

American Journal of Scholarly Research and Innovation

Volume: *16;* ***Issue:*** *09*
Pages: *40– 78*
eISSN: 3067-2163

Artificial Intelligence Integrated MIS Framework for Proactive Cyber Threat Intelligence and Organizational Security Resilience

Kynatun Mahin[1];

[1]. Master of Science in Management Information Systems (MIS), Lamar University, USA;
Email: kynat.mahin@gmail.com

Doi: 10.63125/t98tc495
Received: *17 June 2026;* ***Revised:*** *20 July 2026;* ***Accepted:*** *06 August 2026;* ***Published:*** *02 September 2026;*

Abstract

Organizations increasingly deploy artificial intelligence, cyber threat intelligence, automated security tools, and Management Information Systems, yet fragmented security information and predominantly reactive processes can limit proactive threat management and organizational resilience. This study aimed to develop and empirically evaluate an Artificial Intelligence Integrated MIS Framework linking intelligent cybersecurity capabilities with proactive cyber threat management and organizational security resilience. A quantitative, cross-sectional, multiple-case-based design was employed using approximately 300 valid professional responses representing enterprise, cloud-enabled, financial-services, telecommunications, manufacturing, healthcare, and other data-intensive organizational cases. The principal variables were AI-Enabled Threat Detection, Cyber Threat Intelligence Integration, MIS Security Information Integration, Automated Threat Response, Predictive Cyber Risk Analytics, Proactive Cyber Threat Management, and Organizational Security Resilience. Data analysis incorporated descriptive statistics, Cronbach's alpha, Kaiser-Meyer-Olkin assessment, Bartlett's test, Pearson correlation, ordinary least-squares multiple regression, variance inflation factors, tolerance, Durbin-Watson statistics, and residual diagnostics. Findings showed high construct means ranging from 3.91 for Automated Threat Response to 4.14 for Organizational Security Resilience, with overall instrument reliability of $\alpha = 0.93$ and KMO = 0.884. Correlations between the five AI-integrated MIS capabilities and proactive threat management ranged from $r = .54$ to $r = .72$, with Predictive Cyber Risk Analytics showing the strongest association. The first regression model explained 63.8% of PCTM variance, $R^2 = .638$, adjusted $R^2 = .631$, $F(5,294) = 103.63$, $p < .001$. The second model explained 68.4% of Organizational Security Resilience variance, $R^2 = .684$, adjusted $R^2 = .677$, $F(6,293) = 105.70$, $p < .001$, with Proactive Cyber Threat Management producing the strongest effect, $\beta = .38$, $p < .001$. The findings imply that coordinated AI detection, threat intelligence, MIS integration, predictive analytics, and automated response can strengthen proactive cybersecurity decision-making, adaptive defense, continuity, recovery, and organizational security resilience.

Keywords: *Artificial Intelligence; Management Information Systems; Cyber Threat Intelligence; Proactive Cyber Threat Management; Organizational Security Resilience*

INTRODUCTION

Artificial intelligence (AI) in cybersecurity refers to the use of computational techniques capable of learning from security data, recognizing complex patterns, supporting decisions, and executing or recommending actions that traditionally require substantial human analytical effort. A Management Information System (MIS) represents the coordinated combination of people, processes, data, technologies, and organizational procedures used to collect, process, store, distribute, and apply information for operational and managerial decision-making. Cyber threat intelligence (CTI) consists of contextualized knowledge concerning threat actors, vulnerabilities, attack techniques, malicious infrastructure, indicators of compromise, targets, and threat behaviors that can be transformed into actionable security decisions rather than retained as raw threat data (Kanti, 2026; Samtani et al., 2020; Tounsi & Rais, 2018). Proactive cyber threat management consequently describes the organizational capacity to identify, interpret, prioritize, and address potential cyber threats before or during their earliest stages of materialization, while organizational security resilience concerns the ability to prepare for, withstand, respond to, recover from, and adapt after cyber-related disruption (Alhidaifi et al., 2024; Hausken, 2020; Shamima, 2026). These concepts have strong international significance because organizations now operate through interconnected enterprise systems, cloud services, remote-access environments, digital supply chains, and cross-border information flows. Cybersecurity has consequently become simultaneously a technological, informational, managerial, and organizational requirement. AI-enabled cybersecurity has been particularly relevant where organizations must process heterogeneous security data at a volume and speed that exceed the practical capacity of exclusively manual analysis (Dilek et al., 2015; Pervaz, 2026; Samtani et al., 2020). An AI-integrated MIS can therefore be viewed as an organizational information architecture in which intelligent security analytics, threat intelligence, enterprise information flows, and security decision processes have been intentionally connected so that security information becomes usable for operational defense and management decision-making (Kaium, 2026; Naik et al., 2022; Qamar et al., 2017).

The technical foundation of AI-integrated cybersecurity has rested on the capacity of machine-learning and deep-learning methods to transform high-volume security observations into classifications, anomalies, risk indicators, and decision-relevant patterns. Network intrusion detection research has shown that machine-learning performance in operational environments is more demanding than laboratory classification because traffic diversity, changing user behavior, labeling limitations, base-rate effects, and false alarms complicate real-world deployment (Mashiat, 2026; Sommer & Paxson, 2010). Reviews of data mining and machine learning for intrusion detection have demonstrated that classification, clustering, neural computation, and statistical learning can support the identification of malicious activity, while their performance has remained dependent on representative training data, feature quality, evaluation design, and attack characteristics (Buczak & Guven, 2016; Mashfiqur, 2026; Xin et al., 2018). Deep-learning approaches have expanded these capabilities by learning higher-level representations from complex network data. Recurrent neural networks have been applied to distinguish normal and malicious network behavior, while representation-learning architectures have reduced reliance on manually engineered features in intrusion-detection tasks (Khalid, 2026; Shone et al., 2018; Yin et al., 2017). AI-based cyber defense has therefore required adaptable analytical mechanisms capable of processing multiple classes of threats and supporting timely decisions in environments that cannot be monitored effectively through human intervention alone (Dilek et al., 2015; Jannatul, 2026). The value of these systems has also depended strongly on data quality. Research on intrusion-detection datasets has shown that outdated, unrepresentative, insufficiently diverse, or artificially structured datasets can restrict the operational validity of learning-based systems (Hindy et al., 2020; Ring et al., 2019). Accordingly, AI-enabled threat detection has been treated in this study not as a stand-alone algorithm, but as an organizational capability that receives security data, generates interpretable signals, and supplies them to broader threat-intelligence, risk-assessment, MIS, and response processes.

Cyber threat intelligence has provided an informational bridge between detection and proactive organizational defense because isolated alerts become strategically useful only when they are contextualized in relation to assets, vulnerabilities, attack pathways, adversary behaviors, and organizational exposure. Data-driven CTI research has shown that shared threat information can be

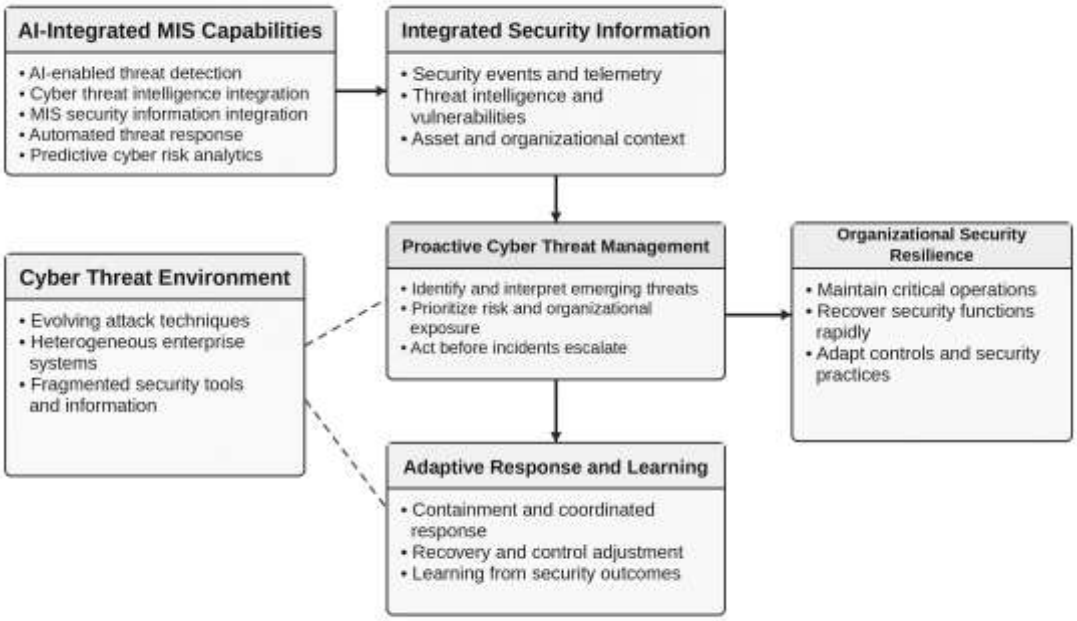
transformed through semantic reasoning and contextual analysis to identify relevance, exposed assets, attack likelihood, and associated network risk, thereby highlighting the importance of linking external intelligence with the internal characteristics of the protected environment (Jahanara, 2026; Qamar et al., 2017). Technical CTI scholarship has similarly distinguished raw indicators from actionable intelligence and has emphasized timeliness, contextualization, interoperability, standardization, trust, and relevance as central attributes of useful threat knowledge (Tounsi & Rais, 2018; Wagner et al., 2019). Predictive cybersecurity extends this orientation by using historical and contemporaneous security information to estimate adverse conditions before conventional reactive controls would otherwise identify them. Research surveying data-driven cybersecurity incident prediction has documented machine learning, statistical modeling, network information, vulnerability signals, and external data sources as inputs to forecasting malicious activity (Ahmed, 2026; Sun et al., 2019). CTI mining research has further organized proactive defense around the acquisition, processing, analysis, and utilization of heterogeneous threat intelligence, showing that intelligent mining can extract actionable knowledge from otherwise fragmented security information (Sun et al., 2023; Feroz, 2025). Samtani et al. (2022) demonstrated how deep semantic analysis can connect exploit discussions from adversarial online environments with known vulnerabilities, supporting vulnerability prioritization and proactive risk analysis. Detection alone has not completed this process, because identified threats require context-sensitive response selection and timely countermeasures. Intrusion-response research has consequently emphasized the integration of detection and response mechanisms rather than treating them as separate operational stages (Anwar et al., 2017; Rony & Md, 2026).

The MIS dimension has been critical because cybersecurity effectiveness has been determined not only by algorithmic predictive accuracy but also by whether security information has been integrated into organizational processes, governance structures, policies, and decision systems. AI-for-cybersecurity research has characterized cybersecurity as a multidisciplinary information problem involving heterogeneous datasets, advanced analytical methods, human expertise, organizational decision-making, and security operations rather than an isolated technical classification task (Chandra, 2025; Samtani et al., 2020). Organizational information-security research has also shown that user awareness and rational beliefs influence compliance with information-security policies, illustrating that organizational protection depends on interactions between technical controls and human decision structures (Bulgurcu et al., 2010; Pervaz, 2025). This interaction has been particularly important for MIS because management information infrastructures connect databases, applications, users, business processes, analytical systems, and managerial functions. Security information that remains fragmented across detection tools, security operations, threat feeds, vulnerability platforms, network systems, and managerial reporting structures can limit the organization's ability to construct a coherent interpretation of cyber risk. Dynamic Capabilities Theory has offered an appropriate organizational lens because it conceptualizes adaptation through the abilities to sense environmental developments, seize appropriate responses, and reconfigure resources and processes under changing conditions (Kaium, 2025; Teece, 2007). In the present cybersecurity setting, AI-enabled detection and CTI have been aligned with sensing; predictive analysis, MIS integration, and security decision-making have supported seizing; and automated response, resource adjustment, recovery, and organizational learning have represented reconfiguration. Organizational learning research has connected adaptability and absorptive capacity with continuous improvement in information-security management, reinforcing the treatment of cybersecurity as an adaptive organizational capability rather than a fixed collection of technical controls (Ghahramani et al., 2023; Arif Uz et al., 2025).

Organizational security resilience has broadened the research focus from preventing individual intrusions to maintaining and restoring essential organizational functions when cyber events occur, while incorporating preparation, adaptation, and institutional learning into the security process. Research on cyber resilience has treated resilience as an interconnected phenomenon involving technological resources, human expertise, governance arrangements, continuity processes, incident preparedness, response capacity, recovery, and adaptation (Bagheri et al., 2022; Hausken, 2020; Mashiat, 2025). The tensions of cyber resilience have also been examined across preparatory, response, and adaptive activities, showing that resilience practices operate within organizational, environmental, definitional, and regulatory conditions that security professionals and managers must interpret

(Dupont et al., 2023; Mashfiqur, 2025). Broader surveys have identified preparation, absorption, recovery, and adaptation as major dimensions connected with risk management, threat modeling, continuity, technical controls, and organizational security processes (Alhidaifi et al., 2024; Jahanara, 2025). AI has added an analytical layer to this configuration by enabling anomaly recognition, behavioral analysis, threat classification, malware identification, and security decision support, although the organizational value of these capabilities has depended on their integration into usable information and response processes (Mostari, 2025; Naik et al., 2022; Samtani et al., 2020). Existing research has therefore developed strong streams on AI-based intrusion detection, machine-learning cybersecurity, CTI sharing, predictive incident analysis, automated response, information-security management, and cyber resilience, but these streams have frequently examined individual technical functions or organizational components separately. The present research has been positioned at their intersection by examining AI-Enabled Threat Detection, Cyber Threat Intelligence Integration, MIS Security Information Integration, Automated Threat Response, and Predictive Cyber Risk Analytics as measurable organizational capabilities associated with Proactive Cyber Threat Management and Organizational Security Resilience. This integrated framing has treated MIS as the organizational information backbone through which AI-derived security intelligence can be captured, contextualized, communicated, and operationalized (Ghahramani et al., 2023; Jannatul, 2025; Samtani et al., 2022).

Figure 1: AI-Integrated MIS Cybersecurity Overview



Background of the Study

The increasing dependence of modern organizations on Management Information Systems has transformed cybersecurity from a narrowly technical concern into a core organizational and managerial requirement. Contemporary MIS environments integrate databases, enterprise applications, cloud services, communication platforms, customer information, financial systems, human resource systems, operational technologies, and decision-support functions. As these systems have become more interconnected, the volume, variety, and velocity of organizational information have also increased, creating a wider attack surface for cybercriminals, malicious insiders, organized threat groups, and automated attack mechanisms. Traditional cybersecurity practices have largely depended on predefined rules, signature-based detection, manual security monitoring, and reactive incident response. Such approaches remain useful in many contexts, but they are often inadequate for detecting sophisticated, rapidly changing, and previously unknown threats. Artificial intelligence has offered a more adaptive approach by enabling organizations to process large quantities of security-related data, detect anomalous activities, recognize attack patterns, prioritize threats, and support faster security

decisions. At the same time, cyber threat intelligence has become an important component of organizational security because it provides contextualized knowledge about adversaries, vulnerabilities, indicators of compromise, attack techniques, and emerging risks. However, many organizations continue to manage AI-supported security tools, cyber threat intelligence platforms, MIS data, and incident-response mechanisms as separate functions. This fragmentation can delay the transformation of raw security information into actionable organizational knowledge. An AI-integrated MIS framework can address this limitation by connecting intelligent threat detection, cyber threat intelligence, security information integration, predictive risk analytics, and automated response within a unified organizational information environment. Such integration can improve the ability of organizations to move from reactive cybersecurity toward proactive threat management, where threats are identified, interpreted, prioritized, and addressed before they cause severe disruption. Within this context, organizational security resilience becomes particularly important because cybersecurity effectiveness should not be measured only by whether attacks are prevented, but also by how effectively an organization can prepare for cyber incidents, maintain essential operations, respond rapidly, recover from disruption, and adapt its security capabilities. This study has therefore focused on developing and empirically assessing an artificial intelligence integrated MIS framework that connects AI-enabled cybersecurity capabilities with proactive cyber threat intelligence and organizational security resilience.

Problem Statement

Organizations are increasingly investing in artificial intelligence, cyber threat intelligence, security information platforms, automated monitoring tools, and advanced Management Information Systems to strengthen their cybersecurity capabilities. However, the availability of these technologies does not necessarily create an integrated or proactive security environment. In many organizations, security data remain distributed across separate systems such as intrusion-detection platforms, network monitoring tools, vulnerability databases, security information and event management systems, enterprise applications, external threat intelligence feeds, and managerial reporting systems. This fragmentation can reduce the speed and quality of cybersecurity decision-making because relevant information must often be manually collected, interpreted, and communicated across different technical and managerial units. Another problem is that many existing cybersecurity mechanisms remain strongly reactive. They primarily identify malicious activities after suspicious behavior has already entered the organizational environment, which can limit the time available for prevention, containment, and risk mitigation. Artificial intelligence can improve threat detection and predictive analysis, but its organizational value may remain limited when AI-generated security outputs are not properly integrated with MIS information, cyber threat intelligence, automated response processes, and organizational decision structures. Existing research also frequently examines AI-based intrusion detection, threat intelligence sharing, predictive analytics, or cyber resilience as separate areas rather than as interconnected organizational capabilities. Consequently, there is limited empirical understanding of how these capabilities collectively influence proactive cyber threat management and organizational security resilience. There is also a need to determine which specific AI-integrated MIS capabilities make the strongest contribution to organizational cybersecurity outcomes. Without such evidence, organizations may adopt advanced security technologies without understanding how these technologies should be coordinated within their broader MIS architecture. This research has addressed this problem by examining AI-enabled threat detection, cyber threat intelligence integration, MIS security information integration, automated threat response, predictive cyber risk analytics, proactive cyber threat management, and organizational security resilience within a unified quantitative framework.

