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

Risk Analysis-based Decision Support System for Designing Cybersecurity of Information Technology

Barna Biswas[1] ✉ Sadia Sharmin[2], Md Azhad Hossain[3], Mohammad Zahidul Alam[4] and Md Imran Sarkar[5]
[145]Department of Information Technology, Westcliff University, 17877 Von Karman Ave 4th Floor, Irvine, CA 92614, United States
[23]Department of Business Administration, International American University, 3440 Wilshire Blvd STE 1000, Los Angeles, CA 90010, United States
Corresponding Author: Barna Biswas, **E-mail**: B.Biswas.133@westcliff.edu

| ABSTRACT
Evaluating risks is essential for ensuring security preparedness from the perspective of technology and information security management. The proposed project aims to develop an IT security system grounded in risk analysis to create a cybersecurity decision support model. In this study, a public retail corporation with over 60 subsidiaries and an on-premises and cloud-based information technology ecosystem was examined. The proposed model focuses on reducing the security threats to the retail industry by acquiring the optimal security system. In this model, the risk was analyzed using the eight steps of the OCTAVE Allegro method. Based on the OCTAVE Allegro method, the proposed model yielded effective results in reducing security threats and demonstrated a correlation between risk and the importance of cybersecurity compliance evaluations in addressing these threats. Furthermore, this study contributed to strategic policymakers by providing recommendations for decision support in cyber security. The recommendations were designed to determine the most effective steps in the process of developing the security system of information technology. In addition, the risk analysis and evaluation of cybersecurity compliance in this research can assist businesses in formulating policies that will develop capable and efficient information technology security systems.

| KEYWORDS
Decision support system, Information technology, Cybersecurity, OCTAVE Allegro

| ARTICLE INFORMATION
ACCEPTED: 07 August 2024 **PUBLISHED:** 29 August 2024 **DOI:** 10.32996/jbms.2024.5.6.3

1. Introduction

Information technology plays a critical role in all the fields in the modern world, such as education, security, transportation, and businesses (Jabin et al., 2024; Kabbo et al.; Sobuz, Joy et al., 2024). Currently, companies need to be on the lookout for security breaches because there has been a considerable increase in the number of security breaches (Xu et al., 2008). In 2020, the number of cybersecurity breaches increased by an incredible 36 billion. This was the worst year ever when it came to the safety of sensitive data stored online (Walsh, 2023). To mitigate security threats and attacks, cybersecurity policymaking needs to be done properly (Engemann & Henderson, 2014). Risk assessment and measurement of security readiness were crucial from the viewpoint of technology and information security management (Hasan et al., 2021). To ensure continuity of business and reduce security risks, companies need risk management strategies for information security (Hasan, Al Mahmud et al., 2024; Hasan, Chy, et al., 2024; Hasan, Farabi, et al., 2024; Mızrak, 2023). To safeguard stakeholders from financial, organizational, and reputational losses, every critical infrastructure must implement an effective risk management process(Hubbard, 2020).

This study examined a public retail corporation with over 60 subsidiaries and an on-premises and cloud-based information technology ecosystem. Company security included a firewall and antivirus. The security system was not the greatest at detecting

and stopping cyberattacks. According to November 2020 statistics, one of the company's domains had an email security attack with 47,460 spam/phishing and 68 viruses/malware incoming traffic. Outbound traffic has 14,493 spams. A brute force attack targeted 147,375 on a corporate server. Of course, attackers can utilize system/application security vulnerabilities to launch cyberattacks. Low cybersecurity standard compliance in system/application configurations that relate to the CIS benchmark (48%) could lead to security risks. Several cybersecurity assaults disrupted the business communication system (email), stopped transaction processing owing to performance degradation, and leaked information. However, the regulator required the corporation to guarantee consumer service platform security in one of its operations. So, risk analysis is crucial to getting the correct security system to mitigate cybersecurity threats and attacks. This study presented a decision support model to analyze the risk to design effective cybersecurity strategies.

