Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 4, 2025

CYBERSECURITY RISK MANAGEMENT IN THE DIGITAL ERA: THE STRATEGIC VALUE OF ETHICAL HACKING

[1]Usman Imtiaz, [2]Dr. Hammad Elbedour
[1]*Cybersecurity, Washington University of Science and Technology (WUST), Virginia, USA*
[2]*Cybersecurity, Washington University of Science and Technology (WUST), Virginia, USA*
[1]usmanimtiaz1992@gmail.com, [2]mailto:hammad.elbedour@wust.edu

DOI: https://doi.org/

Keywords
Cybersecurity Risk Management, Ethical Hacking, Penetration Testing, Cyber Threats, Information Security, Risk Management, Digital Security

Article History
Received on 22 March, 2025
Accepted on 15 April, 2025
Published on 17 April, 2025

Corresponding Author: *

Abstract
Purpose: This study examines the application of ethical hacking in enhancing cybersecurity risk management in the information age. This research aims to evaluate the level of awareness about cybersecurity, use of ethical hacking, its effectiveness in terms of security improvement and issues faced. Design/Methodology/Approach: The current research employed a quantitative approach, primary data was collected via a questionnaire from 320 professionals from various industries. Convenience sampling was applied and the data was analysed statistically in terms of frequencies and percentages. The measurement tool has been proven to be reliable through Cronbach's Alpha (α = 0.86). Findings: The results of the study reveal employees are highly aware (78.1%) of cybersecurity, but the use of sophisticated cybersecurity technologies such as ethical hacking is average (59.4%). The research also reveals that the majority (75%) see the value of ethical hacking in enhancing security. The study reveals that the primary barriers to adopting ethical hacking include cost (37.5%) and a lack of expertise (28.1%) followed by management and regulatory barriers. Research Implications: The study shows a cybersecurity knowledge and practice gap. It implies that companies need to take an active approach, such as ethical hacking, to improve cybersecurity and deal with the new cybersecurity risk factors. Practical Implications: Organisations should increase their cybersecurity investments, training and use ethical hacking in risk management. Improving management support and leveraging the latest technologies can improve the effectiveness of ethical hacking. Originality/Value: This research contributes to the body of knowledge on using ethical hacking as a cybersecurity risk management strategy by providing empirical evidence on the application, benefits and challenges of ethical hacking in the digital era.

Introduction

Organisations are operating, communicating and generating value in the digital environment. The growing use of interconnected systems, cloud computing and Internet of Things (IoT) devices exposes organisations to cybersecurity attacks [1]. Cybersecurity attacks are no longer just isolated, but increasingly sophisticated, persistent and profit-driven attacks that can interfere with an organisation's operations, steal valuable data and damage reputation [2]. This has led to the strategic nature of cybersecurity risk management.

Organisations now need to protect themselves not just through traditional techniques like firewalls and antivirus in the digital world [3]. Cybercriminals are constantly devising new methods to exploit vulnerabilities in technology, software and humans. To adapt to this evolving threat environment, organizations need to take a proactive and dynamic approach to risk identification, assessment and management [4]. Cybersecurity risk management offers a framework to identify and understand cybersecurity threats and mitigation strategies to manage risks [5].

A key technique in today's cybersecurity landscape is penetration testing or ethical hacking [6]. Ethical hacking involves "hacking" to find vulnerabilities that can be exploited. Ethical hackers can identify vulnerabilities that may not be found in traditional security assessments by thinking like a hacker [7]. This enables organisations to build their security and security posture.

Ethical hacking is useful for more than the technical aspect of vulnerability assessment [8]. It aids in risk management by identifying possible attack vectors, vulnerabilities and weaknesses [9]. Organisations can improve their ability to detect, respond to and prevent cyber attacks through the inclusion of ethical hacking in their cybersecurity strategies [10]. It also helps organisations meet regulatory compliance and establishes trust and confidence among customers and stakeholders by showing they have a proactive approach to security [11].

But there are challenges in adopting ethical hacking. Limited budget, resources and understanding of the benefits may prevent organisations from adopting ethical hacking [12]. Sometimes managers may consider ethical hacking to be an unnecessary expense [13]. And the effectiveness of ethical hacking depends on how it is done, how frequently it is done, and how it is integrated into risk management [14].

The aim of this research is to examine the application of ethical hacking in cybersecurity risk management in the digital era. The aim is to understand the awareness of cybersecurity risks, the use of ethical hacking and the impact of ethical hacking on cybersecurity. It also investigates the barriers to adopting ethical hacking and motivations for adopting it.

The research provides an industry overview of cybersecurity and ethical hacking practices and attitudes. It adds to the understanding of using ethical hacking as a proactive approach to risk management. In the end, this study highlights the importance of proactive cybersecurity and that organisations should use ethical hacking as part of their cybersecurity strategy to counter the dynamic threat landscape.

