Journal of Information Technology Management and Business Horizons
"Volume 1, Issue 1, Year 2024"
website: https://www.c5k.com

Research Article

Intelligence-driven Risk Management in Information Security Systems

Anamika Tiwari[1,s*], Md Imran Sarkar[2], Abdullah Al Sakib[2]
[1]*Department of Business Administration, Westcliff University, Irvine, CA 92614, USA*
[2]*Department of Information Technology, Westcliff University, Irvine, CA 92614, USA*
**Corresponding Author: a.tiwari.8501@westcliff.edu*

ARTICLE INFO

Article history:
5 Jul 2024 (Received)
14 Aug 2024 (Accepted)
21 Aug 2024 (Published Online)

Keywords:
Risk management
Information security
Decision making
Cybersecurity

ABSTRACT

The task of making decisions in information security, when faced with unclear probabilities and unforeseen consequences of events in the constantly evolving cyber threat landscape, has gained significant importance. Cyber threat intelligence equips decision-makers with essential information and context to comprehend and predict future threats, hence minimizing ambiguity and enhancing the precision of risk assessments. Addressing uncertainty in decision-making demands the adoption of a new methodology led by threat intelligence (TI) and a risk analysis approach. This is a crucial aspect of evidence-based decision-making. Our proposed solution to this difficulty involves the implementation of a TI-based security assessment methodology and a decision-making strategy that takes into account both known unknowns and unknown unknowns. The proposed methodology seeks to improve decision-making quality by utilizing causal graphs, which provide an alternative to current methodologies that rely on attack trees, hence reducing uncertainty. In addition, we analyze strategies, methods, and protocols that are feasible, likely, and credible, enhancing our capacity to anticipate enemy actions. Our proposed approach offers practical counsel to information security leaders, enabling them to make well-informed decisions in uncertain circumstances. This paper presents a novel approach to tackling the problem of making decisions in uncertain situations in the field of information security. It introduces a methodology that can assist decision-makers in navigating the complexities of the ever-changing and dynamic world of cyber threats.

DOI: https://doi.org/10.63471/jitmbh24003

1. Introduction

The field of information security is undergoing fast changes and now focuses mostly on the concept of managing uncertainty. Risk refers to a possible occurrence that can be recognized and measured, with its probability and consequences able to be assessed (Das et al., 2024). It can be effectively managed by introducing controls and mitigation methods that decrease the probability or consequences of its occurrence. Organizations can utilize risk management frameworks, such as ISO 27005 or NIST CSF, to identify, evaluate, and mitigate risks. These frameworks help organizations make informed decisions on how to allocate resources for risk management (Dekker & Alevizos, 2024). These frameworks encompass holistic methods for managing risks and consist of essential elements such as risk identification, risk assessment, risk treatment, and risk monitoring and review. Risk assessment, particularly risk calculation, is a crucial component of these frameworks as decision-makers rely on the results to guide the risk treatment process and allocate resources (Minkevics & Kampars, 2021; Muckin & Fitch, 2014). As a result, the difficulty of estimating risk is simplified to a familiar financial cost-benefit dilemma, where the expense of mitigating the risk is compared to the value of reducing the damage (El Amin et al., 2024).

Uncertainty refers to the condition of being unable to forecast or assess the probability or consequences of an event. Put simply, the probability distribution of both likelihood and impact is uncertain. Uncertainty emerges due to a lack of information or when the given information is partial or confusing (Wu, 2024). Consequently, managing uncertainty becomes a tough undertaking. Uncertainty is a fundamental element of managing cyber risks, and it can greatly affect the assessment of cybersecurity controls in risk evaluation (Habbal et al., 2024). As a result, it will have an effect on decision-making, specifically in the allocation of resources

*Corresponding author: a.tiwari.8501@westcliff.edu (Anamika Tiwari)