2. Literature Review

The process of risk analysis is putting threats in order of how dangerous they are and deciding if the amount of risk for each threat is acceptable or if steps need to be taken to reduce it (Broder & Tucker, 2011). SAE J3061 (Schmittner et al., 2016) provides an example of the risk analysis process used in the EVITA (Meindl et al., 2020) method. The EVITA risk analysis is influenced by ISO standard 26262 (Salihović et al., 2015). In EVITA, attacks are assessed based on factors such as elapsed time, expertise, knowledge, opportunity, and equipment. The severity vector considers the level of safety, privacy, financial, and operational impacts. Additionally, the controllability of the attack is considered, whether it can be easily controlled, difficult to control, or uncontrollable. Henniger et al. determined the risk level by analyzing the factors mentioned earlier and assessing it based on the risk table established (Sjoberg et al., 2017). EVITA has been improved with the introduction of RACE (Risk Analysis for Cooperative Engines), which stands for Risk Analysis for Cooperative Engines (Boudguiga et al., 2015). RACE is a risk analysis approach for linked automobiles. Instead of using the four values used by EVITA, RACE uses the maximum value of the severity vector to define the severity level. It takes a lot of effort to evaluate and calculate the possible degrees of an individual attack using RACE, which is an extension of EVITA. US^2 presents a comprehensive safety and security analysis method for autonomous vehicles, offering a risk analysis approach (Kavallieratos et al., 2020). It evaluates the risks of attacks by considering factors such as attack probability, severity, and the vehicle's automation level. CSRL (Cyber Security Risk Level) is an extension of US^2, which is applicable to connected vehicles. However, CSRL adopts a table look-up method to determine the risk level, which can be quite time-consuming. CSRL fails to consider human controllability, which is crucial for accurately assessing security risks (Johora et al., 2024; Md Abdullah Al Mahmud et al., 2024; Nur et al., 2024; Rakibul Hasan et al., 2024; Sabaliauskaite et al., 2018; Shahana et al., 2024).

A cybersecurity attack involves cybercriminals executing malicious activities aimed at computers or networks. These attacks, such as those carried out by Maya Attacks, are often driven by harmful intentions, including disabling systems, stealing information, or using compromised devices to initiate further assaults. In virtual environments, attackers employ various strategies to execute their plans. These tactics include brute force attacks, port scanning, malware deployment, phishing, spam, ransomware, denial of service (DoS) attacks, and other malicious methods (Iakovakis et al., 2021). To overcome the cyber security breaches, risk analysis is crucial for the companies.

3. Research Methodology

In this study, we utilized the PDCA (Plan-Do-Check-Act) cycle to guide the problem-solving process, ensuring that all activities were encompassed within each stage. Our proposed model incorporates risk analysis through the OCTAVE Allegro method to evaluate cybersecurity. This analytical method generates priority values for the mitigation of each identified security threat. There are 8 steps in the OCTAVE Allegro method for risk analysis. Fig.1 shows the eight steps risk analysis method.

