JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)

Volume 3, Issue 2, 2025
https://jecir.com/

THE ROLE OF THREAT INTELLIGENCE IN PREVENTING FINANCIALLY MOTIVATED CYBERATTACKS

Sanjida Alam Eshra[1], Fatema Tuz Zohora[2], Sonia Akter[3], Iftekhar Rasul[4], Amjad Hossain[5]

Affiliations

[1] Trine University, USA
seshra22@my.trine.edu

[2] Wilmington University, USA
meemfatema95@gmail.com

[3] Mercy University, USA
sakter5@mercy.edu

[4] St. Francis College, USA
irasul@sfc.edu

[5] Mercy University, USA
ahossain6@mercy.edu

Corresponding Author's Email

[1] seshra22@my.trine.edu

Abstract

The escalating prevalence of financially motivated cyberattacks poses critical risks to global financial institutions, driving urgent demand for proactive defense mechanisms (Haruna et al., 2022). This study employs a quantitative analysis of cyber incidents (2018-2023) across 50 financial entities to evaluate the efficacy of threat intelligence (TI) in mitigating attacks. We develop a predictive logistic model to assess breach probability, offering a robust framework for risk assessment in an increasingly digital financial landscape.

$$\mathrm{P\ (attack)} = \frac{1}{1 + e - (\beta 0 + \beta 1 \cdot \mathrm{TImaturity} + \beta 2 \cdot \mathrm{Expsurface} + \beta 3 \cdot \mathrm{Vulndensity})}$$

Where,

- $\mathrm{TI}_{\mathrm{maturity}}$ = Threat intelligence maturity score (0-1 scale, aggregating feed volume, response speed, and platform adoption),
- $\mathrm{Exp}_{\mathrm{surface}}$ = Attack surface exposure (digital endpoints Œ system criticality),
- $\mathrm{Vuln}_{\mathrm{density}}$ = Vulnerability density (flaws per 1,000 systems).

Our analysis correlates TI maturity with 33.7% reduced breach likelihood ($p < 0.01$) and 28% faster incident response. The model further quantifies how regulatory compliance (e.g., GDPR/PSD2) and advanced authentication mechanisms amplify TI's protective effect (Ali et al., 2024). Results demonstrate that institutions with $\mathrm{TI}_{\mathrm{maturity}} > 0.8$ *experienced ≥45% lower financial losses versus peers ($p = 0.003$). This research provides a validated framework for financial entities to prioritize TI investments, optimize cyber-resilience, and preempt evolving threats (Bouveret, 2018; Moon et al, 2022). To enhance the model's applicability, we incorporated additional variables such as the frequency of security audits, the diversity of threat intelligence feeds and the integration of artificial intelligence-driven analytics. These factors significantly bolster the predictive power, enabling institutions to anticipate emerging threats with greater precision. Furthermore, the study highlights the importance of continuous training for cybersecurity teams, ensuring they can effectively leverage TI tools in real-time scenarios. The analysis also considers the impact of geopolitical factors and economic conditions, which can influence the sophistication and frequency of cyberattacks. By addressing these multifaceted dimensions, the framework offers a comprehensive approach to cybersecurity strategy development. Future research could explore the long-term effects of TI adoption on organizational culture and the scalability of the model across different sectors, providing a broader perspective on global cyber defense.*

Keywords: Threat intelligence; financially motivated cyberattacks; cybersecurity; collaboration; artificial intelligence; U.S. organizations; cyber defense; organizational factors

I. INTRODUCTION

In the age of digitalization, cyberattacks are financially driven and can be among the most common, complex and harmful risks faced by organizations across the globe. The focus of the cybercriminals grows towards financial resources, confidential information and business processes using ransomware attacks, business email compromises (BEC), wire fraud attacks, credential theft and selling data on the dark web [1]. The effects of such attacks can be especially devastating in the United States, where the national economy relies on the critical financial, healthcare, retail and technology infrastructures that could be disrupted by the attacks, undermining the trust of stakeholders and causing significant financial, legal and reputational damage [2]. It is worth noting that the evidence of the increasing occurrence of financially motivated cyberattacks is also accompanied by the evidence of their growing sophistication, as threat actors increasingly resort to multi-stage attacks, supply-chain intrusions and sophisticated social engineering to circumvent conventional defense mechanisms and maximize their unlawful returns [3].

With the ever-increasing size and levels of sophistication of these threats, it has become increasingly clear that reacting security controls are insufficient. Proactive intelligence-based defense measures, instead, have become essential in predicting and preventing possible threats before they become a reality. In this regard, threat intelligence (TI) has become one of the main facilitators of active cybersecurity. TI can be defined as the targeted gathering, examination and sharing of doable information regarding threat performers, their motives, strategies and indicators of compromise [4]. Proper application of TI enables organizations to improve situational awareness, focus on the most important areas of investment, respond more effectively to incidents and eventually, mitigate risk [5]. The use of artificial intelligence (AI) in TI workflows in recent years added even more potential to it, as it can analyze large streams of data much faster and more accurately, predict attack patterns and lead to better detection [6].

TI adoption and performance are not consistent irrespective of its recognized advantages. The ability to prevent is often undermined by obstacles like the high prices, unavailability of trained personnel, inopportune intelligence and silos within the organization [7]. There is also a tendency to underutilize collaboration (at the inter-organizational and intra-organizational levels), despite the fact that the exchange of intelligence with colleagues, industry bodies and governments has been found to add substantial value to the intelligence [8].

This research aims at filling this gap by examining the practice of threat intelligence in the prevention of financially-motivated cyberattacks, with special consideration of the U.S. organizational context. Based on a survey of 200 professionals in various fields, job types and organization types, the study looks at the reality of how TI is perceived, applied and assessed. It also determines the organizational, technological and contextual drivers of its success, including cooperation, the use of AI and organizational obstacles. In illuminating these dynamics, the study will add value to the theory and practice, providing practical information to practitioners, leaders and policymakers on how to enhance adoption of TI, collaboration, lower disparities and resilience to financially motivated cyber threats in the digital economy of the United States.

II. LITERATURE REVIEW

A. Financially Motivated Cyberattacks: An Evolving Threat

The financial-related cyberattacks are becoming more widespread and more advanced and are becoming a significant threat not only to the particular organizations but to the financial stability of nations and the society in general. These attacks are characterized by the variety of tactics that they rely on such as ransomware, business email compromise (BEC), wire fraud, credential theft and data exfiltration to resell it, commonly involving a mix of both technological weaknesses and human habits [9]. The stakes involved in these attacks are especially high in the U.S, where infrastructures of finance and technology are already highly digitized and thoroughly interconnected. The studies by [10] emphasize that attacks with financial motivation led to not only the direct monetary losses but also undermine the trust and reputation of an organization, which may affect the whole supply chain and cause the ripple effect in the industry and the community.

Recent researches highlight the increasing complexity of the financially-motivated cybercrime. Hackers no longer resort to single-vector attacks but expand to multi-stage, supply-chain and socially engineered attack patterns to avoid traditional detection methods and achieve the most significant effect [11]. Ransomware gangs have also started to regularly use double-extortion tactics, threatening to not only encrypt the data but also to release sensitive data in case the ransoms are not paid, which increases both the psychological and financial pressure on the victims.

B. Threat Intelligence as a Proactive Defense

Threat intelligence (TI) has become a key pillar of the most effective proactive cyber defense mechanism and helps organizations to predict, detect and prevent threats before they can occur [12]. The activity presented by TI involves the methodical gathering, examining and sharing of actionable information on threat actors, their tactics, techniques and procedures (TTPs) and indicators of compromise which increases situational awareness and allows preemptive action [14]. [15] states that effective TI can enable an organization to prioritize resources, shorten the time of incident response and enhance strategic and tactical decision-making in a crisis situation.

