Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 2, 2026

STRENGTHENING CYBER DEFENSE THROUGH THREAT INTELLIGENCE: ADDRESSING FINANCIALLY MOTIVATED ATTACKS

Abdul Musawer Zahedi*[1], Latafat Ullah Khan[2], Aziz Khan[3], Zeeshan Khan[4]

[1]School of Computing and Mathematical Sciences, University of Greenwich, London, United Kingdom.
[2]Iqra National University, Peshawar, Pakistan.
[3]School of Computing, Engineering and the Built Environment, University of Roehampton, London, United Kingdom.
[4]Iqra National University, Peshawar, Pakistan
abdulmusawir88@gmail.com , latafatkhan006@gmail.com, khana76@roehampton.ac.uk, zeeshanulhaq022@gmail.com

DOI: https://doi.org/10.5281/zenodo.20593387

Keywords
Threat Intelligence, Cybersecurity, Financially Motivated Cyberattacks, Artificial Intelligence, Threat Detection, Cyber Defense

Article History
Received on 20 May 2026
Accepted on 02 June 2026
Published on 07 June 2026

Corresponding Author: *
Abdul Musawer Zahedi*

Abstract

Background

Organizations are facing great challenges as financially motivated cyberattacks, such as phishing, ransomware, and financial fraud, keep growing and becoming more common. Frequently, traditional cybersecurity methods and solutions are proving inadequate to tackle the new cyber threats, requiring proactive and intelligence-based security strategies. Threat intelligence has become a vital tool for strengthening cyber defense efforts, boosting cyber situational awareness and mitigating operational and financial risk.

Objective

The purpose of this study was to explore how threat intelligence can be used to enhance an organization's cybersecurity response to financially motivated cyberattacks. The study also assessed the workings of AI-based threat detection technologies, organizational preparedness approaches, and threats in implementing threat intelligence frameworks.

Methodology

The research design applied was quantitative research design that was of descriptive and analytical nature. The sample was composed of 310 cybersecurity professionals, IT staff, and network administrators, security managers and executives of different industries. The data collection method used was a structured close-ended questionnaire with 5-point likert scale. Statistical analysis was done using frequencies, percentages, means, standard deviations, Cronbachs Alpha reliability test and chi-square analysis.

Results

It also determined that there was a high level of agreement on the usefulness of threat intelligence in improving cybersecurity defense. Both Financially Motivated Cyber Attacks (M = 4.31, SD = 0.66) and Effectiveness of Threat Intelligence in Cyber Defense (M = 4.24, SD = 0.69) had the highest average scores. Another important point that the respondents agreed upon is that AI integration enhances the threat detection (M = 4.36, SD = 0.61) and phishing attacks still pose a

significant cybersecurity threat (M = 4.42, SD = 0.60). The findings of the reliability check indicated that there is good internal consistency of the scale, with Cronbach Alpha of 0.90. The research also found that there were certain issues with the implementation of the system such as high costs of implementation, shortage of cyber security personnel and the inability to handle a lot of threat data.

Conclusion

The study concludes that threat intelligence, combined with AI and collaborative cybersecurity approaches, can be effective in boosting cybersecurity resilience and organizational cyber defense against financially motivated cyberattacks. Ongoing investments in AI-driven cybersecurity system, staff education, and threat intelligence exchange are crucial for building safe and sustainable cybersecurity environment.

1. INTRODUCTION

Digital technologies and interconnected systems have drastically changed the way businesses operate today. Technology has also given rise to more advanced communication, financial and business tools, but has also exposed to the world the new advanced cyber threats [1]. Of these threats, financial motivated cyberattacks (FMCA) have become one of the most severe and pervasive threats to governments, corporations, healthcare, financial services, and educational institutions around the globe [2]. In recent years, cybercriminals have been targeting digital infrastructures to carry out phishing, ransomware, financial fraud, ID theft and data breaches to generate financial profits [3]. Organizations continue to increasingly depend on cloud computing, artificial intelligence, online banking systems and digital communication platforms, hence the need for more advanced cybersecurity measures is more than ever [4].

Traditional cybersecurity approaches are not enough to handle today's dynamic and evolving nature of cyber threat [5]. Organizations are at risk to disruption of operations and losses due to attackers constantly adjusting their methods to evade traditional security measures [6]. To address these increasing concerns, threat intelligence is now an integral part of modern cybersecurity defense [7]. Threat intelligence is a collection, analysis and interpretation of data on actual and emerging threats. It will assist the organizations to identify malicious activities and forecast attack pattern, and improve the defensive capability prior to the damage being caused.

The integration of threat intelligence into cyber security systems gives organizations a chance to have improved situational awareness and to be more efficient in their incident response [8]. Real-time monitoring systems, predictive analytics, and tools based on artificial intelligence can be used to assist organizations in detecting suspicious activity early and act accordingly [9]. Informed decision making

can also be helped with threat intelligence providing actionable information concerning cyber threats, attacker tactics, and information system vulnerabilities [10]. This is a preemptive approach, which will assist in reducing the threat of effective cyberattacks, along with the possible financial losses, loss of reputation, and lost time.

Hacking techniques, automation, and cybercrime-as-a-service models have become more sophisticated, making financially motivated attacks more complex [11]. Organizations can now be attacked by well organized cybercriminal organizations with regard to their financial and sensitive information [12]. It is specifically this that has led to massive economic losses in most sectors forcing businesses to invest heavily in cybersecurity infrastructure and cybersecurity incident response strategies [13]. Moreover, the rapid adoption of remote working environment and online payment instruments has augmented the attack space of cybercrime.