Problem Statement

Cybersecurity in the digital age is complex and ever-evolving and organisations are struggling to be proactive in cybersecurity. Although ethical hacking has proven to be successful in detecting vulnerabilities, its use in organisations is not consistent. The cost, lack of training and management on-boarding are the reasons for this. And there is no clear understanding about the role of ethical hacking in improving cybersecurity risk management. Companies continue to adopt traditional security controls, which may not be adequate to combat cybersecurity risks. This calls for an evaluation of ethical hacking in the organisational security strategy.

Literature Review

Cybersecurity Risk Management

Cyber security risks form part of an organisation's strategy in the digital world [15]. This involves risk identification, vulnerability management and risk mitigation [16]. Organisations are recognising cybersecurity risks can affect their financial, operational and reputational performance [17]. Risk management should be multidimensional, integrating technological, policy and human considerations.

Modern risk management practices include continuous monitoring and assessment [18]. The evolving nature of cyber threats demands agile measures that may apply to different vulnerabilities and threats [19]. This has led to the adoption of technologies such as artificial intelligence and machine learning to detect and manage risk.

Ethical Hacking and Penetration Testing

Ethical hacking is required to identify security vulnerabilities in the system by simulating attacks [20]. Ethical hacking is a proactive approach to security testing, in contrast to traditional security testing [21]. This helps organisations to understand the security risks and vulnerabilities.

Ethical hacking is penetration testing, which is a proactive approach to testing the vulnerabilities of systems, networks and applications. It helps find vulnerabilities and prioritise security controls [22]. Penetration testing is a cybersecurity best practice because it allows organisations to stay ahead of the hackers.

Strategic Value of Ethical Hacking

The value of ethical hacking in a strategic sense is as an aid to decision-making and risk management [23]. It provides insights into vulnerabilities and helps develop security plans [24]. This allows the focus of effort and resources to combat risks.

Moreover, ethical hacking helps achieve regulatory compliance. Many standards and regulations specify regular testing, like penetration testing [25]. Compliance with standards not only reduces the risk of legal exposure but it also enhances security and trust.

Challenges in Implementation

The benefits of using ethical hacking are many, but its implementation comes with challenges. The expenses of hiring qualified people and conducting frequent tests are high [26]. It can be difficult for small and medium-sized enterprises to find funds to focus on cybersecurity [27].

Moreover, there is a shortage of cybersecurity practitioners. There are not enough ethical hackers to be able to form security teams [28]. Also, a lack of management support can be a barrier to adopting ethical hacking.

Future Trends in Cybersecurity

Cybersecurity issues are becoming more complex. The digital transformation requires advanced and proactive security. The advent of ethical hacking will be more common for risk mitigation [29].

Technologies such as artificial intelligence and automation will improve the use of ethical hacking. This can help to speed up the identification of vulnerabilities to allow for timely risk mitigation. Therefore, ethical hacking will remain an important part of cybersecurity risk management.

Research Questions

1. What is the level of cybersecurity awareness among organizations?
2. To what extent is ethical hacking adopted in organizations?
3. How effective is ethical hacking in improving cybersecurity risk management?
4. What are the major challenges in implementing ethical hacking?
5. Does ethical hacking significantly reduce cybersecurity risks?

Research Objectives

1. To assess the level of cybersecurity awareness among respondents
2. To examine the adoption of ethical hacking practices in organizations
3. To evaluate the effectiveness of ethical hacking in risk management
4. To identify key challenges faced in implementing ethical hacking
5. To analyze the impact of ethical hacking on reducing cybersecurity risks

Methodology

Research Design

This paper uses a quantitative research approach to explore the use of ethical hacking in cybersecurity risk management. The method is descriptive and analytical in nature to explore relationships, patterns and perceptions among the respondents about cybersecurity practices. A quantitative approach was chosen to facilitate statistical analysis of the data, as well as to objectively assess the research questions.

Data Collection Method

The data collection method used is questionnaire with close ended questions. This questionnaire aimed to gather information about cybersecurity awareness, risk mitigation, practice of ethical hacking, effectiveness of ethical hacking, challenges and future of ethical hacking. The close-ended questions had fixed response options and were statistically analysed.

Sampling Technique and Sample Size

The sampling technique used in the study was convenience sampling, with a focus on those having knowledge or experience in cybersecurity. The sample size of 320 surveyed was sufficient. The sample included IT professionals, security analysts, managers, students and other to include various groups.

Instrument Design

The questionnaire included a number of sections to capture the variables. Each variable (cybersecurity awareness, risk management and successful ethical hacking) was measured using a range of items. The responses were obtained in the form of categorical data and, where necessary, through a Likert scale to understand the response's perception and attitude.

Data Analysis Techniques

The analysis of the data used descriptive statistics (frequency and percentage) to provide a description of the characteristics of the sample and the variables of interest. Further, a reliability test (Cronbach's Alpha) was used to test the instrument's reliability. An instrument coefficient of 0.86 suggests that it is highly reliable and it can be analysed.