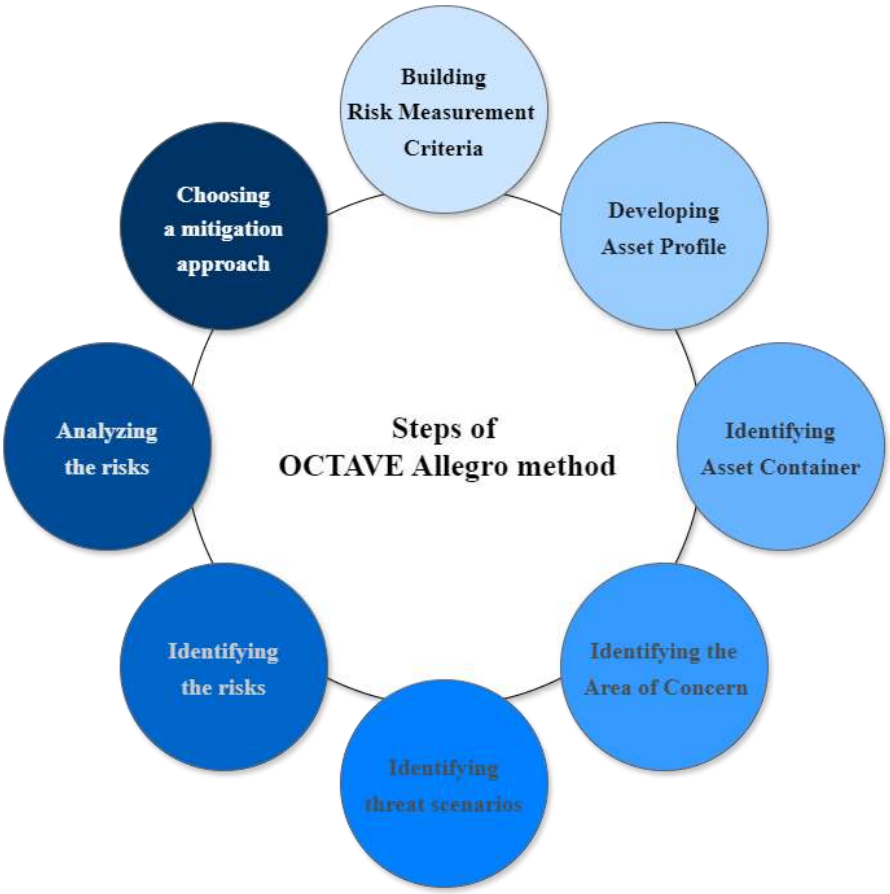

Fig. 1. Eight steps of the OCTAVE Allegro method.

Building risk measurement criteria had three key parameters, including (a) Impact Area, (b) Impact Value, and (c) Risk Measurement Criteria. In developing an asset profile, an interview was conducted with those responsible for using and managing IT assets to assess their criticality to business operations and identify relevant factors. Information was gathered in identifying asset container steps on how assets are stored, managed, and transmitted, considering technical, physical, and human factors. In identifying the area of concern step, a risk profile was developed for IT assets by identifying potential threats from situations or conditions that could jeopardize these assets. A threat scenario was formulated in identifying threat scenarios step to analyze risks to IT assets, concentrating on possible perpetrators, their objectives, methods, and likely outcomes. In analyzing the risks step, risk impacts were evaluated according to the criteria defined in step 1. Evaluate each Area of Concern, identifying and measuring the consequences based on their impact. The risk value was calculated in analyzing the risk step for each information asset to identify and prioritize urgent mitigation efforts based on potential organizational impact. In choosing a mitigation approach step, the risk was prioritized and decided on risk mitigation strategies based on the company's factors and the assigned priority value. The risk mitigation approach is divided into 3 choices (Aditto et al., 2023; Razikin & Soewito, 2022; Sobuz et al., 2023), namely: Accept, Mitigate, Defer.

4. Results and Discussion

In the Planning stage, it was found of rising global security issues by noting similar threats in experimental companies. We began mapping the problem and formulating a strategy. This stage included a literature review of previous solutions and an organizational mapping to identify appropriate resources for implementing the proposed solution. Fig. 2 shows the research stages:

Fig. 2. Research Stage.

4.1. Cybersecurity decision support model

The proposed model involves three layers of processes, but first, it requires identifying all company assets. Management support is crucial for research success. We identified assets through interviews with responsible parties. The IT Infrastructure department manages 11 hardware assets, 6 software assets, 4 system assets, and 5 information assets in the on-premises data center. Fig.3 shows the Cyber security recommendation model.

4.2. Risk analysis

The security threat risk assessment was conducted through direct meetings with several asset BPOs in the IT Infrastructure department and other relevant company departments. Detailed interviews were held to gather information on critical operational assets. Once preparations were complete and the necessary data collected, the risk assessment was performed using the OCTAVE Allegro method, which comprises eight steps.

Step 1: Building risk assessment criteria

Risk assessment criteria determine how much impact there is in the different threat areas. For our study, however, we used those under the Department of Internal Audit, plus the other impact area, which is Well-being and security. The risk assessment criteria are shown in Table 1.

Table 1. Impact of risk assessment criteria.

Priority	Impact Area
5	Reputation and User Trust
4	Financial
3	Fines and legal sanctions
2	Productivity
1	Health and Security

There are five key areas that impact risk assessment: reputation and user trust, financial and legal sanctions and fines, productivity, health, and security. All areas are assessed in the impact from four levels: low, medium, high, and very High (as shown in Table 2). These priority levels are also categorized in the range between the most minor and most important areas, with priority one being the least and priority 5 having the highest significance. The greater the priority level within an effect area, the more important a firm is to the organization.

