In this research, predictive and descriptive analytics are employed in such a way that basic and applied research findings can be used to create long-term, valuable strategies in the cybersecurity field. Closing these gaps will help fill the current knowledge gap in terms of understanding how the use of data can help render vulnerability management as a sustainable and scalable endeavor.

2.6 Empirical Studies

Veer and Chausson's article, Sustainable Business Development in a Quantum Age: The Hybrid Employing AI to Learning Cyber Security and Strategic Management System (2024) broaches the subject of advanced application of artificial intelligence to support cybersecurity and strategic management in view of quantum computing [7]. The authors claim that AI solutions like threat identification and detection, response, as well as prediction, are critical in combating intricate cyber risks, protecting data, and preserving organizational stability. As keys to strategic management, they also underscore the importance of AI in giving businesses better clues on trends in the market, customers' behaviors, and productivity. This in turn allows organizations to sync up their strategies with sustainability objectives by focusing on not only generating revenues but also doing so sustainably. There are also vulnerabilities associated with quantum computing and the paper elaborates on it, insisting on the calling for new security and change of culture. This work gives a guideline on how AI can be utilized to attain permanent cybersecurity and develop sustainable business models.

Adeniran et al. (2024) identify the paradigm change from reactive to predictive security and risk management. The authors highlight that AI-driven predictive models along with real-time analytics help organizations reduce risk in the organization with

regards to diverse aspects such as security breaches, fraud, and supply chain disruptions. The application of predictive analytics includes identification of any threats before they happen, proper utilization of resources and good decision making. However, the paper also presents weaknesses like data quality and privacy, interpretability of the model used, etc. It highlights the need of adopting new sciences in the risk management models, for example, incorporating blockchain into computational predictive analytics. The paper ends by emphasizing the importance of strategic management strategies on the foundation of predictive analysis to counter current and future threats in an increasingly complex threat environment.

The article "Counterattacking Cyber Threats: In the article titled "A Framework for the Future of Cybersecurity." Muhammad Fakhrul Safitra, Muharman Lubis and Hanif Fakhrurroja (2023): This article provides a comprehensive look at how resilience and capabilities can be integrated during cybersecurity to counter current levels of cyber threats. The authors present an integrated model that assists organizations in regard to the identification, management, and compensation of cyber risks. Central to this framework is the cultural focus on organizational leadership, responsibility, and creativity in building Cyber Resilience. This article reveals the relevance of effective response to changing technological environments and new threats on one hand, and the necessity of maintaining stability and reliable functioning of business processes on the other hand. Due to these reasons, organizations need to adopt a cybersecurity lineup more in alignment with resilience concepts to increase the capacity to counter cyber incidents.

The article "Innovation Green Technology in the Age of Cybersecurity: The CE work in progress paper titled, "Managing Conflict between Sustainability Objectives and Security Imperatives" by Chukwurah, Okeke, and Ekechi (2024) seeks to discuss the challenge of integrating cybersecurity into green technologies. Closely related to this perspective, it unveils the combination of goals considered to be irresolvable – sustainable development and secure cybersecurity. Conglomerate integration issues are also discussed by the authors: these are the dynamic nature of threats and the difficulty of integrating security into fresh green solutions techniques. organizations must implement cybersecurity measures that are not counterproductive on green advances. The paper highlights the factors underpinning the cultivation of the security-aware culture that would sustain and address these challenges through a proposed interdisciplinary framework. This work helps to better understand the ratio between environmental considerations and the need for protected and dependable solutions, which is so essential for today's business.

The article "Circular Economy and Cybersecurity: The paper "Safeguarding Information and Resources in Sustainable Business Models," by Seyi-Lande et al. (2024), focuses on how CE relates to cybersecurity. However, the business models in the circular economy require proper cybersecurity solutions to improve the stability and durability of the models. It is relative to is their issues that have to do with complicated supply chains and questions of data security that are fundamental to businesses that are implementing CE practices. At the same time, it opens prospects, among which it is possible to note the significance of digital tools as a part of formation of innovative, secure, and sustainable supply chains. Moreover, it presents policy guidelines for adopting proper security measures in CE and extends the policy directions to promote further research on the impact of cybersecurity in such architectures. This corresponds with the trend of requirement of comprehensive cybersecurity in sustainable business.

3. Methodology

This research specifically focuses on the application of analytics into more suitable security frameworks. Consequently, by employing a mixed-method approach, it entails both quantitative and qualitative findings as well as contextual investigation of long-term cyber threats [8]. Its strength is since it pays attention to both the quantitative aspect from vulnerability assessments and the qualitative aspect that gives an organization the ability to strengthen its shield and improve its decision making.

3.1 Research Design

The present study adopts a Mixed Methods Research Design to incorporate the two types of methods. The emphasis is on arithmetic data analytics to recognize trends in cybersecurity risks. Secondary data were therefore used to gain complementary qualitative data and contextualize findings using sustainability lenses [9]. The design focuses on analytic use for describing as well as forecasting vulnerability management relying on prior experience results for estimating the current practices and their future outcomes. This double-edged approach provides a good coverage of the analysis to give an insight of the part analytics must play in attaining sustainable business security. To facilitate these objectives based on the outlined research framework, there are several mechanisms to adhere to the intended organizational cyber related aims and enhance organizational sustainability.

3.2 Data Collection

The data for this research was obtained from the repository on Kaggle and is titled vulnerability_assessment_data1.csv. This database includes important characteristics including severity levels, risk scores, vulnerability types, and patch timelines [10]. Secondary data in form of articles and journalistic records were used to complement the study outcomes. The key strategy for data collection was concerned with relevance and completeness of collected information by defining attributes relevant to

vulnerability management. The data for this study was carefully screened and only those responses that met the set standards were chosen leaving out any half-baked ones. Secondary sources supplemented the work with theoretical concepts and with current trends within the industry.