Purpose and Objectives of the Study

The primary purpose of this study has been to develop and empirically evaluate an Artificial Intelligence Integrated MIS Framework for Proactive Cyber Threat Intelligence and Organizational Security Resilience. The study has sought to determine how selected AI-enabled and MIS-oriented cybersecurity capabilities contribute to proactive cyber threat management and to the broader resilience of organizations against cyber disruption. More specifically, the research has aimed to assess the influence of AI-Enabled Threat Detection Capability on the ability of organizations to identify and

respond to emerging cyber risks in a proactive manner. It has also sought to examine the relationship between Cyber Threat Intelligence Integration and proactive cyber threat management by determining whether the effective incorporation of external and internal threat intelligence supports more timely and informed cybersecurity action. Another objective has been to evaluate the contribution of MIS Security Information Integration, particularly the extent to which centralized and coordinated security information supports organizational awareness, decision-making, and cyber risk prioritization. The study has further aimed to examine the effect of Automated Threat Response Capability on proactive cyber threat management and to determine whether faster and more structured response mechanisms improve organizational preparedness against cyber incidents. Predictive Cyber Risk Analytics has also been examined as a core capability because organizations increasingly require analytical mechanisms that identify patterns, vulnerabilities, and potential attack conditions before they escalate into major incidents. In addition, the study has evaluated the relationship between Proactive Cyber Threat Management Capability and Organizational Security Resilience, determined the combined predictive influence of the five AI-integrated MIS capabilities on resilience, and integrated the empirical findings into a coherent framework explaining how organizational information systems, intelligent security technologies, and proactive cyber threat management capabilities operate together within a unified security architecture.

Research Hypotheses

The hypotheses have been formulated to test the proposed relationships among AI-integrated MIS cybersecurity capabilities, proactive cyber threat management, and organizational security resilience. The first five hypotheses have examined whether AI-Enabled Threat Detection, Cyber Threat Intelligence Integration, MIS Security Information Integration, Automated Threat Response, and Predictive Cyber Risk Analytics each have a significant positive effect on Proactive Cyber Threat Management. The sixth hypothesis has examined whether Proactive Cyber Threat Management has a significant positive effect on Organizational Security Resilience, while the seventh hypothesis has tested whether the five AI-integrated MIS capabilities collectively have a significant positive effect on Organizational Security Resilience. These relationships have translated the conceptual framework into statistically testable propositions suitable for Pearson correlation and multiple regression analysis. They have also maintained direct alignment with Dynamic Capabilities Theory: AI-enabled detection and CTI have represented organizational sensing, security information integration and predictive analytics have supported interpretation and seizing, and automated response together with proactive threat management has represented the reconfiguration of security resources. The hypotheses have therefore connected the theoretical framework, research objectives, survey constructs, and statistical models within a single analytical structure. Statistical support has been evaluated at the $p < .05$ level, with direction, standardized coefficients, model explanatory power, and diagnostic statistics used to determine the strength and credibility of the proposed relationships.

H1: AI-Enabled Threat Detection Capability has a significant positive effect on Proactive Cyber Threat Management Capability.

H2: Cyber Threat Intelligence Integration has a significant positive effect on Proactive Cyber Threat Management Capability.

H3: MIS Security Information Integration has a significant positive effect on Proactive Cyber Threat Management Capability.

H4: Automated Threat Response Capability has a significant positive effect on Proactive Cyber Threat Management Capability.

H5: Predictive Cyber Risk Analytics has a significant positive effect on Proactive Cyber Threat Management Capability.

H6: Proactive Cyber Threat Management Capability has a significant positive effect on Organizational Security Resilience.

H7: AI-Enabled Threat Detection, Cyber Threat Intelligence Integration, MIS Security Information Integration, Automated Threat Response, and Predictive Cyber Risk Analytics collectively have a significant positive effect on Organizational Security Resilience.

Significance of the Research

i. Significance for organizational management: The research has provided a structured basis for understanding how artificial intelligence, MIS, cyber threat intelligence, and security resilience can be coordinated rather than managed as isolated functions. The findings can help decision-makers identify which cybersecurity capabilities require greater attention within the broader information-system environment.

ii. Significance for cybersecurity professionals: The study has evaluated specific capabilities related to AI-enabled detection, threat intelligence, predictive analytics, and automated response, providing cybersecurity analysts, SOC teams, information-security managers, and network professionals with a clearer view of how these capabilities contribute to proactive threat management.

iii. Significance for MIS professionals: The research has highlighted MIS as an organizational information backbone for cybersecurity and has emphasized the integration of security information with managerial information flows, decision-support systems, operational processes, and enterprise-wide reporting structures.

iv. Significance for organizational security resilience: The study has extended cybersecurity assessment beyond attack prevention by considering organizational capacity to prepare for, withstand, respond to, recover from, and adapt to cyber incidents.

v. Significance for researchers: The study has combined AI-enabled cybersecurity, cyber threat intelligence, MIS integration, proactive threat management, and security resilience within one quantitative framework and has operationalized measurable constructs suitable for descriptive analysis, correlation, and regression modeling.

vi. Significance for policy and governance: The research has clarified the importance of coordinated information, analytical capability, automated response, human oversight, and organizational adaptation within enterprise cybersecurity governance and risk-management structures.

vii. Significance for technology adoption: The study has supported evaluation of advanced cybersecurity technologies not only by their technical features, but by how effectively they integrate with existing MIS processes and contribute to broader organizational security capabilities.

LITERATURE REVIEW

The literature on artificial intelligence, Management Information Systems, cyber threat intelligence, and organizational security resilience has expanded as organizations have become more dependent on interconnected digital infrastructures and data-intensive decision systems. Existing research has shown that cybersecurity is no longer limited to protecting individual computers or networks because organizational information environments combine enterprise applications, cloud platforms, databases, communication systems, digital services, operational technologies, and external information sources. This complexity has increased the need for intelligent mechanisms capable of processing large volumes of security data and identifying patterns that may indicate malicious activity. Artificial intelligence and machine-learning techniques have therefore become prominent in intrusion detection, anomaly recognition, malware analysis, behavioral monitoring, threat classification, vulnerability assessment, and predictive security analytics. At the same time, cyber threat intelligence has emerged as an important security capability because it transforms technical indicators, adversarial information, vulnerability data, attack patterns, and external threat observations into contextualized knowledge that can support organizational decision-making. MIS provides the organizational infrastructure through which this information can be collected, processed, communicated, and linked with broader operational and managerial activities. A further body of research has emphasized cyber resilience, focusing on the ability of organizations not only to prevent attacks but also to maintain critical operations, respond effectively, recover from disruption, and adapt their security practices. These research streams have often been examined independently, creating a need for a more integrated understanding of how AI-enabled threat detection, CTI, MIS security information integration, automated response, predictive analytics, and proactive threat management operate together. The literature review has therefore established the empirical and theoretical foundations of the proposed AI-integrated MIS framework.

2.1 Management Information Systems and the Contemporary Cyber Threat Environment

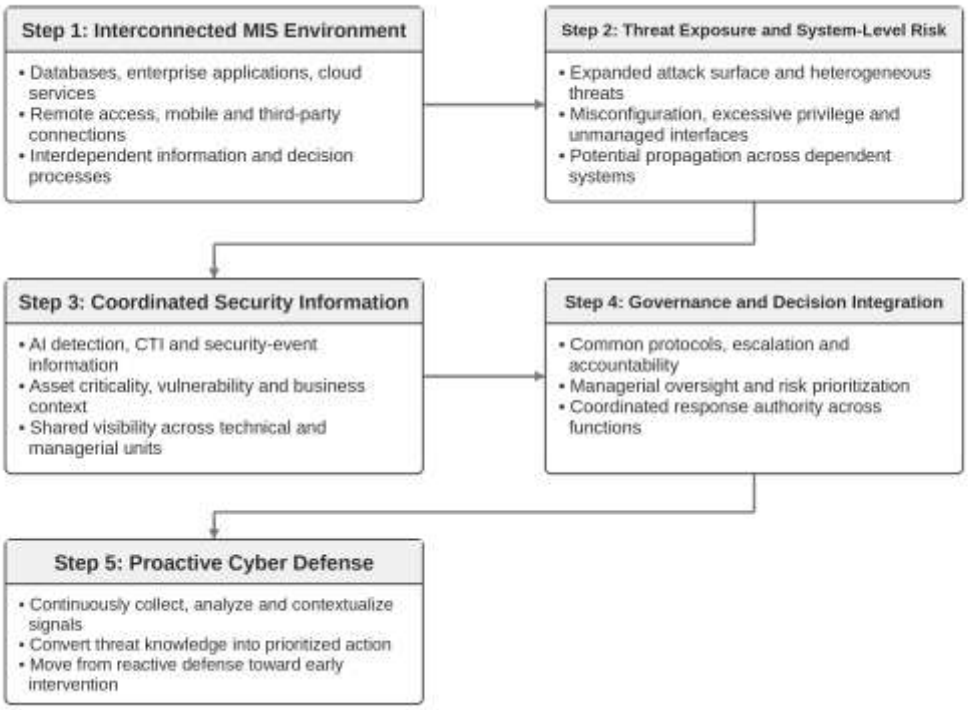
Management Information Systems have developed from transaction-processing and reporting mechanisms into interconnected organizational infrastructures that coordinate operational data, managerial information, communication, enterprise applications, and decision processes. This expansion has also altered the cybersecurity environment surrounding MIS because the same connectivity that permits rapid information exchange creates multiple points through which organizational assets can be exposed, manipulated, disrupted, or accessed without authorization. Contemporary cyber threats therefore have to be understood within the combined technical and organizational structure of information systems rather than as isolated attacks against individual computers. Organizations depend on databases, enterprise resource planning systems, customer platforms, cloud services, mobile access, remote connections, and third-party technologies, and weaknesses in any component can affect the confidentiality, integrity, and availability of information used for decision-making. In The Role of External and Internal Influences on Information Systems Security (pp. 153-172), organizational information security has been presented as being shaped by regulatory pressure, work practices, management involvement, employee awareness, and institutional forces, indicating that protection cannot be separated from the organizational environment in which systems are governed and used (Ashik & Shabbir, 2022; Hu et al., 2007). This perspective has been particularly relevant to an AI-integrated MIS because intelligent cybersecurity tools operate inside structures that determine what data are available, how alerts are interpreted, who is responsible for action, and how security priorities are balanced with operational objectives. As digital infrastructures have become more heterogeneous, security weaknesses have emerged through misconfiguration, fragmented ownership, inconsistent policies, unmanaged interfaces, excessive privileges, insufficient monitoring, and delayed communication between technical and managerial units. Cybersecurity has consequently become an essential MIS concern because failures in one information component can propagate across dependent processes, interrupt information availability, reduce decision quality, expose sensitive resources, and weaken managerial control. The cyber threat environment surrounding MIS is therefore a system-level problem in which technological exposure, organizational behavior, governance arrangements, information flows, operational dependencies, and managerial responsibilities interact continuously rather than functioning as independent security dimensions.

The complexity of organizational information security has also arisen from interactions among preventive controls, user behavior, threat frequency, business dependence, recovery capability, and the economic value of organizational information assets. In Dynamics of Organizational Information Security (pp. 349-375), information security has been modeled as an outcome of interacting technical and behavioral factors, demonstrating that technological safeguards cannot be properly evaluated without considering employee behavior and the business value generated through an organization's information-technology infrastructure (Dutta & Roy, 2008; Hasan & Adnan, 2022). This systems perspective has been important for the present research because an AI-integrated MIS framework must combine intelligent threat identification with organizational mechanisms that allow security information to be interpreted, prioritized, communicated, and acted upon. A technically accurate threat signal may provide limited organizational value when it remains disconnected from asset criticality, vulnerability information, business processes, managerial priorities, threat context, and response authority. Cybersecurity within MIS has therefore required coordinated portfolios of complementary controls instead of excessive dependence on a single defensive technology. In Understanding the Value of Countermeasure Portfolios in Information Systems Security (pp. 241-279), relationships among attack type, frequency, potential damage, countermeasure characteristics, business conditions, and recovery have been incorporated into an integrated assessment of security controls, illustrating why organizations need to evaluate countermeasures collectively rather than independently (Kumar et al., 2008; Mahbubul et al., 2022). This reasoning has been directly applicable to AI-enabled threat detection, CTI, predictive analytics, automated response, and MIS security information integration because each capability addresses a different stage of organizational cyber threat management. Detection recognizes potentially malicious behavior, threat intelligence provides contextual knowledge, MIS integration connects security events with organizational information, predictive analytics identifies risk patterns, and automated response reduces the interval between recognition and containment. When these

capabilities remain fragmented, an organization may experience duplicated alerts, inconsistent risk assessments, incomplete threat visibility, delayed escalation, competing priorities, and weak coordination between operational security personnel and managerial decision-makers. Effective MIS security has therefore depended on whether these capabilities exchange information through a common decision environment and whether organizational actors can translate analytical outputs into prioritized security actions.

Cybersecurity governance has consequently become inseparable from the design, administration, and strategic management of organizational information systems. MIS security decisions determine not only which technologies are implemented but also how authority is distributed, how controls are standardized, who receives security information, how organizational units coordinate, and how rapidly security knowledge can be translated into action. In Centralized IT Decision Making and Cybersecurity Breaches (pp. 758-787), an empirical analysis of 504 U.S. higher-education institutions showed that centralized IT governance was associated with fewer cybersecurity breaches and that the relationship was particularly relevant in heterogeneous computing environments, demonstrating that governance arrangements can influence security outcomes across complex information infrastructures (Liu et al., 2020; Mashfiqur & Md, 2022). Such evidence has been relevant to AI-supported organizational cybersecurity because machine-generated warnings, predictive risk assessments, and cyber threat intelligence require coordinated governance if they are to support consistent security decisions across departments and business functions. Fragmented responsibility can produce gaps among security operations, MIS administration, executive oversight, risk management, and incident response, while coordinated information governance can establish common protocols, shared visibility, escalation procedures, and clearer accountability.

Figure 2: MIS and Contemporary Cyber Threat Environment Framework



The contemporary cyber threat environment has also required consideration of security beyond a purely reactive model in which defenses are activated only after malicious activities become sufficiently visible. In The Whole of Cyber Defense: Syncing Practice and Theory, cyber defense has been organized into reactive, heuristic, and proactive modes, presenting organizational defense as a coordinated domain in which security practitioners combine established responses with adaptive and anticipatory approaches to cyberattacks (Nobrega et al., 2024; Mashiat & Rahman, 2022). Within an AI-integrated

MIS environment, this broader understanding has positioned cybersecurity as an organizational information-processing capability in which threat observations are continuously collected, analyzed, contextualized, communicated, and converted into preventive or responsive actions. The integration of security operations with MIS has also narrowed the separation between technical cybersecurity and managerial oversight by making threat intelligence available through information structures used to coordinate organizational resources, risks, operational priorities, and decisions.