Table 2. Example: impact of risk assessment criteria.

Priority	Impact Area	Low	Medium	High	Very High
5	Reputation and User Trust	Minor reputational sensitivity	Impact on company reputation	Major reputational sensitivity	Significantly lost market shear
		Service failure to one user	Service failure to some user	Major service failure to one user group	Major service failure to all user group

Step 2: Making asset profile

The most important informational and technological resources for firms are critical information technology assets. Nonetheless, determining the possible impact on the organization in the event of an asset compromise or loss is one of the factors used to designate an asset as important. In addition, through conducting interviews with the individual who is responsible for these assets, we were able to gather some information and discover that the organization possesses thirteen information technology assets that are considered to be significant. The subsequent phase, which comes after the identification of key assets, is the creation of an asset profile for each and every asset. The worksheet provided by OCTAVE Allegro functions as the basis for the asset profile that was utilized. Detailed descriptions of the assets are included in this worksheet. These descriptions include components of the justification for selection, description, owner, security requirements, and, most significantly, security needs. These descriptions can be found in Table 3, which can be found below.

Step 3: Identification of asset container

Information asset containers, which are locations in which assets are either processed, conveyed, or stored, are discovered by the writers. Over the course of this procedure, we make use of the Worksheet Information asset risk map in order to categorize container assets as follows:

The term “technical” refers to the hardware, software, or systems that are now in existence. These can be either internal or external to the company, depending on whether they are under the control of the company or not. The term “physical” locations or records that pertain to either the internal side of the company's control or the exterior side of the company-controlled organization. The term “people” refers to individuals who possess knowledge, whether it be on the internal or external side of the control of the firm respectively.

Step 4: Identification of concern area

The authors started listing all the conceivable events that would threaten the IT assets of the organization. To determine problem areas, do the following: First, look for any potential trouble spots, surveying every container registered. Then, ensure you capture all those areas of concern inputting in the report on information asset risk. After that, take a step out to bring out potential risk scenarios. Lastly, document potential risk impacts on the security needs of each IT asset. Repeat steps 1 through 4 for each container in the information asset risk environment maps in order to record any and all potential concerns they may have. By doing this, we are able to collect nine potential issues that are related to hardware assets, seven for software assets, six for system assets, and five for Asset Information.

Table 3. Concern Areas.

Asset	Area of concern
Hardware	Experiencing a temporary blackout or equipment failure resulting in a loss of power supply
	Over time, the device's components wear down and become damaged
Software	Unsupported user device compatibility causes application installation to fail
	Applications used on work devices are not supervised or controlled
System	Program or operating system update causes system crash
	Performance issues caused by the user's unusual actions on the system
Information	Accidental disclosure of sensitive information occurs when users leave their login credentials on publicly accessible physical or digital documents
	By making use of compromised passwords

Step 5: Threat scenario identification
At this point, use the threat scenario that offers substantially more detail about the asset and not the threat. The steps involved include:

1. Fill the risk of asset spreadsheet for each threat scenario identified.
2. In the developed threat scenario, when using a worksheet of the information asset risk, evaluate the likelihood of the event occurring.

Every area of concern is scrutinized in order to extract information that might be connected to the threat. One of the problems listed in Table 9 is access leakage to unauthorized parties, which happens when IT employees are kept on as threat actors and use the default login credentials for device management. This might occur as a result of the officers' likely disregard for hardware hardening security guidelines, which could lead to access leaks, interfere with the effects of leaks, or even completely prohibit device functionality due to unauthorized parties. They inevitably make several gadget tweaks and setup changes. To ensure that these changes are appropriately planned and carried out and that they do not occur, change management protocols must be in place.

Step 6: Risk identification
This stage, known as validation, establishes or verifies the responsibility the circumstance poses to the company. The necessary tasks are:

1. Elaborate on the effects a threat will impose on the organization.
2. Completing, via the information asset risk spreadsheet, the asset impact with at least one potential impact. Other individuals, if needed, can be documented. The recorded impacts must be particular. The impact analysis should align with the risk evaluation of the area impact criteria.