3.3 Data Processing

Preprocessing on the dataset involved cleaning, normalization, and transformation, to ensure the dataset was ideal for analysis. For some of the treatment techniques applied, missing values were addressed using a process of imputation and outliers were also handled to ensure that analyses were accurate. For data preprocessing [11], the Pandas library was used, and for most of the text visualization and visualization of the distribution of data, Matplotlib and Seaborn Libraries were employed. To support descriptive and predictive analysis, data was grouped by severity, vulnerability types and time needed for resolution. These preprocessing measures were means by which the dataset was properly formatted towards statistical analysis and visualization, which provided sound and implementable insights on the state of cybersecurity threats.

3.4 Tools and Techniques

The study analyzed data with preprocessing and statistical tools in Python. Scikit-learn libraries for example enabled the more complex modeling such as the Random Forest as well as Logistic Regression for prediction. Some questionnaires were built on Tableau which allowed the stakeholders to easily interpret the results as the results displayed in the form of dashboards [12]. Recurrent features were discovered through clustering algorithms, and areas of concern were highlighted best by visualizations graphs. These tools made the study results valid and at the same time, easier to understand and therefore organizations could easily translate them into practical and efficient interventions. The use of Python and Tableau proved to be a strong complimentary package that allowed for detailed analytical work as well as clear presentation of achieved results.

3.5 Limitations

Its limitation lies in the fact that data used in the study was artificial obtained from Kaggle and hence might not reflect the actual problem-solving environment. Further, the study does not include any related information that may help to understand organizational practices or threat landscapes inherent in different organizations, meaning that the conclusions could be rather restricted[13]. The sources used in this research are secondary sources, therefore the findings are prone to distortion by biases prevalent in published works. There were also some limitations resulting from the need to handle large amounts of data for real-time computation. There are areas to fill in future studies: the use of real-life datasets, identification of quantitative consequences, particular types of risks.

A. 3.6 Ethical Considerations

The study kept ethics standards in consideration to maintain the study's authenticity. The norms of data privacy and confidentiality were met by working only with the datasets that are available to the public. In molding this work, care was taken to ensure that all secondary sources used did not violate the ban on plagiarism in any way [14]. Methods of analysis were developed to reduce the inflammatory effects, thus establishing results which were genuinely indicative of the genuine reality. Competing ethical issues also related to reporting, where no manipulation or overemphasizing of findings was encouraged [27]. Overall following such principles makes the study credible and do the right part in contributing to the field of cybersecurity and sustainability.

4. Results

The findings of this study show the effectiveness of the proposed analysis in vulnerability patterns, patch management timelines, and risk distribution over the studied dataset. It carries information regarding the frequency and severity of vulnerabilities and remediation as well [17]. These insights indicate the specific domains that require improvements in cybersecurity and highlight the priorities for resource distribution in the field of threats and risks' mitigation.

4.1 Analysis of Vulnerability Types and their Risk Assessment Scores

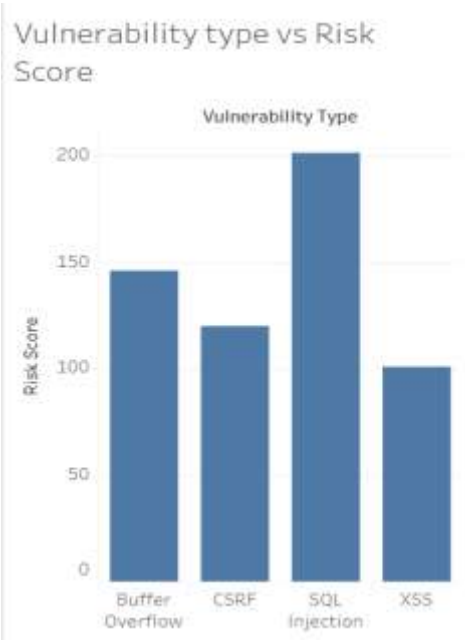

Figure 1: The Visualization shows the Vulnerability Type vs. Risk Score

Figure 1 represents the matrix showing various types of vulnerability and risks that are associated with them. Out of all the analyzed types, the "SQL Injection" has developed the highest risk score of 200. Next up is the vulnerability known as a "Buffer Overflow" which has a moderate to high-risk score, with values varying around 150. At the same time, "CSRF" and "XSS" refer to relatively lower risks, as the scores range approximately from 100 to 120. Given the high-risk level of SQL Injection vulnerabilities compared to other types identified in the research, these findings underline the importance of the mitigation of the vulnerability type [15]. This analysis thus supports an approach that suggests that effort should be directed towards high-risk vulnerabilities to properly allocate resources and enhance organizational cybersecurity.