Organizations are also being asked to develop effective cyber security plans to deal with emerging cyber threats. The development of cyber defense mechanisms is now a necessity that is accompanied by investments in cybersecurity awareness, employee training, AI-based monitoring systems, and threat-sharing programs. Moreover, cooperation between governments and industry and cybersecurity experts is essential to the creation of safe online spaces and the prevention of cybercrime. Thus, to develop long-term cybersecurity strategies to achieve organizational resilience, it is essential to understand its role in countering financially driven cyberattacks.

Problem Statement

Ransomware, phishing and online fraud are increasing, and are seriously affecting organisations financially and operationally all over the world. Many organizations are still using traditional types of cybersecurity that are not adequate to withstand new and advanced cyber threats. Besides the low threat intelligence uptake, there is also a lack of cybersecurity skills and absence of real-time monitoring facilities that further undermine organizational cyber security. Therefore, the potential of threat intelligence should be discussed in order to improve the cybersecurity systems and prevent the threats of financially motivated cyberattacks.

Importance of the Study

The study is significant because it highlights that threat intelligence is becoming increasingly critical to the protection of organizations from financially motivated cyberattacks. The results could help organizations to gauge the success of their proactive cybersecurity efforts, AI-powered monitoring systems, and real-time threat detection capabilities. This study also helps to strengthen cybersecurity policies, enhance the

organizational readiness, and better cyber incident management practices. Moreover, it offers useful information to cybersecurity practitioners, policy makers, researchers, and business stakeholders interested in cyber defense solutions that are sustainable.

Literature Review

Threat Intelligence in Modern Cybersecurity

The complexity of cyber threats has brought threat intelligence as an essential element of the cyber security environment today. Threat intelligence systems help organizations to collect and process data on malicious activity, attacker behaviour and vulnerabilities [14]. This proactive solution will allow cybersecurity units to anticipate potential attacks, enhance their defense, and be better prepared in case of an attack [15]. Efficiency of the threat intelligence is further improved as the AI and machine learning technologies come together where suspicious activities could be automatically identified and analyzed [16].

Financially Motivated Cyber Attacks

One of the most prevalent forms of cyber-crime in the world is financial crimes and financially motivated attacks remain one of the primary forms of cyber-crime [17]. Cybercriminals primarily act out of self-motivation to rob organizations, including ransomware attacks, phishing attacks, banking malware, and online fraud [18]. These attacks may cause financial losses, data breach, operations disruption and reputation damage. The increased use of digital platforms and online financial systems has provided a chance to cybercriminals to exploit system vulnerabilities [19]. This imposes an ongoing pressure on organisations to adopt advanced cyber security measures that can identify and mitigate financial cyber risks.

Role of Artificial Intelligence in Threat Detection

AI has transformed the practice of cybersecurity, enabling it to be more precise and quicker in identifying threats. AI-powered security systems can process large volumes of threat data in real-time and alert to suspicious behavior, which may be an indicator of a cyber attack [20]. AI algorithms have the potential to detect new attack patterns, automate response measures and minimize human errors in cybersecurity. Threat intelligence platforms powered by AI can also enable predictive analysis, and organizations can predict future attacks and be better equipped to deal with cybersecurity threats [21].

Organizational Preparedness and Cybersecurity Strategy

Another critical element of cyber threat protection is the preparedness of an organization. Investments in your security infrastructure, personnel training, and incident response planning should also continue to create effective cybersecurity

measures [22]. A good cybersecurity governance provides a more robust ability to succeed in responding to cyber incidents to a company. Organizations exchange threat intelligence with other organizations and cooperate with cybersecurity experts to increase the defensive capabilities [23]. Nevertheless, to this day, many organisations continue to face issues of limited budgets, obsolete technologies and lack of experience, which have a negative impact on their cybersecurity readiness.

Challenges in Implementing Threat Intelligence

Despite the benefits of using effective threat intelligence systems to organizations, there are a number of challenges that need to be taken into consideration when implementing [24]. Modern cybersecurity tools might not be widely used, especially by small and medium-sized businesses (SMBs), and their implementation and maintenance can be quite expensive. Large amounts of threat data also demand special skills and technology to process and handle [25]. Moreover, the cyber threats are dynamic and organizations can hardly maintain their defense mechanisms current and functional [26]. All these problems underscore the need to adopt continuous innovation, governmental support and joint cybersecurity to ensure organisations become more cyber resilient [27].

Research Questions

1. How does threat intelligence contribute to strengthening organizational cyber defense systems?
2. What are the major financially motivated cyber threats faced by organizations?
3. How effective is threat intelligence in detecting and preventing cyberattacks?
4. What role does artificial intelligence play in improving cybersecurity threat detection?
5. What challenges do organizations face in implementing threat intelligence systems?
6. How can organizations improve cybersecurity preparedness against financially motivated attacks?

Research Objectives

1. To examine the role of threat intelligence in strengthening cybersecurity defenses.
2. To identify major financially motivated cyberattacks affecting organizations.
3. To evaluate the effectiveness of threat intelligence in cyber threat detection and prevention.

4. To analyze the contribution of artificial intelligence to modern cybersecurity practices.
5. To investigate challenges associated with implementing threat intelligence frameworks.
6. To recommend strategies for improving organizational cybersecurity preparedness and resilience.

Methodology

Research Design

The research design employed was a quantitative one in the investigation on the role of threat intelligence in improving the cybersecurity defense against financially-motivated cyberattacks. The perceptions of the respondents to the awareness of threat intelligence, trends of cyberattacks, the preparedness state of the organisations, cybersecurity strategies, and challenges that were identified in the future were analysed using a descriptive and analytical approach. It was decided that quantitative design was appropriate as it allowed for measurable data to be gathered and statistically analysed to identify patterns, relationships and overall trends in cybersecurity practices.