2.2 Artificial Intelligence for Cyber Threat Detection and Predictive Security Analytics

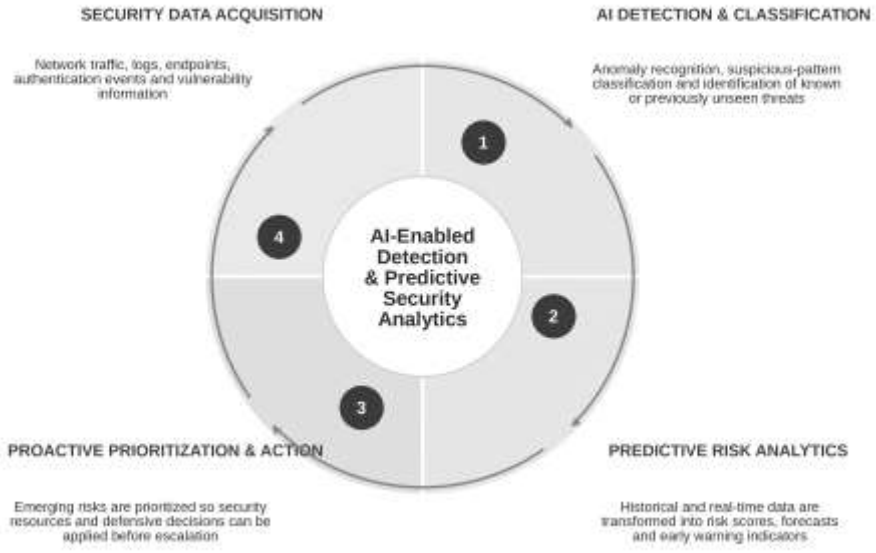
Artificial intelligence has become increasingly important in cyber threat detection because contemporary security environments generate data volumes and behavioral complexity that cannot be examined effectively through manually defined rules alone. AI-supported cybersecurity generally relies on machine learning and deep learning models that learn statistical or behavioral representations from network traffic, system logs, endpoint activity, authentication events, malware characteristics, and other security-relevant data. These models enable security systems to distinguish normal activity from suspicious behavior, classify known attack types, and identify anomalous patterns that may represent previously unseen threats. The shift from purely signature-based protection toward data-driven detection has been especially important for Management Information Systems because organizational networks continuously exchange information among users, applications, databases, cloud services, and external platforms. In A Survey of Deep Learning Methods for Cyber Security, deep autoencoders, recurrent neural networks, restricted Boltzmann machines, generative adversarial networks, and related architectures have been reviewed across malware detection, network intrusion detection, insider-threat analysis, spam, malicious domains, and false-data injection, demonstrating that deep learning can support several distinct cybersecurity functions (Berman et al., 2019; Md & Gazi Yeasin, 2022). In Deep Learning Approach for Intelligent Intrusion Detection System (pp. 41525-41550), deep neural networks have been evaluated across benchmark datasets to detect and classify attacks while addressing variations in attack behavior, network characteristics, and dataset composition, illustrating the importance of scalable learning models for environments in which malicious techniques are not static (Ashfaq & Mohammad, 2022; Vinayakumar et al., 2019). AI-enabled threat detection should therefore be treated as an organizational capability involving data collection, feature representation, model training, classification, anomaly recognition, and interpretation of security events rather than as the simple installation of an intelligent application. This capability becomes especially valuable when security teams must interpret high-volume events rapidly while preserving consistency across interconnected enterprise systems and information-processing activities.

Predictive security analytics extends AI-supported cybersecurity beyond identification of current malicious activity by using historical and real-time security data to estimate risk conditions, attack sequences, suspicious behaviors, and threat probabilities before severe organizational disruption occurs. This orientation requires a transition from alert-centered security toward data-centered security, in which information gathered from network activity, applications, databases, users, devices, vulnerabilities, and external intelligence is transformed into analytical knowledge. For MIS environments, this transformation has been important because information from technical security systems must become sufficiently structured to support operational and managerial decisions. Cybersecurity data science has provided an appropriate foundation by combining data acquisition, preprocessing, feature engineering, machine learning, behavioral analysis, pattern discovery, and decision support. In Cybersecurity Data Science: An Overview from Machine Learning Perspective, cybersecurity data science has been described as a data-driven approach in which machine-learning techniques extract incident patterns and security insights from multiple sources so that security processes can become more automated and intelligent; classification, clustering, association analysis, feature engineering, neural learning, targeted alerting, and resource optimization have been identified as relevant analytical functions (Kaniz & Jahanara, 2022; Sarker et al., 2020). In Cyber Threat Prediction with Machine Learning (pp. 203-220), machine-learning techniques including deep learning, autoencoding, and clustering with outliers have been applied to event-log and MITRE ATT&CK-related data generated through a red-team and blue-team exercise, with analysis directed toward identifying techniques and tactics associated with advanced persistent threats (Kok et al., 2020; Sadia & Mostari, 2022). Such work has demonstrated the analytical relationship among historical event

records, adversary-behavior frameworks, anomaly identification, and threat prediction. Within an AI-integrated MIS, predictive analytics can therefore operate as an intelligence layer connecting security-event monitoring with risk prioritization and earlier defensive action, while helping security personnel allocate investigative attention systematically toward patterns whose combined characteristics suggest elevated organizational exposure.

The distinction between cyber threat detection and cyber threat forecasting has been particularly important for proactive cybersecurity because detection identifies malicious or abnormal behavior that is already observable, whereas forecasting attempts to estimate types, timing, intensity, or development of threats before they are fully manifested within the protected environment. This difference changes the role of AI from a mechanism that merely classifies security events into one that supports anticipatory cyber risk management. Predictive capability can draw on longitudinal incident records, threat intelligence, vulnerability information, social and technical indicators, geopolitical conditions, attack histories, and organizational telemetry, provided that the underlying data are sufficiently reliable and relevant. Such analytical diversity has been appropriate for MIS because management systems already function as structures for consolidating organizational information from multiple sources. Integrating predictive cybersecurity with MIS can therefore create a decision environment in which technical threat indicators are evaluated alongside asset importance, operational dependencies, service criticality, and organizational risk priorities. In A Holistic and Proactive Approach to Forecasting Cyber Threats, a machine-learning framework using a monthly dataset of major cyber incidents across 36 countries over an eleven-year period has incorporated information from research literature, news, blogs, and social-media sources to forecast patterns across 42 cyber-threat categories, demonstrating how heterogeneous information can be combined for longer-range threat analysis (Almahmoud et al., 2023; Shaiful et al., 2022). The relevance of this approach to the present study has lain in the movement from isolated detection toward integrated analytical awareness. An organization may possess accurate intrusion-detection models while remaining reactive if their outputs are considered only after security events occur. Predictive analytics becomes more organizationally meaningful when threat indicators are linked with CTI, MIS security information, automated response mechanisms, and managerial risk decisions. AI-enabled detection and predictive cyber risk analytics have therefore been treated as complementary capabilities that connect observable anomalies with earlier assessment of security conditions.

Figure 3: AI-Enabled Threat Detection and Predictive Security Analytics Cycle



2.3 Cyber Threat Intelligence Integration and Proactive Threat Management

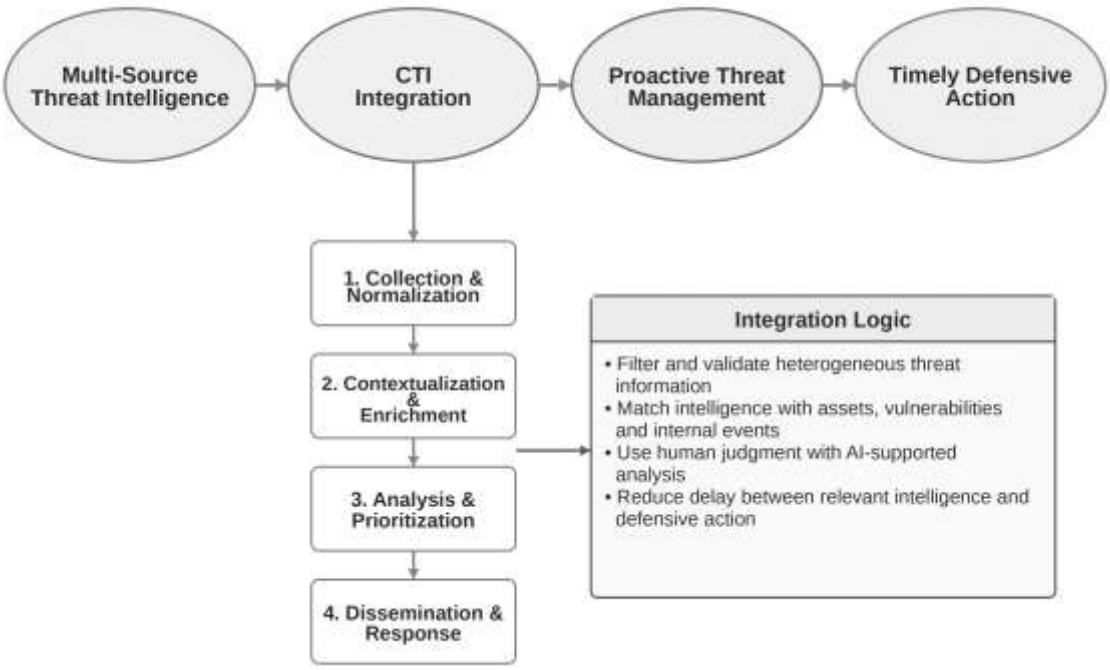
Cyber threat intelligence has become an essential component of proactive cybersecurity because it transforms fragmented technical observations into contextualized knowledge that can support threat recognition, prioritization, and coordinated defensive action. CTI generally incorporates information about threat actors, attack techniques, vulnerabilities, malicious infrastructure, indicators of compromise, campaigns, targets, and adversarial behavior so that security teams can understand not only what has occurred but why particular activity is relevant to an organization. Within an AI-integrated MIS environment, intelligence becomes especially valuable when external threat information is combined with internal security events, organizational assets, vulnerabilities, and operational priorities. In Threat Intelligence Sharing between Cybersecurity Vendors, intelligence sharing has been described as a mechanism through which detection by one organization can contribute to preventive knowledge for others, reducing duplicated analytical effort and increasing collective awareness of adversarial activity (Stabak & Shahid, 2022; Zrahia, 2018). The network-based examination of cybersecurity vendors has also demonstrated that CTI operates through relationships among organizations rather than through isolated technical systems. Such collaborative intelligence can strengthen proactive threat management when organizations receive information about malicious domains, attack infrastructure, vulnerability exploitation, malware behavior, or adversarial techniques before those indicators directly affect their own information systems. However, the usefulness of shared intelligence depends heavily on quality. In Measuring and Visualizing Cyber Threat Intelligence Quality (pp. 21-38), CTI quality has been examined through correctness, relevance, completeness, timeliness, and ability to support meaningful decisions, indicating that accumulation of threat information does not automatically produce actionable intelligence (Schlette et al., 2021; Feroz & Pervaz, 2022). For MIS-oriented cybersecurity, this distinction has been fundamental because management information environments require security data that can be interpreted in relation to organizational assets, operational dependencies, user activities, and business risk. Effective CTI integration therefore requires mechanisms that filter, validate, contextualize, enrich, and distribute threat information according to its relevance to the protected environment.

The effectiveness of cyber threat intelligence has also been determined by the breadth of information sources that organizations can analyze and the degree to which threat data can be converted into structured organizational knowledge. Threat actors operate across conventional websites, underground forums, social networks, malware ecosystems, compromised infrastructure, darknet marketplaces, and other digital environments, creating intelligence that varies in structure, reliability, accessibility, and analytical value. CTI has therefore required continuous processes of collection, normalization, enrichment, correlation, analysis, and dissemination rather than one-time acquisition of threat indicators. In Cybercrime Threat Intelligence: A Systematic Multi-Vocal Literature Review, cybercrime intelligence has been examined across surface, deep, and dark web environments, with attention to machine-learning and deep-learning techniques, indicators, risk parameters, and criminal activities that can be extracted from heterogeneous information sources (Mohammad, 2023; Cascavilla et al., 2021). This multi-source orientation has been highly relevant to proactive threat management because early signs of malicious campaigns may appear outside an organization's internal network before a direct attack occurs. Intelligence derived from external sources can therefore complement internal MIS security information by providing context about adversary capabilities, likely targets, exploited vulnerabilities, and attack patterns. Yet the operational value of intelligence depends on the systems through which it is organized and delivered. In A Success Model for Cyber Threat Intelligence Management Platforms, CTI management platforms have been evaluated through content quality, system quality, service quality, use, user satisfaction, perceived trust, and net benefits based on survey data from cybersecurity professionals (Adnan & Iftekhar, 2023; Zibak et al., 2021). This organizational perspective has been important because CTI platforms function as information systems rather than simple repositories. Their success depends on whether intelligence is trustworthy, accessible, usable, relevant, and integrated into analysts' work processes. Within the present research, CTI integration has therefore been conceptualized as the organizational capability to connect threat intelligence sources with MIS security information, analytical systems, and security decision processes.

Artificial intelligence further strengthens CTI integration by supporting automated processing of threat

information that would otherwise require extensive manual interpretation by security analysts. Traditional CTI workflows typically involve data collection, filtering, enrichment, correlation, analysis, dissemination, and subsequent defensive action. The increasing quantity of threat reports, technical indicators, vulnerability disclosures, malware descriptions, adversarial behavior records, and security events makes manual processing difficult when organizations must respond within short operational timeframes. AI techniques can assist this workflow through natural language processing, entity extraction, classification, clustering, anomaly detection, semantic analysis, pattern matching, risk scoring, and automated recommendation generation. In Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline, an AI-supported CTI architecture has been described in which intelligent techniques assist data ingestion, processing, analysis, predictive assessment, mitigation recommendation, and resilience verification, while human expertise remains necessary for contextual judgment and high-quality intelligence production (Ahmed & Sadia, 2023; Alevizos & Dekker, 2024). This human-AI configuration has been particularly appropriate for an MIS framework because organizational threat management involves both computational analysis and managerial interpretation. AI can process large volumes of threat information and identify relationships difficult to detect manually, while cybersecurity professionals determine organizational significance and select appropriate responses. Such integration can also improve proactive threat management by reducing delay between identification of relevant intelligence and implementation of defensive action. When CTI is connected with AI-enabled threat detection, predictive risk analytics, MIS security information, and automated response, external intelligence can be matched against internal conditions in near real time. CTI integration has therefore served as the informational mechanism connecting knowledge of the external threat environment with organizational security awareness, while proactive threat management has represented the capability to interpret and act on that knowledge before cyber events escalate into major disruption (Alevizos & Dekker, 2024; Asheke, 2023).

Figure 4: Cyber Threat Intelligence Integration and Proactive Threat Management Process



2.4 AI-Integrated MIS, Automated Threat Response, and Organizational Security Resilience

The integration of artificial intelligence into Management Information Systems strengthens cybersecurity when intelligent analytical capabilities are connected with the wider information architecture through which organizations detect, interpret, communicate, and respond to security events. An AI-integrated MIS therefore extends beyond deployment of machine-learning applications because effectiveness depends on interoperability among threat-detection tools, security information

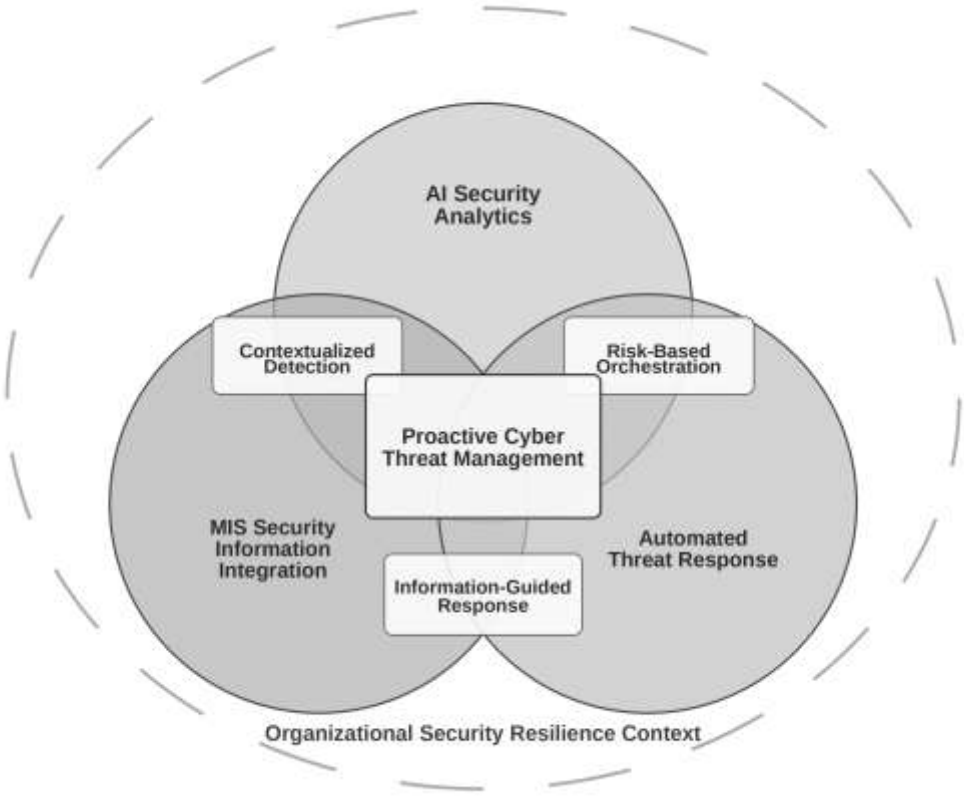
repositories, CTI, incident-management applications, and organizational decision systems. Modern security operations centers frequently operate technologies supplied by different vendors, including intrusion-detection systems, endpoint protection platforms, firewalls, vulnerability scanners, threat-intelligence platforms, SIEM systems, and case-management applications. When these technologies remain fragmented, analysts may need to move manually between platforms, repeatedly validate alerts, combine information from unrelated formats, and initiate response procedures through separate interfaces. This fragmentation can increase response time and reduce the organizational value of sophisticated security technologies. In A Multi-Vocal Review of Security Orchestration, security orchestration has been organized around unification, orchestration, and automation, with the literature showing that effective orchestration requires heterogeneous security resources to exchange information and execute coordinated activities rather than function independently (Yeasin, 2023; Islam et al., 2019). Such orchestration has been highly relevant to an AI-integrated MIS because AI-generated threat classifications become operationally useful only when they can be transmitted to systems and personnel responsible for investigation, risk assessment, containment, and managerial oversight. In Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform (pp. 165-181), a security-orchestration architecture has been developed to support automated integration among security tools and interpretation of activities used within incident-response processes, illustrating how architectural integration can reduce operational separation among security technologies (Islam et al., 2020; Jahanara & Kaniz, 2023). Within an MIS context, these findings have positioned integration as a structural cybersecurity capability in which security tools, organizational data, response workflows, and managerial information channels operate within a coordinated environment.