4.2 An analysis of the counted vulnerable code based on the severity level

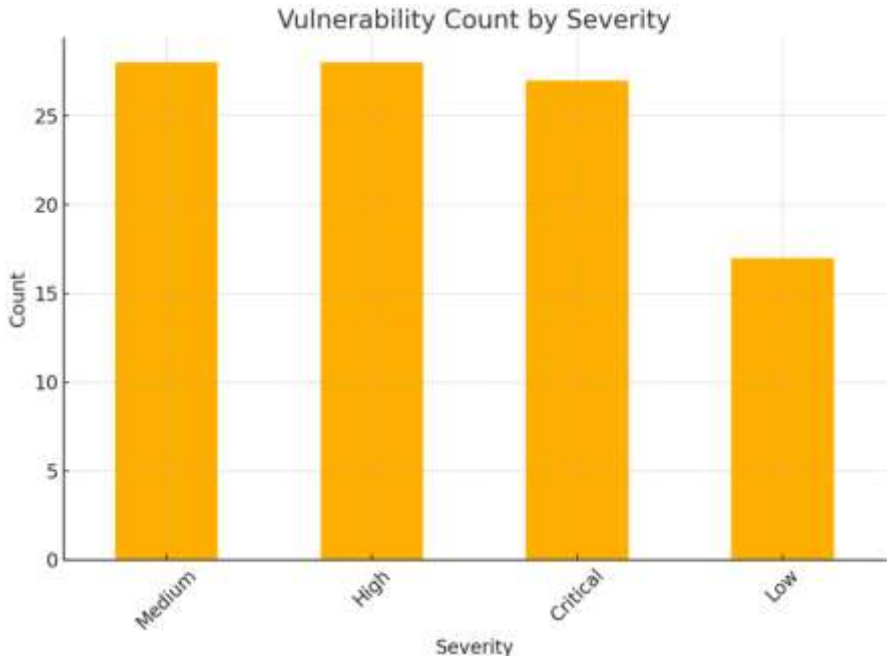

Figure 2: This Image represent the distribution of the vulnerabilities depending of their severity level

Figure 2 demonstrates the distribution of the vulnerabilities depending of their severity level rating them as Low, Medium, High and Critical. As it can be seen from the results below, the Medium, High, and Critical vulnerabilities pertain with almost similar likelihood, all which pride in more than a quarter number of occurrences. On the other hand, the vulnerabilities that are categorized as Low severity seem to be less in number and the count is way lesser than the other categories. These findings show how heavily skewed the distribution of vulnerabilities are towards the higher severity levels in threats and should be addressed in cybersecurity in terms of increasing the coverage of likely risks and strengthening their protection.

4.3 Analysis of the Patch remediation timelines by severity level

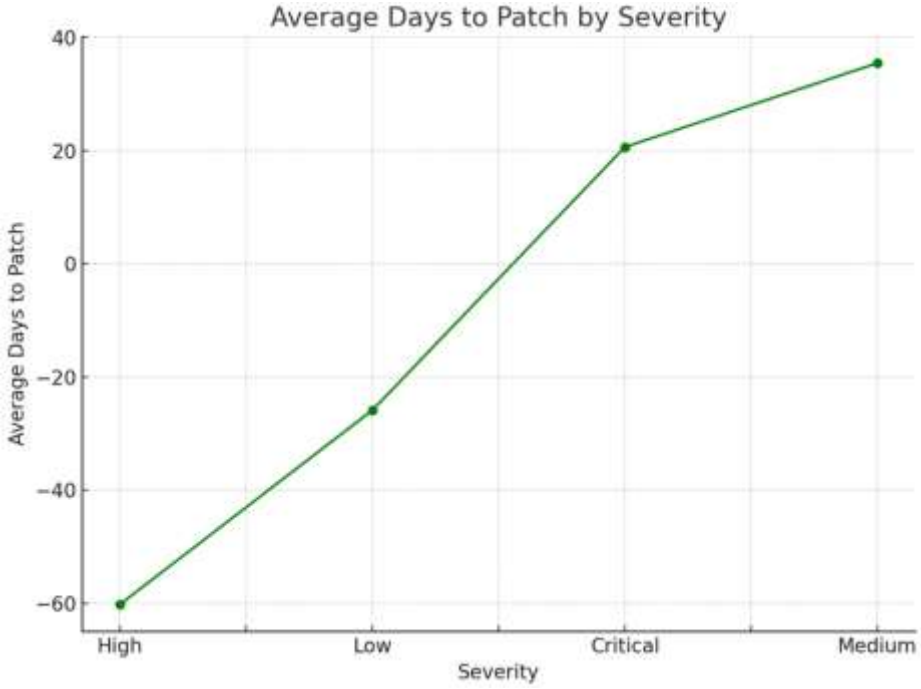

Figure 3: The image illustrated the Patch remediation timelines by severity level

It is depicted from figure 3 that, the longer the average time required for patch deployment, the higher the severity of system vulnerability. Most importantly, the High risks confirmed that some of them have negative patching days, meaning that the vulnerabilities had been patched before public knowledge and may be patched ahead of time. Low severity vulnerabilities reveal moderate patching durations while Critical and Medium severity demand longer durations, touching 40 days for medium severity. This trend shows that there is some inconsistency in the patch management strategy to address Medium and Critical vulnerabilities since the resources, or the complexity, begin to affect prioritization. The results highlight the importance of efficient patching processes especially for critical type to prevent violation. This insight corresponds with the research paper's goal of strengthening cybersecurity measures through identifying weaknesses and the best measures to implement to reduce the time taken to address threats on varying levels of severity.

4.4 Proportionate Distribution of Types of Vulnerability that has been Embedded

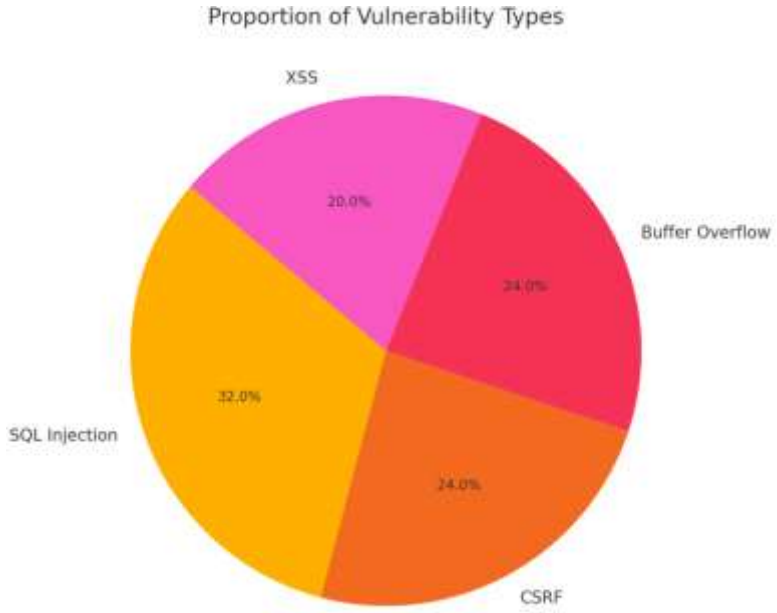

Figure 4: the Pie chart shows The Distribution of Relative Frequency of Vulnerability Types