Research Population and Sample

The study population included cybersecurity professionals, IT staff, network administrators, cybersecurity analysts, security managers, and executives in government, private, financial, educational and healthcare organizations. A total of 310 people participated in the study. A purposive sampling technique was employed to make sure that people that have relevant cybersecurity knowledge and profession experience were included in the research process.

Data Collection Instrument

Data collection was done using a structured close ended questionnaire, which was formulated using the study objectives and available literature on cybersecurity. The questionnaire was divided into four sections: Threat Intelligence Awareness and Adoption, Financially Motivated Cyberattacks, Threat Intelligence in Cyber Defense, Organization Preparedness and Cybersecurity Strategy, and Challenges and Future Directions. The perception and opinion of the respondents regarding the practices of cybersecurity and the implementation of cyber threat intelligence was measured on a five point Likert Scale (Strongly Disagree to Strongly Agree).

Validity and Reliability of the Instrument

To achieve validity of the instrument, the questionnaire items were designed using the purpose of the study and the literature on the subject of threat intelligence and cybersecurity defense. Cronbachs Alpha was utilized to achieve reliability analysis in

order to achieve internal consistency of the questionnaire items. The total Cronbachs Alpha was 0.90 which is excellent and all the constructs were above the acceptable level of 0.70 and this means that the instrument was suitable in collecting and analysing data.

Data Collection Procedure

The questionnaire was sent to the respondents who are employed in the sphere of cybersecurity through online resources and professional communication channels. During the study, the participants were made aware of the academic purpose of the study and the responses were maintained in the form of confidentiality. The responses received were analyzed comprehensively, classified and tabulated to be analyzed statistically.

Data Analysis Techniques

Statistical analysis of the data collected was used to evaluate the study aims and research questions. Demographic information and respondents' perceptions were summarized using descriptive statistics such as frequencies, percentages, means, and standard deviations. Reliability analysis was conducted on the questionnaire constructs in terms of Cronbach alpha. Further, a chi-square test was conducted to determine the statistical significance of the views of the respondents regarding the threat intelligence practices and cybersecurity strategies. The findings are given in tables, charts and graphical form to be easily interpreted and understood.

Results

In a research paper, the Results section presents the findings of the study objectivley, i.e. with no interpretation or bias. It represents information collected, which may be presented in tables, graphs, and statistical summaries, and draws conclusions that answer the research questions or hypotheses. This section deals only with discoveries, while the implications and analyses are handled in the Discussion section.