Cite: Anamika Tiwari, Md Imran Sarkar, Abdullah Al Sakib, Md Redwan Hussain, and Jarin Tias Meraj (2024). Intelligence-driven Risk Management in Information Security Systems. *Journal of Information Technology Management and Business Horizons*, 1(1), pp. 10-15.

and the level of trust in security controls. This is true in numerous fields, but it is particularly significant in the realm of security, where, as a result of agency problems, security dangers are frequently either overestimated or underestimated by individuals who lack specialized knowledge (Webb et al., 2013). Given this differentiation, it is crucial for firms to possess diverse techniques to effectively handle each one. Prior studies on the management of cyber hazards and decision-making have predominantly concentrated on comprehending the consequences of cyber-attacks, methods of averting them, and the overarching risk management procedure (Webb et al., 2014).

Organizations must prioritize the development and implementation of robust cyber risk management strategies that are in line with contemporary risk analysis methodologies that take into account uncertainty (Jangampeta & Makani, 2024; Kolluri & OF). This study investigates the current orientations of risk assessment analysis and introduces a methodical and rigorous approach based on threat intelligence (TI). The technique builds upon existing notions but acknowledges uncertainty as a fundamental element, thereby aligning with the contemporary understanding of risk (Roberts & Brown, 2017). Three Decision-makers are provided with information to effectively navigate through uncertainty and make adjustments to their cyber defenses depending on the current threat landscape and the effectiveness of their IT landscape-specific security controls (Kreutz & Jahankhani, 2024). The main impetus for this study arises from the growing significance of making decisions in the presence of uncertainty in the realm of information security. Decision-makers encounter uncertain probabilities and impacts of events in the dynamic and constantly changing cyber threat ecosystem, which poses challenges for risk analysis and mitigation. The incorporation of uncertainty within the ISO standards highlights the necessity for enterprises to modify their risk management practices (Sontan & Samuel, 2024). Prior studies have primarily focused on comprehending cyber-attacks and managing risks but have given little consideration to directly resolving uncertainty (Aditto et al., 2023; Kabbo et al., 2023; Sobuz et al., 2024). Hence, this paper aims to bridge this deficiency by presenting a methodology driven by cyber threat intelligence (CTI) that recognizes and tackles uncertainty. It offers practical advice for information security leaders to navigate the intricacies of the changing cyber threats and make well-informed decisions in uncertain circumstances.

2. Research methodology

This section provides an overview of the TIBSA, a methodology that aims to achieve two primary goals: promote interoperability among different IT, security, and other capabilities, and assist decision-makers in constructing robust cyber defenses in both predictable and unpredictable circumstances. TIBSA can be executed in its whole form, or there is also a quick version of TIBSA available. This means that the amount of strictness used in TIBSAs can be adjusted to a higher or lower level as needed (Webb et al., 2016). When specifically addressing known unknowns, such as when the probability distribution of TTPs (Tactics, Techniques, and Procedures) can be determined, these can be categorized as risks. Consequently, many standard analysis methodologies, such as rapid-TIBSA, can be utilized. However, in situations when there are unknown unknowns and consequently ambiguity, such as when the probability distribution of TTPs is not known, the key features of TIBSA (refer to Fig. 1) will assist in achieving much-improved outcomes, leading to superior decision-making.

2.1. Process of decision making

TIBSA empowers decision-makers to detect, rank, and address cyber threats by assessing the efficiency of security measures and their execution, ultimately decreasing vulnerability to cyber-attacks. Various functionalities can be enhanced through technical or administrative adjustments in order to prevent or identify certain issues. Efficient security measures do not necessarily require additional security controls, and the presence of more security controls does not automatically guarantee effective defense. An organization's effectiveness in defense ultimately relies on its capacity to deliver the appropriate quantity and caliber of information to decision-makers. Fig. 1 illustrates the fundamental elements of the TIBSA technique, which will be further examined in the following section.