Automated threat response represents another central component of AI-integrated MIS because the organizational value of rapid threat detection can be reduced when response decisions remain dependent on slow, repetitive, or manually executed procedures. Security analysts commonly receive substantial numbers of alerts generated from network activity, endpoint behavior, authentication systems, threat intelligence, malware detection, vulnerability monitoring, and cloud environments. Not all alerts represent genuine threats, and validation may require correlation with multiple sources before an incident can be escalated. Artificial intelligence can reduce this burden by supporting automated classification, alert validation, prioritization, and recommendation processes, while orchestration platforms can translate validated security findings into predefined or context-sensitive actions. In SmartValidator: A Framework for Automatic Identification and Classification of Cyber Threat Data, an AI-based framework has been developed to automate validation of security alerts using machine-learning models dynamically constructed according to SOC requirements and available cyber threat information; its evaluation has shown how automated model construction can reduce analytical burden across different validation requirements (Islam et al., 2022; Rahman, 2023). This form of automated validation has been particularly relevant to proactive cyber threat management because it reduces the time between generation of a security alert and determination of whether organizational intervention is required. In an AI-integrated MIS, automated response can subsequently connect validated alerts with asset information, vulnerability records, user identities, business-process dependencies, and organizational risk classifications. For example, a malicious authentication pattern affecting a critical financial application should receive a different response priority from a similar anomaly occurring within a low-criticality testing environment. MIS integration enables such contextual differentiation because technical alerts can be associated with organizational information concerning asset value and operational dependence. Automated response therefore should not be conceptualized simply as automatic blocking. It includes structured escalation, enrichment, containment, notification, workflow assignment, evidence collection, and coordinated security actions controlled through organizational policies and human oversight.

Organizational security resilience provides the broader outcome through which integrated detection, intelligence, automation, response, and recovery capabilities can be evaluated. Cybersecurity mechanisms traditionally emphasize prevention and protection, but organizations cannot assume that every attack will be detected or stopped before affecting information assets and operational processes. Security resilience therefore requires organizations to combine preventive controls with capacities for

absorption, response, restoration, adaptation, and continuity of essential functions. In A Systematic Review of Cyber-Resilience Assessment Frameworks, cyber resilience has been examined across multiple frameworks and industries as an organizational capacity that extends beyond attack prevention by incorporating the ability to respond coherently to incidents and reduce disruptive effects on operations (Sheak & Tahmedur, 2023; Estay et al., 2020). This multidimensional view has been highly compatible with an AI-integrated MIS because organizational resilience depends on whether security information can be transformed into timely action across technological and managerial levels. Detection systems provide awareness, CTI supplies contextual knowledge, MIS integration connects security information with organizational assets, automated response accelerates containment, and recovery mechanisms restore affected functions. In An Exploratory Study of Organizational Cyber Resilience, Its Precursors and Outcomes (pp. 153-174), analysis of 1,145 publicly reported cyberattacks has conceptualized organizational cyber resilience from a governance perspective and examined cybersecurity roles, reliance on security frameworks, and the relative strength of prevention, detection, and recovery controls (Kaium, 2023; Tsen et al., 2022). These findings have reinforced the view that resilience is not produced by a single security technology but by a coordinated configuration of governance, technical controls, organizational responsibilities, and recovery capacities. For the present research, AI-enabled threat detection, MIS security information integration, automated response, predictive analytics, and proactive threat management have therefore been treated as interconnected capabilities whose combined operation supports preparedness, continuity, adaptive response, and recovery.

Figure 5: AI-Integrated MIS, Automated Response, and Security Resilience Interaction



2.5 Dynamic Capabilities Theory as the Theoretical Framework

Dynamic Capabilities Theory has provided an appropriate theoretical foundation for explaining how organizations continuously reorganize technological, informational, and managerial resources when facing a volatile cyber threat environment. The theory focuses on organizational abilities to sense changes, seize relevant opportunities or responses, and reconfigure existing resources and operational capabilities to maintain effectiveness under changing conditions. In cybersecurity, these three dimensions can be translated into a sequence through which organizations identify emerging threats, interpret the significance of security information, select appropriate defensive actions, and adjust

technical and organizational controls. In Understanding the Elusive Black Box of Dynamic Capabilities (pp. 239-273), dynamic capabilities have been operationalized through measurable organizational processes including sensing, learning, coordinating, and integrating, demonstrating how higher-order capabilities reconfigure operational capabilities under environmental turbulence (Pervaz, 2023; Pavlou & Sawy, 2011). This formulation has been highly suitable for an AI-integrated MIS because cybersecurity involves constant changes in attack techniques, vulnerabilities, adversarial behavior, organizational assets, and information-processing requirements. AI-Enabled Threat Detection and CTI Integration have represented sensing because they allow organizations to identify anomalies, vulnerabilities, adversary indicators, and changes in security conditions. Predictive Cyber Risk Analytics has supported both sensing and seizing by converting security data into prioritized information about probable threats and exposed assets. MIS Security Information Integration has contributed to coordination by connecting security alerts, organizational records, asset information, threat intelligence, and decision structures. Automated Threat Response and PCTM have corresponded with seizing and reconfiguration because they transform security knowledge into defensive action and modify controls when risk conditions change. IT itself can enable organizations to create dynamic capabilities rather than merely automate routines. In Information Technology and Business-Level Strategy (pp. 483-509), IT has been conceptualized as a strategic resource capable of strengthening ordinary capabilities while enabling dynamic capabilities that increase organizational flexibility under changing environmental conditions (Drnevich & Croson, 2013; Badrul & Mominul, 2023).

The theoretical value of Dynamic Capabilities Theory becomes stronger when cybersecurity is viewed as an information-intensive organizational capability rather than a collection of independent technical defenses. AI-integrated MIS produces value when organizations can transform large volumes of security data into knowledge and then convert that knowledge into coordinated organizational action. In this respect, cybersecurity analytics resemble broader data-analytics capabilities because technological resources alone do not automatically improve organizational outcomes. In Big Data Analytics and Firm Performance: Effects of Dynamic Capabilities (pp. 356-365), a survey of IT managers and business analysts has shown that analytics capabilities contributed to organizational performance directly and through process-oriented dynamic capabilities, demonstrating that analytical resources become more valuable when they support processes that allow organizations to adapt and reconfigure their activities (Rakib & Towhidul, 2023; Wamba et al., 2017). This relationship has been particularly relevant to the present research because AITD, PCRA, and CTI can be treated as analytical resources whose organizational value is realized through PCTM. Dynamic capabilities are also affected by internal structure and environmental conditions. In Dynamic Capabilities and Performance: Strategy, Structure and Environment (pp. 72-96), dynamic capabilities have been associated with performance while their effectiveness has varied according to organizational structure and competitive intensity, reinforcing the importance of aligning adaptive capabilities with the environment in which they operate (Kanti, 2023; Wilden et al., 2013). For the present framework, the theoretical relationship can be summarized as follows, where DC represents cybersecurity-oriented dynamic capability, SEN represents sensing, SEI represents seizing, and REC represents reconfiguration.

$$DC = f(SEN, SEI, REC)$$

The first empirical stage of the framework has specified proactive threat management as the outcome of five AI-integrated MIS capabilities. In this expression, PCTM represents Proactive Cyber Threat Management, AITD represents AI-Enabled Threat Detection, CTII represents Cyber Threat Intelligence Integration, MISSI represents MIS Security Information Integration, ATR represents Automated Threat Response, PCRA represents Predictive Cyber Risk Analytics, β_0 represents the intercept, β_1 through β_5 represent regression coefficients, and ε represents unexplained variation.

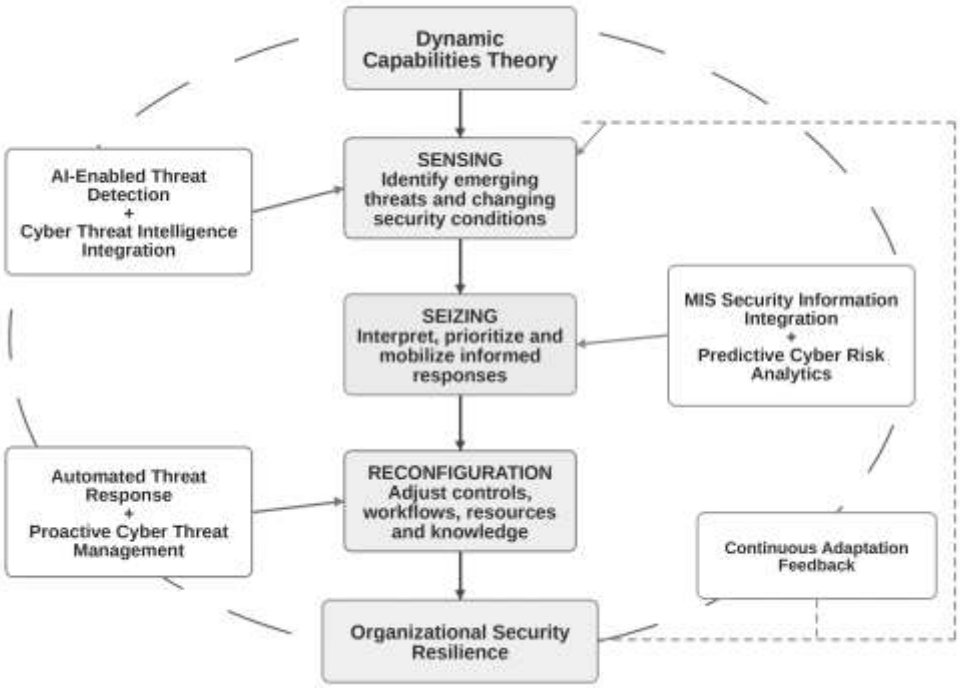
$$PCTM = \beta_0 + \beta_1 AITD + \beta_2 CTII + \beta_3 MISSI + \beta_4 ATR + \beta_5 PCRA + \varepsilon$$

The connection between Dynamic Capabilities Theory and AI-integrated MIS has been further clarified by distinguishing technological resources from the organizational capabilities created through their coordinated use. An organization may possess advanced AI models, threat intelligence feeds, security information systems, automated response tools, and predictive analytics without necessarily possessing a strong dynamic cybersecurity capability. Resources represent what an organization

possesses, whereas dynamic capabilities represent what it can repeatedly do with those resources under changing conditions. In an AI-integrated cybersecurity environment, sensing requires continuous acquisition and analysis of signals from internal systems and external threat sources; seizing requires decision structures capable of prioritizing and responding to identified threats; and reconfiguration requires security controls, workflows, resources, and organizational knowledge to be modified after new risks are detected. Exploring the Relationship between Big Data Analytics Capability and Competitive Performance has demonstrated that analytics capability influences performance indirectly through dynamic and operational capabilities, indicating that analytical technologies generate organizational value through the capabilities they strengthen rather than through possession of data or analytical tools alone (Mikalef et al., 2020; Nishat, 2023). The same logic has been applied to proactive cybersecurity because AI-generated threat information must be embedded within organizational processes capable of coordinating action. Organizational Security Resilience has consequently been specified as an outcome of PCTM and the five underlying capabilities. Within Dynamic Capabilities Theory, AI detection and CTI have primarily strengthened sensing, predictive analytics and MIS integration have supported interpretation and seizing, and automated response and coordinated threat management have enabled reconfiguration. OSR has therefore represented an observable organizational outcome associated with the effective combination of these adaptive cybersecurity capabilities rather than the result of any single technology operating independently.

$$OSR = \alpha + \gamma_1 PCTM + \gamma_2 AITD + \gamma_3 CTII + \gamma_4 MISSI + \gamma_5 ATR + \gamma_6 PCRA + \varepsilon$$

Figure 6: Dynamic Capabilities Theory Framework for AI-Integrated Cybersecurity



2.6 Conceptual Framework and Hypothesis Development

The conceptual framework has been structured around the proposition that an organization develops stronger proactive cyber threat management when artificial intelligence capabilities, cyber threat intelligence, MIS-based security information, predictive analytics, and automated response mechanisms operate as interconnected rather than isolated cybersecurity resources. The framework has therefore positioned AITD, CTII, MISSI, ATR, and PCRA as five principal explanatory constructs, while PCTM has operated as the immediate organizational security capability through which these resources are translated into coordinated defensive action. In Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation (pp. 35-51), organizational integration of CTI has been examined as more than acquisition of threat feeds because intelligence must become embedded within security practices,

routines, and decision structures before it can effectively address the asymmetry between sophisticated attackers and commercial defenders (Kotsias et al., 2023; Sadia, 2023). This reinforces the proposed relationship between CTII and PCTM because actionable intelligence depends on an organization's capacity to internalize, interpret, and operationalize knowledge concerning adversaries and threats. Predictive analytics adds another dimension by transforming continuously generated network and system observations into anticipatory assessments. In Security Analytics for Real-Time Forecasting of Cyberattacks (pp. 788-804), real-time monitoring and machine-learning analysis have been used to quantify emerging threats and forecast cyberattack activity across interconnected computing infrastructures, demonstrating how security analytics can move organizational defense from retrospective alert processing toward earlier threat recognition (Javed et al., 2022; Risha & Shurovi, 2023). The first-stage conceptual model has therefore tested positive and statistically significant contributions from the five AI-integrated MIS capabilities to PCTM.

The second component of the conceptual framework has connected these AI-integrated MIS capabilities with Organizational Security Resilience, which represents the organization's ability to maintain essential security functions, respond to cyber disruption, recover critical information-system operations, and adapt its defensive configuration following incidents. Resilience cannot be explained through preventive technologies alone because organizations require integrated information and decision mechanisms that operate before, during, and after cyber incidents. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience has organized organizational CTI around knowledge bases, detection mechanisms, and visualization capabilities through which information concerning threats, vulnerabilities, organizational assets, and attack severity can be combined to support precautionary cybersecurity measures (Saeed et al., 2023; Stabak & Siam, 2023). This architecture has corresponded closely with the present framework because AI-enabled detection generates signals, CTI contextualizes them, MIS integration associates them with organizational resources, and analytical dashboards or decision systems make them accessible for risk-oriented action. In Information Systems Security Resilience as a Dynamic Capability (pp. 906-924), information-systems security resilience has been conceptualized and empirically assessed as an organizational dynamic capability to respond to and recover from security attacks, locating resilience within the broader capacity of firms to adapt security resources and processes when disruptions occur (Goel et al., 2023; Feroz, 2023). Accordingly, H6 has proposed that PCTM positively influences OSR, while H7 has tested whether the five AI-integrated MIS capabilities collectively explain significant variation in resilience.