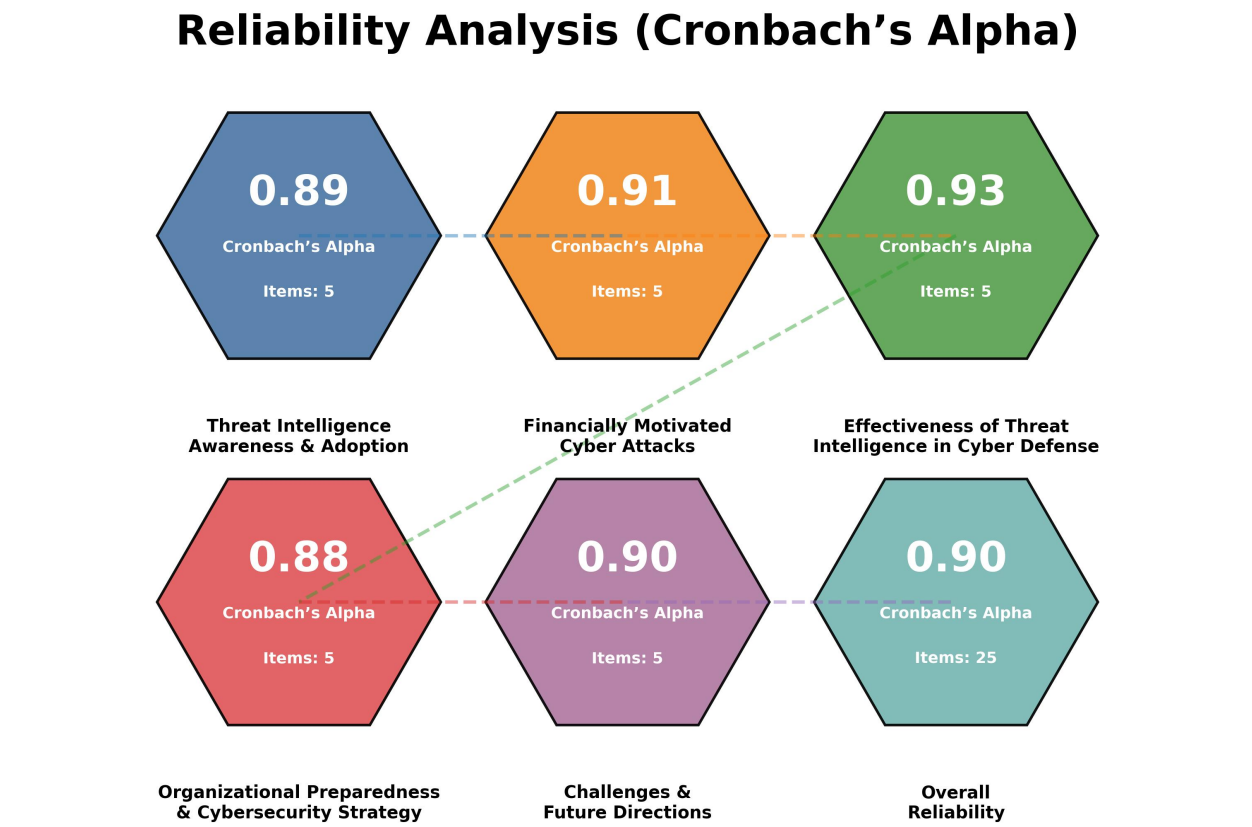

Figure 1: Reliability Analysis

The reliability analysis shows that all the study constructs had a high degree of internal consistency with all Cronbachs Alpha values being above the acceptable level of 0.70. The construct Effectiveness of Threat Intelligence in Cyber Defense had the highest reliability (α= 0.93), which means that the questionnaire items are very consistent. Likewise, Financially Motivated Cyber Attacks (α = 0.91) and Challenges and Future Directions (α = 0.90) had very high reliability. High levels of reliability also were observed in constructs Threat Intelligence Awareness and Adoption (α=0.89) and Organizational Preparedness and Cybersecurity Strategy (α=0.88). The general reliability of the instrument (α= 0.90) ascertains that the questionnaire is quite reliable and can be utilized to measure the perceptions associated with threat intelligence and cybersecurity measures.

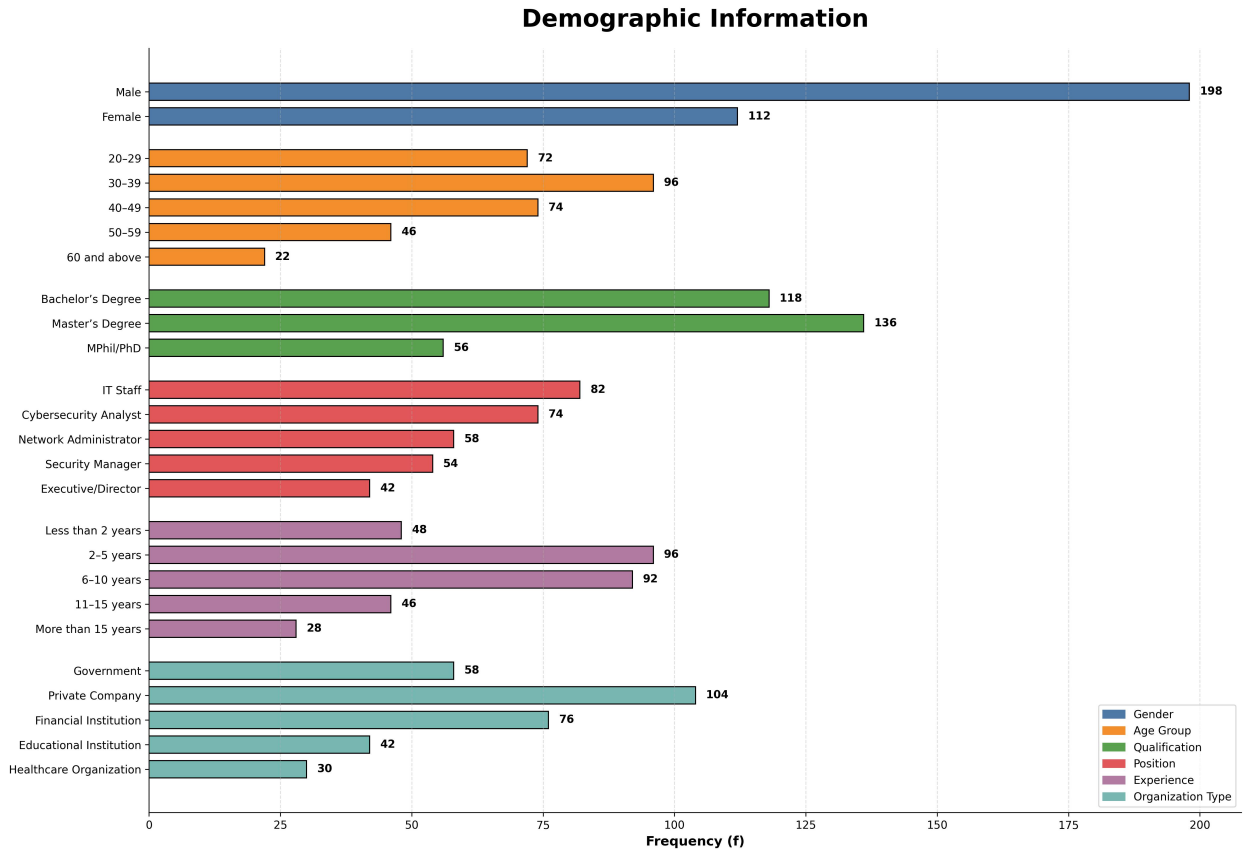

Figure 2: Demographic Information

Demographic analysis shows that the sample was mainly composed of males (63.9%), with females comprising 36.1% of the sample. Majority of the participants represented the 30-39 age group (31.0%), then the 40-49 years (23.9%), and 20-29 years (23.2%) age groups, with mid-career professionals being well represented. Regarding education level, the highest proportion of respondents (43.9%), were Master degree holders, with another significant proportion of 38.1% being Bachelor degree holders indicating a highly educated sample.

In terms of professional roles, the largest percentage was constituted by IT Staff (26.5%), then Cybersecurity Analysts (23.9%), and Network Administrators (18.7%), meaning that the study was mostly able to capture the knowledge of technical cybersecurity professionals. The experience profile showed that most respondents had between 2–5 years (31.0%) and 6–10 years (29.7%) of professional experience, suggesting a balanced representation of early and mid-level practitioners.