Step 7: Analysis of risks
The risk level determination includes identifying the risk level; by this time, it is required that:

1. The impact of the risk on important assets is identified, and a level of severity is set (very high, high, moderate, or low) for each asset in the concerned area.
2. This stage calculates the relative risk score, which is to be used in the next analysis to help the firm choose the best risk management strategy.

$I = \text{A x C}$ ..... (1)

In equation (1), I represent impact score, A indicates impact area priority, and C presents impact area criticality. The total value of the effects occurring in all impact regions against danger scenarios is derived from Table 5, which is a relative risk score matrix. The value of the impact area's priority is multiplied by the weight value of the area to get the matrix value of the impact area. For instance, if a threat's impact is very high with a criticality value of Very High and a score value of 5, then the number of priority values for the reputation and customer trust impact area is 5; hence, the threat to an impact with very high criticality would be scored as 5 x 5 = 25. The same approach is followed for each region of effect on the criticality value of the impact on assets.

Table 4. Effect of relative risk score matrix.

Impact Priority	Impact Area	Low (2)	Medium (3)	High (4)	Very High (5)
5	Reputation and User Trust	10	15	20	25
4	Financial	8	12	16	20
3	Fines and legal sanctions	6	9	12	15
2	Productivity	4	6	8	10
1	Health and Security	2	3	4	5

The calculation of the relative score is illustrated in Fig. 3. The risk value of a threat scenario on assets is added against every area the company will be affected if the threat comes to pass. In Table 5, it is indicated that the risk value is calculated by multiplying the danger matrix of the region's impact weight value with the criticality weight value. This is indicated in Table 4, which now states that access is leaking to unauthorized parties. Here, the score for such a threat would be 5 x 4 = 20 over the effect towards reputation and user trust, where 4 is the high threat risk value upon the weight of 3 and 5 is the priority weight of the impact area.

The score is 4 x 3 = 12 in the financial dimension; the fines and legal sanctions dimension has a score of 3 x 2 = 6; the productivity dimension has a score of 2 x 4 = 8; the health and security dimension has a score of 1 x 2 = 2. The relative risk score of the Sophos SG leak threat scenario is 20 + 12 + 6 + 8 + 2 = 48. This allows unauthorized individuals to access key assets.

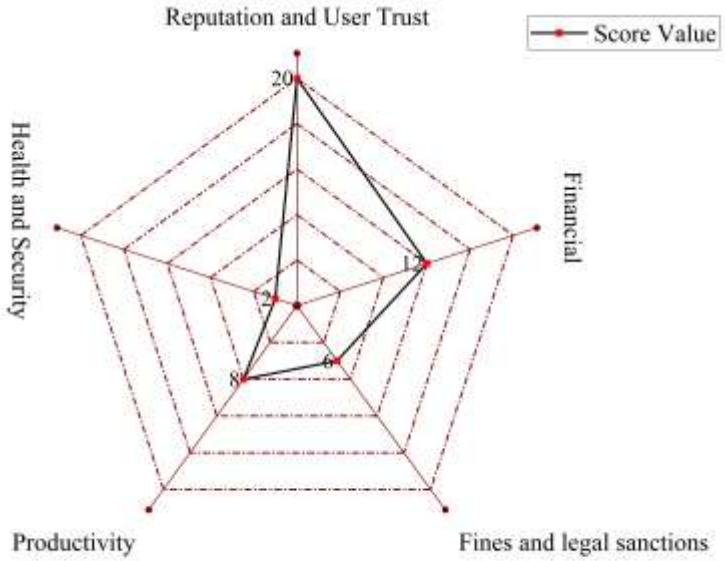

Fig. 3. Risk analysis (score value)

Step 8: Selecting mitigating methods
Risk identification was stored in this phase by its level of risk. The identified risks' relative risk scores are used for classification:

The risk categories regarding the relative risk score ascertained at step 7 and the steps involved in threat reduction are mapped out in Table 6 below. Assets in Risk Pool 1, with a relative risk score between 46 and 60, fall into an extreme risk category, whereas assets in Risk Pool 2, with a relative risk score between 31 and 45, fall into a major risk category. After that, a mitigation plan is implemented for both groups. The threat is mitigated, which means that measures will be taken to lessen or completely eradicate the possibility that its effects would have unanticipated detrimental repercussions. Threats in risk pool 3 that have a relative score between 16 and 30 are still being evaluated about whether or not they should be mitigated; if the mitigation is going to take place, it will take place during the subsequent procurement cycle of an information technology project. As a result, the risk level that falls into the Minor category would be considered acceptable. Threats to the assets that have relative risk scores that range between 0 and 15 are placed into the risk pool 4, respectively. Specifically, it indicates that the organization will not allocate funds to the acquisition of new projects based on information technology (IT) but would instead prioritize the acquisition of projects based within the department.