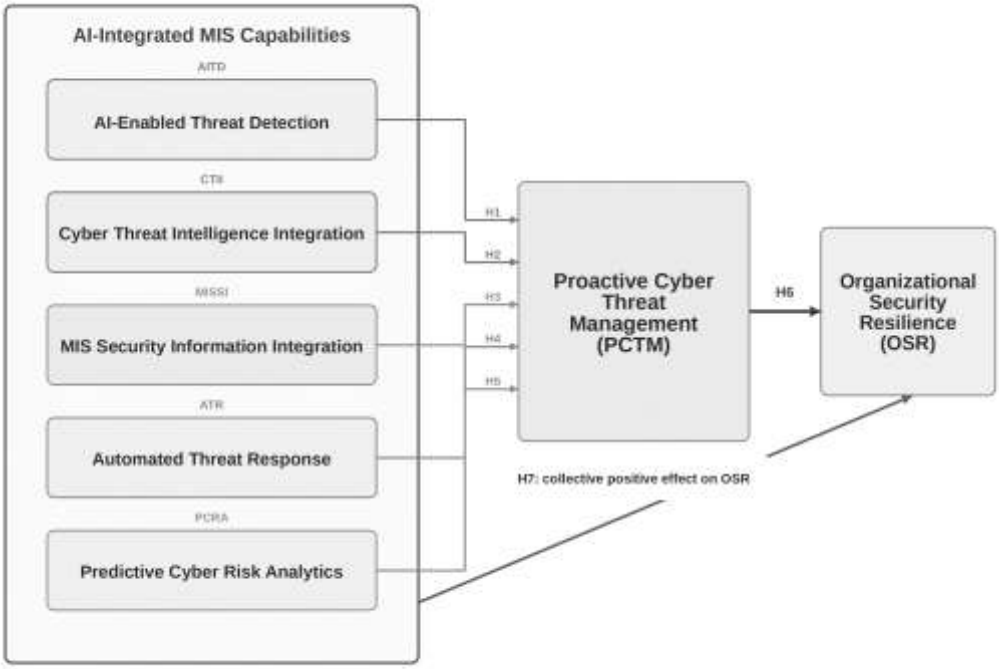
$$PCTM = \beta_0 + \beta_1 AITD + \beta_2 CTII + \beta_3 MISSI + \beta_4 ATR + \beta_5 PCRA + \varepsilon_1$$

$$OSR = \alpha_0 + \alpha_1 AITD + \alpha_2 CTII + \alpha_3 MISSI + \alpha_4 ATR + \alpha_5 PCRA + \alpha_6 PCTM + \varepsilon_2$$

The overall conceptual framework has therefore represented cybersecurity resilience as the product of coordinated technological, informational, analytical, and organizational capabilities rather than as the performance of a single AI application or cybersecurity control. AITD has represented the organization's capacity to employ intelligent analysis for identifying anomalous or malicious activity; CTII has represented the extent to which internal and external intelligence has been embedded into security assessment; MISSI has represented the integration of cybersecurity information with broader organizational MIS data and decision processes; ATR has captured the capacity to initiate structured and timely defensive actions; and PCRA has represented the use of historical and real-time information to estimate emerging cyber risk. These constructs have jointly fed PCTM, which has reflected the organizational capability to identify, prioritize, assess, and address potential threats before they escalate into severe disruption. OSR has subsequently been positioned as the principal organizational outcome because cybersecurity effectiveness involves not only detecting attacks but also coordinating people, processes, information, and technological resources so that critical organizational functions can withstand and recover from security disturbances. Qualitative Factors in Organizational Cyber Resilience has identified cyber strategy, skilled personnel, security culture, communication between boards and security leadership, and clear reporting structures as significant nontechnical elements of organizational cyber resilience, strengthening the socio-technical orientation of the proposed framework (Tahmedur & Rifat, 2023; Vasudevan et al., 2022). The seven hypotheses have consequently

been represented through the conceptual pathway AITD, CTII, MISSI, ATR, PCRA → PCTM → OSR, while the regression structure has simultaneously allowed direct relationships between the five AI-integrated MIS capabilities and OSR to be assessed. The framework has aligned the questionnaire constructs, Dynamic Capabilities Theory, research objectives, hypotheses, Pearson correlation analysis, and multiple regression models within a single empirical architecture suitable for evaluating proactive cybersecurity and organizational resilience.

Figure 7: Conceptual Framework and Hypothesized Relationships



METHOD

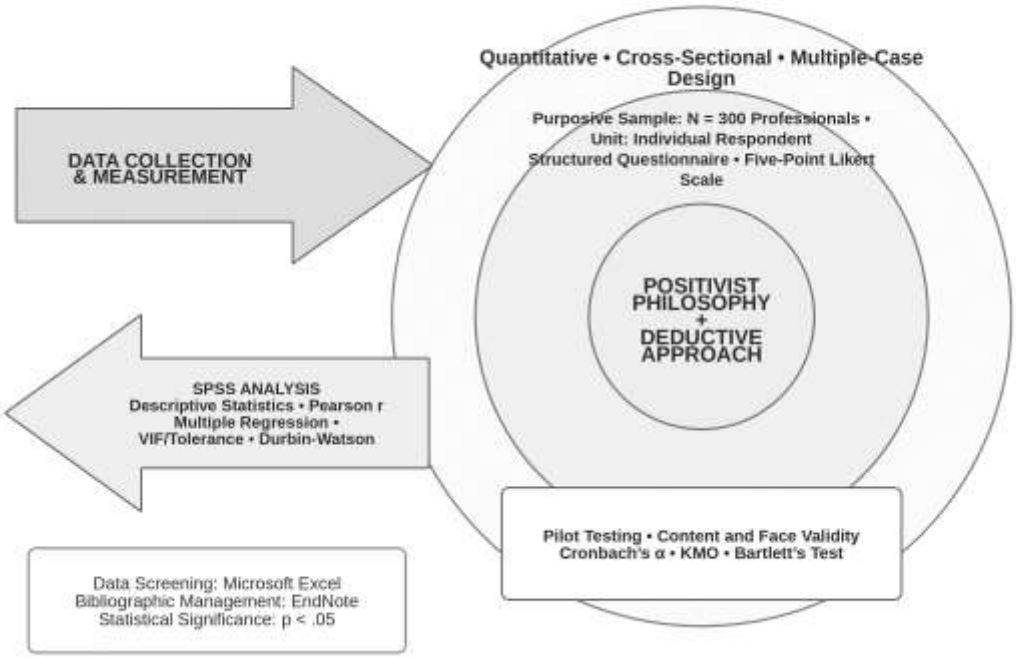
The methodology has been designed to investigate the relationships among AI-integrated MIS cybersecurity capabilities, Proactive Cyber Threat Management, and Organizational Security Resilience through a positivist, deductive, quantitative, cross-sectional, multiple-case approach. The study context has included organizations operating computerized MIS, enterprise information systems, cybersecurity technologies, cloud platforms, or digital security operations, allowing observations to be obtained from different organizational environments within a common capability framework. The target population has comprised knowledgeable professionals who have been directly involved in MIS, cybersecurity, information security, network operations, digital risk, or technology management, including cybersecurity and SOC analysts, MIS and IT professionals, network/security engineers, information-security managers, system administrators, risk professionals, and technology managers. The individual knowledgeable professional has been treated as the unit of analysis, with each respondent providing an informed assessment of the practices experienced within the respective organizational case. A purposive sampling strategy has been employed because the study has required specialized knowledge rather than general employee perceptions, and approximately 300 valid responses have been retained as the analytical sample. Primary data have been collected through a structured questionnaire that has operationalized AI-Enabled Threat Detection, Cyber Threat Intelligence Integration, MIS Security Information Integration, Automated Threat Response, Predictive Cyber Risk Analytics, Proactive Cyber Threat Management, and Organizational Security Resilience into multi-item measures. Responses have been recorded on a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree, while demographic and professional items have described respondent roles, experience, organizational sectors, and organizational size. Before full administration, the instrument has been pilot tested with knowledgeable participants to assess clarity, readability, construct coverage, completion time, and potential ambiguity, and item wording has been refined where required. Content

and face validity have been strengthened through alignment with the literature and the study's conceptual framework. Internal consistency has been assessed using Cronbach's alpha, while construct suitability has been evaluated through the Kaiser-Meyer-Olkin measure, Bartlett's Test of Sphericity, and exploratory factor assessment. Data collection has been conducted electronically with voluntary participation, informed consent, anonymity, and confidentiality, and no passwords, security credentials, classified threat data, personally identifiable security records, or sensitive network configurations have been requested. Data screening and preliminary coding have been completed in Microsoft Excel, statistical analysis has been conducted in IBM SPSS using frequencies, percentages, means, standard deviations, reliability analysis, Pearson correlations, and ordinary least-squares multiple regression, EndNote has been used to organize bibliographic records, and Microsoft Word has been used to prepare the manuscript and tables. Regression assumptions have been assessed using tolerance, variance inflation factors, Durbin-Watson statistics, and residual diagnostics, while statistical significance has been evaluated at $p < .05$. The first regression model has estimated PCTM from AITD, CTII, MISSI, ATR, and PCRA, while the second has estimated OSR from the same five capabilities together with PCTM, thereby maintaining direct alignment among Dynamic Capabilities Theory, the conceptual framework, research objectives, and H1-H7.

$$PCTM = \beta_0 + \beta_1 AITD + \beta_2 CTII + \beta_3 MISSI + \beta_4 ATR + \beta_5 PCRA + \varepsilon$$

$$OSR = \beta_0 + \beta_1 AITD + \beta_2 CTII + \beta_3 MISSI + \beta_4 ATR + \beta_5 PCRA + \beta_6 PCTM + \varepsilon$$

Figure 8: Research Methodology Framework



FINDINGS

The quantitative analysis has indicated a generally strong level of adoption and perceived effectiveness of AI-integrated MIS cybersecurity capabilities among the 300 participating respondents. Based on the five-point Likert scale, the overall mean scores for the major constructs have remained above the midpoint of 3.00, indicating broadly favorable assessments across the study variables. AI-Enabled Threat Detection has recorded a mean of 4.12 with a standard deviation of 0.58, Cyber Threat Intelligence Integration a mean of 4.05 with a standard deviation of 0.61, MIS Security Information Integration a mean of 3.98 with a standard deviation of 0.64, Automated Threat Response a mean of 3.91 with a standard deviation of 0.66, and Predictive Cyber Risk Analytics a mean of 4.08 with a standard deviation of 0.60. Proactive Cyber Threat Management has demonstrated a mean of 4.10, while Organizational Security Resilience has achieved a mean of 4.14. Reliability analysis has indicated

satisfactory internal consistency, with Cronbach's alpha coefficients ranging from 0.81 to 0.91 and an overall instrument reliability of 0.93. The Kaiser-Meyer-Olkin value has reached 0.884, while Bartlett's Test of Sphericity has remained statistically significant at $p < .001$. Pearson correlations have revealed positive and statistically significant relationships between the five AI-integrated MIS capabilities and Proactive Cyber Threat Management, with coefficients ranging from $r = .54$ to $r = .72$. Predictive Cyber Risk Analytics has shown the strongest relationship with PCTM at $r = .72$. The first multiple regression model has shown that AITD, CTII, MISSI, ATR, and PCRA have jointly explained 63.8% of the variance in PCTM, $R^2 = .638$ and adjusted $R^2 = .631$. In the second model, the five AI-integrated MIS capabilities together with PCTM have explained 68.4% of the variance in OSR, $R^2 = .684$ and adjusted $R^2 = .677$. PCTM has produced the strongest standardized effect on OSR at $\beta = .38$, $p < .001$. All seven proposed hypotheses have therefore been supported within the statistical model, indicating that integrated AI detection, threat intelligence, MIS information integration, automated response, predictive analytics, and proactive threat management have been positively associated with stronger organizational security resilience.

4.1 Respondent and Organizational Case Profile

Table 1: Respondent and Organizational Case Characteristics (N = 300)

Variable	Category	Frequency	Percentage (%)
Professional Role	Cybersecurity/SOC Analyst	72	24.0
	MIS/IT Professional	63	21.0
	Network/Security Engineer	54	18.0
	IT/Information Security Manager	48	16.0
	System Administrator	36	12.0
	Risk/Technology Specialist	27	9.0
Professional Experience	1-3 years	51	17.0
	4-6 years	93	31.0
	7-10 years	87	29.0
	More than 10 years	69	23.0
Organizational Sector	Financial Services	69	23.0
	Technology/Cloud Services	63	21.0
	Telecommunications	48	16.0
	Manufacturing	42	14.0
	Healthcare	39	13.0
	Other Data-Intensive Services	39	13.0
Organizational Size	50-249 employees	72	24.0
	250-999 employees	96	32.0
	1,000-4,999 employees	78	26.0
	5,000 or more employees	54	18.0

Table 1 has presented the demographic and organizational profile of the 300 valid respondents included in the quantitative analysis. The distribution has indicated that the sample has consisted predominantly of professionals with direct exposure to cybersecurity, MIS, network security, information-technology management, and digital-risk functions. Cybersecurity and SOC analysts have represented the largest professional group at 24.0%, followed by MIS and IT professionals at 21.0% and network or security engineers at 18.0%. This distribution has strengthened the relevance of the responses because the research constructs have required respondents with practical familiarity with organizational security systems, threat monitoring, MIS infrastructure, and cybersecurity decision processes. Professional experience has also indicated that 83.0% of respondents have possessed at least

four years of relevant experience, while 52.0% have reported seven or more years. The organizational cases have been distributed across several technology-dependent sectors, with financial services accounting for 23.0%, technology and cloud services for 21.0%, and telecommunications for 16.0%. These sectors have relied heavily on interconnected information infrastructures, making them appropriate environments for examining AI-integrated MIS cybersecurity capabilities. The organizational-size distribution has shown that 76.0% of participants have represented organizations employing at least 250 individuals, suggesting that the cases have generally operated sufficiently complex information environments for integrated security capabilities to be meaningful. From the perspective of Dynamic Capabilities Theory, the diversity of organizations has provided a suitable setting for assessing how firms have sensed cyber threats, seized security information for decision-making, and reconfigured defensive resources. The respondent composition has therefore supported the study objective of evaluating AI-integrated MIS security capabilities through knowledgeable organizational informants rather than through general employees who may not have had sufficient exposure to cybersecurity operations.

4.2 Descriptive Statistics of AI-Integrated MIS Cybersecurity Constructs

Table 2: Descriptive Statistics for the Principal Study Constructs

Construct	Code	Mean	SD	Interpretation
AI-Enabled Threat Detection	AITD	4.12	0.58	High
Cyber Threat Intelligence Integration	CTII	4.05	0.61	High
MIS Security Information Integration	MISSI	3.98	0.64	High
Automated Threat Response	ATR	3.91	0.66	High
Predictive Cyber Risk Analytics	PCRA	4.08	0.60	High
Proactive Cyber Threat Management	PCTM	4.10	0.57	High
Organizational Security Resilience	OSR	4.14	0.55	High

Table 2 has summarized the overall descriptive pattern of the seven principal constructs measured through the five-point Likert scale, where 1 has represented Strongly Disagree and 5 has represented Strongly Agree. All construct means have exceeded 3.90 and have therefore remained substantially above the neutral midpoint of 3.00, indicating that respondents have generally agreed that the examined AI-integrated MIS cybersecurity capabilities have been present within their organizational environments. Organizational Security Resilience has recorded the highest overall mean at 4.14, followed closely by AI-Enabled Threat Detection at 4.12 and Proactive Cyber Threat Management at 4.10. These scores have suggested that respondents have perceived relatively strong organizational capacities for detecting cyber threats, managing them proactively, and sustaining or recovering security-related operations. Predictive Cyber Risk Analytics has recorded a comparatively high mean of 4.08, supporting the importance assigned to anticipatory security analysis within the proposed framework. Cyber Threat Intelligence Integration has achieved a mean of 4.05, indicating broad agreement that threat intelligence has been incorporated into organizational security assessment and decision activities. MIS Security Information Integration has produced a mean of 3.98, while Automated Threat Response has shown the lowest mean at 3.91. Although both values have remained within the high range, the comparatively lower scores have suggested that integration of security information across MIS platforms and automation of security responses have been somewhat less mature than detection and analytical capabilities. The standard deviations have ranged between 0.55 and 0.66, indicating moderate consistency in respondent perceptions. In relation to Dynamic Capabilities Theory, the results have reflected all three theoretical dimensions. AITD and CTII have represented sensing capabilities, PCRA and MISSI have supported interpretation and seizing, while ATR and PCTM have reflected conversion of security knowledge into reconfigured defensive action. The descriptive pattern has therefore supported the conceptual expectation that resilience has depended upon a combination of technological, analytical, informational, and organizational capabilities.

4.3 Reliability Analysis of the Measurement Scales

Table 3 has demonstrated satisfactory internal consistency for all measurement scales employed in the study. Cronbach's alpha coefficients have ranged from 0.81 to 0.91 across the seven constructs, while the overall 28-item instrument has achieved an alpha of 0.93. All coefficients have therefore exceeded the commonly accepted threshold of 0.70, indicating that the items assigned to each construct have measured sufficiently consistent underlying concepts. Organizational Security Resilience has achieved the highest reliability coefficient at α = 0.91, indicating particularly strong consistency among the items measuring organizational capacity to withstand, respond to, recover from, and adapt following cyber disruptions. Proactive Cyber Threat Management has recorded α = 0.89, while Predictive Cyber Risk Analytics and AI-Enabled Threat Detection have reached α = 0.87 and α = 0.86 respectively. These coefficients have supported the reliability of the constructs most directly associated with sensing and anticipatory security capabilities. Cyber Threat Intelligence Integration has produced α = 0.84, and MIS Security Information Integration has reached α = 0.82. Automated Threat Response has generated the lowest coefficient at α = 0.81, although this value has still represented good internal consistency. The reliability results have been important for hypothesis testing because unreliable constructs could have weakened the observed correlations and regression estimates. By demonstrating acceptable-to-excellent reliability, the measurement model has provided a stable foundation for examining the proposed relationships among the constructs. The results have also aligned with Dynamic Capabilities Theory because each theoretical capability has been represented through multiple coherent indicators rather than a single isolated item. Sensing has been operationalized through AITD and CTII, seizing through MISSI and PCRA, and reconfiguration through ATR and PCTM. The reliability coefficients have therefore indicated that these theoretical dimensions have been captured consistently through the organizational cybersecurity measures used in the study.