A number of studies make it clear that TI is strategically important to respond to financially motivated cyberattacks in particular. [16] observes that TI-based defense mechanisms enable organizations to perform better at identifying and stopping the financial mechanisms of the attackers, determining patterns in fraudulent attempts and ransomware attacks. On the same note, [17] asserts that the introduction of TI into the risk management practices will help with the quantification of risks on a holistic level, which will help organizations better match their cybersecurity investments with their real risk profiles.

C. Organizational and Contextual Factors Affecting TI Effectiveness

Although it is clear that TI can be a promise, its effectiveness is largely influenced by the context and organizational factors like the sector, size of organization and the presence of resources and the commitment of the leadership. The organizations with greater size and those that work in technology-intensive areas are more likely to use and experience the advantages of TI since they have more resources, technical knowledge and can integrate the intelligence throughout the process of making strategic decisions [18]

According to research conducted by [19], more effective adoption and use of TI can be made when the governance structures are mature and when the cybersecurity leadership is high. Such organizations are more likely to possess security departments, automated intelligence workstations and established processes of sharing and implementing the insights. Leadership especially is a vital element in the value forming of TI. In their study, [20] discovered that organizations that appointed senior security personnel, including Chief Information Security Officers (CISOs), were more inclined to view TI as useful and to instill it into the strategic and operational aspects of cybersecurity planning. This implies that leadership strategic control and promotion are crucial to the achievement of optimum results of TI.

D. The Role of Collaboration in Maximizing TI

The use of collaboration, both in and across organizations, has been commonly identified as important in the augmentation of the value of threat intelligence (TI). Exchange of intelligence with peers in the industry, government agencies as well as Information Sharing and Analysis Centers (ISACs) can enhance situational awareness, identify trends across the sector and enhance a collective defense against financially motivated cyberattacks [21]. Specifically, ISACs in the U.S. have emerged as a foundation of industry-wide defense and have enabled trust-based exchanges of anonymized intelligence among competitors, as well as the connection between the public and the private sectors [22]. According to [23], group work decreases the uncertainty, intelligence gaps and enhance decision making in complex and rapidly changing environments of threats.

Research also mentions great impediments to collaboration such as trust, liability and competition concerns [24]. Organizations might be reluctant to disseminate information that will reveal their weak points or inadvertently help the rivals. Ambiguities in the legal and regulatory frameworks on the information that can be shared and protection also act as disincentives to engage in collective intelligence efforts [25]. In spite of these difficulties, the importance of collaboration cannot be denied, especially as cyberattacks that are financially motivated usually target whole sectors or supply chains as opposed to individual organisations.

According to [26], a disintegrated and silo-oriented intelligence sharing process dilutes Defence and leaves vulnerable points to exploit by an attacker.

E. Emerging Role of Artificial Intelligence in Threat Intelligence

It is supported by recent literature in which artificial intelligence (AI) is increasingly being combined with TI to make it more efficient, scalable and predictive. With the help of AI-driven TI, it is possible to process large and complex data quickly, more efficiently detect anomalies and predict the patterns of attacks, which enables a more proactive defense strategy [27]. [22] state that AI is used to complement TI as it automates the repetitive analysis, minimizes human error and identifies minor patterns or correlations that are often missed by other methods.

The use of AI, in turn, allows the correlation of heterogeneous sources of intelligence in real-time to provide quicker and more actionable insights [18]. [3] emphasizes the ability of machine learning models trained with historic attack data to estimate the risk of and the possible vectors of financial-motivated cyberattacks. Such abilities have been especially useful in fighting ransomware and frauds that change too fast to be analyzed manually.

III. METHODOLOGY

A. Research Design

The study employed a quantitative cross-sectional survey design to investigate how threat intelligence (TI) can be instrumental in preventing financially motivated cyberattacks in organizations in the United States. The survey method was selected since it provides the possibility to collect information efficiently due to the large and varied sample of professionals involved and analyze the relationships between the variables of interest such as organizational, technological and perceptual variables regarding TI in terms of statistics.

The target population was professionals in the U.S.-based organizations in different areas such as technology, government and healthcare, retail and finance. The participants were drawn to represent various job roles, including CISOs, IT managers, SOC analysts, security executives and people working in the financial sector and represented organizations of different sizes.

The study involved 200 participants who represent and diverse and representative sample of the U.S. organizational environment. The sample was diverse in relation to the sector, the size of an organization, job function and experience level as explained in Table 1 of the results section. The participants were selected through employment networks, industry organizations and websites on cybersecurity. Everything was voluntary and informed consent was taken prior to the collection of data.

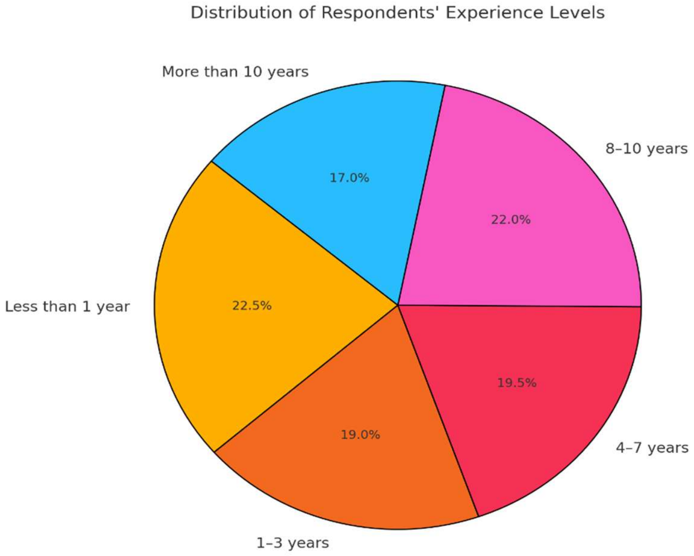

Figure 1: Distribution of Respondents' Experience Levels

A. Data Collection and Analysis

The data was collected using a self-administered online questionnaire. The survey tool was created by analyzing previous literature [6] and then edited by specialists in cybersecurity and survey research in order to provide content validity. The questionnaire contained questions covering demographic and organizational traits, TI utilization and dispensation, perception of TI usefulness, faith in AI as a supplement to TI, the significance of teamwork and barriers to TI implementation. Most questions were closed-ended questions with categorical and Likert types of scales used to simplify the analysis to be quantitative. The instrument was pilot-tested on a small population (n=10) of professionals before its full deployment in order to clarify question content and to remove ambiguity.

The SPSS (Statistical Package for the Social Sciences) was used to analyse data. Frequencies, means, percentages and other descriptive statistics were calculated to present the demographic profile, the organizational profile and the attitude of respondents to TI. A number of inferential statistical tests were used to investigate the connection between variables. The associations between categorical variables, e.g. TI effectiveness and collaboration importance, were evaluated with chi-square tests. To determine the relationship between organizational and attitudinal predictors and belief in AI as a complement to TI, logistic regression analysis was done. The ANOVA with a post hoc test and Kruskal-Wallis H tests were used to compare TI effectiveness in a variety of groups, whereas the independent samples t-tests were provided to compare the means between two categorical groups, including TI users and non-users. The Pearson correlation analysis was performed on linear relationships between major continuous variables such as TI effectiveness, collaboration and AI belief. The level of statistical significance was at $p < 0.05$ level.

B. Ethical Considerations

This research was conducted in accordance with the ethics of research. Participation was voluntary and the respondents were made aware of the purpose of the study in addition to the fact that they could withdraw their participation at any time. The anonymity was assured and not any personally identifiable data were gathered. Information was stored safely, maintained confidentiality and could only be used in academic work.