Table 5. Core matrix risk.

Risk Score	Risk Pool	Criticality Level	Mitigation approach
40-60	1	Extreme	Mitigate
30-45	2	Major	Mitigate
16-29	3	Moderate	Defer
0-15	4	Minor	Accept

4.3. Risk analysis result

Right from the beginning, a threat category and risk level are associated with each and every Asset ID. Once the outcomes of a risk assessment have been presented, it is possible to notice the many types of dangers that could befall assets based on the extent of the risk that was experienced (refer to Figure 4). In spite of the fact that it is possible that every asset will be subjected to the same kind of risk, the degree of danger that they face may vary from one asset to the next. When the threat scenarios have been generated, this indicates that there will be five distinct sorts of threat scenarios for each key asset. This is the case once the threat scenarios have been.

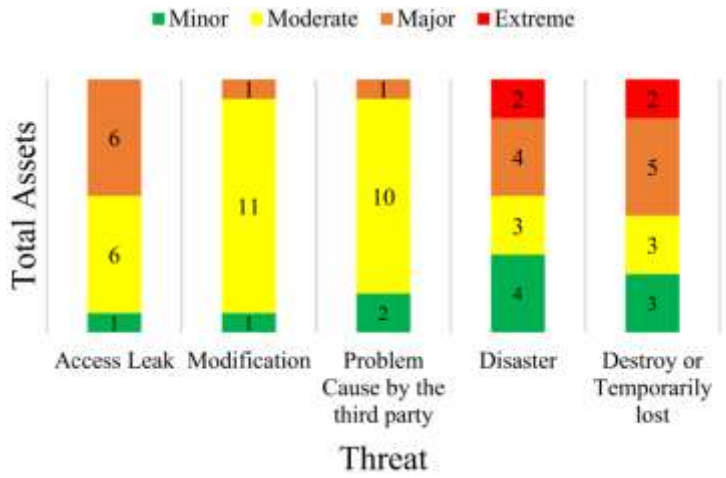

Fig. 4. Result of Risk Analysis.

5. Conclusions and Future recommendations

A significant increase in the number of assaults and threats that have been aimed against information technology security systems has been observed over the course of the past several years. In order for organizations to lessen the amount of security risk that they face, it is essential for them to engage in risk management and evaluate the readiness of their information security systems. Additionally, this will guarantee that the operations of the corporation will proceed without interruption. By utilizing risk analysis and cybersecurity compliance evaluation, it is feasible to ascertain the level of risk that is connected to each danger and security gap that is present within the company. This can be accomplished. Assisting organizations in creating policies that will result in the establishment of information technology security systems that are both capable and efficient can be accomplished through the use of risk assessment and evaluation of cybersecurity compliance. Research that we have conducted on companies that are involved in the retail industry reveals that the model that has been offered is capable of giving successful results in minimizing security concerns. This research was carried out on firms that are involved in the retail industry. Moreover, it reveals that there is a

connection between risk and the usefulness of cybersecurity compliance evaluations in regard to security threats. This is demonstrated by the fact that the correlation exists.

Besides application in risk analysis and cybersecurity, information technology and advanced algorithms are now also a crucial part of higher education (Aditto et al., 2023; Hasan et al., 2023; Sobuz, Khan, et al., 2024). The advancement of information technology will continue to increase the number of security threats. Businesses' infrastructure has also started to be dominated by cloud-based infrastructure. One of the shortcomings of this research is that the analysis does not take into account the enterprise resource planning application and the surrounding application, which together constitute the primary system that the organization uses to run its business operations. Due to the fact that business operational applications are susceptible to vulnerabilities, threats can be created that lead to security breaches. A great number of things need to be demonstrated and studied in order to mitigate the risks associated with cybersecurity. The development of the proposed method is one of the next works that will be done. This method will be developed by taking into consideration the security control that is based on the Open Web Application Security Project (OWASP) on the enterprise resource planning application and surrounding applications. This control is considered to be one of the important aspects in mitigating cyber security attacks. In addition, this study does not investigate the influence that enacting policies regarding information technology has on the work routines of employees in terms of minimizing security hazards. The purpose of this follow-up work is to evaluate the level of security awareness on the connection between the application of information technology policy and the level of threat risk posed by cybersecurity.

