International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 2 (2025)
https://doi.org/10.31436/ijpcc.v11i2.572

Event-Based Cybersecurity Risk Assessment: Identifying Potential Cyber-Attacks in Organisations

Wan Azlena Wan Mohamad, Noor Hayani Abd Rahim, Nurul Nuha Abdul Molok
Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

*Corresponding author: noorhayani@iium.edu.my
(Received: 19th February 2025; Accepted: 17th July, 2025; Published on-line: 30th July, 2025)

Abstract— Cybersecurity risk assessment is crucial for organisations since cyber threats are becoming increasingly sophisticated and dynamic. This study investigates how organisations identify potential cyber-attacks within an event-based risk assessment context. Using a qualitative approach, semi-structured interviews were conducted with ten cybersecurity experts from diverse organisations. The experts possess extensive strategic, technical, and advisory expertise in the field. Thematic analysis of the data revealed four key practices: (i)collaborative brainstorming involving diverse stakeholders, (ii)referring to historical data and past incident logs, (iii)staying updated on current cyber-attacks trends, and (iv)using established frameworks such as ISO/IEC 27005 supplemented with dynamic resources. These findings underscore the importance of integrating diverse methods and perspectives into event-based cybersecurity risk assessments to address evolving threats. The study contributes to theory and practice by offering actionable insights for organisations to identify potential cyber-attacks within an event-based cybersecurity risk assessment framework. Limitations are acknowledged, including reliance on self-reported data and a small sample size, with recommendations provided for future research.

Keywords— Cybersecurity Risk Assessment, Event-Based Approach, Cyber Attack Identification

I. Introduction

In an increasingly digital world, the complexity and frequency of cyber-attacks continue to grow rapidly. This phenomenon poses critical challenges to organisations globally. The stakes are particularly high for public and private sector organisations, where the impact of a successful cyber-attacks can lead to severe financial, operational, and reputational losses. As organisations modernise, their computing systems become increasingly vulnerable, with even minor weaknesses potentially being exploited [1]. Consequently, digital transformation has not only accelerated innovation but also heightened organisational exposure to cyber risks [2].

Cybersecurity risk management encompasses a comprehensive process to protect organisations from cyber risks [3], [4], [5]. At the heart of this process lies the cybersecurity risk assessment, a fundamental exercise to identify and assess potential cyber threats [6], [7]. An event-based cybersecurity risk assessment focuses on identifying potential cyber-attacks or events that may compromise an organisation's systems [6], [7]. This approach emphasises the identification of potential cyber-attacks or possible events and their impact, enabling organisations to prepare for and mitigate risks properly [7].

Despite the increasing sophistication of cyber-attacks, there is a lack of clarity on how organisations systematically identify these threats. This gap is due to the existing cybersecurity framework that lacks comprehensive guidance on identifying potential cyber-attacks and response mechanisms [8]. Furthermore, many organisations still struggle with situational awareness regarding the threat landscape, which is crucial for risk assessment [9].

This study aims to address this gap by examining how organisations identify potential cyber-attacks or events in the context of event-based cybersecurity risk assessment. The qualitative data was collected through interviews with ten well-qualified cybersecurity experts across diverse organisations. The study employs thematic analysis based on [10], [11], and [12]. The findings provide valuable insights into organisational approaches to identifying potential cyber-attacks. These findings contribute to the development of event-based cybersecurity risk assessment strategies. By focusing on the identification of potential cyber-attacks, this study offers practical recommendations and theoretical contributions to enhance the efficacy of event-based cybersecurity risk assessments.

II. Literature Review

This section presents the reviews of academic literature to understand event-based cybersecurity risk assessment, including the definitions, key elements and its focus on identifying potential cyber-attacks or events.