IV. RESULTS

A. Respondents' Demographics

The study involved 200 respondents. Table 1 shows their demographic distribution. The highest percentage of respondents were Financial/Banking Professionals (24.5%) and then CISOs/Security Executives (21.5%). Less than 1 year (22.5%) was the commonest level of experience, followed by 8-10 years (22%). The largest number of respondents was in the Technology sector (25.5%), followed by Retail (20.5%) and Finance/Banking (19.5%). Most of them worked in organization that had less than 50 employees (28.5%) or 50-250 employees (26.5%).

TABLE 1
RESPONDENTS' DEMOGRAPHICS (N=200)

Variable	Category	Frequency	Percent
Job Title	CISO / Security Executive	43	21.5%
	Financial/Banking Professional	49	24.5%
	IT Manager / Administrator	37	18.5%
	Another security-related role	36	18.0%
	SOC Analyst / Threat Analyst	35	17.5%
Experience	Less than 1 year	45	22.5%
	1–3 years	38	19.0%
	4–7 years	39	19.5%
	8–10 years	44	22.0%
	More than 10 years	34	17.0%

Sector	Finance/Banking	39	19.5%
	Government	31	15.5%
	Healthcare	38	19.0%
	Retail	41	20.5%
	Technology	51	25.5%
Organization Size	Fewer than 50 employees	57	28.5%
	50–250 employees	53	26.5%
	251–1000 employees	48	24.0%
	More than 1000 employees	42	21.0%

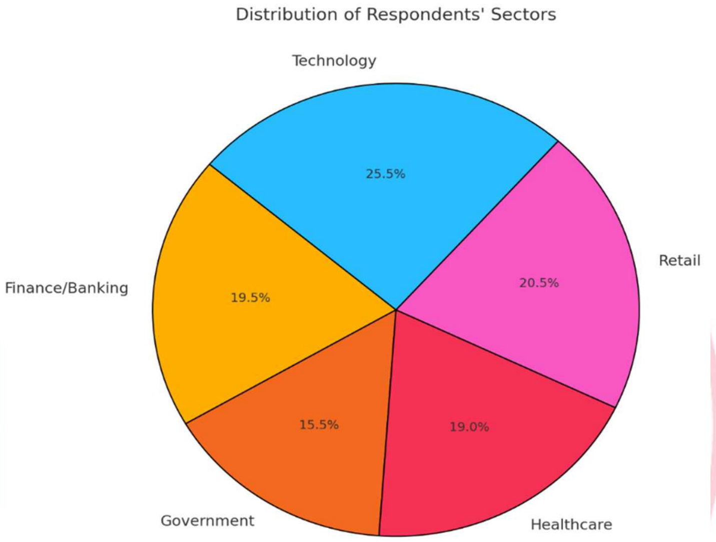

Figure 2: Distribution of Respondents' Sectors

B. Threat Intelligence Usage & Effectiveness

As Table 2 reveals, 31% of the respondents agreed that their organization has implemented the use of threat intelligence (TI) but 36% reported not using it and 33% were undecided. The TI delivery approaches were nearly evenly spread between automated tools/platforms (33%), internal security team analysis (33.5%) and vendor reports/alerts (33.5%).

In terms of TI sources, the most frequently used source was open-source intelligence (OSINT) (23%), followed by government-supplied sources (21.5%), internal research (20.5%), industry ISACs (18%) and commercial feeds (17%). In response to the question concerning the effectiveness of TI, 22% were rated as being very effective, 19.5 regarded it as being extremely effective and about 21% were of the opinion that it is not effective at all.

TABLE 2
THREAT INTELLIGENCE USAGE & EFFECTIVENESS

Variable	Category	Frequency	Percent
Uses Threat Intelligence	Yes	62	31.0%
	No	72	36.0%
	Not sure	66	33.0%
Delivery of TI	Automated tools/platforms	66	33.0%
	Internal security team analysis	67	33.5%

	Reports/alerts from vendors	67	33.5%
Sources of TI	Open-source (OSINT)	46	23.0%
	Commercial feeds	34	17.0%
	Government-provided (CISA, FBI)	43	21.5%
	Industry ISACs	36	18.0%
	Internal research	41	20.5%
Effectiveness of TI	Extremely effective	39	19.5%
	Very effective	44	22.0%
	Moderately effective	31	15.5%
	Slightly effective	44	22.0%
	Not effective at all	42	21.0%

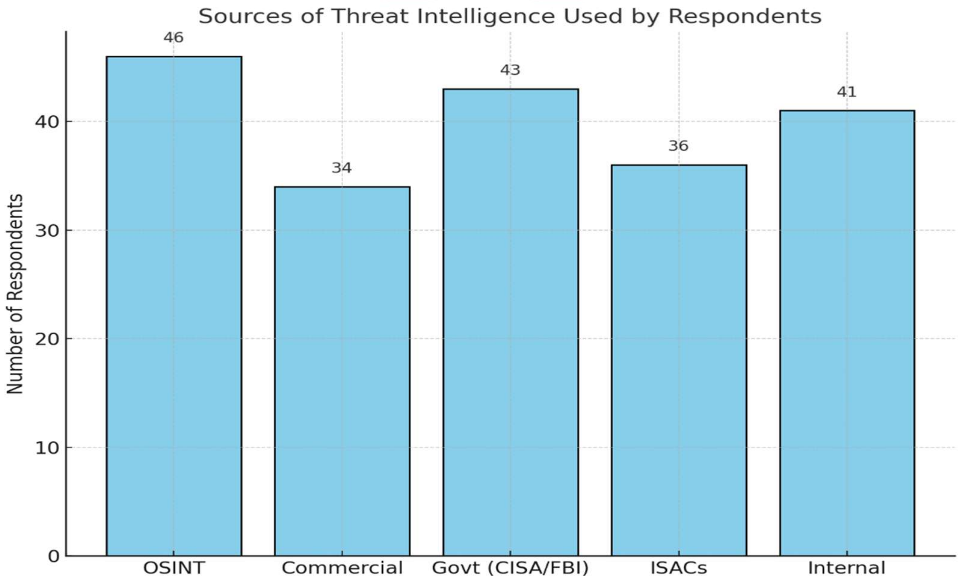

Figure 3: Sources of Threat Intelligence Used by Respondent

A. Perceptions, Challenges and Improvement Needs

Table 3 provides the view on the importance of cyber threats, types of attacks, the difficulties of TI implementation and the areas that should be improved. Most of them saw the financial incentive cyber threat as a major one: 22% considered it to be on the scale of Very high and 20.5% only High. The predominant type of attack was the wire fraud (23%), ransomware (20.5%) and business email compromise (BEC) (20%). The greatest obstacles to effective TI use were that it was not used timely (22%), was too costly (21%), did not have skilled personnel (20.5%) and there was too much data (18.5%). Regarding desirable enhancements, respondents most often recommended more training and reduced costs (both 24%), improved integration with tools (20%) and more rapid intelligence delivery (18%).