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] Aditto, F. S., Sobuz, M. H. R., Saha, A., Jabin, J. A., Kabbo, M. K. I., Hasan, N. M. S., & Islam, S. (2023). Fresh, mechanical and microstructural behaviour of high-strength self-compacting concrete using supplementary cementitious materials. *Case Studies in Construction Materials*, *19*, e02395.
[2] Boudguiga, A., Boulanger, A., Chiron, P., Klaudel, W., Labiod, H., & Seguy, J.-C. (2015). RACE: Risk analysis for cooperative engines. 2015 7th International Conference on New Technologies, Mobility and Security (NTMS),
[3] Broder, J. F., & Tucker, E. (2011). *Risk analysis and the security survey*. Elsevier.
[4] Engemann, K. J., & Henderson, D. M. (2014). *Business continuity and risk management: essentials of organizational resilience*. Rothstein Publishing.
[5] Hasan, N. M. S., Sobuz, M. H. R., Shaurdho, N. M. N., Meraz, M. M., Datta, S. D., Aditto, F. S., Kabbo, M. K. I., & Miah, M. J. (2023). Eco-friendly concrete incorporating palm oil fuel ash: Fresh and mechanical properties with machine learning prediction, and sustainability assessment. *Heliyon*, *9*(11).
[6] Hasan, R., Al Mahmud, M. A., Farabi, S. F., Akter, J., & Johora, F. T. (2024). Unsheltered: Navigating California's Homelessness Crisis. *Sociology*, *14*(3), 143-156.
[7] Hasan, R., Chy, M. A. R., Johora, F. T., Ullah, M. W., & Saju, M. A. B. (2024). Driving Growth: The Integral Role of Small Businesses in the US Economic Landscape. *American Journal of Industrial and Business Management*, *14*(6), 852-868.
[8] Hasan, R., Farabi, S. F., Kamruzzaman, M., Bhuyan, M. K., Nilima, S. I., & Shahana, A. (2024). AI-Driven Strategies for Reducing Deforestation. *The American Journal of Engineering and Technology*, *6*(06), 6-20. https://doi.org/10.37547/tajet/Volume06Issue06-02
[9] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.
[10] Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it*. John Wiley & Sons.
[11] Iakovakis, G., Xarhoulacos, C.-G., Giovas, K., & Gritzalis, D. (2021). Analysis and classification of mitigation tools against cyberattacks in covid-19 era. *Security and Communication Networks*, *2021*, 1-21.
[12] Jabin, J. A., Khondoker, M. T. H., Sobuz, M. H. R., & Aditto, F. S. (2024). High-temperature effect on the mechanical behavior of recycled fiber-reinforced concrete containing volcanic pumice powder: An experimental assessment combined with machine learning (ML)-based prediction. *Construction and Building Materials*, *418*, 135362. https://doi.org/https://doi.org/10.1016/j.conbuildmat.2024.135362
[13] Johora, F. T., Hasan, R., Farabi, S. F., Jahanara, A., & Mahmud, M. A. A. (2024). AI-POWERED FRAUD DETECTION IN BANKING: SAFEGUARDING FINANCIAL TRANSACTIONS. *The American Journal of Management and Economics Innovations*, *6*(06), 8-22. https://doi.org/10.37547/tajmei/Volume06Issue06-02
[14] Kabbo, M., Sobuz, M., & Khan, M. Combined influence of Waste Marble Powder and Silica Fume on the Mechanical Properties of Structural Cellular Lightweight Concrete.
[15] Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2020). Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey. *Future Internet*, *12*(4), 65.
[16] Md Abdullah Al Mahmud, Md Azhad Hossain, Md Abdul Barek Saju, Md Wali Ullah, Rakibul Hasan, & Suzer, G. (2024). INFORMATION TECHNOLOGY FOR THE NEXT FUTURE WORLD: ADOPTION OF IT FOR SOCIAL AND ECONOMIC GROWTH: PART II. *International Journal of Innovative Research in Technology*, *10*(12), 742-747.