Cybersecurity risk assessment is a critical component of organisational risk management, focusing on safeguarding operations, assets, reputation, and national security. It plays a central role in managing risks at multiple levels [13]. It as an integrated approach that combines identification,

https://doi.org/10.31436/ijpcc.v11i2.572

analysis, and assessment into a unified strategy for simplifying and managing cybersecurity risks [14]. There are two main approaches for risk assessment: an event-based approach and an asset-based approach [7]. In an event-based approach, the underlying concept is that risks can be identified and assessed through an evaluation of events and consequences [7].

An event-based approach can establish high-level or strategic scenarios without spending a considerable amount of time on the identification of assets on a detailed level [7]. This allows the organisation to focus its risk treatment efforts on the critical risks. The key elements in event-based cybersecurity risk assessment encompass three (3) primary processes: risk identification, analysis and evaluation [6], [7], [14]. An event-based approach to cybersecurity risk assessment focuses on identifying potential cyberattack scenarios by considering risk sources and their impact on organisations [6], [7]. It specifically recommends referring to examples and typical attack methods, such as those summarised in Table 1, to assist organisations in systematically identifying potential cyber-attacks [7]. This structured approach supports organisations in recognising vulnerabilities and preparing for possible attack scenarios.

TABLE 1:
THE EXAMPLES AND USUAL METHODS OF ATTACK [7]

Risk Source	Examples and Usual Method of Attacks
State-related	States, intelligence agencies
	Method: Attacks generally conducted by professionals, working under a calendar and a method of attack that are predefined. This attacker profile is characterized by its ability to carry out an offensive operation over a long period of time (stable resources, procedures) and to adapt its tools and methods to the topology of the target. By extension, these actors have the means of purchasing or discovering 0-Day vulnerabilities and some are able to infiltrate isolated networks and to conduct successive attacks in order to reach a target or targets (e.g. by means of an attack aimed at the supply chain).
Organized crime	Cybercriminal organizations (mafias, gangs, criminal outfits)
	Method: Online scams or in person, ransom request or attack via ransomware, use of bot-nets, etc. Due in particular to the proliferation of attack kits that are readily available online, cybercriminals are conducting increasingly sophisticated and organized operations for lucrative or fraudulent purposes. Some have the means of purchasing or discovering 0-Day vulnerabilities.
Terrorist	Cyber-terrorists, cyber-militias
	Method: Attacks that are usually not very sophisticated but which are conducted with determination for the purposes of destabilization and destruction: denial of service (aimed for example at making the emergency services of a hospital centre unavailable, untimely shutdowns of an energy production industrial system), exploitation of vulnerabilities of Internet sites and defacement.
Ideological activist	Cyber-hacktivists, interest groups
	Method: The methods of attack and sophistication of the attacks are relatively similar to those of cyber-terrorists but are motivated by less destructive intentions. Some actors conduct these attacks in order to convey an ideology, a message (e.g. massive use of social networks as a sounding board).
Specialized outfits	"Cyber-mercenary" profile with IT capacities that are generally high from a technical standpoint. Because of this, it should be distinguished from script-kiddies with whom it shares however the spirit of a challenge and search for recognition but with a lucrative objective. Such groups can be organized as specialized outfits that propose veritable hacking services.
	Method: This type of experienced hacker is often at the origin of the designing and creating of attack kits and tools that are available online (possibly for a fee) which can then be used "turnkey" by other groups of attackers. There are no particular motivations other than financial gain.
Amateur	Profile of the script-kiddies hacker or who has good IT knowledge; motivated by the quest for social recognition, fun, challenge.
	Method: Basic attacks but with the capacity of use the attack kits that are available
Avenger	The motivations of this attacker profile are guided by a spirit of acute vengeance or a feeling of injustice (e.g. employee dismissed for serious fault, discontented service provider following a contract that was not renewed, etc.).
	Method: This attacker profile is characterized by its determination and its internal knowledge of the systems and organizational processes. This can make it formidable and provide it with substantial power to do harm.
Pathological attacker	The motivations of this attacker profile are of a pathological or opportunistic nature and are sometimes guided by the motive for a gain (e.g. unfair competitor, dishonest client, scammer, and fraudster).
	Method: Here, either attackers have a knowledge base in computing that leads them to attempt to compromise the IS of their target, or they use the attack kits available online, or decide to subcontract the IT attack by calling upon a specialized outfit. In certain cases, attackers can direct their attention to an internal source (discontented employee, unscrupulous service provider) and attempt to corrupt the latter.