In addition, the majority of the respondents worked in Private Companies (33.5%) and Financial Institutions (24.5%),

which indicates a high level of industry involvement in cybersecurity and threat intelligence practices. In general, the demographic composition shows a mixed and highly qualified sample in terms of investigation of the threat intelligence and cybersecurity defense measures.

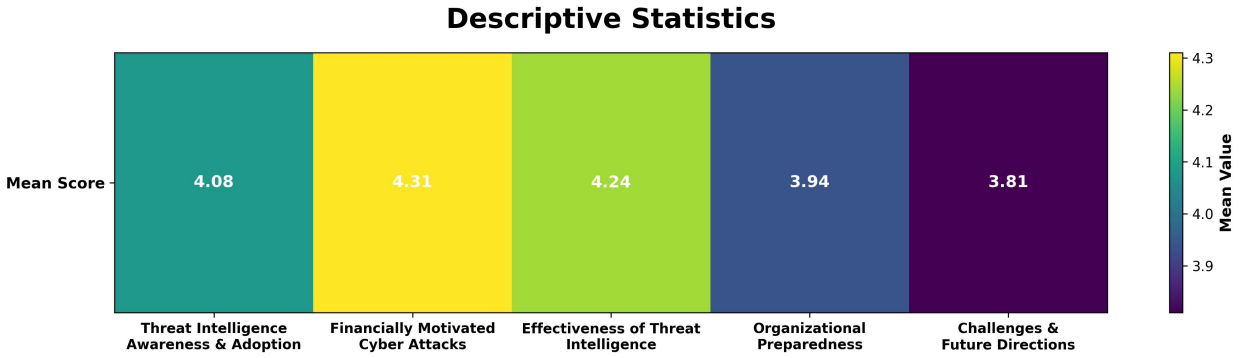

Figure 3: Descriptive Statistics

The descriptive statistics reveal the overall high impression of the role of threat intelligence in cybersecurity defense. The highest average score was registered in the category Financially Motivated Cyber Attacks (M = 4.31, SD = 0.66) which means that the respondents were strongly in favor of the increasing role of financially motivated cyber threats. In the same way, the Effectiveness of Threat Intelligence in Cyber Defense had a high mean (M = 4.24, SD = 0.69) value implying that the respondents were highly confident in the use of threat intelligence to enhance cyber defense capabilities.

Another construct that showed high level of agreement was Threat Intelligence Awareness and Adoption (M = 4.08, SD = 0.71), which implies that organizations are becoming more aware and are adopting threat intelligence practices. Organizational Preparedness and Cybersecurity Strategy received a mean score of 3.94 (SD = 0.76), which means that the respondents tend to think that their organizations are fairly prepared to respond to the cybersecurity threat.

Conversely, Challenges and Future Directions had the lowest mean score (M = 3.81, SD = 0.82) with a moderate-high level of agreement and demonstrates the presence of current challenges in the implementation, resource allocation, and future cybersecurity developments. On the whole, the results indicate a high recognition of the strategic value of threat intelligence in contemporary cybersecurity settings.

Table 1: Threat Intelligence Awareness and Adoption

Item	Mean	SD	χ^2	Sig.
Importance of threat intelligence in cybersecurity	4.15	0.70	28.11	0.001
Threat intelligence tools are actively used	4.01	0.75	26.44	0.002

Employees receive cyber threat training	3.96	0.78	24.92	0.003
Threat intelligence improves early attack detection	4.18	0.67	31.56	0.000
Cyber threat information is regularly shared	4.10	0.69	27.84	0.001

Table 1 shows that there is a high awareness and adoption of threat intelligence practices by the respondents. The highest mean score (M = 4.18, SD = 0.67) was obtained with the statement Threat intelligence improves early attack detection, which demonstrates high levels of agreement that threat intelligence can improve proactive cyber defense capabilities. On the same note, the respondents greatly recognized the significance of threat intelligence in cybersecurity (M = 4.15, SD = 0.70), and its strategic importance in the contemporary security management process.

There was also a high level of agreement on the regular exchange of cyber threat information (M = 4.10, SD = 0.69), which indicates that organizations are appreciating the importance of sharing intelligence among themselves as a way of mitigating cyber threats. Moreover, the respondents affirmed that threat intelligence solutions are already in operation in their companies (M = 4.01, SD = 0.75), which means that there is an increasing use of intelligence-based security solutions.

The relatively smaller mean score among employees that have undergone cyber threat training (M = 3.96, SD = 0.78) however, indicates that although there are awareness programs, organizations might need to reinforce employee-based programs on cybersecurity education and training. In addition, the chi-square values were all statistically significant ($p < 0.05$), which validated the fact that the opinions of respondents were not arbitrary and they were based on a meaningful agreement about the role of threat intelligence in cybersecurity practices.

Table 2: Financially Motivated Cyber Attacks

Item	Mean	SD	χ^2	Sig.
Financial cyberattacks are increasing rapidly	4.36	0.63	35.21	0.000
Phishing attacks are a major threat	4.42	0.60	37.80	0.000
Ransomware significantly affects operations	4.28	0.66	33.11	0.000
Financial fraud is a serious concern	4.30	0.65	34.22	0.000
Attackers are becoming more advanced	4.19	0.74	29.65	0.001

The findings in Table 2 indicate that the issue of financially motivated cyberattacks is of great concern among respondents. The sentence Phishing attacks are a major threat had the largest mean score (M = 4.42, SD = 0.60), which implies that there

was a high level of agreement that phishing is one of the greatest cybersecurity threats affecting organizations. Equally, the respondents were in strong agreement that financial cyberattacks are on the rise (M = 4.36, SD = 0.63) indicating a rise in awareness of the rising rate of cybercrime attacks on financial assets and sensitive information.