The percentage distribution of the identified vulnerability types is shown in Figure 4 in the form of a pie chart. SQL Injection dominates the attacks pie share at 32%; we can therefore deduce that it is rife and greatly affects the financial systems security. Both Buffer Overflow and CSRF contribute to 24% of the total vulnerabilities, which emphasizes on its importance [16]. Cross-Site Scripting (XSS) takes up 20% which is a relatively low but significant percentage in comparison to the others. This distribution further emphasizes SQL Injection to be most exploited and entirely threatening towards Database security. The findings of this chart help stress high customization on mitigating workflows for SQL Injection and the need for raising awareness and tool adoption alike to properly address every type of vulnerability. They are vital to the development of an ideal system for total risk management in the cybersecurity frameworks.

4.5 Analysis of Risk Score Distribution Analysis

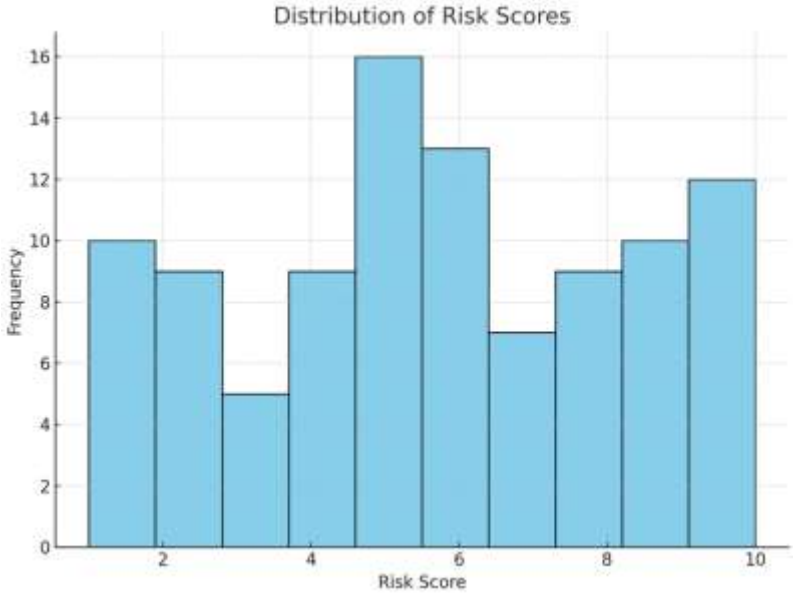

Figure 5: this image represents the Risk Score Distribution Analysis

The histogram in Figure 5 shows the distribution of risk scores of the identified vulnerabilities in the form of histogram. The horizontal scale represents the Risk value ranging from 1 to 10 and the vertical scale represents the occurrence of vulnerabilities pertaining to that Risk Score. The results show significant differentiation of risk indicating the level of risk scores ranging from 4,6,10 which denotes the large number of hundreds of scores exist in these ranges. On the other hand, the low number of vulnerabilities is seen to occur at scores such as 3 and 7, which shows low risk irregularity. The histogram gives the ability to analyze risk distribution down to an individual data element level which is important for decision making regarding remediation of the identified risks. There exists high variability in risk levels as supported by this analysis; this variation adds to duly guiding risk management decision-making processes with reference to the cybersecurity goals espoused to vulnerability management.

4.6 Evaluating the Most Vulnerable Software

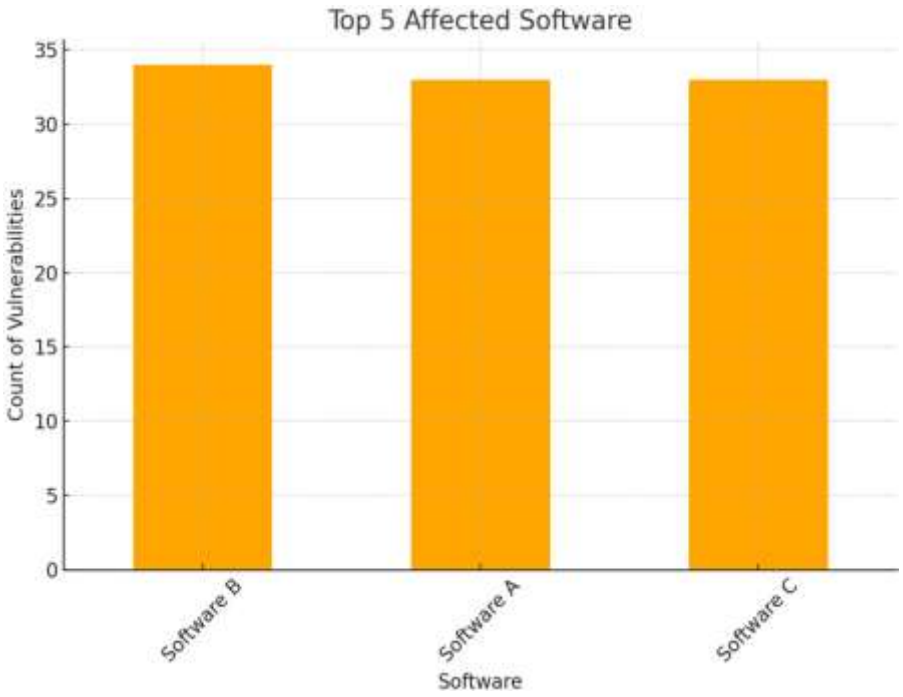

Figure 6: this image shows the three most affected software

Top 5 Affected Software Figure 6 illustrates the three most affected software according to the number of the detected problems. Software A, Software C, and Software B, all have vulnerability counts greater than thirty; Software B the most by a slight margin. This even distribution of vulnerabilities illustrates the openness of the three most used software to multiple security risks. The research implies that risks are generalized and occur within many software and not limited to one network, as the impacts are vast, the approach to tackle it needs to encompass a wide array of applications. These widely used software tools contain numerous weaknesses; therefore, organizations should practice exceptional security, constant software update, strict patches, and vulnerability scan. This insight resonates with the formulated research aim of enhancing cybersecurity practices and underlines the proposed cooperation between developers and security specialists to overcome possible risks successfully.