The potential for cyber-attacks is based on a variety of factors, including the capabilities and intentions of the attacker [15]. Besides that, risk identification can also involve historical data, theoretical analysis, informed and expert opinions, and interested parties' needs [7].

Organisations are suggested to determine which type of potential cyber-attacks or events to consider during risk assessments [6]. The level of detail needed to describe such events. Descriptions of potential cyber-attacks can be expressed in highly general terms, in more descriptive terms

https://doi.org/10.31436/ijpcc.v11i2.572

using tactics, techniques, and procedures, or in highly specific terms [6].

Therefore, it is important to understand risk and threat sources to recognise potential cyber-attacks [6], [7]. It is recommended to use examples and typical attack methods to guide organisations in systematically identifying threats [7]. It also incorporates historical data, expert opinions, and stakeholder needs. It is also suggested to vary levels of detail in describing potential attacks, from general overviews to specific tactics and techniques [6].

III. Methodology

This research adopts a qualitative approach to explore how organisations identify potential cyber-attacks within the context of event-based cybersecurity risk assessment. A qualitative methodology was considered appropriate for this study as it enables a rich and in-depth exploration of expert perspectives and practices, particularly valuable in a rapidly evolving field like cybersecurity. In an interdisciplinary domain such as cybersecurity, qualitative approaches are essential for capturing the diversity of knowledge, experiences, and contextual insights that may not be evident through quantitative methods alone [16]. Moreover, qualitative research allows for a deeper understanding of complex, real-world issues by examining how participants interpret them within their organisational contexts [17].

Research Design: The study is focused on uncovering the strategies and methods organisations use to identify potential cyber-attacks within the event-based cybersecurity risk assessment framework. Data were collected through semi-structured interviews with cybersecurity experts, allowing flexibility to probe deeper into participants' insights while maintaining a structured alignment with the research objectives and questions.

Participants: Participants are experts who were selected using purposive sampling based on predefined criteria: at least 10 years of experience, involvement in organisational-level cybersecurity, and decision-making roles. Expert interviews are a widely used qualitative interview method, often aiming at gaining information about or exploring a specific field of action [18]. The sampling strategy was guided by the principle of information power, which posits that the more relevant and information-rich the participants are in relation to the study objectives, the fewer participants are required to generate meaningful data[19]. The selected participants, outlined in Table 2, were recruited via professional networks and referrals to ensure their relevance and expertise in the field.

TABLE II
IDENTIFIED PARTICIPANTS

Participants	Organisation Specialisation	Gender	Portfolio	Total Years of Service
Participant 1	Specializes in national cybersecurity policies, strategies, and incident management	Female	Officer, Expert, Consultant	20
Participant 2	Focuses on construction, public works, and infrastructure development	Male	Officer, Expert	17
Participant 3	Responsible for coordinating national policies, strategic planning, and high-level governance	Female	Officer, Expert	15
Participant 4	Specializes in public sector training and professional development	Female	Officer, Expert, Consultant	16
Participant 5	Oversees human resources, policies, and operations for the Malaysian civil service	Male	Officer, Expert, Consultant	17
Participant 6	Manages cross-ministerial coordination, national projects, and strategic initiatives	Male	Officer, Expert, Consultant	21
Participant 7	Focuses on immigration management, passport services, and border control.	Female	Officer, Expert	15
Participant 8	Responsible for driving national digitalization and ICT development	Female	Officer, Expert, Consultant	24
Participant 9	Manages national finances, budgeting, and economic policy	Female	Officer, Expert, Consultant	21
Participant 10	Oversees national security, law	Female	Officer, Expert	18

https://doi.org/10.31436/ijpcc.v11i2.572

Participants	Organisation Specialisation	Gender	Portfolio	Total Years of Service
	enforcement, and internal affairs.			