[17] Meindl, C., Hochadel, M., Frankenstein, L., Bruder, O., Pauschinger, M., Hambrecht, R., von Scheidt, W., Pfister, O., Hartmann, A., & Maier, L. S. (2020). The role of diabetes in cardiomyopathies of different etiologies—Characteristics and 1-year follow-up results of the EVITA-HF registry. *PloS one*, *15*(6), e0234260.

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

[19] Nur, M., Mani, P., Sadia, S., Rabeya, K., & Md Ahsan Ullah, I. (2024). COMBATING BANKING FRAUD WITH IT: INTEGRATING MACHINE LEARNING AND DATA ANALYTICS. *The American Journal of Management and Economics Innovations*, *6*(07), 39-56. https://doi.org/10.37547/tajmei/Volume06Issue07-04

[20] Rakibul Hasan, Syeda Farjana Farabi, Md Abdullah Al Mahmud, Jahanara Akter, & Hossain, M. A. (2024). Information Technologies For The Next Future World: Implications, Impacts And Barriers: Part - I. *International Journal of Creative Research Thoughts (IJCRT),*, *12*(5), a323-a330.

[21] Razikin, K., & Soewito, B. (2022). Egyptian Informatics Journal.

[22] Sabaliauskaite, G., Cui, J., Liew, L. S., & Zhou, F. (2018). Integrated safety and cybersecurity risk analysis of cooperative intelligent transport systems. 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS),

[23] Salihović, S. S., Dacić, S. F., & Ferizović, A. A. (2015). Road vehicles functional safety in accordance with series ISO 26262 standards. *Tehnika*, *70*(1), 134-138.

[24] Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., & Puschner, P. (2016). Using SAE J3061 for automotive security requirement engineering. Computer Safety, Reliability, and Security: SAFECOMP 2016 Workshops, ASSURE, DECSoS, SASSUR, and TIPS, Trondheim, Norway, September 20, 2016, Proceedings 35,

[25] Shahana, A., Hasan, R., Farabi, S. F., Akter, J., Al Mahmud, M. A., Johora, F. T., & Suzer, G. (2024). AI-Driven Cybersecurity: Balancing Advancements and Safeguards. *Journal of Computer Science and Technology Studies*, *6*(2), 76-85.

[26] Sjoberg, K., Andres, P., Buburuzan, T., & Brakemeier, A. (2017). Cooperative intelligent transport systems in Europe: Current deployment status and outlook. *IEEE Vehicular Technology Magazine*, *12*(2), 89-97.

[27] Sobuz, M. H. R., Datta, S. D., & Akid, A. S. M. (2023). Investigating the combined effect of aggregate size and sulphate attack on producing sustainable recycled aggregate concrete. *Australian Journal of Civil Engineering*, *21*(2), 224-239. https://doi.org/10.1080/14488353.2022.2088646

[28] Sobuz, M. H. R., Joy, L. P., Akid, A. S. M., Aditto, F. S., Jabin, J. A., Hasan, N. M. S., Meraz, M. M., Kabbo, M. K. I., & Datta, S. D. (2024). Optimization of recycled rubber self-compacting concrete: Experimental findings and machine learning-based evaluation. *Heliyon*, *10*(6).

[29] Sobuz, M. H. R., Khan, M. H., Kabbo, M. K. I., Alhamami, A. H., Aditto, F. S., Sajib, M. S., Alengaram, U. J., Mansour, W., Hasan, N. M. S., & Datta, S. D. (2024). Assessment of mechanical properties with machine learning modeling and durability, and microstructural characteristics of a biochar-cement mortar composite. *Construction and Building Materials*, *411*, 134281.

[30] Walsh, K. (2023). *Security-first Compliance for Small Businesses*. CRC Press.

[31] Xu, W., Grant, G., Nguyen, H., & Dai, X. (2008). Security Breach: The Case of TJX Companies, Inc. *Communications of the Association for Information Systems*, *23*(1), 31.