Ethical Considerations

The research was conducted with voluntary participation of the respondents and their data was maintained in confidentiality. No identifying information was gathered, and the data was only used for research purposes. The study provided participants with information about the research, maintaining integrity and ethical standards throughout the study.

Results

In the results section, the findings of the study are presented, based on the analysis of the data. This section presents the main findings without interpretation, employing tables, figures and statistical parameters such as mean, percentage and standard deviation. This section reports findings of patterns, associations and important trends in the data, tackling the research questions and objectives.

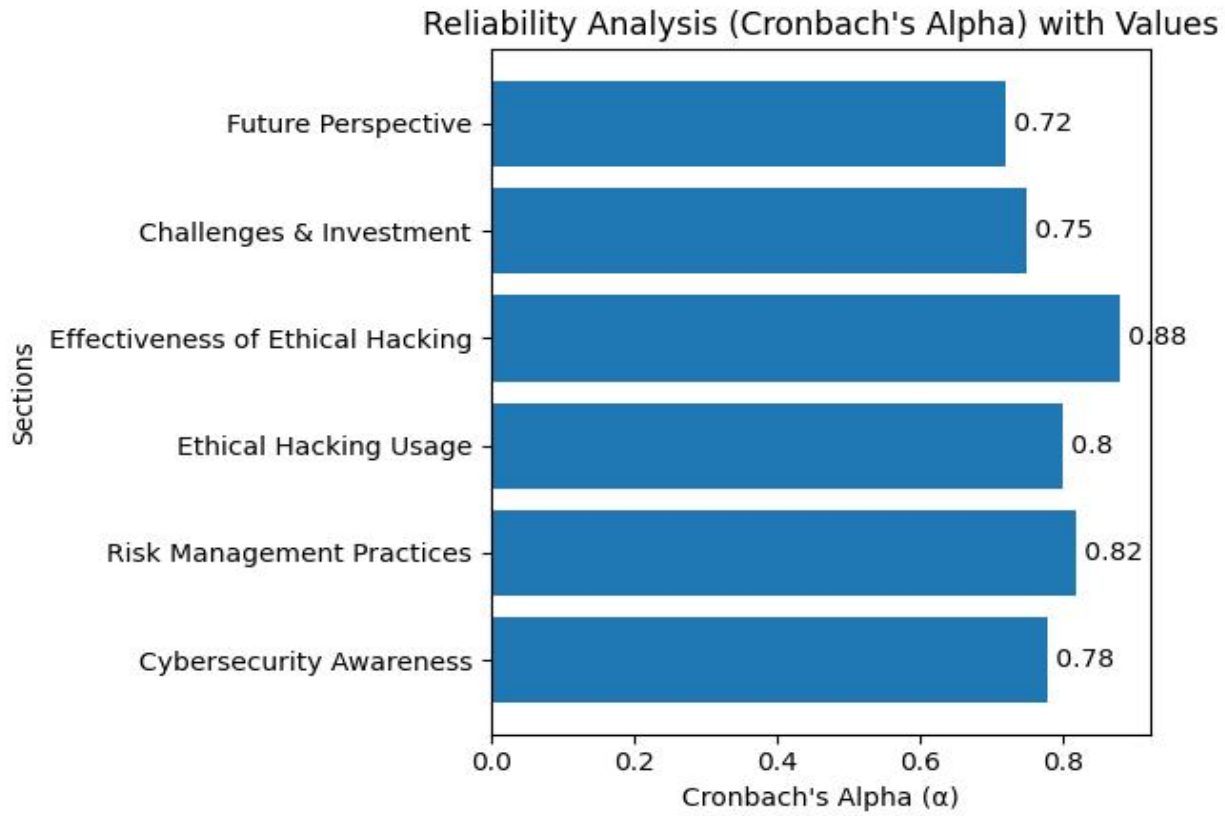

Fig 1: Reliability Test

The reliability analysis shows that the measurement tool is statistically reliable and internally consistent for all the constructs. The Cronbach's Alpha of 0.86 for the entire scale is very high, confirming that the scale is reliable and measures the concept of cybersecurity risk management.

At the construct level, Effectiveness of Ethical Hacking has the highest internal consistency ($\alpha = 0.88$), suggesting that the participants were very consistent in their understanding and responses to these items. Similarly, Risk Management Practices ($\alpha = 0.82$) and

Ethical Hacking Usage (α = 0.80) have good reliability, suggesting the constructs are reliable.

The constructs Cybersecurity Awareness (α = 0.78), Challenges & Investment (α = 0.75) and Future Perspective (α = 0.72) are relatively reliable, implying that, while less consistent, these are acceptable. But while these are slightly lower than the acceptable level, they still meet the acceptable level (α ≥ 0.70) and therefore, can be considered for further analysis.