The participants represent a mix of strategic, technical, and advisory roles. These criteria make them ideal contributors to understanding how organisations identify potential cyber-attacks within the event-based cybersecurity risk assessment framework. Their responsibilities include shaping, supporting, and implementing cybersecurity risks in their respective organisations.

Data Collection: The primary method of data collection was semi-structured interviews conducted with the selected experts. Each interview was guided by open-ended questions designed to explore their approaches, experiences, and challenges in identifying potential cyber-attacks or events. The interviews were audio-recorded, transcribed verbatim, and anonymised to ensure participant confidentiality. Follow-up questions were asked where necessary to gain further clarification or depth in responses.

Data Analysis: Thematic analysis was employed to analyse the interview data. This method was chosen for its ability to systematically identify, organise, and interpret patterns (themes) within qualitative data. The data in this study were analysed using the following steps [10], [11], [12]:

i. Preparing the transcriptions
ii. Reading, understanding and translating the transcripts
iii. Highlighting the key statements that are relevant to the research objectives
iv. Grouping and coding the key statements
v. Deriving the themes and sub-themes
vi. Finalising and writing the results

The themes and sub-themes were directly aligned with the research objective and question. It provides a structured and meaningful interpretation of the data.

Trustworthiness: To ensure the trustworthiness of the study, a credibility strategy is employed. Credibility refers to confidence in the truth of the findings. One effective method to enhance credibility is through data triangulation [16]. Data triangulation was achieved by including diverse participants from different organisations and roles. By including diverse participants from various organisations and roles, researchers can obtain a more comprehensive understanding of the phenomenon under study [16], [20]. This approach helps to mitigate biases that may arise from relying on a single source of data.

Ethical Considerations: Ethical approval was obtained before data collection to ensure the study adhered to ethical research principles. All participants were provided with detailed information about the study and signed an informed consent form before participating. Confidentiality and anonymity were strictly maintained throughout the research process. This practice aligns with the ethical principle of confidentiality, which mandates that researchers safeguard participants' private information [21].

IV. Findings

This section presents the findings of this study, which explores how organisations identify potential cyber-attacks in the context of event-based cybersecurity risk assessment. Thematic analysis of the data collected from ten expert participants yielded four primary themes: (i)brainstorming and collaboration, (ii)referring to past incidents and logs, (iii)staying updated on current trends and (iv)using ISO/IEC 27005 and other relevant references.

1. Collaborative Brainstorming

A collaborative brainstorming approach to identify potential cyber-attacks is essential. 6 out of 10 participants explicitly agreed that brainstorming sessions involving multiple stakeholders help provide a well-rounded perspective on cybersecurity risks. Participant 1 emphasised the importance of cross-department collaboration: *"Brainstorming with all the officers involved, including top management. Each person has their views and experiences, so there needs to be collaboration in this process"*. Different departments may face unique cybersecurity risks, making their input valuable. Participant 5 reinforced this point: *"Through collaborative brainstorming sessions involving officers at all levels, each department can contribute unique perspectives on the specific threats they encounter"*. Additionally, Participant 9 suggested including specialised cybersecurity personnel to provide technical insights: *"Brainstorming sessions should involve all relevant stakeholders, including the IT team, cybersecurity experts, and even top management"*. By fostering brainstorming and collaboration, organisations can have a comprehensive understanding of potential cyberattack scenarios, ensuring no critical threats are overlooked.