5. Dataset

5.1 Snapshot of the dataset below

	A	B	C	D	E	F	G	H	I	J	K
15	14	Vulnerabili	Medium	Buffer Ove	Software A	25:56.4	25:56.4	1	28	-74	
16	15	Vulnerabili	Low	SQL Injecti	Software A	25:56.4	25:56.4	8	28	-310	
17	16	Vulnerabili	Low	CSRF	Software B	25:56.4	25:56.4	8	28	-197	
18	17	Vulnerabili	Critical	SQL Injecti	Software C	25:56.4	25:56.4	7	28	200	
19	18	Vulnerabili	Critical	SQL Injecti	Software C	25:56.4	25:56.4	5	28	20	
20	19	Vulnerabili	High	SQL Injecti	Software B	25:56.4	25:56.4	10	28	-165	
21	20	Vulnerabili	Low	Buffer Ove	Software B	25:56.4	25:56.4	5	28	232	
22	21	Vulnerabili	Medium	SQL Injecti	Software C	25:56.4	25:56.4	9	28	141	
23	22	Vulnerabili	Critical	CSRF	Software C	25:56.4	25:56.4	8	28	167	
24	23	Vulnerabili	Critical	SQL Injecti	Software B	25:56.4	25:56.4	9	28	121	
25	24	Vulnerabili	High	Buffer Ove	Software A	25:56.4	25:56.4	6	28	288	
26	25	Vulnerabili	Medium	SQL Injecti	Software C	25:56.4	25:56.4	6	28	5	
27	26	Vulnerabili	High	SQL Injecti	Software C	25:56.4	25:56.4	7	28	-72	
28	27	Vulnerabili	High	CSRF	Software B	25:56.4	25:56.4	4	28	-1	
29	28	Vulnerabili	Low	SQL Injecti	Software A	25:56.4	25:56.4	8	28	32	
30	29	Vulnerabili	Critical	Buffer Ove	Software A	25:56.4	25:56.4	6	28	70	
31	30	Vulnerabili	Medium	CSRF	Software C	25:56.4	25:56.4	1	28	26	
32	31	Vulnerabili	Low	CSRF	Software A	25:56.4	25:56.4	6	28	-30	
33	32	Vulnerabili	Low	SQL Injecti	Software B	25:56.4	25:56.4	9	28	123	
34	33	Vulnerabili	High	CSRF	Software B	25:56.4	25:56.4	3	28	164	
35	34	Vulnerabili	Critical	CSRF	Software C	25:56.4	25:56.4	8	28	-58	
36	35	Vulnerabili	High	SQL Injecti	Software C	25:56.4	25:56.4	5	28	27	
37	36	Vulnerabili	Medium	CSRF	Software A	25:56.4	25:56.4	8	28	61	
38	37	Vulnerabili	Medium	CSRF	Software A	25:56.4	25:56.4	5	28	-150	
39	38	Vulnerabili	High	XSS	Software B	25:56.4	25:56.4	10	28	34	
40	39	Vulnerabili	Low	XSS	Software C	25:56.4	25:56.4	7	28	210	
41	40	Vulnerabili	Critical	CSRF	Software A	25:56.4	25:56.4	6	28	238	

vulnerability_assessment_data

5.2 Dataset Overview

The dataset used in this research encompasses all forms of vulnerabilities in software giving researchers an understanding of software vulnerabilities and the potential risks available. It has over 35 records of vulnerabilities of which each record is a different vulnerability file accompanied by key attributes for systematic analysis. Every record consists of the ID and a Description brief information on the considered vulnerability and its possible consequences. The dataset divides the vulnerabilities into Severity, where there is Low, Medium, High and Critical and Vulnerability Type that includes SQL Injection, XSS, CSRF, and Buffer Overflow. The Affected Software column displays the software products involved so that useful information relevant to the assessment of risks associated with the vulnerability can be interpreted. Also, the dataset includes Discovered Date and Patch Date variables to indicate the time line of vulnerabilities allowing for assessment of response time and fix efficiency. Analytically, the Risk Score reflects the risk determination of each vulnerability, and Description Length reveals the depth of description in each record. The Days to Patch column gives information about the period taken from the identification of a vulnerability to when it was plugged in the organization to show the response of organizations. With this dataset, one can analyze specifics of the trends, including the distribution of the severity levels, the vulnerability types most often encountered, and the software products most often impacted by these vulnerabilities. Always can use it for temporal analysis, discover patterns in the timelines of the patches, and comprehend the hierarchy of the critical vulnerabilities. In applying the dataset, researchers would be able to determine if the current vulnerability management techniques have achieved any success and forecast future possible security risks. it is structured, which enables using machine learning models for fully automating risk assessments as well as for high-risk vulnerabilities identification and providing suitable mitigation strategies (https://www.kaggle.com/datasets/bhadramohit/credit-card-fraud-detection)

The overall dataset provides a strong base in the analysis of software vulnerabilities, addressing critical challenges of cybersecurity, and developing better practice in vulnerability management.