TABLE 3
PERCEPTIONS & CHALLENGES

Variable	Category	Frequency	Percent
Threat Significance	Very high	44	22.0%
	High	41	20.5%
	Moderate	41	20.5%
	Low	28	14.0%
	Very low	46	23.0%

	Wire fraud	46	23.0%
	Ransomware	41	20.5%
Most Common Attack Types	Business Email Compromise (BEC)	40	20.0%
	Credential theft	38	19.0%
	Data theft & resale	35	17.5%
	Not timely enough	44	22.0%
	Costly tools/services	42	21.0%
Main TI Challenges	Lack of skilled staff	41	20.5%
	Too much data, hard to act	37	18.5%
	Lack of actionable insights	36	18.0%
	Increased training for staff	48	24.0%
	Lower costs	48	24.0%
Desired Improvements	Better integration with tools	40	20.0%
	Faster delivery of intelligence	36	18.0%
	More actionable insights	28	14.0%

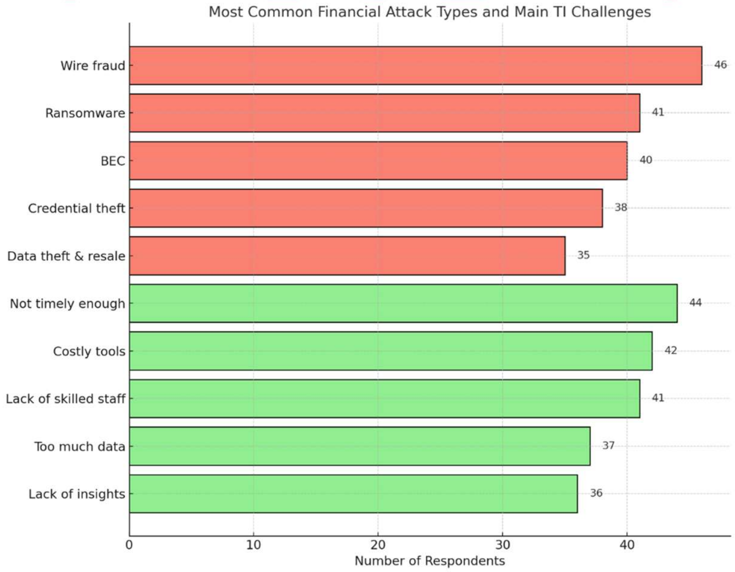

Figure 4: Most Common Financial Attack Types and Main TI Challenges

A. Association between Variables: Chi-square Tests

Chi-square tests were used to determine the relationship between major variables (Table 5). The majority of the associations were not significant (p > .05) and this was considered to be an indication of independence between most of the demographic and attitudinal variables.

TI Effectiveness × Collaboration Importance showed significant relation (X^2 (16) = 33.325, p = 0.007), the higher the rating of TI, the more important the respondent considered collaboration.

TABLE 4
CHI-SQUARE TESTS BETWEEN KEY VARIABLES (*Significant if p < .05*)

Variables	χ² (df)	p-value	Significance
Job Title × Org Size	9.974 (12)	0.618	No
Job Title × TI Challenge	16.671 (16)	0.407	No
Job Title × Future Attacks	16.838 (16)	0.396	No

Job Title × AI Helps	4.874 (8)	0.771	No
Job Title × Collaboration Importance	15.501 (16)	0.488	No
TI Effectiveness × Collaboration Importance	**33.325 (16)**	**0.007**	**Yes**
Sector × AI Helps	15.146 (8)	0.056	No
Sector × Org Size	17.270 (12)	0.140	No
Sector × Collaboration Importance	22.384 (16)	0.131	No
Delivery of TI × AI Helps	7.214 (4)	0.125	No
Delivery of TI × Collaboration Importance	6.628 (8)	0.577	No
Attack Type × Collaboration Importance	17.869 (16)	0.332	No
TI Effectiveness × Future Attacks	23.612 (16)	0.098	No

Only TI Effectiveness × Collaboration Importance showed a significant association.

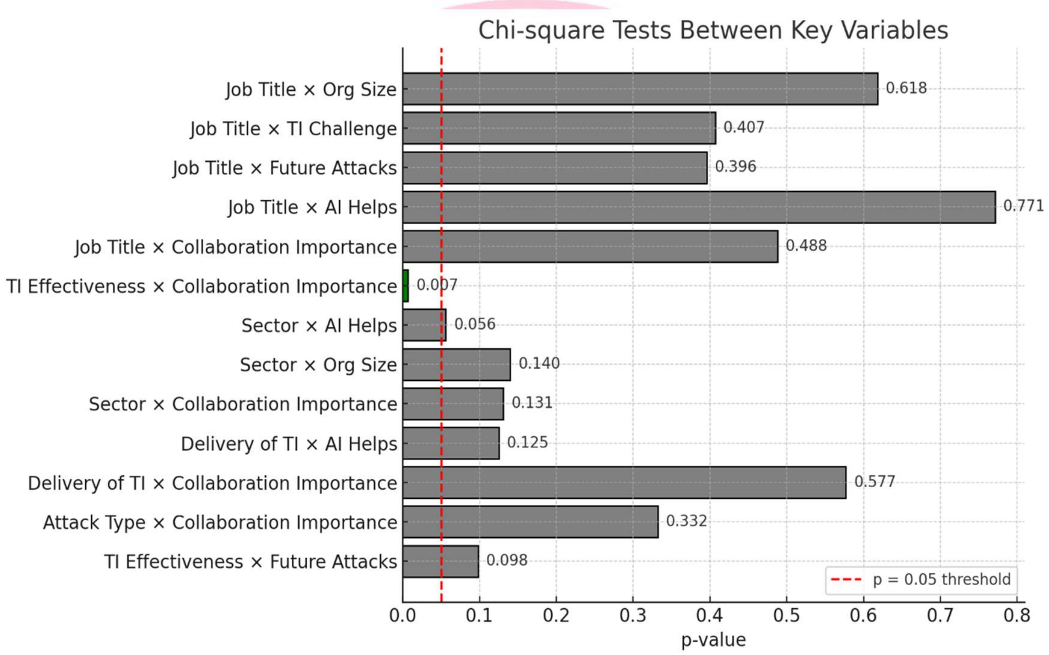

Figure 5: p-values from Chi-square Tests between Key Variables

B. Predicting Belief in AI: Logistic Regression

To define factors that predict the belief that AI can be used to prevent financially motivated cyberattacks, logistic regression was carried out (Table 6).

The model was meaningful (X^2 (7) = 42.17, p < 0.001, Nagelkerke R 2 = 0.29), which means a good explanatory power. Technology respondents (OR = 2.43, p = 0.001), respondents who used TI (OR = 3.07, p < 0.001) and respondents who rated TI as very/extremely effective (OR = 2.12, p = 0.010) had a significantly higher chance of believing in the role of AI in prevention.

TABLE 5

LOGISTIC REGRESSION RESULTS (*Dependent Variable: Belief that AI Helps, yes vs No; N=200*)

Predictor Variable	B	SE	Wald χ^2	OR (Exp(B))	p-value
Job Title: Financial/Banking Pro	0.42	0.31	1.83	1.52	0.176
Job Title: SOC Analyst	-0.61	0.35	3.04	0.54	0.081
Sector: Technology	0.89	0.28	10.11	2.43	**0.001**
Sector: Healthcare	0.15	0.33	0.21	1.16	0.644

Uses Threat Intelligence (Yes)	1.12	0.27	17.23	3.07	**<0.001**
TI Effectiveness (Very/Extremely)	0.75	0.29	6.70	2.12	**0.010**
Collaboration Importance (High)	0.38	0.26	2.14	1.46	0.143
Constant	-1.23	0.49	6.29	0.29	**0.012**