2. Referring to Past Incidents and Logs

Analysing historical cybersecurity incidents provides valuable insights into recurring attack patterns and vulnerabilities. 9 out of 10 participants agreed that analysing historical cybersecurity incidents provides valuable insights into recurring attack patterns and vulnerabilities. Participant 1 stressed the need for historical data review: *"Refer to the history of past events. Look back at the records of previous cyber-attacks and check the log records"*. Similarly, Participant 2 emphasised leveraging previously documented incidents to improve threat detection: *"Organisations can also refer to past incidents. Look at past attack records or log records for attempted attacks"*. Beyond internal records, organisations should also study global cybersecurity incidents and emerging threat trends. Participant 9 recommended expanding the scope of reference:

https://doi.org/10.31436/ijpcc.v11i2.572

"Organisations should always refer to past incidents, both locally and internationally, and keep an eye on the latest cyberattack trends". By analysing past incidents, organisations can better understand the evolving threat landscape, allowing them to strengthen defences against future attacks.

3. Staying Updated on Current Trends

The cybersecurity landscape evolves rapidly, with new threats emerging daily. 9 out of 10 participants agreed on the necessity of staying informed about current attack trends at both domestic and international levels. Participant 1 highlighted the importance of cybersecurity awareness: *"We must stay alert to current issues, both domestically and internationally. Cyber-attacks are constantly evolving, so we need to stay up-to-date"*. Similarly, Participant 5 reinforced the need for continuous monitoring: *"We also need to stay aware of current issues, both locally and internationally, because cyber threats evolve rapidly"*. To support real-time threat identification, organisations should integrate threat intelligence feeds, advisories, and cybersecurity reports into their risk assessment processes. Participant 6 emphasised the importance of using threat intelligence: *"It's important to incorporate threat intelligence into this process to ensure we stay updated on the latest threats"*. By staying informed on evolving cyber threats, organisations can identify vulnerabilities early and implement proactive event-based cybersecurity risk assessment.

4. Using Usual Methods of Attack by ISO/IEC 27005 and Other Relevant Sources as References

All participants acknowledged the examples and commonly used attack methods outlined in ISO/IEC 27005 (as presented in Table 1) as a valuable reference for identifying typical cyberattack techniques. However, 7 out of 10 participants also stressed the importance of supplementing it with additional resources to keep up with dynamic and emerging threats. Participant 5 pointed out that ISO/IEC 27005 alone is insufficient: *"ISO/IEC 27005 is a good reference, but we need to combine it with up-to-date information from other sources as well"*. To enhance cyberattack identification, participants recommended integrating MITRE ATT&CK and other intelligence platforms for a more comprehensive approach. Participant 6 supported this view: *"ISO/IEC 27005 is a good reference, but we also need to refer to other sources, such as the MITRE ATT&CK matrix. Combining references can provide a more complete picture of the potential threats"*. Similarly, Participant 9 reinforced the need for multiple sources to improve cybersecurity risk assessments: *"ISO/IEC 27005 is a good reference, but agencies should also refer to platforms like MITRE ATT&CK or other intelligence sources"*. By referring to multiple sources of threat intelligence, agencies can implement a risk identification that stays aligned with evolving cyber risks.

V. Discussion Of Findings

This section presents the discussion of this study, which explored how organisations identify potential cyber-attacks within an event-based cybersecurity risk assessment framework. Our findings highlighted a multifaceted approach encompassing brainstorming and collaboration, historical data analysis, staying updated on current trends, and using established frameworks.

According to our findings, a collaborative approach is useful for identifying potential cyber-attacks. Based on the majority of the participants' feedback, brainstorming sessions involving multiple stakeholders, including technical teams and top management, offer diverse perspectives that contribute to a more accurate and comprehensive understanding of risk. This aligned with [22] and [23], which encourages consultation with both senior management and process owners to help identify relevant threat events and consequences.

Our findings show that analysing historical cybersecurity incidents is a valuable practice. Based on the majority of the participants' feedback, reviewing past incidents provides critical insight into recurring attack patterns, vulnerabilities, and organisational weaknesses. We found that it allows organisations to better anticipate and address similar threats in the future. This aligned with [24], [25], [26] and [27], who argue that the evolving nature of cyber threats demands a historical understanding of incidents to effectively categorise and mitigate risks.