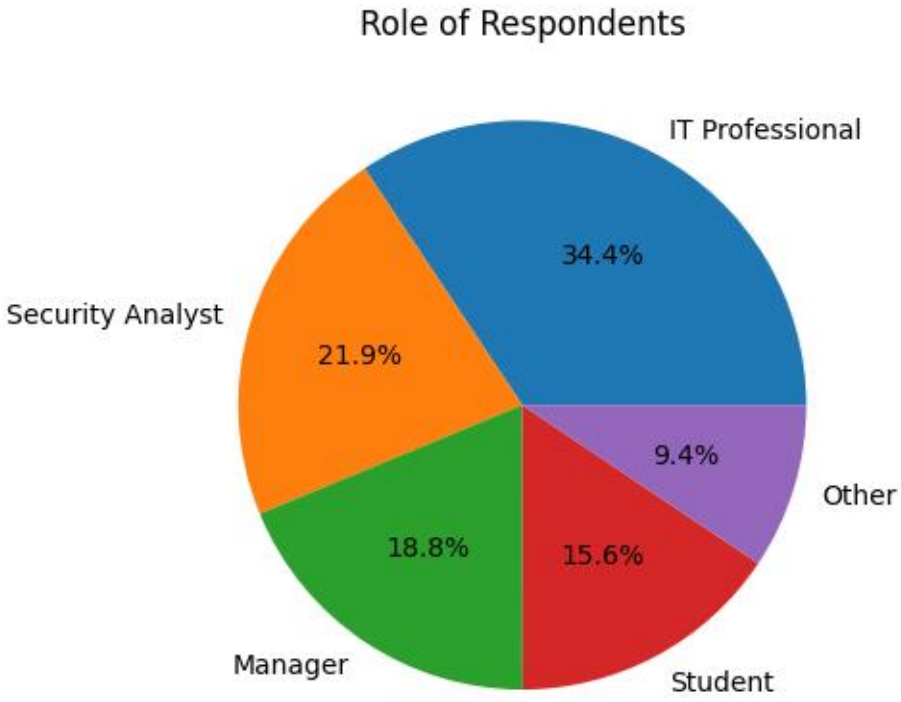

Fig 2: Role of Respondents

The profile of the respondents suggests that the sample is mainly of people who have technical and professional experience in cybersecurity. The largest group of respondents are IT Professionals (34.4%) so the results of the survey are largely weighed in favour of those with technical cybersecurity experience.

The next largest group is Security Analyst (21.9%) who are also involved in cybersecurity and threat analysis and therefore also provides technical validation of the results. Managers (18.8%) offer a management view, and provide insight into governance.

The inclusion of Students (15.6%) provides the student view on the study and presents the perceptions of future generations. For their part, the "Other" (9.4%) ensures representation by including respondents from other or unspecified backgrounds.

Overall, study respondents are a mix of technicians, managers, and students who bring a range of technical and managerial skills, making it a valid study.

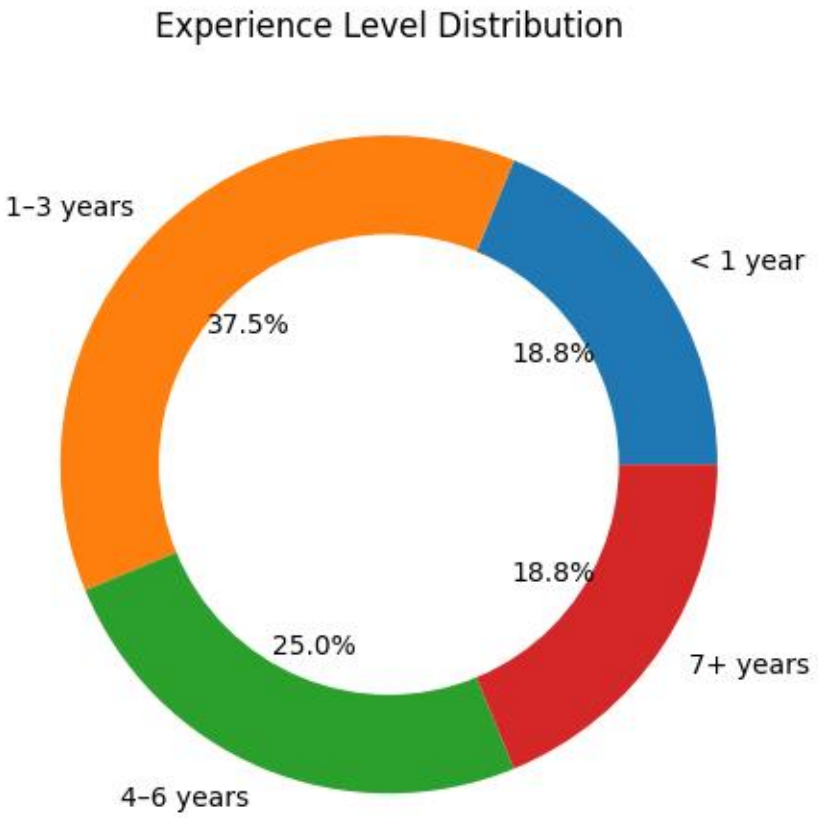

Fig 3: Experience Level Distribution

The mix of experience of the respondents is a middle-aged sample, but with a strong mid-career representation. Most have 1-3 years of experience (37.5%) which indicates that the study is strongly influenced by respondents who have cybersecurity experience.