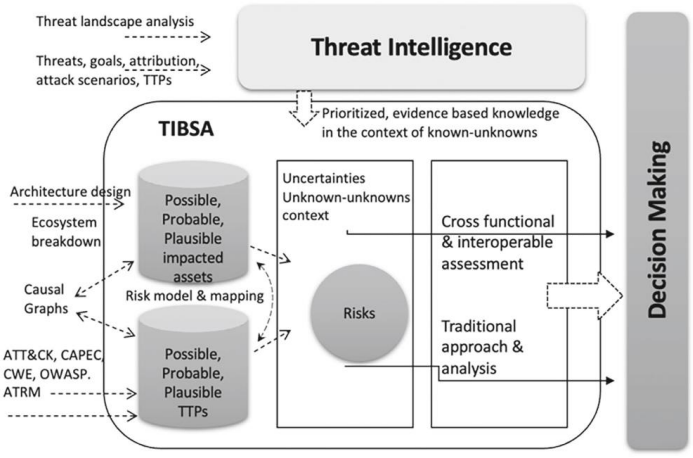

Fig. 1. Key elements of TIBSA at a strategic level

2.2. Cyber threats for information security systems

The first phase in TIBSA involves the use of high-quality, evidence-based knowledge, including information about threat context, indicators, implications, mechanisms, behaviors, and action-oriented guidance provided by TI. To clarify, comprehending the cyber threat landscape necessitates the presence of a well-developed and advanced Cyber Threat Intelligence (CTI) system that operates effectively at strategic, operational, and tactical levels. This enables the gathering, manipulation, and examination of data to comprehend the objectives, motivations, targets, trends, behaviors, and attribution of the threat source.35 CTI serves as a facilitator for making well-informed security decisions based on data, making it the initial and essential step to initiate the TIBSA. Currently, CTI is being applied in several scenarios. For instance, it provides C-level executives with valuable information that can assist in making quicker and more effective decisions. Additionally, it illuminates potential dangers that are specific to the organization, allowing security teams to make more informed decisions. This includes enhancing security measures by prioritizing the resolution of vulnerabilities and fine-tuning prevention and detection systems. In addition, the strategic and tactical level capabilities of CTI enhance other security capabilities by uncovering enemy objectives, reasons, characteristics, methods of operation, and specific tactics, techniques, and procedures (TTPs) 36, and conducting thorough threat research. The purpose of this paragraph is not to extensively analyze CTI's role and details in the cyber domain. However, it is essential to establish CTI as the guiding force for TIBSA by consistently monitoring and analyzing the cyber threat landscape across all strategic, operational, and tactical aspects. Therefore, it is crucial for CTI to deliver practical, fact-based information on possible threats, their objectives, and/or their tactics, techniques, and procedures (TTPs) for TIBSA to begin. Fig. 2 presents the major threats detected in information systems.

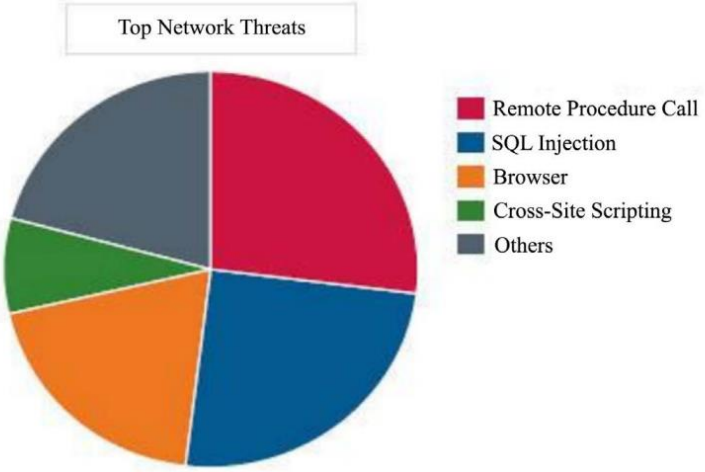

Fig. 2. Major threats detected in information systems (Minkevics & Kampars, 2021).