Our findings also emphasise the importance of staying current with emerging cybersecurity threat trends. Based on the majority of the participants' feedback, organisations should actively monitor the threat landscape to ensure their defences and response strategies remain effective. This aligned with [22], [28] and [29], who argue that by understanding these trends, organisations can adopt a forward-thinking and innovative approach to cybersecurity that strengthens long-term resilience. Our findings also align with [30], who reinforces advocating cyber threat intelligence for automated threat analysis across all levels of an organisation to combat increasingly sophisticated cyber threats. However, while participants emphasised the value of real-time cyber threat intelligence, implementation may be hindered by cost, staffing, or technological readiness, especially in resource-constrained organisations [31].

Based on our findings, the ISO/IEC 27005 standard was acknowledged as a valuable reference for identifying common cyberattack methods (as shown in Table 1). However, our findings also stressed the importance of supplementing this with dynamic and up-to-date sources such as the MITRE ATT&CK framework. We found that the MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based

on real-world observations. This aligned with [32], [33] and [34], who highlight the role of MITRE ATT&CK in helping organisations assess risks and understand adversarial behaviour. Combining multiple references fosters a collaborative, informed, and adaptive approach that allows organisations to strengthen their cybersecurity posture.

We found that identifying potential cyber-attacks requires a multidimensional approach. While established frameworks offer structured guidance, proactive practices such as collaborative brainstorming, historical incident analysis, and monitoring emerging threat trends are equally vital to effective cybersecurity risk assessment.

Contribution to Theory: This study contributes to the body of knowledge on event-based cybersecurity risk assessment. It identifies practical strategies that organisations can employ to identify potential cyber-attacks. It bridges the gap between theoretical frameworks and practical implementation, offering a roadmap for organisations to enhance their event-based risk assessment practices.

Practical Implications: The study provides actionable recommendations for organisations to improve their event-based cybersecurity risk assessments:

i. Regularly conduct brainstorming sessions involving diverse stakeholders.
ii. Develop and maintain comprehensive logs of past incidents and use them to anticipate future threats.
iii. Keeping up with emerging cyber threats and, if possible, investing in real-time threat intelligence tools to stay updated on emerging trends.
iv. Combine established frameworks with dynamic resources to ensure a robust and adaptive approach to risk assessment.

By adopting these practices, organisations can enhance their ability to identify potential cyber-attacks proactively within event-based cybersecurity risk assessment. This study highlights the importance of integrating collaboration, historical insights, current trends, and authoritative references into event-based cybersecurity risk assessments, providing a comprehensive and adaptive approach for mitigating evolving cyber threats.

VI. Limitations

This study is subject to several limitations. First, it employed a qualitative research design, relying on semi-structured interviews with ten cybersecurity experts. Although the participants were carefully selected for their expertise and experience, the relatively small sample size may constrain the generalisability of the findings to the broader organisational context. Second, the study's reliance on self-reported data introduces the potential for biases, such as recall bias and social desirability bias, which could influence the accuracy of the responses.

Future research could expand the sample size to include a broader and more diverse range of stakeholders across multiple organisations. In addition, incorporating quantitative methods or a mixed-methods approach could offer more robust validation and enable better triangulation of data. To address potential biases in self-reported data, future research could incorporate direct observations, document analysis or simulation-based assessments to complement interview findings.

VII. Conclusion

This study explored how organisations identify potential cyber-attacks within an event-based cybersecurity risk assessment framework. Through qualitative analysis of interviews with ten cybersecurity experts, key practices and considerations were uncovered. The findings reveal that organisations rely on a combination of brainstorming and collaboration, leveraging historical data, staying updated on current trends, and using established frameworks such as ISO/IEC 27005, supplemented with dynamic threat intelligence platforms like MITRE ATT&CK. These practices highlight the importance of a multifaceted and proactive approach to managing cybersecurity risks.