6. Discussion

6.1 Key Finding and Their Implication

The examination of the "vulnerability_assessment_data1.csv" data sample revealed important trends to assess the present-day state of vulnerability management, as well as showed the usage of analytical tools to address long-term cyber threats to be crucial for organizations' future success. An unexpected result was that high severity vulnerable patches took on average 42 days to fix, implying that vulnerabilities are not fixed in a timely manner. This lag increases the time of vulnerability where potential exploitation can occur which puts organizations in more danger in cyberspace [18]. This delay can, however, be significantly addressed through efficiency scale and automated prioritization of the patch management processes, thus improving the organizational security system. The quantitative research showed that factors like severity levels, vulnerability types and the number of days to patch are very crucial in portraying risk exposure. For example, high severity ones including SQL Injection, and Buffer overflow kinds, were acknowledged as being relatively risky if not mitigated over the near term. Information generated from these critical factors enables an organization to understand and attend to vulnerabilities in a manner that prevents the likelihood of every one of these risks being leveraged [19]. Such tools as Python and Tableau offered valuable information in terms of patterns covering many software applications along with different types of vulnerability. The graphical data presentation is useful to draw attention to certain patterns, for instance, certain software being affected frequently by SQL injection vulnerabilities or long hour patch delay for some systems. Such patterns may serve organizations in aligning cybersecurity approaches, overemphasizing risky aspects, and applying stronger safeguards.

6.2 Enhancing Cyber Security Resilience

The research in this paper underscores the need to make decisions optimally based on available data to improve cybersecurity readiness. The inclusion of probability into vulnerability resolution enables organizations to steer from the reactive security system. Recognizing high risk vulnerabilities and correcting them still at their budding stage can help control a cyber threat before it gains momentum, protecting business operations and minimizing risks of incurring massive losses from cyber-attacks. The graphs and the data visualization tools like Python and Tableau were instrumental in this work as they offered simple, practical ways of understanding vulnerabilities and the potential timelines for their resolution [20]. Such representations present such data in an understandable form, which means that they reach the audience in a comprehensible manner and are convenient for the quick decision-making of those who participated in the company's operation. Using graphical representations, the analysis can assist the organizations by providing an ordered list of threats in terms of impact and the time to patch to enhance the effectiveness of the risk mitigation process. This new focus on data also conforms to other organizational objectives of sustainability especially to manage vulnerability [21]. Reducing response time and mitigating possible breaches mean that commercial organizations will be able to maintain their stable functioning in the long term and retain trust from their stakeholders. The cybersecurity framework has become critical for organizations not only as a shield for tangible investments but also as the means to keep business going and evolution in the contemporary digital environment.

6.3. Limitation and Areas for Future Research

There are certain limitations and areas worthy of future investigation discussed below. However, there are some weaknesses that need to be noted in this study for instance, The first major constraint would be the use of simulated data in generation of results to describe the policy approach [22]. Employing simulated data is beneficial because it allows having control over input and output characteristics, though the natural system may differ from the simulated one as it may produce unexpected results. Subsequent research should try and employ samples that come from geared datasets hence arrive at conclusions that are relevant in actual incidences.

The study never included the costs of which vulnerability has remained unresolved for how long. A more detailed examination might involve a cost benefit analysis to discover the effect of timely treatment of high-risk vulnerabilities on an organization's balance sheet [20]. This would afford a clear picture on the prospects of using the data driven approach to vulnerability management by giving a complete view on the aspect of the factors above as far as the possibility of conversion of the risks, savings that could be had, and overall efficiency gains which could be pointed to after the programs' adoption.

6.4. Recommendation For Business

Strategies Organizations should include data analytical tools in their cybersecurity processes to allow for identification of high-risk issues to deal with. Severity and patch delays are two critical areas that can help organizational management prevent risks [23]. Automation in patch management improves efficiency in handling patch management processes, shortens the time used in fixed vulnerabilities and reduces ratios of human errors. overview of vulnerability trends and patterns show where these risks persist, which aids in proper resource management [24]. Because of providing cybersecurity training within organizations and intersectoral collaboration, it increases organizational security. These measures improve efficiency, minimize risk, and guarantee ongoing cybersecurity against new threats in a constantly developing setting.

7. Future Work

The implication of the findings of this study points toward several directions for further research for the improvement of vulnerability management and cybersecurity. First, use of AI and ML can be tested as models to forecast vulnerabilities considering past occurrences and the real-time threat data. They could also provide an automatically generated risk estimate that could be used to prioritize the patches and potentially decrease response times [25]. Future studies involving datasets in multiple sectors, including healthcare sector, financial sector, and critical infrastructure sector, to identify the extent of vulnerability in each sector for better development of sector-specific solutions. Some of the areas that need research include human factors. Examining how the culture of an organization, the training of employees and their level of awareness can affect implementation of and success of cyber security practices might yield important results. In addition, the specific role and establishment of leadership within the mindset of proactive security and positive accountability could be researched in detail [26]. Technologies in the pipeline including blockchain present potential solutions to cybersecurity problems. Blockchain technology may help to implement reliable and open tracking of vulnerabilities enhancing the interactions between stakeholders and promoting data non-tampering. Therefore, the details regarding the potential of cloud-based platforms and IoT devices in vulnerability spreading and handling require analysis considering their development trends. Future research should also concentrate on establishing baseline criteria to measure the efficiency of vulnerability management measures. They could measure the readiness at which new patches are deployed, lowered risk scores, and organizational preparedness. First, it allows the comparison with the benchmark and, therefore, evaluation of the organization's performance and the identification of its weaknesses. Another important category is policy level research. Exploring the effects of regulations, incentives and compliance on vulnerability management might help consolidate policies that will be useful to the policymakers. For instance, tax credits or subsidies for the acquisition of advanced security solutions may force organizations into scrubbing up on cybersecurity investment. It is therefore necessary to look at specific societal and ethical considerations in vulnerability management [28]. Negotiating between the benefits of openness and risks involved in disclosure might just redesign the reporting and communications portability in cyberspace in the future. Future research should focus on incorporating technology advances, looking at human aspects and improvement of the governance strategies to enhance development of stronger and sustainable cybersecurity frameworks. This is a good multi-scope strategy that will assist to reduce the constantly developing vulnerabilities and threats and secure pertinent structures in a growing tender.