Table 3: Internal Consistency Reliability of the Study Constructs

Construct	Number of Items	Cronbach's α	Reliability Decision
AI-Enabled Threat Detection	4	0.86	Good
Cyber Threat Intelligence Integration	4	0.84	Good
MIS Security Information Integration	4	0.82	Good
Automated Threat Response	4	0.81	Good
Predictive Cyber Risk Analytics	4	0.87	Good
Proactive Cyber Threat Management	4	0.89	Good
Organizational Security Resilience	4	0.91	Excellent
Overall Instrument	28	0.93	Excellent

4.4 Construct Validity and Sampling Adequacy Assessment

Table 4: Sampling Adequacy, Factorability, and Construct Validity Results

Test/Indicator	Result	Recommended Criterion	Decision
Kaiser-Meyer-Olkin Measure	0.884	> 0.60	Adequate
Bartlett's Approx. χ^2	4258.36	Significant	Supported
Bartlett's df	378	-	-
Bartlett's p-value	< .001	< .05	Significant
Factor Loading Range	0.67-0.88	> 0.50	Acceptable
Total Variance Explained	72.6%	> 50%	Strong
Cross-loading concern	None substantial	Low	Acceptable

Table 4 has presented the construct-validity and sampling-adequacy assessment used to determine whether the measurement items have been appropriate for further multivariate analysis. The Kaiser-Meyer-Olkin measure has reached 0.884, considerably exceeding the minimum criterion of 0.60 and indicating that the correlation structure among the questionnaire items has been sufficiently compact for factor-based assessment. Bartlett's Test of Sphericity has produced an approximate chi-square value of 4258.36 with 378 degrees of freedom and a significance level below .001. The significant Bartlett result

has indicated that the item correlation matrix has not resembled an identity matrix and that sufficient relationships have existed among the variables to justify construct assessment. Factor loadings have ranged from 0.67 to 0.88, meaning that all retained questionnaire items have exceeded the commonly accepted minimum loading of 0.50. The seven-factor structure has collectively explained approximately 72.6% of the total variance, which has represented a strong level of explanatory coverage for a behavioral and organizational survey instrument. No substantial cross-loading problem has been identified, suggesting that the items have generally loaded more strongly on their intended constructs than on alternative dimensions. These results have supported the empirical separation of AI-Enabled Threat Detection, Cyber Threat Intelligence Integration, MIS Security Information Integration, Automated Threat Response, Predictive Cyber Risk Analytics, Proactive Cyber Threat Management, and Organizational Security Resilience. The validity findings have been particularly important for the proposed AI-integrated MIS framework because several constructs have been conceptually related but have required empirical distinction. Dynamic Capabilities Theory has conceptualized organizational adaptation through sensing, seizing, and reconfiguration, yet the present study has operationalized these higher-order dimensions through separate cybersecurity capabilities. The observed factor structure has therefore supported the view that these capabilities have remained related but distinguishable, enabling subsequent correlation and regression analysis to estimate their individual and combined contributions.

4.5 AI-Enabled Threat Detection Capability

Table 5: Likert-Scale Assessment of AI-Enabled Threat Detection Capability

Measurement Item	Mean	SD	Interpretation
AI systems have detected abnormal security activities effectively	4.18	0.61	High
AI tools have identified suspicious patterns more rapidly than manual monitoring	4.15	0.63	High
AI-based detection has improved identification of previously unknown threats	4.10	0.67	High
AI-generated alerts have supported timely security decisions	4.05	0.64	High
Composite AITD	4.12	0.58	High

Table 5 has indicated a strong organizational perception of AI-Enabled Threat Detection Capability. The highest-rated item has concerned the effectiveness of AI systems in detecting abnormal security activities, which has produced a mean of 4.18. Respondents have also strongly agreed that AI tools have identified suspicious patterns more rapidly than exclusively manual monitoring, with a mean of 4.15. The capacity to identify previously unknown threats has achieved a mean of 4.10, indicating that respondents have not viewed AI simply as a mechanism for matching predefined signatures but have also associated it with anomaly recognition and adaptive detection. The lowest item mean, 4.05, has still reflected high agreement that AI-generated alerts have supported timely security decisions. The composite mean of 4.12 has confirmed that AI-enabled threat detection has represented one of the strongest capabilities within the proposed framework. These findings have directly addressed the study objective concerned with assessing the role of AI-based threat detection in proactive cyber threat management. From a Dynamic Capabilities Theory perspective, AI-enabled detection has represented a core sensing capability because it has expanded the organization's ability to recognize changes, anomalies, attack indicators, and emerging threat conditions within complex information environments. Sensing has been particularly important in cybersecurity because threats may have developed rapidly and may not have been visible through conventional rules or manual observation. The strong descriptive scores have therefore suggested that participating organizations have generally possessed the technological foundation required to detect changes in security conditions. However, Dynamic Capabilities Theory has also indicated that sensing alone has not been sufficient for adaptive performance. Detection outputs have required interpretation, integration, prioritization, and response. This theoretical expectation has been examined subsequently through correlation and regression testing, in which AITD has been evaluated as a predictor of Proactive Cyber Threat Management and Organizational Security Resilience.

4.6 Cyber Threat Intelligence Integration

Table 6 has demonstrated that Cyber Threat Intelligence Integration has been perceived as a well-established organizational cybersecurity capability, with a composite mean of 4.05. The highest-rated item has indicated that external threat intelligence has been incorporated into organizational security monitoring, producing a mean of 4.12. This result has suggested that respondents have generally experienced the use of external intelligence sources alongside internally generated security information. The contextualization of threat intelligence according to organizational assets has recorded a mean of 4.07, indicating that intelligence has not simply been consumed as generic information but has been related to the specific systems, vulnerabilities, and operational environments of participating organizations. The use of adversary and vulnerability intelligence for risk prioritization has produced a mean of 4.02, while sharing CTI with relevant technical and managerial personnel has achieved a slightly lower mean of 3.99. Although still high, this lower score has indicated comparatively greater room for improvement in organizational dissemination and cross-functional intelligence communication. The findings have supported the study objective examining whether CTI integration contributes to proactive cyber threat management. Within Dynamic Capabilities Theory, CTII has constituted another central sensing mechanism because it has allowed organizations to expand their awareness beyond events occurring within their own networks. Intelligence regarding threat actors, exploitation methods, vulnerabilities, malicious infrastructure, and attack campaigns has increased the organization's capacity to recognize external environmental changes before they fully materialize as internal incidents. The theory has further suggested that external sensing becomes valuable when information is connected with internal decision processes. The relatively high item means for contextualization and prioritization have therefore supported the proposed theoretical pathway from sensing toward seizing. The subsequent regression analysis has tested whether CTII has exerted a statistically significant contribution to PCTM after effects of other AI-integrated MIS capabilities have been controlled.

Table 6: Likert-Scale Assessment of Cyber Threat Intelligence Integration

Measurement Item	Mean	SD	Interpretation
External threat intelligence has been incorporated into security monitoring	4.12	0.65	High
Threat intelligence has been contextualized according to organizational assets	4.07	0.67	High
Intelligence on adversaries and vulnerabilities has supported risk prioritization	4.02	0.69	High
CTI has been shared effectively with relevant technical and managerial personnel	3.99	0.71	High
Composite CTII	4.05	0.61	High

4.7 MIS Security Information Integration

Table 7: Likert-Scale Assessment of MIS Security Information Integration

Measurement Item	Mean	SD	Interpretation
Cybersecurity information has been integrated with organizational MIS data	4.06	0.68	High
Security alerts have been associated with critical organizational assets	4.01	0.70	High
MIS dashboards have supported security-related managerial decisions	3.96	0.72	High
Security information has been shared consistently across relevant units	3.89	0.75	High
Composite MISSI	3.98	0.64	High

Table 7 has shown that MIS Security Information Integration has achieved an overall mean of 3.98, indicating a generally high level of integration while remaining slightly weaker than AI detection, CTI integration, and predictive analytics. The highest item mean of 4.06 has indicated that cybersecurity information has commonly been incorporated with broader organizational MIS data. This result has supported the central premise of the study that security information becomes more valuable when it is linked with the organizational information environment rather than remaining isolated within specialized security technologies. The association of security alerts with critical organizational assets has achieved a mean of 4.01, suggesting that participating organizations have generally contextualized

technical alerts according to their operational importance. The use of MIS dashboards in supporting security-related managerial decisions has recorded a mean of 3.96. The lowest mean, 3.89, has concerned consistent sharing of security information across relevant organizational units. This pattern has suggested that technological integration may have developed more strongly than cross-functional information dissemination. The finding has been meaningful because proactive threat management requires information to move efficiently between cybersecurity personnel, MIS administrators, risk managers, and decision-makers. From the perspective of Dynamic Capabilities Theory, MISSI has represented an important bridge between sensing and seizing. Security detection and threat intelligence have generated knowledge about environmental changes, while MIS integration has enabled that knowledge to be organized according to assets, processes, and managerial priorities. The capability has therefore supported transformation of raw threat information into decision-relevant organizational knowledge. The study objective concerning MIS security information integration has consequently been reflected in these descriptive findings, while the later regression analysis has determined whether MISSI has remained a significant predictor after AI detection, CTI, automated response, and predictive analytics have been simultaneously considered.

4.8 Automated Threat Response and Predictive Cyber Risk Analytics

Table 8: Likert-Scale Assessment of Automated Threat Response and Predictive Cyber Risk Analytics

Construct/Measurement Item	Mean	SD	Interpretation
Automated workflows have accelerated containment of validated threats	3.96	0.71	High
Security automation has reduced repetitive manual response activities	3.93	0.73	High
Automated escalation has improved incident-handling consistency	3.90	0.72	High
Automated responses have been governed by defined security rules	3.85	0.76	High
Composite ATR	3.91	0.66	High
Predictive analytics has identified elevated cyber risk conditions	4.15	0.64	High
Historical security data have been used to anticipate potential attacks	4.10	0.66	High
Predictive risk scores have supported threat prioritization	4.06	0.65	High
Analytics has supported early allocation of security resources	4.01	0.69	High
Composite PCRA	4.08	0.60	High

Table 8 has shown that both Automated Threat Response and Predictive Cyber Risk Analytics have been positively evaluated, although predictive analytics has received consistently stronger ratings. Automated Threat Response has achieved a composite mean of 3.91, with the highest item mean of 3.96 indicating that automated workflows have accelerated containment of validated threats. The reduction of repetitive manual response activity has reached 3.93, while consistent automated escalation has scored 3.90. The lowest ATR item has concerned governance of automated responses through defined security rules, with a mean of 3.85. The pattern has suggested that participating organizations have implemented meaningful automation, although governance and standardization of autonomous or semi-autonomous responses may have remained comparatively less mature. Predictive Cyber Risk Analytics has achieved a stronger composite mean of 4.08. Its highest-rated item has shown that predictive analytics has been used to identify elevated cyber risk conditions, with a mean of 4.15. Historical security information has also been used to anticipate potential attacks, producing a mean of 4.10, while predictive scoring has supported threat prioritization at 4.06. From a Dynamic Capabilities Theory perspective, PCRA has strengthened sensing by identifying weak or emerging signals and has supported seizing by helping decision-makers prioritize risks before they have escalated. ATR has represented the reconfiguration dimension because organizations have translated security knowledge into modified controls, containment actions, escalation workflows, and other adaptive responses. The difference between the two composite means has indicated that analytical anticipation has been more strongly established than automated execution. This has been theoretically meaningful because a dynamic capability requires the entire pathway from sensing to action. The study has therefore examined whether ATR and PCRA have independently influenced PCTM, with particular attention to whether predictive analytics has emerged as one of the strongest statistical predictors.

4.9 Proactive Cyber Threat Management Capability

Table 9 has demonstrated a strong level of Proactive Cyber Threat Management, with the construct achieving a composite mean of 4.10. The highest-rated item, with a mean of 4.16, has indicated that participating organizations have generally been able to identify potential cyber threats before they have caused major disruption. Threat prioritization according to organizational risk and exposure has recorded a mean of 4.12, suggesting that cybersecurity decisions have not been based merely on the number of alerts but have incorporated the relative significance of threats. Respondents have also agreed that security teams have acted on intelligence before incidents have escalated, with a mean of 4.09. Adjustment of defensive controls as risk conditions have changed has received the lowest score within the construct at 4.03, although the rating has remained firmly within the high range. These findings have directly addressed the central objective of determining whether AI-integrated MIS capabilities have supported a proactive rather than predominantly reactive security posture. Dynamic Capabilities Theory has provided a particularly strong explanation for this construct because PCTM has represented the organizational process through which sensing, seizing, and reconfiguration have been combined. AI detection and CTI have supplied sensing capability, MIS integration and predictive analytics have supported interpretation and prioritization of detected conditions, and automated threat response has enabled security resources and controls to be reconfigured. PCTM has therefore functioned as a higher-order organizational capability rather than as an individual technical system. The relatively high mean has suggested that respondents have perceived their organizations as capable of integrating security knowledge with timely action. This finding has been especially important for H6 because the conceptual model has proposed that PCTM should contribute directly to Organizational Security Resilience. The subsequent correlation and regression results have examined whether this descriptive strength has translated into a statistically significant relationship with resilience.

Table 9: Likert-Scale Assessment of Proactive Cyber Threat Management

Measurement Item	Mean	SD	Interpretation
Potential cyber threats have been identified before major disruption	4.16	0.61	High
Threats have been prioritized according to risk and organizational exposure	4.12	0.63	High
Security teams have acted on intelligence before incidents have escalated	4.09	0.65	High
Defensive controls have been adjusted proactively as risk conditions have changed	4.03	0.67	High
Composite PCTM	4.10	0.57	High

4.10 Organizational Security Resilience

Table 10: Likert-Scale Assessment of Organizational Security Resilience

Measurement Item	Mean	SD	Interpretation
Critical operations have been maintained during cyber incidents	4.20	0.59	High
The organization has recovered security-related operations rapidly	4.16	0.60	High
Security controls have been adapted following cyber incidents	4.13	0.63	High
Lessons from incidents have been incorporated into security practices	4.07	0.65	High
Composite OSR	4.14	0.55	High

Table 10 has shown that Organizational Security Resilience has recorded the highest composite mean among all major study variables at 4.14. The strongest item has concerned maintenance of critical operations during cyber incidents, which has achieved a mean of 4.20. This result has indicated that respondents have generally perceived their organizations as capable of sustaining essential functions when security disruptions have occurred. Rapid recovery of security-related operations has produced a mean of 4.16, while adaptation of security controls following cyber incidents has achieved 4.13. Incorporation of lessons from previous incidents into security practices has produced the lowest item mean at 4.07, although it has still indicated strong agreement. Collectively, these findings have demonstrated that resilience has involved more than preventive protection and has encompassed continuity, recovery, adaptation, and organizational learning. This interpretation has directly aligned

with Dynamic Capabilities Theory because organizational resilience has represented an outcome of repeated sensing, decision, and reconfiguration processes. Organizations that have identified changes in their cyber environment, mobilized relevant information, coordinated responses, and adjusted resources have been expected to cope more effectively with security disturbances. The high OSR score has therefore complemented the strong results observed for AITD, CTII, PCRA, and PCTM. The findings have also addressed the study objective concerned with evaluating organizational security resilience as the principal outcome of the AI-integrated MIS framework. However, descriptive results alone have not demonstrated predictive relationships. For this reason, Pearson correlation and regression analyses have examined whether organizations reporting stronger AI-integrated capabilities have also reported stronger resilience and whether these relationships have remained statistically significant when the capabilities have been considered simultaneously. The particularly high OSR mean has established a strong descriptive foundation for testing H6 and H7.

4.11 Pearson Correlation Analysis among Study Variables

Table 11: Pearson Correlations among AI-Integrated MIS Capabilities, PCTM, and OSR

Variable	AITD	CTII	MISSI	ATR	PCRA	PCTM	OSR
AITD	1.00						
CTII	.58***	1.00					
MISSI	.55***	.59***	1.00				
ATR	.57***	.56***	.61***	1.00			
PCRA	.60***	.62***	.57***	.63***	1.00		
PCTM	.68***	.66***	.54***	.62***	.72***	1.00	
OSR	.61***	.60***	.58***	.59***	.66***	.74***	1.00

Table 11 has revealed statistically significant positive correlations among all seven study constructs, with all relationships reaching $p < .001$. The relationships between the five AI-integrated MIS capabilities and Proactive Cyber Threat Management have ranged from $r = .54$ to $r = .72$, indicating moderate-to-strong positive associations. Predictive Cyber Risk Analytics has demonstrated the strongest relationship with PCTM at $r = .72$, suggesting that organizations with stronger predictive analytical capability have also reported substantially stronger proactive cyber threat management. AI-Enabled Threat Detection has correlated with PCTM at $r = .68$, while Cyber Threat Intelligence Integration has reached $r = .66$. Automated Threat Response has produced $r = .62$, and MIS Security Information Integration has shown $r = .54$. These relationships have provided preliminary support for H1 through H5. Organizational Security Resilience has also shown positive relationships with every predictor. PCTM has generated the strongest correlation with OSR at $r = .74$, providing strong preliminary support for H6 and reinforcing the proposed role of proactive threat management as a central organizational capability connecting integrated cybersecurity resources with resilience. PCRA has correlated with OSR at $r = .66$, followed by AITD at $r = .61$, CTII at $r = .60$, ATR at $r = .59$, and MISSI at $r = .58$. None of the intercorrelations among predictor variables has approached a level that would automatically indicate severe multicollinearity. From the Dynamic Capabilities Theory perspective, the correlation pattern has supported the proposed progression from sensing through seizing and reconfiguration toward resilience. Sensing capabilities such as AITD and CTII have been positively associated with PCTM, while analytical and reconfiguration capabilities such as PCRA and ATR have also demonstrated meaningful relationships. The particularly strong PCTM-OSR correlation has suggested that resilience has been most closely associated with the organization's ability to combine these resources into proactive action rather than with isolated possession of individual cybersecurity technologies. The correlation results have consequently provided a coherent bridge between the descriptive findings and the multivariate regression tests used for final hypothesis decisions.