2.3. Utilize the scoring model

TIBSA's design necessitates and requires attentive activities. However, it is important to note that different organizations may possess varying resources, aims, mission, and vision. Some businesses may choose to conduct a comprehensive evaluation of all relevant security measures against potential, likely, and possible tactics, techniques, and procedures (TTPs) by implementing a full-scale Threat Intelligence-Based Security Assessment (TIBSA). However, other organizations may prefer a more condensed version known as rapid-TIBSA. Irrespective of the selected TIBSA version, implementing a scoring model is an essential step in prioritizing the coverage of TTPs. Scoring models can be implemented using several techniques. For example, a scoring model produces impressive outcomes when implemented using the most basic method, spreadsheets. Alternatively, it can be integrated into an AI-powered system to enhance user-friendliness, streamline processes, perhaps decrease reliance on highly skilled professionals, mitigate subjectivity, or even minimize prejudice. It is recommended to personalize and execute the model in an automated manner and offer a web-based user interface. Therefore, optimal outcomes and the most satisfactory user experience can be attained.

3. Evaluate the security measures

TIBSA is specifically intended to ensure seamless compatibility and cooperation between different systems. It promotes collaboration across security capabilities, regardless of their placement within an organization. For instance, the ability to collaborate across different divisions can be utilized to create virtual teams that are assigned to achieve a common objective. This enables the elimination of potential barriers between divisions. This, in turn, not only enhances collaboration but also facilitates the consolidation of diverse expert ideas, resulting in greatly enhanced and, to the greatest extent feasible, unbiased judgments. It is crucial to allocate the most suitable capability to assess the efficiency of a security control, in line with the Tactics, Techniques, and Procedures (TTPs). Assessors may be assigned to evaluate controls through technical workshops and interviews, while controls requiring thorough technical validation may be

allocated to technically proficient professionals like penetration testers. TIBSA could potentially collaborate with threat-intelligence-based ethical red teaming (TIBER) for control assessment, resulting in a significant impact. As outlined in the TIBER-EU framework, TIBER 44 conducts a capture-the-flag exercise that is led by threat intelligence. Therefore, TIBSA may incorporate TIBER as a precise assessment for various Tactics, Techniques, and Procedures (TTPs). Conversely, TIBER has the potential to stimulate more extensive ecosystem-driven TIBSAs. To ensure successful collaboration and clearly defined job distribution, it is essential to create a mapping of controls comparing the use of a third-party provider (TTP) vs in-house controls.

Table 1. Assessing criteria and measures of effectiveness for mitigation (El Amin et al., 2024).

	Mitigating criteria and scoring			
Effectiveness	**Prevent**	**Detect**	**Constrain**	**Recover**
High	PR.H = 12	DT.H = 8	CS.H = 7	RE.H = 5
Medium	PR.M = 10	DT.M = 6	CS.M = 5	RE.M = 3
Low	PR.L = 8	DT.L = 4	CS.L = 3	RE.L = 1

Table 2. TTPs with currently implemented controls and Benefit/Cost (B/C) ratio (El Amin et al., 2024).

	Control ID	TTPs IDs							Benefit	Cost	B/C ratio
		T1134	**T1087**	**T1110**	**T1059.001**	**T1059.007**	**T1078**	**T1562.001**	12	1	12
In place security controls—Mitigation effectiveness matrix	**ST7.C098**	PR.H DT.H	PR.H DT.H		CS.M	CS.L			11	1	11
	ST6.C121	PR.H		DT.M	DT.M RE.L				11	1	11
	ST1.C007			CS.M			RE.L	RE.L	18	2	9
	ST5.C051		DT.M CS.M	PR.L DT.L		RE.H		PR.M CS.M	16	2	8
	ST9.C101						RE.H		16	3	5.3
	ST5.C054		DT.H			CS.H DT.H			10	4	2.5
	ST3.C038	PR.L DT.H		PR.L DT.H	CS.M		RE.M	RE.H	7	3	2.3