Those with 4-6 years (25.0%) have more experienced insights, and represent experienced cybersecurity professionals. However, those with less than 1 year (18.8%) are early career and bring their more recent academic learning.

Similarly, those with 7+ years of experience (18.8%) bring seasoned viewpoints, and contribute more experienced and strategic insights to the data.

Overall, the sample is comprised of a balanced representation of experience levels with a slight tilt towards early-career. This enhances the ability of the study to capture both emerging trends and experiential perspectives in cybersecurity.

Table 1: ***Cybersecurity Awareness and Practices***

Item	Response	Frequency	Percentage
Awareness of Cybersecurity Risks	Yes	250	78.1%
	No	70	21.9%
	Total	320	100%
Cybersecurity Training Availability	Yes	233	68.8%
	No	87	31.3%

	Total	320	100%
Risk Management Strategy	Yes	221	62.5%
	No	99	21.9%
	Total	320	100%
Use of Ethical Hacking	Yes	240	59.4%
	No	80	25.0%
	Total	320	100%

This research indicates that respondents are aware of cybersecurity and use basic cybersecurity practices. The high percentage (78.1%) of respondents who reported being aware of cybersecurity risks, indicates that awareness of cybersecurity risks and threats is common. Training and practices include 68.8% who said they have cybersecurity training in their organisation. This is a good thing and training initiatives are required.

The use of formal risk management techniques (62.5%) indicates that most of the organisations are involved in risk management. But this is lower than the awareness of these, suggesting a knowledge gap.

Likewise, 59.4% of the survey participants reported carrying out ethical hacking, which suggests moderate integration of advanced cybersecurity measures. This indicates organisations appreciate the importance of advanced cybersecurity practices, but it is still an evolving practice.

In summary, the survey responses show that there is a high awareness, but moderate use of advanced security practices, suggesting the need for organisations to enhance their cybersecurity practices.