The results also indicate that financial fraud is a critical issue (M = 4.30, SD = 0.65) and that ransomware has a strong impact on operations (M = 4.28, SD = 0.66), which can be interpreted as the dire operational and financial impact of contemporary cyber threats. Moreover, respondents also admitted the fact that attackers are becoming more sophisticated (M = 4.19, SD = 0.74), which implies that cyberattack methods and approaches are getting more sophisticated.

The chi-square values were all statistically significant ($p < 0.05$) and this indicates that the responses were based on the meaningful agreement and not random variation. On the whole, the results show that organizations consider financially motivated cyber threats as quickly changing, highly advanced, and able to provide significant operational and financial damage.

Table 3: Effectiveness of Threat Intelligence in Cyber Defense

Item	Mean	SD	χ^2	Sig.
Threat intelligence helps prevent data breaches	4.25	0.67	32.70	0.000
Real-time monitoring improves incident response	4.29	0.64	34.91	0.000
Threat intelligence enhances decision-making	4.18	0.70	29.22	0.001
AI integration improves threat detection	4.36	0.61	36.44	0.000
Threat intelligence reduces financial losses	4.12	0.72	27.83	0.001

Table 3 shows that the perception of the effectiveness of threat intelligence in improving cybersecurity defense mechanisms is very strong. The most popular statement (M = 4.36, SD = 0.61) was the statement that AI integration enhances threat detection, which means that the respondents are convinced that artificial intelligence plays a significant role in enhancing threat detection and analysis. By the same note, incident response is enhanced by real-time monitoring which received a high degree of consensus (M = 4.29, SD = 0.64) with an emphasis on the role of continuous monitoring in reducing the response time and alleviating cyber incidents.

The respondents also concurred that threat intelligence is useful in averting data breach (M = 4.25, SD = 0.67), which is the proactive nature of intelligence-based cybersecurity systems in safeguarding sensitive data. In addition, the results indicate that threat intelligence improves

decision-making (M = 4.18, SD = 0.70), which implies that organizations use intelligence information to aid in strategic planning of cybersecurity and operational response. The phrase Threat intelligence minimises financial losses scored a relatively low yet a significant mean (M = 4.12, SD = 0.72) indicating awareness of its financial benefits in mitigating the effects of cyberattack.

The significance of all chi-square values was statistically significant ($p < 0.05$), which proved that the opinions of respondents were not meaningless and unstable. In sum, the findings indicate a high degree of trust in the efficiency of threat intelligence and AI-driven cybersecurity systems to enhance the ability of organizations to defend against cyber threats.

Table 4: Organizational Preparedness and Cybersecurity Strategy

Item	Mean	SD	χ^2	Sig.
Organization has a cybersecurity strategy	4.01	0.75	28.13	0.001
Incident response plans are updated regularly	3.92	0.80	25.42	0.002
Investment in cybersecurity infrastructure is sufficient	3.84	0.83	23.17	0.003
External cybersecurity collaboration strengthens defense	3.96	0.77	24.95	0.002
Threat intelligence should be central in future strategies	4.16	0.69	31.84	0.000

The findings in Table 4 suggest that there is an overall high organizational preparedness to cybersecurity strategy and threat intelligence integration. The most frequently rated statement (M = 4.16, SD = 0.69) was the statement that threat intelligence needed to be at the heart of future strategies, which again reflected a high level of agreement that threat intelligence is a crucial component to enhance future cybersecurity structures and strategies. Similarly, respondents agreed that their organization has a cybersecurity strategy (M = 4.01, SD = 0.75), suggesting that many organizations have already established formal cybersecurity policies and defense mechanisms.

The results also demonstrate a positive attitude toward external collaboration in cybersecurity in order to enhance defense (M = 3.96, SD = 0.77) that demonstrates the significance of partnerships, information exchange and joint security initiatives in combating cyber threats. Moreover, the respondents also partly agreed that the incident response plans are being updated on a regular basis (M = 3.92, SD = 0.80), thus showing that they are still eager to be prepared to the changing cyber threats.

Nevertheless, the relatively low average rating of the investment in cybersecurity infrastructure as adequate (M = 3.84, SD = 0.83) indicates that all organizations might not be resource-free, technologically ready,

or have established infrastructure. The chi-square values were all found to be significant ($p < 0.05$) and this was used to conclude that the responses were based on meaningful and consistent perceptions. Altogether, the results show that organizations have already understood the strategic value of cybersecurity preparedness, but also accepted that they need to invest more and keep on improving cyber defense capabilities.

Table 5: Challenges and Future Directions

Item	Mean	SD	χ^2	Sig.
Lack of skilled professionals limits effectiveness	3.88	0.82	22.14	0.004
High implementation costs are barriers	3.79	0.85	21.30	0.005
Difficulty analyzing large threat data volumes	3.74	0.86	20.81	0.005
Government-private collaboration is necessary	4.02	0.74	27.26	0.001
Future frameworks should rely on AI-driven intelligence	3.93	0.81	24.33	0.002

As indicated in Table 5, the use of threat intelligence in cybersecurity has several critical issues and future implications. The most frequent one was the statement that Government-private cooperation is necessary ($M = 4.02$, $SD = 0.74$), which implies that the level of agreement that government and private cooperation is needed to increase cybersecurity resilience at national and organizational levels is high. Similarly, participants agreed that the upcoming framework should be founded on the basis of AI-driven intelligence ($M = 3.93$, $SD = 0.81$), which shows that they trust in the growing role of artificial intelligence in enhancing the threat detection, prediction, and response systems.