This is the first task that needs to be completed in this step. The level of effectiveness can vary in granularity, and it is the responsibility of companies to establish their own based on their own needs and maturity levels. Table 1 is an illustration of the efficacy scale in comparison to pre-established criteria. TIBSA employs a set of two-letter notations, influenced by Reference 45 and based on the criteria of prevention, detection, constraint, and recovery, to streamline and expedite the execution of this task. The third letter (L, M, and H) indicates the level of effectiveness. For instance, certain controls may be extremely efficient in preventing a TTP (threat to process) but offer little to no value in terms of recovery. Some may have a high level of effectiveness in detecting Tactics, Techniques, and Procedures (TTPs) and a moderate level of effectiveness in limiting or restricting a TTP. The purpose of this stage is to thoroughly evaluate and determine the efficiency of the security controls currently being used against a variety of feasible, probable, and plausible Tactics, Techniques, and Procedures (TTPs). TIBSA employs a straightforward and efficient method to determine the efficacy evaluation of a control that is currently in use, using the principles of benefit-cost analysis (BCA). The number is 46. A linear scale ranging from 1 to 12 is allocated, as seen in Table 1. It is important to mention that the score falls in a left-to-right direction, with the left side indicating that prevention controls are intrinsically valued higher than recovery controls. Consequently, prioritizing prevention strategies would be preferred above reactive and recovery strategies. However, this can still be modified based on the specific needs of the company. To determine the initial component, the benefit, it is necessary to add up the scores corresponding to the range of attenuated TTPs as indicated in Table 1. Table 2 presents a comprehensive overview of the effectiveness of in-use controls in mitigating a range of TTPs. The controls are arranged in descending order according on their benefit-to-cost ratio.

3.1. Uncertainty to risk strategy

First and first, it is necessary to provide a clear definition of the phrases "known unknown" and "unknown unknown" within the specific context being discussed. A known unknown refers to a circumstance in which the occurrence of an event is acknowledged, but the precise details and the probability distribution of this event remain uncertain. An "unknown unknown" refers to a circumstance when both the occurrence and the probability distribution are unknown. TIBSA initiates the process by acquiring knowledge that is supported by evidence through CTI. Strategic-level Cyber Threat Intelligence (CTI) serves a vital role in conducting an analysis of the uncertainties of the threat landscape. The input given could potentially indicate a threat that includes Tactics, Techniques, and Procedures (TTPs), or it could be a targeted and sophisticated attack known as an Advanced Persistent Threat (APT) campaign, with distinct TTPs employed during each step of the attack. On the other hand, reliable and well-founded CTI may assign a probability distribution to threats by doing a thorough analysis. This allows for the transformation of these threat events from being completely unknown to being partially known. To clarify, we need to move those instances of potential harm into the realm of risk. That is because we have information indicating that a malicious actor is focusing on a particular sector of businesses. We are aware of their methods and tactics, which allows us to determine the probability distribution of their actions. It is important to consider the Ellsberg dilemma in this context.

4. Conclusions

This study presents a versatile and pragmatic analysis method driven by TI (technology integration), which takes into account uncertainty and enhances decision-making. By integrating uncertainty into assessment analysis, particularly in the evaluation of cybersecurity control efficacy, chief information security officers (CISOs) can enhance their decision-making about resource allocation and strategies to mitigate cyber threats. By assessing the level of uncertainty surrounding various risks and controls, Chief Information Security Officers (CISOs) can gain a clearer understanding of the potential consequences of different risks and the efficacy of current measures in reducing those risks. This can assist in guaranteeing that resources are distributed efficiently and effectively according to the organization's requirements and that the organization's security position remains consistently appropriate for the evolving threat landscape. Decision-makers can potentially prevent excessive expenditure by employing a cost-benefit approach, as suggested, to discover the most economically efficient measures for reducing the identified risks. Consequently, this offers reliable data and practical knowledge to Chief Information Security Officers (CISOs) in order to prevent the typical mistake of placing too much or too little trust in security controls. As a result, they may refine their security defenses.