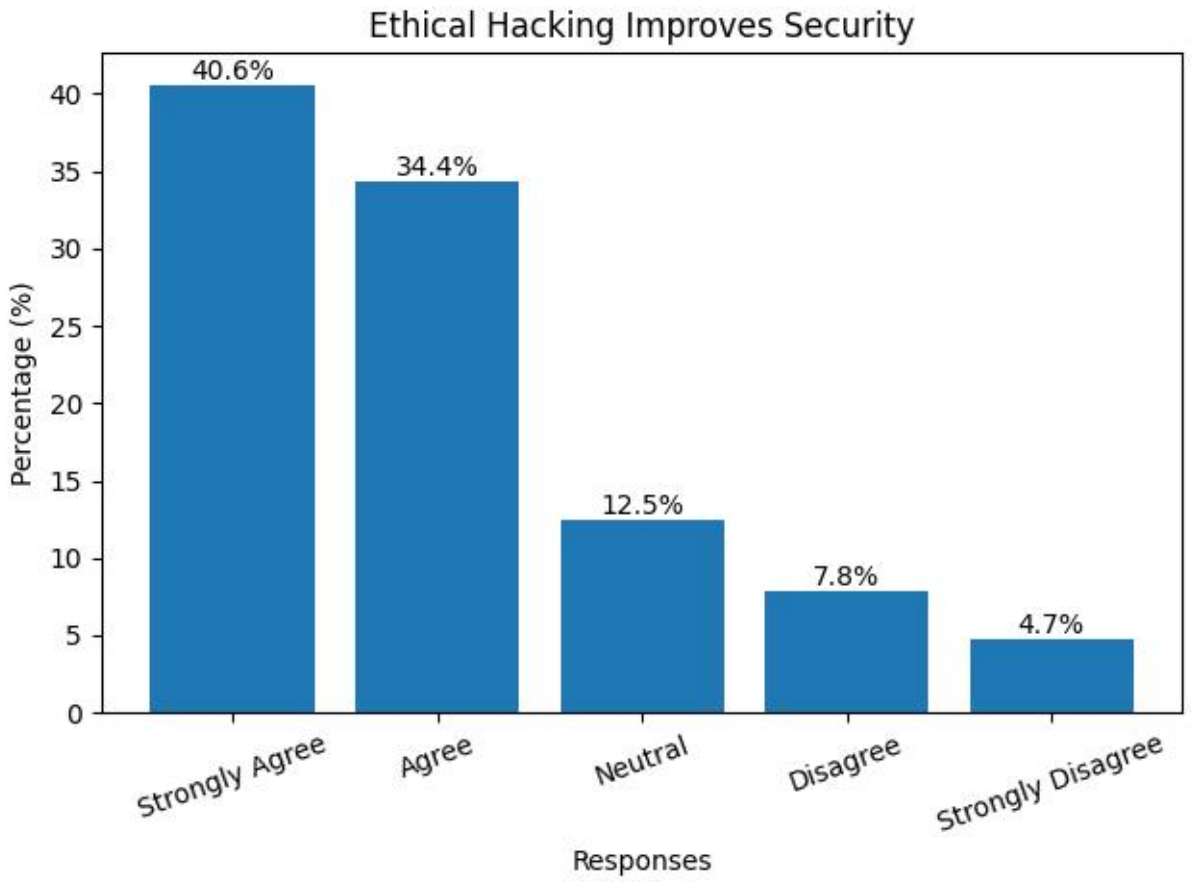

Fig 4: Ethical Hacking Improves Security

There is a positive view about the benefits of ethical hacking. The vast majority (75.0%) strongly agree (40.6%) or agree (34.4%) that ethical hacking improves security, which implies that people have a high faith in the value of ethical hacking.

A small number are unsure (12.5%), perhaps due to inexperience, or scepticism about its effectiveness. However, a few (12.5%) disagree which suggests that they are not against the practice of ethical hacking or sceptical about the value of ethical hacking.

In summary, the survey findings indicate a strong agreement that ethical hacking improves cybersecurity, and confirm the value of ethical hacking in contemporary risk management and security strategies in organisations.

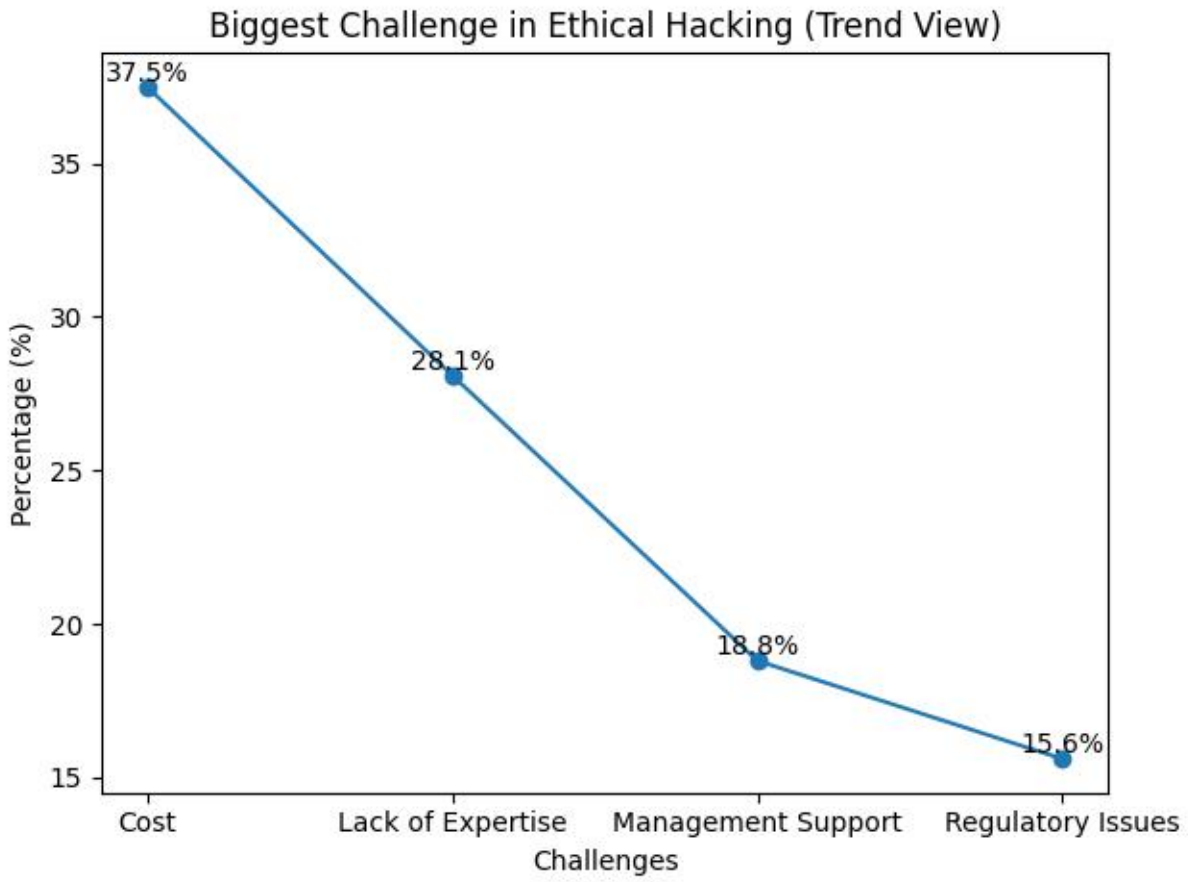

Fig 5: Biggest Challenge in Ethical Hacking

According to the survey, the biggest obstacle for organisations to implement ethical hacking is cost (37.5%), which suggests that the main reason organisations cannot implement ethical hacking is related to cost. This implies that while organisations may see the benefits, they may not be able to afford top-notch cybersecurity initiatives.