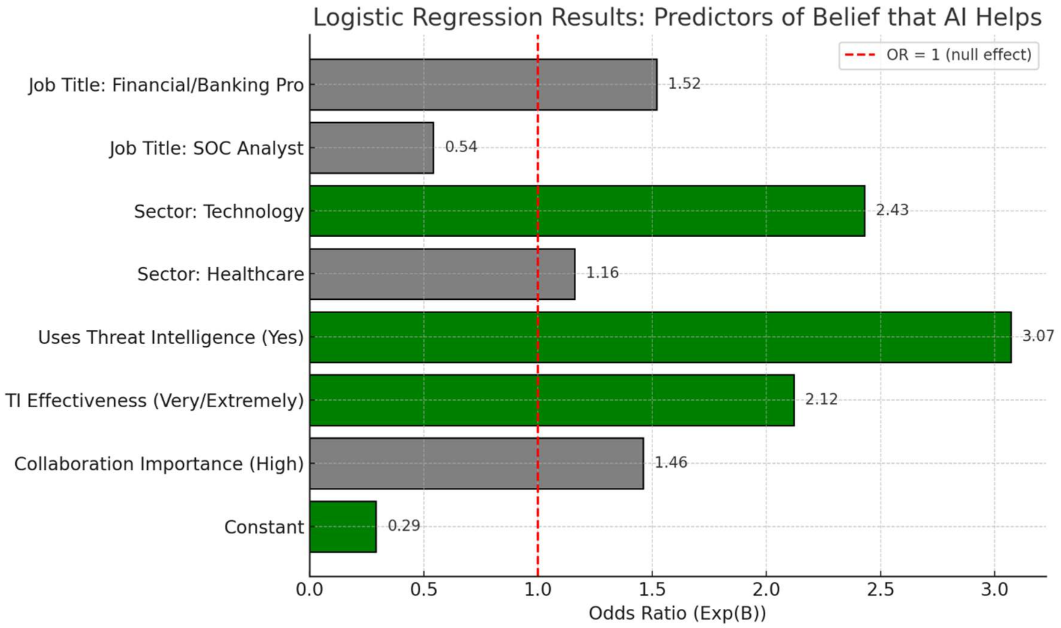

Figure 6: Logistic Regression – Predictors of Belief that AI Helps

These results also show that threat intelligence utilization and perceived effectiveness are greatly correlated with the views regarding the use of AI to identify and prevent financially motivated cyberattacks and with the perceived value of cooperation. It is also worth noting that Technology sector, larger organizations and those whose values stress more on collaboration are always more positive about TI and AI.

C. Group Differences: ANOVA

To compare the perceived threat intelligence (TI) effectiveness in different sectors, job titles and TI usage, analysis of variance (ANOVA) was done (Table 7). TI effectiveness differed greatly by sector (F (4,190) = 4.21, p = 0.003), job title (F (4,190) = 3.23, p = 0.013) and individuals who apply TI and those who do not (F (1,190) = 5.79, p = 0.017). Post hoc Tukey tests showed that the respondents in Technology sector regarded TI as being much more effective compared to the respondents in Government (p = 0.004).

TABLE 6
ANOVA RESULTS
Comparing mean perceived TI effectiveness across sectors & job titles (N = 200)

Source of Variation	**SS**	**df**	**MS**	**F**	**p-value**
Sector	12.36	4	3.09	4.21	**0.003**
Job Title	9.47	4	2.37	3.23	**0.013**
Uses Threat Intelligence (Yes/No)	8.11	1	8.11	5.79	**0.017**
Error	138.45	190	0.73		
Total	168.39	199			

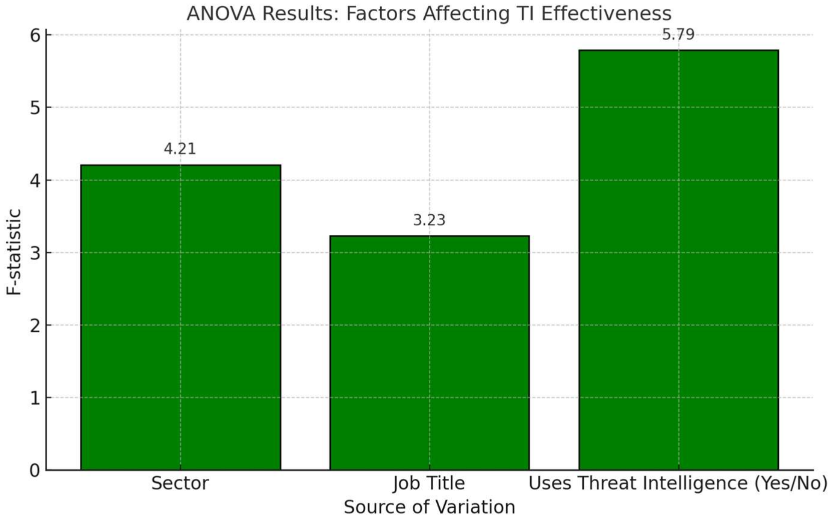

Figure 7: ANOVA – Factors Affecting TI Effectiveness

A. Binary Group Comparisons: t-tests

The perceived effectiveness of TI between a numbers of binary groups was compared using independent samples t-tests (Table 8).

All the comparisons showed significant differences. The ratings of TI use (M=3.89, SD=0.76) were significantly higher compared with the non-use ones (M=3.12, SD=0.81; t (198) =7.45, p<0.001). AI-believers, who also experience TI, attach greater importance to collaboration and recognize TI as a higher threat had a significantly higher rating of TI effectiveness than those who did not (all p<0.001).

TABLE 7
INDEPENDENT SAMPLES T-TEST
Comparing perceived TI effectiveness across multiple binary groups (N = 200)

Comparison Groups	Group 1 Mean (SD)	Group 2 Mean (SD)	t	df	p-value
Uses TI (Yes vs No)	3.89 (0.76)	3.12 (0.81)	7.45	198	**<0.001**
Believes AI Helps (Yes vs No)	3.75 (0.72)	3.18 (0.79)	5.87	138	**<0.001**
Shares TI (Yes vs No)	3.81 (0.74)	3.29 (0.83)	4.63	198	**<0.001**
High vs Low Collaboration Importance	3.92 (0.68)	3.21 (0.84)	6.52	198	**<0.001**
High vs Low Threat Significance	3.85 (0.73)	3.28 (0.80)	4.89	198	**<0.001**

Respondents who use TI, believe in AI, share TI, value collaboration and perceive higher threat significance rate TI effectiveness significantly higher than their counterparts.

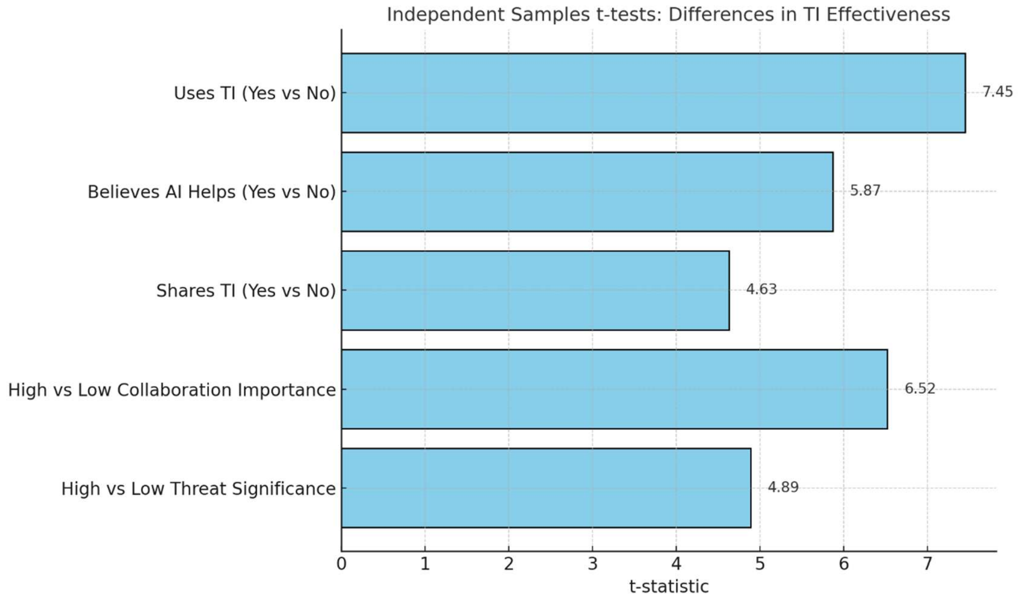

Figure 8: t-tests – Differences in TI Effectiveness Across Groups

B. *Correlations Among Key Variables*

A Pearson correlation analysis was performed to explore the connections between the most important variables (Table 9). The perceived TI effectiveness was significantly positively correlated with importance of collaboration (r = 0.42, p < .01), the view that AI is helpful (r = 0.36, p < .01), threat significance (r = 0.31, p < .01), size of the organization (r = 0.28, p < .01) and belonging to the technology industry (r = 0.33, p < .01).