The study contributes to both theory and practice by addressing the gap in understanding how organisations identify cyber threats within an event-based risk assessment context. It emphasises the value of integrating static and dynamic resources, fostering cross-departmental collaboration, and maintaining a forward-looking approach to mitigate evolving cyber threats. These insights provide a practical roadmap for organisations aiming to enhance their cybersecurity risk assessment strategies and align them with the demands of an ever-changing threat landscape.

Acknowledgment

We greatly appreciate the Public Service Department of Malaysia (JPA), for sponsoring this study.

Conflict of Interest

The authors declare that there is no conflict of interest

References

[1] M. Z. S. Mohd Nasharuddin and A. Abubakar, "Analyzing Threat Level of the Backdoor Attack Method for an Organization's Operation," *International Journal on Perceptive and Cognitive Computing*, vol. 10, no. 2, pp. 51–59, Jul. 2024, doi: 10.31436/ijpcc.v10i2.484.

[2] V. B. Krishtanosov and N. A. Brovko, "Conceptual-Analytical Approaches to Threats in the Digital Economy," *AlterEconomics*, vol. 20, no. 1, pp. 216–245, 2023, doi: 10.31063/AlterEconomics/2023.20-1.11.

[3] A. Sukumar, H. A. Mahdiraji, and V. Jafari- Sadeghi, "Cyber risk assessment in small and medium- sized enterprises: A multilevel decision- making approach for small e- tailors," *Risk Analysis*, vol. 43, no. 10, pp. 2082–2098, Oct. 2023, doi: 10.1111/risa.14092.

[4] J. Chen, Q. Zhu, and T. Başar, "Dynamic Contract Design for Systemic Cyber Risk Management of Interdependent Enterprise Networks," *Dyn*

Games Appl, vol. 11, no. 2, pp. 294–325, Jun. 2021, doi: 10.1007/s13235-020-00363-y.

[5] P. Lau, L. Wang, Z. Liu, W. Wei, and C.-W. Ten, "A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability," *IEEE Transactions on Power Systems*, vol. 36, no. 6, pp. 5512–5524, Nov. 2021, doi: 10.1109/TPWRS.2021.3078730.

[6] NIST, "NIST SP 800-30: Guide for Conducting Risk Assessments," *U.S. Department of Commerce*, 2012, doi: 10.6028/NIST.SP.800-30r1.

[7] ISO/IEC, "ISO/IEC 27005: Information Security, Cybersecurity and Privacy Protection-Guidance on Managing Information Security Risks," 2022. Accessed: Apr. 14, 2025. [Online]. Available: https://www.iso.org/standard/80585.html

[8] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020, doi: 10.1109/ACCESS.2020.2968045.

[9] Z. Amin, "A practical road map for assessing cyber risk," *J Risk Res*, vol. 22, no. 1, pp. 32–43, Dec. 2019, doi: 10.1080/13669877.2017.1351467.

[10] N. N. Abdul Molok, S. Chang, and A. Ahmad, "Disclosure of Organizational Information on Social Media: Perspectives from Security Managers," *Pacific Asia Conference on Information Systems (PACIS)*, 2013, [Online]. Available: http://aisel.aisnet.org/pacis2013/108

[11] V. Braun and V. Clarke, *Thematic Analysis - A practical guide*. SAGE publications, 2022.

[12] M. B. Miles, A. M. Huberman, and J. Saldana, *Qualitative Data Analysis: A Methods Sourcebook*, 4th Edition. SAGE Publications, 2018.

[13] NIST SP 800-37, "NIST 800-37 : Risk management framework for information systems and organizations," Gaithersburg, MD, Dec. 2018. doi: 10.6028/NIST.SP.800-37r2.

[14] M. E. Whitman and H. J. Mattord, *Management Of Information Security*, Sixth Edition. 2018.

[15] A. A. Elmarady and K. Rahouma, "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment," 2021, doi: 10.1109/ACCESS.2021.3121230.