The second most common challenge is lack of expertise (28.1%) which is a lack of cybersecurity skills. This implies there is a lack of professionals who can conduct ethical hacking.

Lack of management support (18.8%) is another big challenge and it could indicate a lack of understanding or support from managers for ethical hacking.

Finally, the regulatory challenges (15.6%) are the least attended but still important, which suggests legal and regulatory issues may affect ethical hacking and its adoption, but are not as constraining as the cost and human resource challenges.

Overall, the results suggest that cost and a lack of skills are the major concerns, but management and regulatory concerns are less restrictive but still important for implementing ethical hacking.

Discussion

The findings from this study confirm the growing focus on proactive cybersecurity in the digital era, particularly the use of ethical hacking to improve cybersecurity. The respondents' perception of cybersecurity issues is in line with other studies that indicate that modern organisations are more knowledgeable about emerging cyber threats, and the impact of cybersecurity on their operational efficiency and data integrity [1], [2]. But our study reveals a gap between awareness and management, highlighting the belief that traditional security measures are ineffective to protect against sophisticated attacks [3], [4].

The relatively low level of ethical hacking reveals a stage in the evolution of cybersecurity risk management. Although ethical hacking is recognised by most respondents as effective, its adoption is low. This is in line with previous studies that recognise ethical hacking offers a proactive approach to detect

vulnerabilities not identified by traditional security measures [20], [21]. The consensus on its effectiveness among the respondents also supports its strategic importance in increasing organisational readiness and supporting decision-making [23], [24].

However, the research shows that there are significant challenges to adopting ethical hacking, namely cost and technical expertise. These issues are commonly cited in the literature, where cost and lack of expertise are acknowledged as significant barriers to implementing state-of-the-art cybersecurity measures [26], [28]. Furthermore, while not as significant, the support of management is important as it affects resource allocation and strategy [13].

The respondents' experience level, which is skewed towards early- to mid-career practitioners, indicates the results capture both the latest and the applied views in cybersecurity. This adds to the credibility of the findings and confirms that a blend of technical and strategic skills is crucial to effective cybersecurity risk management.

Overall, our study supports the argument that ethical hacking is an important component of cybersecurity risk management. But they can only achieve this potential if the challenges of cost, human resource issues and organisational support are overcome. The growing cyber threats, should make it imperative to include ethical hacking in risk management plans to develop effective security strategies [14], [29].

Conclusion and Recommendations

The research findings demonstrate that cybersecurity risk management is crucial in the digital age due to the dynamics of cyber risks. This research reveals that although the respondents are cybersecurity aware, they have average knowledge in the use of current cybersecurity frameworks, such as ethical hacking. This knowledge-practice gap presents a security challenge. The respondents' strong awareness of the benefits of ethical hacking shows that it is an effective tool for vulnerability detection and enhancing security. But it is limited by integration factors, such as its cost, skill gap and management buy-in, which inhibit its integration into the security process.

Based on the insights gained, some recommendations can be made for cybersecurity risk management. Organisations should consider ethical hacking as a core component of cybersecurity and not as an add-on. Cybersecurity resources, especially training and development, should be expanded to overcome the lack of cybersecurity professionals and to build their skills. We should also see an increased awareness and commitment from managers to cybersecurity, who should ensure they have the resources to tackle cyber threats.

Finally, companies should conduct regular penetration testing and continuous monitoring to prevent cyber attacks. Governments and regulators also need to promote compliance and adopt an ethical hacking code of conduct. Finally, new technologies such as automation and artificial intelligence should be used for cybersecurity. In conclusion, ethical hacking with adequate resources, staff and support from management is essential to ensure safe and proactive cybersecurity practices in the digital era.

References

[1] A. Rayhan, "Cybersecurity in the digital age: Assessing threats and strengthening defenses," in *Proc. Cybersecurity Awareness Conf.*, Apr. 2024, pp. 1–26.

[2] F. Mızrak, "Integrating cybersecurity risk management into strategic management: A comprehensive literature review," *Res. J. Bus. Manage.*, vol. 10, no. 3, pp. 98–108, 2023.

[3] E. M. Onyema *et al.*, "Cyber threats, attack strategy, and ethical hacking in telecommunications systems," in *Security and Privacy in Cyberspace*. Singapore: Springer, 2022, pp. 25–45.