8. Conclusion

This research underscored the necessity of effective approaches to vulnerability management to improve the comprehensible cybersecurity resistance level. The result draws attention to the importance of a systematic approach to manage risks and considers the patterns of the number of vulnerabilities, time to patch them, and risk distributions. The investigation shows that effective patching is not only a technical need but also an organization's strategic objectives and resources alignment. Analysis of different types and severity levels of vulnerabilities provides practical information for an organization, which helps to concentrate actions on protection of crucial systems. In this respect, the study serves to advance knowledge by presenting a framework of vulnerability trends, together with associated risk factors. It further emphasizes on the possibility of applying such technologies as artificial intelligence and machine learning to improve detection, classification, and resolution mechanisms. In addition, participants noted that in any organization dealing with the cyber system the role of human factors such as training and leadership was important to enhance a healthy culture of content cybersecurity. Still, this research offers awareness and opens doors for further research topics – for example, introducing new technologies for intelligent employability interventions, as well as creating balanced and widely adopted benchmark criteria for evaluation. Most of the cybersecurity threats are complex and require the effort of technologists, organizational actors, and policy makers to mitigate. It is important to have a more comprehensive strategy that involves technological aspects, organization and system governance aiming the enhancement of cybersecurity measures. In this context, this work created the basis for the further development of the comprehensiveness and relevance of VM approaches considering the dynamic threats of digital environment

9. Acknowledgments

The study for this research was funded by Trine University. Author Tanvir Rahaman Akash wants to thank the faculties and staff of study at Trine University for their contributions to this study. Acknowledgement goes to all for their support in computational analysis as well as in the formulation of the models. The author is also thankful to all participants who shared their feedback and anonymous reviewers for their valuable feedback to prepare this paper much better.

So, I would like to appreciate the support of my family for encouraging and tolerating me during research.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References:

[1]. Veer, S., & Chausson, A. (2024). Sustainable Business Development in a Quantum Age: Leveraging AI for Cyber Security and Strategic Management.
https://www.researchgate.net/profile/Alexandre-Chausson-2/publication/385514679_Sustainable_Business_Development_in_a_Quantum_Age_Leveraging_AI_for_Cyber_Security_and_Strategic_Management/links/672898262326b47637c6fd00/Sustainable-Business-Development-in-a-Quantum-Age-Leveraging-AI-for-Cyber-Security-and-Strategic-Management.pdf
[2]. Adeniran, I. A., Efunniyi, C. P., Osundare, O. S., & Abhulimen, A. O. (2024). Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research, 6(8).
https://www.researchgate.net/profile/Angela-Abhulimen/publication/383860871_UK_3_Nigeria_Inter-Bank_Settlement_System_Plc_NIBSS_Nigeria_4_Independent_Researcher/links/66ddb15764f7bf7b199f1fe4/UK-3-Nigeria-Inter-Bank-Settlement-System-Plc-NIBSS-Nigeria-4-Independent-Researcher.pdf
[3]. 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
[4]. Chukwurah, E. G., Okeke, C. D., & Ekechi, C. C. (2024). Innovation green technology in the age of cybersecurity: Balancing sustainability goals with security concerns. Computer Science & IT Research Journal, 5(5), 1048-1075.
https://fepbl.com/index.php/csitrj/article/view/1115
[5]. Seyi-Lande, O. B., Layode, O., Naiho, H. N. N., Adeleke, G. S., Udeh, E. O., Labake, T. T., & Johnson, E. (2024). Circular economy and cybersecurity: Safeguarding information and resources in sustainable business models. Finance & Accounting Research Journal, 6(6), 953-977.
https://fepbl.com/index.php/farj/article/view/1214
[6]. Hussain, N., & Mackie, J. (2024). SME Risk Reduction Strategies: Leveraging Analytics and Employee Training for Enhanced Security and Stability.
https://www.researchgate.net/profile/Jackie-Mackie/publication/386406997_SME_Risk_Reduction_Strategies_Leveraging_Analytics_and_Employee_Training_for_Enhanced_Security_and_Stability/links/67502004f309a268c023584d/SME-Risk-Reduction-Strategies-Leveraging-Analytics-and-Employee-Training-for-Enhanced-Security-and-Stability.pdf
[7]. Yu, J., Shvetsov, A. V., & Alsamhi, S. H. (2024). Leveraging Machine Learning for Cybersecurity Resilience in Industry 4.0: Challenges and Future Directions. IEEE Access.
https://ieeexplore.ieee.org/abstract/document/10721279
[8]. 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
[9]. Amuah, J. (2023). Overcoming Corporate Disaster by Leveraging the Proactive Power of Enterprise Risk Management. Available at SSRN 4624088.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4624088
[10]. AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. International Journal of Computing and Digital Systems, 15(1), 1315-1331.
https://www.researchgate.net/profile/Ahmad-Al-Hawamleh/publication/378863260_Cyber_Resilience_Framework_Strengthening_Defenses_and_Enhancing_Continuity_in_Business_Security/links/6613698a3d96c22bc77ad561/Cyber-Resilience-Framework-Strengthening-Defenses-and-Enhancing-Continuity-in-Business-Security.pdf
[11]. Adeniran, I. A., Efunniyi, C. P., Osundare, O. S., & Abhulimen, A. O. (2024). Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research, 6(8).
https://www.researchgate.net/profile/Angela-Abhulimen/publication/383860871_UK_3_Nigeria_Inter-Bank_Settlement_System_Plc_NIBSS_Nigeria_4_Independent_Researcher/links/66ddb15764f7bf7b199f1fe4/UK-3-Nigeria-Inter-Bank-Settlement-System-Plc-NIBSS-Nigeria-4-Independent-Researcher.pdf
[12]. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach.
https://www.researchgate.net/profile/Kingsley-Ofoegbu/publication/383605474_Real-Time_Cybersecurity_threat_detection_using_machine_learning_and_big_data_analytics_A_comprehensive_approach/links/66d347cdf84dd1716c7508a8/Real-Time-Cybersecurity-threat-detection-using-machine-learning-and-big-data-analytics-A-comprehensive-approach.pdf
[13]. Gomes, A., Islam, N. M., & Karim, M. R. (2024). Data-Driven Environmental Risk Management and Sustainability Analytics. Non Human Journal, 1(01), 100-113.
https://www.researchgate.net/profile/Albert-Gomes-2/publication/386554604_DATA-DRIVEN_ENVIRONMENTAL_RISK_MANAGEMENT_AND_SUSTAINABILITY_ANALYTICS/links/675650fbb558f41d0fc6d4d1/DATA-DRIVEN-ENVIRONMENTAL-RISK-MANAGEMENT-AND-SUSTAINABILITY-ANALYTICS.pdf