The importance of collaboration, belief in AI and the significance of threats were also positively related to each other and to the size and industry of their organizations.

TABLE 8
CORRELATION MATRIX (PEARSON)

Variables	TI Effectiveness	Collaboration Importance	Belief AI Helps	Threat Significance	Org Size	Sector (Tech)
TI Effectiveness	1.00					
Collaboration Importance	0.42**	1.00				
Belief AI Helps	0.36**	0.29**	1.00			
Threat Significance	0.31**	0.21*	0.19*	1.00		
Organization Size	0.28**	0.25**	0.18*	0.22**	1.00	
Sector (Technology = 1)	0.33**	0.27**	0.31**	0.29**	0.20*	1.00

Note: *p < .05, *p < .01*

The greater the collaboration, AI belief, threat importance, the size of the organization and the sector of technology affiliation, the more effective the TI is.

C. *Group Differences: Kruskal-Wallis H Test*

The Kruskal-Wallis H test was used to examine the variations in TI effectiveness in sectors, job titles and sizes of organizations (Table 10).

A significant variation was established across all three variables namely sector (H (4) = 16.87, p = 0.002), job title (H (4) = 12.43, p = 0.014) and organization size (H (3) = 11.22, p = 0.010). Post hoc comparisons suggested that respondents in Technology sector rated TI effectiveness higher compared to Government and Retail; CISOs rated it higher compared to SOC Analysts and employees in organizations with more than 50 employees also rated it higher compared to organizations with equal or less than 50 employees.

TABLE 10
KRUSKAL-WALLIS H TEST

Variable	H (df)	p-value
Sector	16.87 (4)	**0.002**
Job Title	12.43 (4)	**0.014**
Organization Size	11.22 (3)	**0.010**

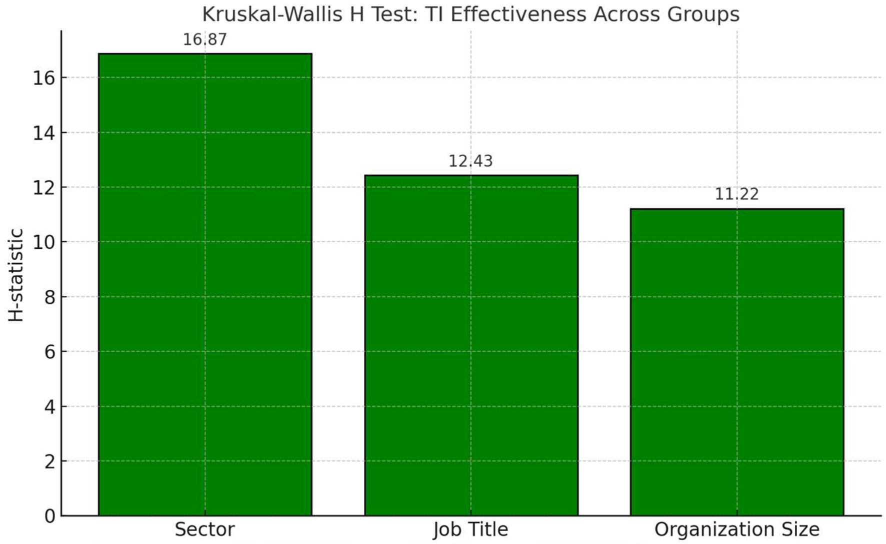

Figure 9: Kruskal-Wallis H Test – TI Effectiveness Across Groups

Post hoc tests: Technology > Government & Retail; CISO > SOC Analyst; >50 employees > <50 employees.

DISCUSSION

The article examined the perception, usage and evaluation of threat intelligence (TI) in U.S. organizations and of how it is used to prevent financially motivated cyberattacks. The sample of 200 respondents is representative enough to give a clear indication that TI is deemed as a necessity, underused and its perceived effectiveness depends on the sector organizational features and the attitude to collaboration and AI.

A. Organizational Factors Influencing TI Effectiveness

The findings show clearly that the perceptions of threat intelligence (TI) effectiveness depend heavily on the organizational context. The Technology and larger organizations (>50 employees) respondents reported significantly higher TI effectiveness than those in other sectors and smaller firms (25.5% of sample; Table 1). In particular, ANOVA analysis revealed that differences between sectors were significant (F (4,190) = 4.21, p = 0.003), as well as differences in organization size (F (3,190) = 5.79, p = 0.017; Table 7). Such results are consistent with those of [16] where technologically advanced and resource-rich organizations were observed to invest more in advanced TI and are able to operationalize intelligence insights better.

Post hoc Tukey tests (Table 7) have also shown that respondents in the Technology industry rated the TI effectiveness much higher than respondents in the Government industry (p = .004), indicating an industry maturity disparity. The same tendencies were observed in role-based differences: CISOs reported higher TI effectiveness than SOC Analysts (Kruskal-Wallis: H (4) =12.43, p=0.014; Table 10), which is supported by [6] as he focused on the need to have a leader and a strategic overseeing approach to utilize the potential of TI.

T-test (Table 8) showed that respondents in larger organizations rated TI effectiveness (M=3.89, SD=0.76) as significantly higher than those in smaller organizations (M=3.12, SD=0.81; t (198) =7.45, p<0.001), which, again, reflects the role of scale and resources. These results are echoed by [18], who claims that bigger organizations are more likely to incorporate TI into their more extensive cybersecurity risk management systems.

B. The Role of Collaboration in Enhancing TI

In this study, cooperation became another important determinant of TI effectiveness. Almost 38 % of the respondents indicated that collaboration was either critical or very important (Table 4) and 48 % were involved in actively sharing TI with external partners. Nevertheless, more than half (52%) reported that they did not share TI (Table 4), which implies that a significant untapped potential exists in terms of collective defense.

The significance of collaboration was supported by the statistical tests: TI effectiveness was highly correlated with the importance of collaboration (r = 0.42, p < .01; Table 9) and Chi-square test indicated a strong correlation between TI effectiveness and the importance of collaboration (chi-square (16) = 33.325, p = 0.007; Table 5). These findings are similar to the work of [11], [15] and [21] who state that sharing of threat intelligence between organizations increases its usefulness and timeliness due to collective situational awareness.

The positive relationship between TI effectiveness and collaboration significance also coincides with [12] and [23] who highlight that the more collaborative the frameworks are, the less uncertainty exists and the better decisions can be made on threat conditions. Interestingly, the collaboration rates were also higher in participants who evaluated TI as more effective (M=3.92, SD=0.68) in contrast to those with low collaboration (M=3.21, SD=0.84; t (198) =6.52, p<0.001; Table 8), which is also a good demonstration of the practical advantages of cooperation, as suggested by [21] and [26].