The findings also demonstrate the issues of workforce constraints since the respondents admitted that the lack of skilled professionals limits the performance ($M = 3.88$, $SD = 0.82$). This implies that companies might not be able to hire and keep cybersecurity professionals who can handle sophisticated threat intelligence tools. In addition, implementation cost ($M = 3.79$, $SD = 0.85$) and failure to handle vast amounts of threat data ($M = 3.74$, $SD = 0.86$) also turned out to be key obstacles to effective threat intelligence adoption and management.

All the values of chi-square were statistically significant ($p < 0.05$) which confirmed that the responses were significant agreement among the participants. Altogether, the results suggest that, although organizations have started to recognize the strategic value of AI-enhanced threat intelligence and cooperative cybersecurity activities, they still struggle to cope with more practical issues regarding expertise, financial investments, and data management complexity.

Discussion

This study has revealed that the threat intelligence is emerging as a more significant strategic tool that is utilized in assisting organizations to enhance their cybersecurity controls against the financially motivated cyberattacks. The findings showed that the effectiveness of the threat intelligence in enhancing the early detection of threats, incident responses and cybersecurity decisions were strongly agreed. The findings can be contrasted with the previous studies that have emphasized the significance of proactive threat intelligence frameworks to enhance the resilience of organizations to the new cyber threats [1], [3]. The opinion that phishing, ransomware, and financial fraud are notable cybersecurity threats was largely shared between the respondents, which agrees with the prior studies that financial-motivated attacks were one of the most recurrent threats to the current digital infrastructure [17], [18].

The paper also revealed the growing role of artificial intelligence in the contemporary cybersecurity activities. The high agreement on the potential of AI to identify threats and track them in real-time aligns with prior research indicating that AI and machine learning-based technology can increase the speed, accuracy, and efficiency of cyber threat detection and response to incidents [2], [20]. These findings suggest that organizations are beginning to recognize the value of implementing such smart automation in their cybersecurity initiatives to be more responsive to sophisticated cyberattacks. Furthermore, the findings indicated that the threat intelligence would help reduce financial losses and avoid data breaches, which corresponds to the arguments expressed in the former body of literature on cybersecurity [8], [19].

Along with these favorable perceptions, the study also discovered that there are other implementation barriers like high infrastructural cost, lack of access to qualified experts in the field of cybersecurity and difficulties in handling large amounts of threat information. These findings are consistent with the previous research studies that had identified resource limitations and lack of expertise as the major barriers to effective implementation of threat intelligence [5], [24], [26]. Moreover, the government-private collaboration and new AI-based cybersecurity systems also received a very warm reception among the respondents, as they align with the recent proposals of collaborative systems in cybersecurity and intelligence-sharing programs to meet new cyber threats [13], [27]. On the whole, the research suggests that threat intelligence, based on AI technologies and cooperative cybersecurity systems, is a valuable factor in enhancing cybersecurity and ensuring organizations are better equipped to combat financially-driven attacks.

Conclusion and Recommendations

The paper has concluded that threat intelligence is now one of the most significant elements to enhance organizational cybersecurity measures to counter cyberattacks with financial interests. The results showed that companies are becoming more aware of the need to use proactive cybersecurity systems, AI-powered surveillance systems, and real-time threat detection processes to mitigate data breaches, minimize operational challenges, and losses. The respondents were of high level of agreement on the effectiveness of threat intelligence in enhancing incident response, decision making and cyber resilience in general. The paper also confirmed that organizations in different sectors are still being threatened by attacks with monetary intentions such as phishing, ransomware, and financial fraud.

Although the threat intelligence has its benefits, the research revealed that numerous obstacles exist in implementing the threat intelligence such as high cost of implementation, lack of trained cybersecurity experts and the issue of dealing with large volumes of threat information. These problems demonstrate that investing in technology and training of the staff should not be discontinued to make sure that the cybersecurity defenses are efficient. The findings suggest that organizations should consider adopting the use of artificial intelligence and machine learning technologies in cybersecurity systems to improve predictive threat detection and automatic response systems. It should also reinforce regular education of employees on cyber security to enhance the awareness and minimize human vulnerability. In addition, it also encourages cooperation with the government and cybersecurity professionals as well as the partners in the private sector, so that they could exchange intelligence and jointly defend against cyber threats by organizations. It will be necessary to constantly invest in cybersecurity systems infrastructure, policy formulation, and state-of-the-art threat intelligence systems to create resilient and future-oriented cybersecurity environments that can address the new financial cyber threats.

References

[1] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *International Journal of Computer Applications Technology and Research*, vol. 13, no. 8, pp. 11–27, 2024.

[2] R. Muppalaneni, A. C. Inaganti, and N. Ravichandran, "AI-driven threat intelligence: Enhancing cyber defense with machine learning," *Journal of Computing Innovations and Applications*, vol. 2, no. 1, pp. 1–11, 2024.

[3] O. Eltayeb, "The crucial significance of cyber threat intelligence in mitigating cyber

attacks," *Journal of Ecohumanism*, vol. 3, no. 4, pp. 2422–2434, 2024.

[4] M. O. Ijiga, H. S. Olarinoye, F. A. B. Yeboah, and J. N. Okolo, "Integrating behavioral science and cyber threat intelligence (CTI) to counter advanced persistent threats (APTs) and reduce human-enabled security breaches," *International Journal of Scientific Research and Modern Technology*, vol. 4, no. 3, pp. 1–15, 2025.