In addition, the utilization of AI and machine learning (ML) to create automated tools and methodologies would greatly enhance the implementation of TIBSA in real-world situations, resulting in improved efficiency, scalability, and accuracy. Artificial intelligence (AI) and machine learning (ML) algorithms have demonstrated significant potential in the analysis of extensive datasets, the identification of patterns, and the generation of predictions. By incorporating artificial intelligence (AI) and machine learning (ML) functionalities, such as Bayesian inference, into the TIBSA approach, it becomes feasible to automate specific processes, including data gathering, threat analysis, and uncertainty modeling. Finally, it is essential to incorporate TIBSA into current risk management frameworks and standards in order to establish a comprehensive methodology for analyzing and managing risks. Further investigation is needed to examine the compatibility and potential collaboration between TIBSA and frameworks like the NIST CSF v2 or ISO 27001/27005. Integrating TIBSA can improve the compatibility and implementation of TIBSA within enterprises.

Funding: This research did not receive any specific funding.

Conflicts of interest: The authors declare no conflict of interest that could have appeared to influence the work reported in this paper.

References

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.

Das, P., Gupta, I., & Mishra, S. (2024). Artificial intelligence driven cybersecurity in digital healthcare frameworks. In *Securing Next-Generation Connected Healthcare Systems* (pp. 213-228). Elsevier.

Dekker, M., & Alevizos, L. (2024). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, *7*(1), e333.

El Amin, H., Samhat, A. E., Chamoun, M., Oueidat, L., & Feghali, A. (2024). An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. *Journal of Cybersecurity and Privacy*, *4*(2), 357-381.

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*, 122442.

Jangampeta, S., & Makani, S. T. (2024). The Future of Threat Intelligence-Driven Security: Integrating Emerging Technologies for Enhanced Decision-Making. *Journal ID*, *9471*, 1297.

Kabbo, M., Sobuz, M., & Khan, M. (2023). Combined influence of Waste Marble Powder and Silica Fume on the Mechanical Properties of Structural Cellular Lightweight Concrete. *International Conference on Planning, Architecture & Civil Engineering*.

Kolluri, V., & OF, A. E. I. I. G. *THE DIGITAL REALM: AI-DRIVEN ANTIVIRUS AND CYBER THREAT INTELLIGENCE*‖.

Kreutz, H., & Jahankhani, H. (2024). Impact of Artificial Intelligence on Enterprise Information Security Management in the Context of ISO 27001 and 27002: A Tertiary Systematic Review and Comparative Analysis. *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation*, 1-34.

Minkevics, V., & Kampars, J. (2021). Artificial intelligence and big data driven IS security management solution with applications in higher education organizations. 2021 17th International Conference on Network and Service Management (CNSM),

Muckin, M., & Fitch, S. C. (2014). A threat-driven approach to cyber security. *Lockheed Martin Corporation*.

Roberts, S. J., & Brown, R. (2017). *Intelligence-driven incident response: Outwitting the adversary*. " O'Reilly Media, Inc.".

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.

Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*, *21*(2), 1720-1736.

Webb, J., Ahmad, A., Maynard, S., & Shanks, G. (2016). Foundations for an intelligence-driven information security risk-management system. *Journal of Information Technology Theory and Application (JITTA)*, *17*(3), 3.

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2013). Towards an intelligence-driven information security risk management process for organisations.

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2014). Information security risk management: An intelligence-driven approach. *Australasian Journal of Information Systems*, *18*(3).

Wu, H. (2024). Security Situation Awareness System Based on Artificial Intelligence. *Scalable Computing: Practice and Experience*, *25*(3), 1301-1310.