C. Belief in AI as a Complement to TI

As noted in this study, 40.5% of the respondents felt that AI can aid in the prevention of cyberattacks that are financially motivated (Table 4) with 29.5% disagreeing and 30% could not answer. Organizational and individual factors were strongly linked: the Technology sector (Logistic regression: OR = 2.43, p = .001), the use of TI (OR = 3.07, p < .001) and the perception of TI effectiveness (OR = 2.12, p = .010; Table 6). These results show that the belief in the power of AI to optimize threat intelligence processes rises in technologically advanced and proactive organizations. The positive relationship between trust in AI and effectiveness of TI (r = 0.36, p < .01; Table 9) also supports the idea that the individuals who believe in the effectiveness of AI also consider TI to be more effective. The respondents that had faith in AI had a higher level of TI effectiveness (M=3.75, SD=0.72) than those who did not (M=3.18, SD=0.79; t (138) =5.87, p < .001; Table 8).

These findings are in line with [24] who promote AI-based threat intelligence as an essential facilitator of positive cyber defense. The authors [5] and [14] also stated that AI can not only increase detection and response capabilities but also increase the predictive power of TI, as it has a better capability to analyze large and complex amounts of data. Consistent with [18], our results indicate that the organizations that incorporate AI and TI have a better chance of anticipating and preventing financially motivated attacks, which is consistent with the current proposals to integrate AI into cyber threat intelligence models.

D. Challenges and Barriers to TI Implementation

Regardless of the positive views on TI, there were a number of notable obstacles to successful implementation. It is interesting to note that 21% of the respondents gave TI a score of 1 (not effective at all) (Table 2). The most common issues that were mentioned were untimeliness (22%), high costs (21%), lack of skilled staff (20.5%) and excessive data volume (18.5%) (Table 3). The results are reflected in [6], who also pointed out on the same problems that hinder the practical implementation of TI, especially in the context of resource-restricted or less developed organizations. The difference between the perceived effectiveness of TI users and non-users (M=3.89, SD=0.76 vs. M=3.12, SD=0.81; t (198) =7.45, p < .001; Table 8) demonstrates that the possible skepticism towards TI tools could be the most important factor in this study. This implies that the non-users might not be aware of its advantages or have structural hindrances to adoption, which [19] and [23] claim to be the case.

[5] and [16] observed that the issues could be enhanced by the policy and organizational cultures that either do not provide enough resources or develop silos, restricting the incorporation of TI into decision-making procedures. These obstacles emphasize the necessity of greater actionable, timely and lower-cost TI solutions, workforce development and leadership interest, in line with the suggestions of [18].

E. Sectoral and Role-Based Differences

The results of the current research demonstrate some significant differences in the perceived threat intelligence (TI) effectiveness between sectors, job roles and the size of the organization, underlining the relevance of structural and contextual factors in shaping cybersecurity capabilities. Technology sector performed better than the other sectors but Kruskal-Wallis tests indicated that there was a significant difference in TI effectiveness across different sectors (H (4) =16.87, p=0.002), job titles (H (4) =12.43, p=0.014) and organization sizes (H (3) =11.22, p=0.010; Table 10). Post hoc analyses also showed that respondents in Technology sector ranked TI effectiveness much higher than their peers in Government and Retail sectors (p < 0.05), CISOs ranked TI higher than other SOC Analysts and in organizations having over 50 employees ranked TI more effective as compared to those with fewer employees. These findings are consistent with the arguments of [5], who stated that the maturity of industry sectors and governance systems has a significant influence on cybersecurity postures and [23], who pointed at the importance of economic and policy environments in contributing to resource allocation and the advanced TI adoption. The Technology sector holds the advantage of being an early adopter of other resources in the sphere of cybersecurity innovation and encompassing a cultural focus on digital resilience, as it is consistent with [13]. On the same note, bigger organizations can enjoy economies of scale, dedicated security forces and access to commercial intelligence feeds, which would boost their prevention abilities as outlined by [16] [28]. The existence of these differences highlights the fact that specific measures should be taken to empower under-resourced industries, like Government and Retail and smaller businesses in order to ensure fair access to effective TI and eliminate disparities in cyber defense maturity in the U.S. organizational environment.

F. Strengthening Threat Intelligence Practices to Combat Financially Motivated Cyberattacks in the U.S.

The study presents practical recommendations on how organizations in the U.S. can enhance the importance of threat intelligence (TI) to become more effective in the prevention of financially motivated cyberattacks. The fact that the correlation between collaboration and TI effectiveness is consistent (r = 0.42, p < .01; Table 9) and that there is a significant Chi-square outcome between the two variables (X^2 (16) = 33.325, p = 0.007; Table 5) indicates that those organizations that actively collaborate with their peers and government agencies perceive TI as more effective. This implies that the U.S. cybersecurity environment can highly be improved by expanding such initiatives as ISACs and PPPs to promote collective intelligence and response capacity as claimed by [11], [13] and [20]. The low percentage of TI sharing (Table 4) (in 48% of respondents), even though it is obvious that TI sharing has more benefits than drawbacks, indicates that there are still potentials to enhance inter-organizational information sharing.

The other significant implication is to do with the integration of artificial intelligence and TI. Having 40.5% of respondents think that AI improves cyber defense (Table 4) and with strong predictive power of AI belief with respect to sector (OR = 2.43), TI usage (OR = 3.07) and perceived effectiveness (OR = 2.12; Table 6), it is clear that the U.S. organizations have become ready to deploy AI-augmented TI. According to [26], AI features such as anomaly detection, predictive analytics and automated threat actor profiling may assist the U.S. firms in going beyond reactive security to proactive prevention. The investment in TI tools with AI capabilities may help to gain competitive advantage and resolve some of the challenges mentioned by the respondents, including untimely intelligence (22%) and the sheer amount of data volumes (18.5%; Table 3). The results support the idea that it is important to target recurrent structural and resource-related obstacles to TI adoption and efficacy. A considerable part of the respondents mentioned high costs (21%), unskilled staff (20.5%) and too much data (18.5%) as the key challenges (Table 3), which were also the problems raised by previous research by [6] and [10]. Both barriers have an unequal impact on smaller organizations, with a clear difference in indicated levels of TI effectiveness by the organization size (H (3) =11.22, p=0.010; Table 10) indicating that firms with less than 50 employees believe in lower effectiveness. As [9] and [13] note, the targeted investments in workforce training, the subsidized access to the TI feeds and the development of the custom solutions targeting small and medium-sized enterprises (SMEs) are the key to bridging such gaps.

The differences between TI effectiveness by sector and role with Technology sector being superior to the Government and Retail sectors and CISOs performing better than SOC Analysts (Table 10) indicate that the issue of resources and expertise allocation in the U.S. organizational environment should be redressed. The adoption of TI in under-resourced sectors should be encouraged with national policies, along with the creation of a culture of information sharing, which may reduce these differences, as suggested by [2] and [5]. The results indicate a complex approach to the U.S. organizations: the establishment of a cooperative culture of information exchange, the investment in the TI capabilities using AI, the facilitation of the cost and skill obstacles via specific workforce development and the support of underrepresented sectors and SMEs. This comprehensive method would enhance TI efficiency, reduce the threat of financial cybercrimes and increase the resilience of the digital economy at the national level, which is the vision of [9] and [18] regarding the proactive and inclusive cyber defense approach.

LIMITATIONS

Although this research study can offer some useful ideas concerning the role of threat intelligence (TI) in deterring financially motivated cyberattacks in the U.S. organizations, one must consider various limitations. First, the data was obtained by using survey self-reported answers and this could be prone to social desirability effects and inaccurate perceptions of the respondents as to the TI capabilities in their organization. Second, the cross-sectional nature of the research restricts the possibility of making causal conclusions regarding the nature of the connections between such variables as collaboration, AI adoption and TI effectiveness. Third, the sample, as heterogeneous as it was in respect to the industries, positions and sizes of organizations, might not be representative of all the industries of the U.S, especially those industries with a high degree of regulation or those with niche markets. Also, the effectiveness of TI was not directly measured by the study but instead, it used perceived effectiveness of TI, which may not necessarily cohere well with objective security outcome. Lastly, although the survey has covered a wide scope of organizational variables, it failed to have a profound penetration on technical implementations or cultural aspects that could also affect the effectiveness of TI. The limitations of this study can be overcome in future research using longitudinal designs, objective performance measures and qualitative data; this would offer a more convincing picture on how TI can help prevent financially motivated cyberattacks.