[16] D. Fujs, A. Mihelič, and S. L. R. Vrhovec, "The power of interpretation: Qualitative methods in cybersecurity research," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2019. doi: 10.1145/3339252.3341479.

[17] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches.*, 4th Edition. SAGE Publication, 2016.

[18] S. Döringer, "'The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge," *Int J Soc Res Methodol*, vol. 24, no. 3, pp. 265–278, 2021, doi: 10.1080/13645579.2020.1766777.

[19] K. Malterud, V. D. Siersma, and A. D. Guassora, "Sample Size in Qualitative Interview Studies," *Qual Health Res*, vol. 26, no. 13, pp. 1753–1760, Nov. 2016, doi: 10.1177/1049732315617444.

[20] J. W. , Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches.* . Sage publications., 2017.

[21] S. Nifakos *et al.*, "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," *Sensors*, vol. 21, no. 15, p. 5119, Jul. 2021, doi: 10.3390/s21155119.

[22] H. M. Melaku, "Context-Based and Adaptive Cybersecurity Risk Management Framework," *Risks*, vol. 11, no. 6, Jun. 2023, doi: 10.3390/risks11060101.

[23] Z. R. Pitafi and T. M. Awan, "Perspective Chapter: Cybersecurity and Risk Management—New Frontiers in Corporate Governance," in *Corporate Governance - Evolving Practices and Emerging Challenges [Working Title]*, IntechOpen, 2024. doi: 10.5772/intechopen.1005153.

[24] S. O. Dawodu, O. Adedolapo, A. Odunayo Josephine, A. Abimbola Oluwatoyin, and E. Sarah Kuzankah, "Cybersecurity Risk Assessment In Banking: Methodologies And Best Practices," *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 220–243, Dec. 2023, doi: 10.51594/csitrj.v4i3.659.

[25] S. Krenn, P. Cheimonidis, and K. Rantos, "Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review," 2023, doi: 10.3390/fi15100324.

[26] A. Y. Abohatem, A. A. Al-Khulaidi, and F. M. M. Ba-Alwi, "Suggestion Cybersecurity Framework (CSF) for Reducing Cyber-Attacks on Information Systems,", vol. 1, no. 3, Sep. 2023, doi: 10.59628/jast.v1i3.248.

[27] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Pap Risk Insur Issues Pract*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[28] D. J. Ferreira, N. Mateus-Coelho, and H. S. Mamede, "Methodology for Predictive Cyber Security Risk Assessment (PCSRA)," *Procedia Comput Sci*, vol. 219, pp. 1555–1563, Jan. 2023, doi: 10.1016/J.PROCS.2023.01.447.

[29] A. Bayewu, Y. Patcharaporn, O. S. Folorunsho, and T. P. Ojo, "An In-depth Review of Cybersecurity Controls in Mitigating Legal and Risk-Related Challenges," *Advances in Multidisciplinary and scientific Research Journal Publication*, vol. 8, no. 4, pp. 1–10, Dec. 2022, doi: 10.22624/AIMS/SIJ/V8N4P1.

[30] I. Naseer, "Machine Learning Applications in Cyber Threat Intelligence: A Comprehensive Review," *The Asian Bulletin of Big Data Management*, vol. 3, no. 2, pp. 190–200, Jan. 2024, doi: 10.62019/abbdm.v3i2.85.

[31] J. Ophoff and A. Berndt, "Exploring the Value of a Cyber Threat Intelligence Function in an Organization," pp. 96–109, 2020, doi: 10.1007/978-3-030-59291-2_7ï.

[32] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," *Sensors*, vol. 21, no. 9, p. 3267, May 2021, doi: 10.3390/s21093267.

[33] G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, "Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns," *IEEE Access*, vol. 8, pp. 128440–128475, 2020, doi: 10.1109/ACCESS.2020.3007960.

[34] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Comput Appl*, vol. 34, no. 18, pp. 15241–15271, Sep. 2022, doi: 10.1007/s00521-022-06959-2.