[4] N. Allahrakha, "Balancing cyber-security and privacy: Legal and ethical considerations in the digital age," *Legal Issues in the Digital Age*, no. 2, pp. 78–121, 2023.

[5] N. M. A. Chisty, P. R. Baddam, and R. Amin, "Strategic approaches to safeguarding the digital future," *Engineering International*, vol. 10, no. 2, pp. 69–84, 2022.

[6] S. M. H. Shah, F. Amin, and A. Khan, "Cyber-resilient mobile edge computing: A deep neural approach," *Asian Bull. Big Data Manage.*, vol. 5, no. 1, pp. 200–215, 2025.

[7] F. Amin *et al.*, "The tokenized business marketplace," *Int. J. Bus. Manage. Sci.*, vol. 5, no. 4, pp. 318–328, 2024.

[8] L. Smith, M. M. Chowdhury, and S. Latif, "Ethical hacking: Skills to fight cybersecurity threats,"

EPiC Series Comput., vol. 82, no. 5, pp. 102–111, 2022.

[9] A. Shaheen, "Cybersecurity in the modern era," *J. Eng. Comput. Intell. Rev.*, vol. 1, no. 1, pp. 39–50, 2023.

[10] A. H. K. Choain *et al.*, "Integrating blockchain-enhanced enterprise systems," *J. Eng. Comput. Intell. Rev.*, vol. 1, no. 1, pp. 51–63, 2023.

[11] L. Smith, M. M. Chowdhury, and S. Latif, "Ethical hacking: Skills to fight cybersecurity threats," *EPiC Series Comput.*, vol. 82, no. 5, pp. 102–111, 2022.

[12] N. S. J. Abubakar *et al.*, "Hacking incidents and their long-term implications," *Cognizance J. Multidisciplinary Stud.*, vol. 4, no. 12, pp. 443–454, 2024.

[13] F. Jimmy, "Emerging threats and AI in cybersecurity," *Valley Int. J. Digital Library*, vol. 1, no. 2, pp. 564–574, 2021.

[14] A. Pawlicka *et al.*, "Future of cybersecurity and ethics," *IEEE Access*, vol. 11, pp. 58796–58807, 2023.

[15] M. R. Haque *et al.*, "Liquidity traps and digital currencies," *Inverge J. Soc. Sci.*, vol. 2, no. 3, pp. 148–165, 2023.

[16] A. Mosaddeque *et al.*, "AI and ML in cybersecurity systems," *Inverge J. Soc. Sci.*, vol. 1, no. 2, pp. 70–81, 2022.

[17] M. Shahinuzzaman *et al.*, "Mental health of women breast cancer survivors," *Jagannath Univ. J. Earth Life Sci.*, vol. 5, no. 1, pp. 1–12, 2019.

[18] T. A. Shiva *et al.*, "Optimizing early intervention strategies for neurodiverse children," *Apex J. Soc. Sci.*, vol. 3, no. 1, pp. 30–52, 2024.

[19] M. Almaayah and R. B. Sulaiman, "Cyber risk management in IoT," *STAP J. Security Risk Manage.*, no. 1, pp. 3–23, 2024.

[20] M. Malaga, "Cybersecurity in the digital age," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 9, pp. 10268–10280, 2021.

[21] T. N. E. Al-Tawil, "Ethical implications for teaching hacking," *J. Money Laundering Control*, vol. 27, no. 1, pp. 21–33, 2024.

[22] A. Juneja, S. S. Goswami, and S. Mondal, "Cyber security and digital economy," *J. Technol. Innov. Energy*, vol. 3, no. 2, pp. 1–22, 2024.

[23] K. Agarwal and M. Shah, "Corporate governance in cybersecurity risk management," *LawFoyer Int. J. Doctrinal Legal Res.*, vol. 2, p. 352, 2024.

[24] N. Y. Conteh, "Ethical hacking, threats, and vulnerabilities," in *Ethical Hacking Techniques and Countermeasures*. IGI Global, 2021, pp. 1–18.

[25] Y. He *et al.*, "AI-based ethical hacking for health systems," *J. Med. Internet Res.*, vol. 25, e41748, 2023.

[26] B. Gunawan, B. M. Ratmono, and A. G. Abdullah, "Cybersecurity and strategic management," *Foresight STI Governance*, vol. 17, no. 3, pp. 88–97, 2023.

[27] A. Juneja *et al.*, "Legality of ethical hacking in data mining," in *Proc. Int. Conf. Innovations Data Analytics*, Dec. 2024, pp. 457–467.

[28] K. Kaushik *et al.*, "Ethical considerations in AI-based cybersecurity," in *Next-Generation Cybersecurity*. Singapore: Springer, 2024, pp. 437–470.

[29] R. Gadge *et al.*, "Managing cybersecurity risks in emerging technologies," in *Proc. ICAIQSA*, 2024, pp. 1–9.