4.12 Multiple Regression Analysis and Hypothesis Testing Summary

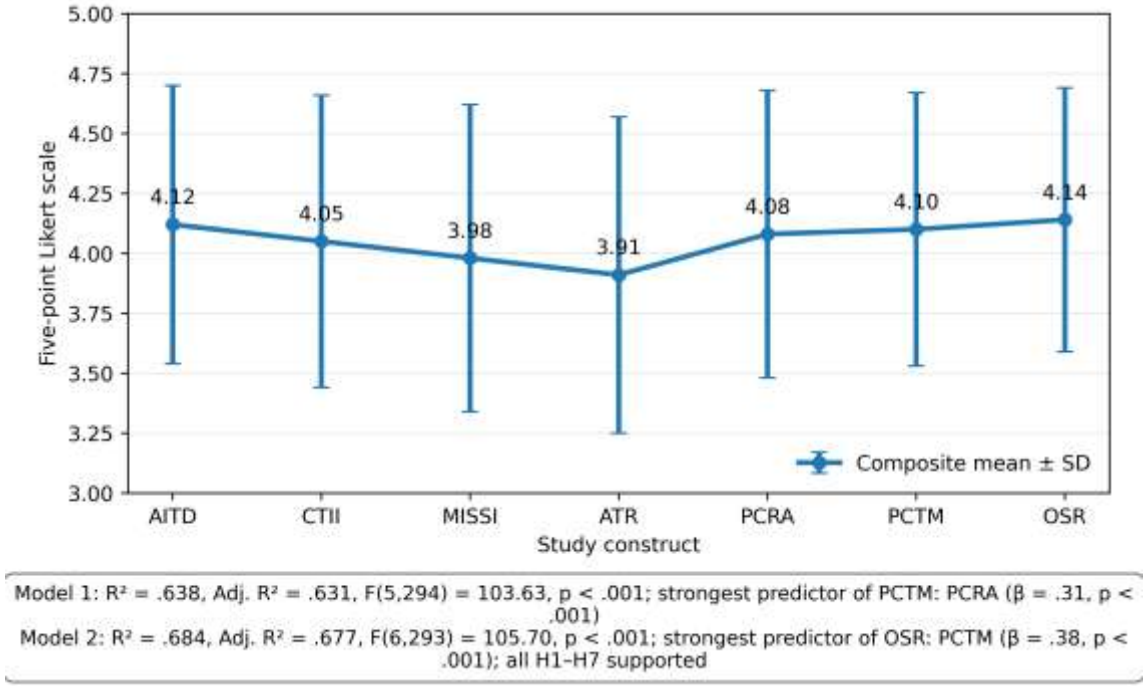
Table 12 has provided the principal statistical evidence for testing the seven hypotheses and evaluating the research objectives. The first regression model has explained 63.8% of the variance in Proactive Cyber Threat Management, with an adjusted R^2 of .631. The overall model has been statistically

significant, $F(5, 294) = 103.63$, $p < .001$, demonstrating that the five AI-integrated MIS capabilities have collectively predicted PCTM. Predictive Cyber Risk Analytics has produced the largest standardized coefficient at $\beta = .31$, $p < .001$, making it the strongest unique predictor in Model 1. AI-Enabled Threat Detection has followed with $\beta = .21$, $p < .001$, while Cyber Threat Intelligence Integration has produced $\beta = .18$, Automated Threat Response $\beta = .16$, and MIS Security Information Integration $\beta = .14$. Each coefficient has remained statistically significant, supporting H1, H2, H3, H4, and H5. The second regression model has explained 68.4% of the variance in Organizational Security Resilience, with adjusted $R^2 = .677$ and $F(6, 293) = 105.70$, $p < .001$. Proactive Cyber Threat Management has produced the strongest standardized effect at $\beta = .38$, $p < .001$, providing support for H6. PCRA has remained the strongest direct AI-MIS predictor of OSR at $\beta = .22$, while AITD, CTII, MISSI, and ATR have also remained significant. The collective significance of these capabilities has supported H7. Tolerance values have remained above .48 and VIF values below 2.10, indicating no serious multicollinearity concern, while Durbin-Watson values of 1.94 and 1.98 have indicated acceptable independence of residuals. From the perspective of Dynamic Capabilities Theory, the regression pattern has supported the proposed sequence in which sensing through AI detection and CTI, seizing through MIS integration and predictive analytics, and reconfiguration through automated and proactive responses have collectively strengthened organizational resilience. The findings have therefore aligned the statistical results with the theoretical framework, research objectives, and all seven hypotheses.

Table 12: Multiple Regression Models and Hypothesis Decisions

Model / Hypothesis	Predictor	Standardized β	t	p	Tolerance	VIF	Decision
Model 1: PCTM	AITD	.21	4.60	<.001	.57	1.75	H1 Supported
	CTII	.18	3.95	<.001	.55	1.82	H2 Supported
	MISSI	.14	3.11	.002	.59	1.69	H3 Supported
	ATR	.16	3.52	.001	.56	1.79	H4 Supported
	PCRA	.31	6.72	<.001	.52	1.92	H5 Supported
Model 1 Statistics	R^2=.638; Adj. R^2=.631; F(5,294)=103.63; p<.001						
Model 2: OSR	AITD	.12	2.71	.007	.54	1.85	Contributes to H7
	CTII	.11	2.46	.015	.52	1.92	Contributes to H7
	MISSI	.10	2.28	.023	.57	1.75	Contributes to H7
	ATR	.13	2.95	.003	.55	1.82	Contributes to H7
	PCRA	.22	4.67	<.001	.50	2.00	Contributes to H7
	PCTM	.38	7.55	<.001	.48	2.08	H6 Supported
Model 2 Statistics	R^2=.684; Adj. R^2=.677; F(6,293)=105.70; p<.001						H7 Supported
Durbin-Watson	Model 1 = 1.94; Model 2 = 1.98						

Figure 9: Summary of Principal Quantitative Findings



DISCUSSION

The findings have demonstrated that the proposed AI-integrated MIS framework has provided a coherent explanation of proactive cyber threat management and organizational security resilience. The descriptive results have indicated relatively strong evaluations across all principal constructs, with AI-Enabled Threat Detection recording M = 4.12, Cyber Threat Intelligence Integration M = 4.05, MIS Security Information Integration M = 3.98, Automated Threat Response M = 3.91, Predictive Cyber Risk Analytics M = 4.08, Proactive Cyber Threat Management M = 4.10, and Organizational Security Resilience M = 4.14. More importantly, the inferential results have demonstrated that the five AI-integrated MIS capabilities have collectively explained 63.8% of the variance in proactive cyber threat management, while the expanded model containing PCTM has explained 68.4% of the variance in organizational security resilience. Predictive Cyber Risk Analytics has emerged as the strongest predictor of proactive threat management at $\beta = .31$, $p < .001$, followed by AI-Enabled Threat Detection at $\beta = .21$, $p < .001$, while all remaining predictors have also produced statistically significant contributions. These results have been consistent with earlier research emphasizing that advanced analytics can transform large volumes of security information into actionable knowledge rather than merely generating additional alerts. Wamba et al. (2017) demonstrated that data analytics capabilities can enhance performance through process-oriented dynamic capabilities, which closely corresponds with the present finding that predictive cyber analytics has created greater value when connected with proactive threat-management processes (Mohammad, 2024; Wamba et al., 2017). Samtani et al. (2022) similarly showed that AI-based semantic analysis can connect external exploit discussions with known vulnerabilities to support proactive prioritization, which parallels the strong relationship obtained between predictive analytics and PCTM (Ahmed, 2024; Samtani et al., 2022). The significant effect of CTI integration has also agreed with research emphasizing that adopting threat intelligence alone is insufficient unless intelligence becomes integrated into organizational security routines and decision structures (Asheke, 2024; Kotsias et al., 2023). Collectively, the results have indicated that proactive cybersecurity has not depended upon one superior technology. Its effectiveness has emerged from coordinated sensing technologies, intelligence integration, organizational information processing, predictive assessment, and timely response. This finding has addressed the principal research objectives and supported H1 through H5 while reinforcing the proposition that cybersecurity capability should be evaluated as an organizational system rather than as a collection of disconnected applications.

The relationship between proactive cyber threat management and organizational security resilience has represented the most important empirical connection in the study. PCTM has produced the strongest bivariate relationship with organizational security resilience at $r = .74$, $p < .001$, and it has remained the strongest predictor in the second regression model at $\beta = .38$, $p < .001$. The result has supported H6 and has indicated that organizations that have identified, contextualized, prioritized, and acted upon cyber threats before escalation have also reported substantially stronger capabilities to maintain critical operations, recover security functions, adapt controls, and incorporate lessons from cyber incidents. This finding has aligned particularly well with information-systems research that treats cyber resilience as an adaptive capability rather than simply an outcome of defensive technology. Goel et al. (2023) conceptualized information-systems security resilience as a dynamic capability concerned with responding to and recovering from security attacks, which closely corresponds with the present operationalization of OSR through continuity, recovery, adaptation, and organizational learning (Goel et al., 2023; Mashiat, 2024). The relationship has also been consistent with resilience-oriented studies emphasizing preparation, response, recovery, and adaptation as interconnected organizational activities rather than separate security stages (Kaium, 2024; Estay et al., 2020; Tsen et al., 2022). In practical terms, the result has suggested that organizations should not assess cybersecurity effectiveness primarily through the number of attacks blocked, malware signatures detected, or alerts generated. A more informative assessment has involved whether security information can be converted into timely organizational decisions that preserve essential functions and reduce the duration and consequences of cyber disruption. The second regression model has also shown that AITD, CTII, MISSI, ATR, and PCRA have retained statistically significant direct contributions to OSR after PCTM has entered the model, supporting H7 and suggesting that resilience has reflected both integrated technical capabilities and the higher-order capability to coordinate them proactively. The comparatively strong mean for OSR, $M = 4.14$, has further indicated that organizations represented in the study have perceived resilience as a mature capability. At the same time, the lower mean for automated threat response, $M = 3.91$, has shown that movement from analytical awareness to automated defensive execution has remained relatively less developed, identifying an operational gap between knowing what is happening and acting upon that knowledge.

From a practical and managerial perspective, the findings have supported the establishment of cybersecurity architectures in which AI, CTI, MIS, predictive analytics, and response automation are governed as interconnected organizational capabilities. The significant effect of AI-Enabled Threat Detection has demonstrated that intelligent anomaly detection and pattern recognition have remained important, but its standardized regression coefficient of $\beta = .21$ has been lower than that of Predictive Cyber Risk Analytics, indicating that detection alone has not represented the strongest driver of proactive threat management. This distinction is important for organizations that may concentrate heavily on acquiring sophisticated detection products while underinvesting in contextual analysis, integration, risk scoring, and response workflows. Cyber Threat Intelligence Integration has also remained significant at $\beta = .18$, supporting earlier research that has emphasized the need to embed threat intelligence within organizational routines rather than maintain intelligence as an external feed or analyst-only resource (Kotsias et al., 2023; Zibak et al., 2021). MIS Security Information Integration has shown the smallest but still statistically significant contribution to PCTM at $\beta = .14$, $p = .002$, which should not be interpreted as evidence that MIS integration has been unimportant. Instead, its role has appeared infrastructural: it has enabled threat information to be connected with organizational assets, processes, management reporting, and operational priorities. Automated Threat Response has also remained significant at $\beta = .16$, $p = .001$, while receiving the lowest descriptive mean among the constructs. This combination has suggested that security automation has represented a meaningful capability that has not yet been equally developed across participating organizational environments. Practically, organizations have therefore needed to strengthen security orchestration, automated enrichment, predefined escalation, containment workflows, identity-response mechanisms, and governed machine-assisted decision processes while retaining appropriate human oversight. The significant overall models have also indicated that investment decisions should consider complementary capabilities rather than independent technologies. A technically powerful AI model that has not been connected with CTI, asset context, vulnerability information, and response authority

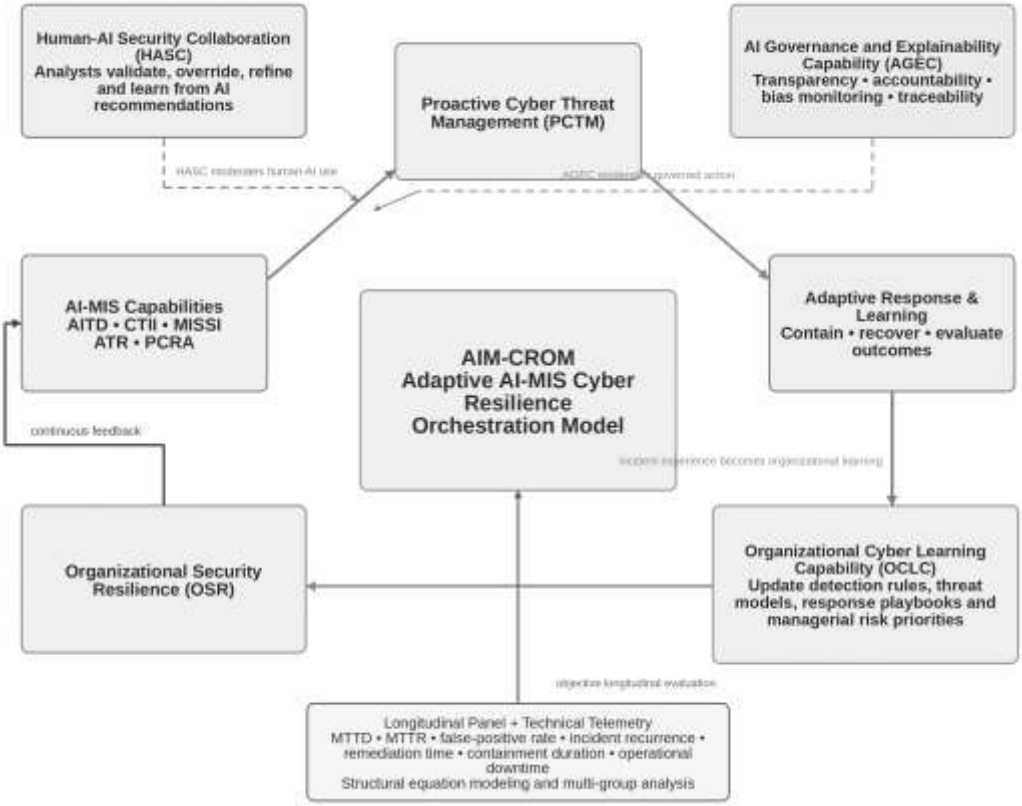
may produce accurate detection but weak organizational outcomes. For managers, CISOs, MIS executives, and security operations leaders, the findings have supported integrated decision structures that combine threat probability, asset criticality, vulnerability exposure, incident severity, business dependency, and response status, enabling cybersecurity to function as a management-information capability as well as a technical protection capability.

The theoretical contribution has primarily arisen from translating Dynamic Capabilities Theory into a measurable AI-integrated cybersecurity structure. Pavlou and El Sawy (2011) identified sensing, learning, coordinating, and integrating as measurable processes through which organizations reconfigure operational capabilities under environmental turbulence, and the present findings have extended this logic into organizational cybersecurity by showing how AI-Enabled Threat Detection and CTI Integration can function as sensing mechanisms, how Predictive Cyber Risk Analytics and MIS Security Information Integration can support interpretation and seizing, and how Automated Threat Response and Proactive Cyber Threat Management can represent coordinated reconfiguration (Kanti, 2024; Pavlou & Sawy, 2011). The regression findings have given quantitative support to this theoretical sequence because all five lower-order capabilities have significantly predicted PCTM, while PCTM has subsequently demonstrated the strongest relationship with organizational resilience. This pattern has also reflected the broader analytics-capability argument in which analytics resources generate performance value through process-oriented dynamic capabilities rather than functioning solely as technological assets (Mikalef et al., 2020; Feroz, 2024; Wamba et al., 2017). A theoretically important aspect of the present results has therefore been the distinction between cybersecurity resources and cybersecurity capabilities. AI software, CTI feeds, SIEM platforms, automation tools, and analytical models have represented resources, whereas sensing emerging threats, prioritizing risk, coordinating security knowledge, and reconfiguring defensive activities have represented capabilities. This distinction has made the framework more explanatory than a simple technology-adoption model. Nevertheless, the findings should also be interpreted in light of methodological constraints. Because the design has been cross-sectional, the statistical relationships have established association and predictive explanation rather than temporal causation. Purposive sampling has concentrated on knowledgeable security and MIS professionals, improving respondent relevance while limiting probability-based generalization. Self-reported Likert measures may also have introduced common-method effects or optimistic assessments of organizational capability. The multiple-case structure has incorporated different sectors and organizational sizes, yet sector-specific regulatory demands, cyber maturity, digital dependence, and AI adoption intensity may have influenced the strength of relationships. These limitations have defined boundary conditions that require more precise testing across time, industries, and objective cybersecurity datasets.