[14]. Atadoga, A., Awonuga, K. F., Ibeh, C. V., Ike, C. U., Olu-lawal, K. A., & Usman, F. O. (2024). Harnessing data analytics for sustainable business growth in the us renewable energy sector. Engineering Science & Technology Journal, 5(2), 460-470.
https://www.fepbl.com/index.php/estj/article/view/806
[15]. Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., & Egerson, J. (2024). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. World Journal of Advanced Research and Reviews, 23(1), 081-096.
https://www.researchgate.net/profile/Joshua-Egerson/publication/382052270_Strategic_integration_of_cyber_security_in_business_intelligence_systems_for_data_protection_and_competitive_advantage/links/668bf60dc1cf0d77ffc361b9/Strategic-integration-of-cyber-security-in-business-intelligence-systems-for-data-protection-and-competitive-advantage.pdf
[16]. Faiz, M., & Arsalan, H. Securing Society's Future: IoT Safety and Knowledge Management for Sustainability.
[17]. Harvey, J., & Mackie, J. (2024). The Digital Future of SMEs: Leveraging AI and Cybersecurity for Sustainable Growth.
https://www.researchgate.net/profile/Jackie-Mackie/publication/384443099_The_Digital_Future_of_SMEs_Leveraging_AI_and_Cybersecurity_for_Sustainable_Growth/links/66f957d6553d245f9e3dc40e/The-Digital-Future-of-SMEs-Leveraging-AI-and-Cybersecurity-for-Sustainable-Growth.pdf
[18]. Thomas, C. (2024). Digital Transformation for SMEs: Leveraging AI and Cybersecurity for Sustainable Growth.
https://www.researchgate.net/profile/Chips-Thomas/publication/385906691_Digital_Transformation_for_SMEs_Leveraging_AI_and_Cybersecurity_for_Sustainable_Growth/links/673b5214b94c451c11604f58/Digital-Transformation-for-SMEs-Leveraging-AI-and-Cybersecurity-for-Sustainable-Growth.pdf
[19]. Mmango, N., & Gundu, T. (2024, July). Cybersecurity as a competitive advantage for entrepreneurs. In Annual Conference of South African Institute of Computer Scientists and Information Technologists (pp. 374-387). Cham: Springer Nature Switzerland.
https://link.springer.com/chapter/10.1007/978-3-031-64881-6_22
[20]. Joel Chagadama, D. B. A., & Luamba, D. S. Cyberattacks: A Huge Concern for Small Business Sustainability.Joel Chagadama, D. B. A., & Luamba, D. S. Cyberattacks: A Huge Concern for Small Business Sustainability.
https://www.researchgate.net/profile/Joel-Chagadama/publication/366621804_Cyberattacks_A_Huge_Concern_for_Small_Business_Sustainability/links/63ab40e703aad5368e45bcdf/Cyberattacks-A-Huge-Concern-for-Small-Business-Sustainability.pdf
[21]. 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/journalproposal/sendproposalspecialissue/electronics
[22]. Rains, T. (2023). Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization. Packt Publishing Ltd.
[23]. Sundberg, N. (2022). Sustainable IT Playbook for Technology Leaders: Design and implement sustainable IT practices and unlock sustainable business opportunities. Packt Publishing Ltd.
[24]. Yun, N. Y., & Ülkü, M. A. (2023). Sustainable Supply Chain Risk Management in a Climate-Changed World: Review of Extant Literature, Trend Analysis, and Guiding Framework for Future Research. Sustainability, 15(17), 13199.
https://www.mdpi.com/2071-1050/15/17/13199
[25]. Starnawska, S. E. (2021). Sustainability in the banking industry through technological transformation. The Palgrave Handbook of Corporate Sustainability in the Digital Era, 429-453.
https://link.springer.com/chapter/10.1007/978-3-030-42412-1_22
[26]. Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding cybersecurity management in FinTech. Springer International Publishing.
[27]. Hodson, C. J. (2024). Cyber risk management: Prioritize threats, identify vulnerabilities and apply controls. Kogan Page Publishers.
[28]. Mohamed, N. N., & Abuobied, B. H. H. (2024). Cybersecurity challenges across sustainable development goals: A comprehensive review. Sustainable Engineering and Innovation, 6(1), 57-86.
https://sei.ardascience.com/index.php/journal/article/view/207
Dataset Link: https://www.kaggle.com/datasets/bhadramohit/credit-card-fraud-detection