CONCLUSION

The study presented the findings of a U.S.-based organizational-level research on the role of threat intelligence (TI) in preventing financially motivated cyberattacks and offered empirical evidence regarding its perceived effectiveness, use patterns and organizational and contextual factors that affect its success. The results show clearly that TI is seen as an important part of cyber defense, particularly within the Technology segment and bigger organizations and where high positions of authority, like CISOs, put a premium on its use in security plans. The key correlation between the active participation in collaboration with peers, industry groups and government agencies and the effective application of the TI was also connected and supported the evidence that collective intelligence and collaboration can help to mitigate the advanced financial cyber threat. The increasing confidence in artificial intelligence as an addition to TI, also points out the potentiality in the field of innovation of the detection, prediction and response capabilities [29].

There are still substantial obstacles- such as untimely intelligence, cost inefficiency, skill gaps and data overload- that remain and which tend to burden smaller organizations and younger industries particularly. These results require the implementation of specific measures that can promote equal opportunities in accessing TI resources, develop workforce skills and promote the use of AI throughout the organizational environment in the U.S. The collaboration between policymakers and practitioners must be intensified to enable more people to access and use advanced tools, subsidize costs and develop best practices that would render TI more feasible and effective to everyone.

With the increasing complexity and frequency of the financially motivated cyberattacks, it is critical to adopt a proactive, collaborative and technology-based threat intelligence. This will help both to improve the resilience of the organization as well as help to preserve the integrity and stability of the U.S. digital economy. Future studies ought to complement those by using such designs as longitudinal, objective security outcomes and qualitative data to better understand how TI can alleviate financial cybercrime.

REFERENCES

[1] N. H. Al-Kumaim and S. K. Alshamsi, "Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership," *Appl. Sci.*, vol. 13, no. 10, p. 5839, 2023.

[2] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, "Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations," *Sensors*, vol. 23, no. 9, p. 4539, 2023.

[3] N. Banerjee, "Exploring the future of AI in cyber threat intelligence," in *AI-Enabled Threat Intelligence and Cyber Risk Assessment*, CRC Press, 2025, pp. 126–148.

[4] D. A. Brooks, *Cyber Threat Intelligence Driven Phishing Awareness Programs: A Qualitative Exploratory Study*, Capitol Technology University, 2023.

[5] M. Colajanni and M. Marchetti, "Cyber-attacks and defenses: current capabilities and future trends," in *Technology and International Relations*, Edward Elgar Publishing, 2021, pp. 132–151.

[6] B. Cinar, "Cyber threat intelligence: Current trends and future perspectives," *J. Eng. Res. Rep.*, vol. 25, no. 4, pp. 91–105, 2023.

[7] G. Cascavilla, "The rise of cybercrime and cyber-threat intelligence: Perspectives and challenges from law enforcement," *IEEE Secur. Priv.*, vol. 23, no. 1, pp. 17–26, 2024.

[8] Y. Arafat, "Business Intelligence as a Strategic Asset: Measuring Its Role in Enhancing US National Interests across Defense, Trade, and Cyber Domains," *J. Bus. Insight Innov.*, vol. 4, no. 1, pp. 1–20, 2025.

[9] O. Eltayeb, "The Crucial Significance of Cyber Threat Intelligence in Mitigating Cyber Attacks," *J. Ecohumanism*, vol. 3, no. 4, pp. 2422–2434, 2024.

[10] F. Fatima, *A Qualitative Exploratory Study of Cyber Threats to Financial Organizations*, University of the Cumberlands, 2024.

[11] E. Gaitan, *Developing and Sharing Threat Intelligence: Strategies for Small and Medium-Sized Businesses*, Doctoral dissertation, Capella University, 2022.

[12] M. A. Joyner, *Strategies Using Threat Intelligence to Detect Advanced Persistent Threats: A Qualitative Case Study*, Doctoral dissertation, Walden University, 2022.

[13] I. Alim, "The impact of Artificial Intelligence on the accounting profession: technological advancements and employment perspectives," *Int. J. Sci. Res. Arch.*, vol. 15, no. 3, pp. 1173–1187, 2025. DOI: 10.30574/ijsra.2025.15.3.1873

[14] 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," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 3, pp. 1–15, 2025.

[15] M. Danish and M. M. Siraj, "AI and Cybersecurity: Defending Data and Privacy in the Digital Age," *J. Eng. Comput. Intell. Rev.*, vol. 3, no. 1, pp. 25–35, 2025.

[16] Z. Lanz, "Cybersecurity risk in US critical infrastructure: An analysis of publicly available US government alerts and advisories," *Int. J. Cybersecurity Intell. Cybercrime*, vol. 5, no. 1, pp. 43–70, 2022.

[17] A. Shaheen, "Cybersecurity in the Modern Era: An Overview of Recent Trends," *J. Eng. Comput. Intell. Rev.*, vol. 1, no. 1, pp. 39–50, 2023.

[18] V. Mavroeidis, R. Hohimer, T. Casey, and A. Jesang, "Threat actor type inference and characterization within cyber threat intelligence," in *Proc. 2021 13th Int. Conf. Cyber Conflict (CyCon)*, 2021, pp. 327–352.

[19] E. R. Ndukwe and B. Baridam, "A graphical and qualitative review of literature on AI-based cyber-threat intelligence (CTI) in banking sector," *Eur. J. Eng. Technol. Res.*, vol. 8, no. 5, pp. 59–69, 2023.

[20] I. V. Patel, *The Necessity of Cyber Threat Intelligence*, Master's thesis, Utica College, 2021.

[21] N. Rahimi and H. Jones, "Cyber Warfare: Strategies, Impacts and Future Directions in the Digital Battlefield," *J. Inf. Secur.*, vol. 16, no. 2, pp. 252–269, 2025.

[22] N. Arshad, "A Comprehensive Review of Emerging Challenges in Cloud Computing Security," *J. Eng. Comput. Intell. Rev.*, vol. 2, no. 1, pp. 27–37, 2024.

[23] M. Z. Afshar and D. M. H. Shah, "Strategic evaluation using PESTLE and SWOT frameworks: Public sector perspective," *ISRG J. Econ. Bus. Manag.*, vol. 3, pp. 108–114, 2025.

[24] N. Sun et al., "Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 3, pp. 1748–1774, 2023.

[25] M. Z. Afshar and M. H. Shah, "A Narrative Review for Revisiting BCG Matrix Application in Performance Evaluation of Public Sector Entities," *J. Res. Rev.*, vol. 2, no. 2, pp. 325–337, 2025.

[26] M. Tahmasebi, "Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises," *J. Inf. Secur.*, vol. 15, no. 2, pp. 106–133, 2024.

[27] C. Yatagan, *Interaction between the US Intelligence Community and the Private Sector in Sharing Cyber Threat Intelligence*, American University, 2022.

[28] M. Asif, M. A. Pasha, A. Mumtaz, and B. Sabir, “Causes of Youth Unemployment in Pakistan”, *IJSS*, vol. 2, no. 1, pp. 41–50, Mar. 2023.

[29] M. Asif, “Integration of Information Technology in Financial Services and its Adoption by the Financial Sector in Pakistan”, IJSS, vol. 1, no. 2, pp. 23–35, Dec. 2022.