[5] O. Kayode-Ajala, "Applications of cyber threat intelligence (CTI) in financial institutions and challenges in its adoption," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 6, no. 8, pp. 1–21, 2023.

[6] F. Amin, M. A. But, I. Amin, and A. Khan, "The tokenized business marketplace: A blockchain and AI-powered framework for democratizing business ownership and investment," *International Journal of Business and Management Sciences*, vol. 5, no. 4, pp. 318–328, 2024.

[7] S. M. H. Shah, F. Amin, and A. Khan, "Cyber-resilient mobile edge computing: A deep neural approach for secure and efficient task offloading," *The Asian Bulletin of Big Data Management*, vol. 5, no. 1, pp. 200–215, 2025.

[8] M. Dekker and L. Alevizos, "A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making," *Security and Privacy*, vol. 7, no. 1, p. e333, 2024.

[9] K. Nandini, A. Yaramsetty, and M. Tulasirama, "Enhancing cybersecurity resilience: A study of threat detection and mitigation techniques in modern networks," *Library of Progress - Library Science, Information Technology & Computer*, vol. 44, no. 3, 2024.

[10] U. Imtiaz and H. Elbedour, "Cybersecurity risk management in the digital era: The strategic value of ethical hacking," *Spectrum of Engineering Sciences*, pp. 1076–1086, 2025.

[11] A. A. Mohammed, M. S. Islam, and K. M. Zubair, "Threat intelligence for business analysts: Bridging the gap between security and strategy," *American Journal of Business*, vol. 2, no. 7, 2025.

[12] M. Baber, K. Islam, A. Ullah, and W. Ullah, "Libraries in the age of intelligent information: AI-driven solutions," *International Journal of Applied and Scientific Research*, vol. 2, no. 1, pp. 153–176, 2024.

[13] S. Lee, A. A. H. Mujammami, and K. Kim, "Leveraging social networks for cyber threat intelligence: Analyzing attack trends and TTPs in the Arab world," *IEEE Access*, vol. 13, pp. 5679–5693, 2024.

[14] N. Sultana, M. A. Nasir, C. Majumder, and A. H. K. Choain, "Exploring AI-driven approaches for safeguarding sensitive ERP,

HR, and defense data within US organizations," *Journal of Business Insight and Innovation*, vol. 3, no. 2, pp. 43–59, 2024.

[15] M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," *Sustainability*, vol. 15, no. 18, p. 13369, 2023.

[16] O. O. Val, T. M. Kolade, M. O. Gbadebo, O. Selesi-Aina, O. O. Olateju, and O. O. Olaniyi, "Strengthening cybersecurity measures for the defense of critical infrastructure in the United States," *Asian Journal of Research in Computer Science*, vol. 17, no. 11, pp. 25–45, 2024.

[17] M. Usman and A. Ullah, "Blockchain technology implementation in libraries: An overview of potential benefits and challenges," *AVE Trends in Intelligent Computing Systems*, vol. 1, no. 1, pp. 42–53, 2024.

[18] U. Imtiaz, "Investigating the impact of phishing attacks on organizational cybersecurity posture," *Spectrum of Engineering Sciences*, pp. 1758–1780, 2025.

[19] S. A. Eshra, F. T. Zohora, S. Akter, I. Rasul, and A. Hossain, "The role of threat intelligence in preventing financially motivated cyberattacks," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 2, pp. 20–37, 2025.

[20] S. T. Hasan, "Machine learning models for forecasting employee demand in healthcare HR," *Journal of Engineering and Computational Intelligence Review*, vol. 3, no. 2, pp. 159–172, 2025.

[21] M. A. Hasan, M. T. R. Mazumder, M. C. Motari, M. S. H. Shourov, and M. J. Howlader, "A data-centric evaluation of AI-powered fraud detection and BI dashboards in strengthening trust and ROI in US e-commerce," *Spanish Journal of Innovation and Integrity*, vol. 49, pp. 157–175, 2025.

[22] F. T. Zohora and P. Paul, "Maternocare prediction for maternal and child well-being using survey data and machine learning approaches," *Excel International Journal of Technology, Engineering and Management*, vol. 11, no. 4, pp. 170–180, 2024.

[23] M. T. Islam, A. Azeem, M. Jabir et al., "An inventory model for a three-stage supply chain with random capacities considering disruptions and supplier reliability," *Annals of Operations Research*, vol. 315, pp. 1703–1728, 2022, doi: 10.1007/s10479-020-03639-z.

[24] A. A. M. Jabir and F. Jahan, "High entropy alloy at high temperature and pressure," *International Journal of Advances in Engineering & Technology*, vol. 16, no. 6, pp. 500–517, 2023.

[25] S. T. Hasan, "Mitigating algorithmic bias in AI-driven hiring systems in the

United States," *Journal of Business Insight and Innovation*, vol. 5, no. 1, pp. 78–90, 2026.

[26] K. I. Nnaka, P. O. Mbamalu, J. C. Nwaigbo, P. C. Ozo-ogueji, V. I. Njoku, and C. C. Ekechi, "AI-powered threat detection: Opportunities and limitations in modern cyber defense," *World Journal of Advanced Research and Reviews*, vol. 27, no. 2, pp. 210–223, 2025.

[27] A. El-Kosairy, H. Aslan, and N. Abdelbaki, "Transforming cybersecurity: Leveraging blockchain for enhanced threat intelligence sharing," *International Journal of Safety & Security Engineering*, vol. 14, no. 4, 2024.