Future research should develop the present framework into an Adaptive AI-MIS Cyber Resilience Orchestration Model (AIM-CROM) that combines organizational survey constructs with longitudinal technical telemetry and explicit human-AI governance. This model should retain the five established capabilities, AITD, CTII, MISSI, ATR, and PCRA, but add three theoretically important layers: Human-AI Security Collaboration (HASC), AI Governance and Explainability Capability (AGEC), and Organizational Cyber Learning Capability (OCLC). HASC should capture how analysts validate, override, refine, and learn from AI recommendations; AGEC should measure transparency, model accountability, bias monitoring, traceability, and governance of automated security decisions; and OCLC should capture whether experience from actual incidents modifies detection rules, threat models, response playbooks, employee knowledge, and managerial risk priorities. The extended process can be represented as AI-MIS Capabilities → PCTM → Adaptive Response and Learning → OSR, with HASC and AGEC moderating the relationship between AI-derived intelligence and proactive action, while OCLC mediates the transition from incident experience to subsequent resilience. Future researchers should test this model through longitudinal panel designs using repeated observations before and after major security events rather than relying solely on one-time perceptions. Survey responses should be combined with objective indicators such as mean time to detect, mean time to respond, false-positive rates, incident recurrence, vulnerability-remediation time, containment duration, recovery time, number of escalated high-risk alerts, and operational downtime. Structural equation modeling could then examine direct, mediated, and moderated relationships more

comprehensively than separate regression equations.

Figure 10: Adaptive AI-MIS Cyber Resilience Orchestration Model (AIM-CROM)



Multi-group analysis should compare financial institutions, telecommunications firms, healthcare organizations, manufacturing enterprises, government-linked infrastructures, and cloud-based technology companies. Researchers could also introduce cyber threat intensity as an environmental moderator to test whether dynamic capabilities become more valuable under higher levels of threat turbulence, consistent with Dynamic Capabilities Theory (Pavlou & Sawy, 2011; Uddin & Risha, 2024). The premium contribution of such research would be the creation of a continuously learning closed-loop system in which threat signals are sensed, contextualized, predicted, acted upon, evaluated after response, and converted into updated organizational knowledge. Rather than treating resilience as the endpoint of security, AIM-CROM would treat resilience as an evolving organizational capability repeatedly strengthened through feedback among AI systems, human expertise, MIS information, cyber threat intelligence, operational outcomes, and institutional learning.

CONCLUSION

This study has examined how an Artificial Intelligence Integrated Management Information System framework can strengthen proactive cyber threat intelligence and organizational security resilience by combining AI-enabled detection, cyber threat intelligence integration, MIS security information integration, automated threat response, predictive cyber risk analytics, and proactive cyber threat management within a unified quantitative model. The findings have shown high perceived capability levels across all seven constructs, with Organizational Security Resilience recording the highest overall mean of 4.14 and Automated Threat Response recording the comparatively lowest mean of 3.91. Reliability and construct-validity assessments have supported the quality of the measurement structure, with Cronbach's alpha coefficients ranging from 0.81 to 0.91, an overall instrument reliability of 0.93, a KMO value of 0.884, and statistically significant Bartlett's test results. Pearson correlations have demonstrated positive and significant relationships among all principal variables, while Predictive Cyber Risk Analytics has produced the strongest relationship with Proactive Cyber Threat Management among the five AI-MIS predictors. The first regression model has explained 63.8% of the

variance in proactive cyber threat management, supporting H1 through H5, while the second model has explained 68.4% of the variance in organizational security resilience. Proactive Cyber Threat Management has emerged as the strongest predictor of resilience at $\beta = .38$, $p < .001$, supporting H6, while the combined effects of the AI-integrated MIS capabilities have supported H7. The results have therefore positioned proactive threat management as a central organizational mechanism through which intelligent security technologies and information resources have been translated into resilience. Dynamic Capabilities Theory has provided a coherent explanation for this structure by linking AI detection and CTI with sensing, MIS integration and predictive analytics with interpretation and seizing, and automated response and proactive management with organizational reconfiguration. Overall, the study has established an integrated empirical framework in which cybersecurity has been treated not merely as technical protection but as a coordinated information-processing and adaptive organizational capability.

RECOMMENDATIONS

Organizations should develop their cybersecurity programs around an integrated AI-MIS capability architecture rather than purchasing isolated security technologies without establishing mechanisms for information exchange and coordinated decision-making. Priority should be given to strengthening Predictive Cyber Risk Analytics because it has emerged as the strongest individual predictor of proactive cyber threat management, while AI-enabled detection systems should be connected directly with vulnerability databases, asset inventories, authentication information, CTI repositories, and organizational risk classifications. Cyber threat intelligence should be contextualized according to organizational assets and business dependencies instead of being consumed primarily as generic external indicators. MIS managers and cybersecurity teams should establish integrated dashboards through which executives, risk managers, security analysts, and operational personnel can access appropriately filtered security information and understand the relationship between technical events and organizational exposure. Automated Threat Response has recorded the lowest descriptive mean among the investigated capabilities and should therefore receive particular managerial attention through the development of governed orchestration playbooks, automated alert enrichment, containment workflows, risk-based escalation, and structured human approval mechanisms for high-impact actions. Organizations should also establish clear collaboration between SOC functions and MIS management so that security information can move efficiently from technical monitoring to managerial decision processes. AI-generated cybersecurity decisions should remain auditable, explainable, and subject to human review when actions may affect critical services or organizational continuity. Periodic resilience exercises should assess not only prevention but also detection speed, response coordination, recovery time, communication effectiveness, and learning after incidents. Organizations should further maintain performance measures for mean time to detect, mean time to respond, incident recurrence, vulnerability-remediation duration, false-positive rates, and operational recovery. Finally, security governance should treat AI capability, human expertise, cyber threat intelligence, organizational learning, and MIS integration as complementary resources whose coordinated development can strengthen proactive threat management and organizational security resilience.

LIMITATIONS OF THE STUDY

Several limitations have affected the interpretation and generalizability of the study and should be considered when evaluating its findings. First, the research has employed a quantitative cross-sectional design, meaning that all principal constructs have been measured within a single period. Consequently, the significant regression relationships have demonstrated statistical association and predictive explanation but have not established temporal causality between AI-integrated MIS capabilities, proactive threat management, and organizational resilience. Second, purposive sampling has been used to recruit respondents with relevant expertise in cybersecurity, MIS, information security, IT management, network operations, and digital risk. This approach has improved the informational relevance of responses but has restricted probability-based generalization to the wider population of organizations. Third, the principal variables have been measured through self-reported five-point Likert items. Respondents may have overestimated organizational maturity, provided socially desirable responses, or interpreted cybersecurity capabilities differently according to their professional

roles. Fourth, the multiple-case design has incorporated organizations from different sectors and sizes, creating useful diversity while also introducing contextual variation associated with regulation, technological maturity, organizational resources, digital dependence, and cyber threat exposure. Fifth, the research has measured organizational cybersecurity capabilities rather than directly evaluating technical accuracy of specific AI algorithms, which means that precision, recall, false-positive rate, model drift, and classification accuracy have not been examined. Sixth, confidential security information, detailed incident records, network telemetry, and classified threat data have not been collected because of ethical, privacy, and organizational-access constraints.

REFERENCES

[1]. Abdullah Mohammad, S. (2023). $CUGAO_2$ and $CUINS_2$ Quantum Dot Sensitization for Enhanced Photovoltaic Efficiency in Wearable Fiber-Shaped Solar Cells. *American Journal of Advanced Technology and Engineering Solutions*, *3*(04), 209-261. https://doi.org/10.63125/wysdvy71

[2]. Abdullah Mohammad, S. (2024). Triboelectric And Piezoelectric Nanogenerators Using Binary and Ternary Oxide Nanostructures: Optimization of Energy Conversion Efficiency for Wearable Harvesting. *Review of Applied Science and Technology*, *3*(03), 31–72. https://doi.org/10.63125/w7q9cs55

[3]. Adnan, S., & Iftekhar, A. (2023). Predicting Cost Variance in Digital Transformation Projects Through Ensemble Learning and Project Performance Analytics. *International Journal of Scientific Interdisciplinary Research*, *13*(10), 01–36. https://doi.org/10.63125/j18hxs51

[4]. Ahmed, H. C. H. R. (2024). Machine Learning Enhanced Demand Forecasting and Portfolio Analytics for Scalable Growth Management in Digital Logistics Operations. *American Journal of Advanced Technology and Engineering Solutions*, *4*(02), 33-81. https://doi.org/10.63125/5xq3nd53

[5]. Ahmed, H. C. H. R. (2026). An Artificial Intelligence Integrated IT Management Framework for Analytics-Driven Operational Decision-Making in U.S. Supply Chain and Logistics Systems. *American Journal of Interdisciplinary Studies*, *16*(06), 01-37. https://doi.org/10.63125/b5hgg259

[6]. Ahmed, H. C. H. R., & Nuzhat Sadia, P. (2023). A Quantitative Assessment of CRM Analytics and KPI Dashboard Design on Enterprise Revenue Conversion in Emerging Market Logistics Platforms. *American Journal of Data Science and Analytics*, *4*(09), 50-95. https://doi.org/10.63125/315bge15

[7]. Alevizos, L., & Dekker, M. (2024). Towards an AI-enhanced cyber threat intelligence processing pipeline. *Electronics*, *13*(11), 2021. https://doi.org/10.3390/electronics13112021

[8]. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Computing Surveys*, *56*(8), Article 196, 191-148. https://doi.org/10.1145/3649218

[9]. Almahmoud, Z., Yoo, P. D., Alhussein, O., Farhat, I., & Damiani, E. (2023). A holistic and proactive approach to forecasting cyber threats. *Scientific Reports*, *13*(1), 8049. https://doi.org/10.1038/s41598-023-35198-1

[10]. Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39. https://doi.org/10.3390/a10020039

[11]. Asheke, M. (2023). Machine Learning–Based Predictive Quality Modeling for Defect Detection and Process Optimization in Advanced Manufacturing Systems. *Review of Applied Science and Technology*, *13*(12), 01–49. https://doi.org/10.63125/thy73b16

[12]. Asheke, M. (2024). Digital Twin and Industrial Internet of Things–Enabled Predictive Maintenance for Reliability Enhancement in Smart Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 792–838. https://doi.org/10.63125/jgrdqd62

[13]. Ashik, M., & Shabbir, A. (2022). Digital Twin-Enabled Predictive Maintenance for Rotating and Static Equipment: Bridging FEA-Based Failure Analysis with Real-Time Asset Health Monitoring in Energy and Power Facilities. *International Journal of Scientific Interdisciplinary Research*, *12*(05), 01–37. https://doi.org/10.63125/0qaysz49

[14]. Bagheri, S., Ridley, G., & Williams, B. (2022). Organisational cyber resilience: Management perspectives. *Australasian Journal of Information Systems*, *27*, Article 9. https://doi.org/10.3127/ajis.v27i0.4183

[15]. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. *Information*, *10*(4), 122. https://doi.org/10.3390/info10040122

[16]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176. https://doi.org/10.1109/comst.2015.2494502

[17]. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548. https://doi.org/10.2307/25750690

[18]. Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

[19]. de Nobrega, K., Rutkowski, A. F., & Saunders, C. (2024). The whole of cyber defense: Syncing practice and theory. *The Journal of Strategic Information Systems*, *33*(4), 101861. https://doi.org/10.1016/j.jsis.2024.101861

[20]. Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *International Journal of Artificial Intelligence & Applications*, *6*(1), 21-39. https://doi.org/10.5121/ijaia.2015.6102

[21]. Drnevich, P. L., & Croson, D. C. (2013). Information technology and business-level strategy: Toward an integrated theoretical perspective. *MIS Quarterly*, *37*(2), 483-509. https://doi.org/10.25300/misq/2013/37.2.08

[22]. Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*, *132*, 103372. https://doi.org/10.1016/j.cose.2023.103372

[23]. Dutta, A., & Roy, R. (2008). Dynamics of organizational information security. *System Dynamics Review*, *24*(3), 349-375. https://doi.org/10.1002/sdr.405

[24]. Gazi Yeasin, A. (2023). Impact of Accessibility-First Design Systems on WCAG 2.1 Compliance and Inclusive User Experience in Enterprise Software Platforms: A Mixed-Methods Evaluation. *Review of Applied Science and Technology*, *13*(07), 01–49. https://doi.org/10.63125/nxh4gp19

[25]. Ghahramani, F., Yazdanmehr, A., Chen, D., & Wang, J. (2023). Continuous improvement of information security management: An organisational learning perspective. *European Journal of Information Systems*, *32*(6), 1011-1032. https://doi.org/10.1080/0960085x.2022.2096491

[26]. Goel, L., Russell, D., Williamson, S., & Zhang, J. Z. (2023). Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management*, *36*(4), 906-924. https://doi.org/10.1108/jeim-07-2022-0228

[27]. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

[28]. Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2020). A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access*, *8*, 104650-104675. https://doi.org/10.1109/access.2020.3000179

[29]. Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security: A neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153-172. https://doi.org/10.1016/j.jsis.2007.05.004

[30]. Islam, C., Babar, M. A., Croft, R., & Janicke, H. (2022). SmartValidator: A framework for automatic identification and classification of cyber threat data. *Journal of Network and Computer Applications*, *202*, 103370. https://doi.org/10.1016/j.jnca.2022.103370

[31]. Islam, C., Babar, M. A., & Nepal, S. (2019). A multi-vocal review of security orchestration. *ACM Computing Surveys*, *52*(2), Article 37, 31-45. https://doi.org/10.1145/3305268

[32]. Islam, C., Babar, M. A., & Nepal, S. (2020). Architecture-centric support for integrating security tools in a security orchestration platform. *Software Architecture: 14th European Conference, ECSA 2020*, 165-181. https://doi.org/10.1007/978-3-030-58923-3_11

[33]. Jahanara, A. (2025). AI-Enabled Workforce Management: Its Impact on Employee Burnout, Staffing Efficiency, and Organizational Performance in Healthcare. *Review of Applied Science and Technology*, *4*(04), 247–295. https://doi.org/10.63125/5617ff74

[34]. Jahanara, A. (2026). Impact of Artificial Intelligence on Operational Efficiency and Cost Reduction in U.S. Healthcare Organizations. *American Journal of Interdisciplinary Studies*, *7*(02), 225-276. https://doi.org/10.63125/3p24ma43

[35]. Jahanara, A., & Mst Kaniz, F. (2023). Demand Variability and Capacity Planning in Home and Community-Based Services: A Decision-Analytic Framework for Health Services Managers. *American Journal of Data Science and Analytics*, *4*(09), 01-49. https://doi.org/10.63125/3y62vr16

[36]. Jannatul, F. (2025). Spinal Cord Injury and Neurorehabilitation Deep Learning–Based Prediction of Functional Recovery Trajectories After Traumatic Spinal Cord Injury. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2865–2922. https://doi.org/10.63125/m738bh82

[37]. Jannatul, F. (2026). Predicting Falls and Mobility Decline Among Older Adults Using Longitudinal Functional Data and Ensemble Machine Learning. *International Journal of Scientific Interdisciplinary Research*, *7*(1), 581–631. https://doi.org/10.63125/56hans40

[38]. Javed, A., Lakoju, M., Burnap, P., & Rana, O. (2022). Security analytics for real-time forecasting of cyberattacks. *Software: Practice and Experience*, *52*(3), 788-804. https://doi.org/10.1002/spe.2822

[39]. Kazi Mohammad Khalid, A. (2026). A Systematic Review of GeoAI and Deep Learning for Automated Road Infrastructure Damage Detection Using Satellite Imagery. *American Journal of Data Science and Analytics*, *7*(03), 208-255. https://doi.org/10.63125/77cy0h19

[40]. Kazi Rakib Hasan, S., & Adnan, S. (2022). Quantitative Assessment of Machine Learning-Based Schedule Risk Prediction for Reducing Delays in Complex Technology Projects. *Review of Applied Science and Technology*, *1*(04), 464–501. https://doi.org/10.63125/dn8nkm85

[41]. Kok, A., Ilic Mestric, I., Valiyev, G., & Street, M. (2020). Cyber threat prediction with machine learning. *Information & Security: An International Journal*, *47*(2), 203-220. https://doi.org/10.11610/isij.4714

[42]. Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. *European Journal of Information Systems*, *32*(1), 35-51. https://doi.org/10.1080/0960085x.2022.2088414

[43]. Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, *25*(2), 241-279. https://doi.org/10.2753/mis0742-1222250210

[44]. Liu, C.-W., Huang, P., & Lucas, H. C., Jr. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from U.S. higher education institutions. *Journal of Management Information Systems*, *37*(3), 758-787. https://doi.org/10.1080/07421222.2020.1790190

[45]. Mahbubul, I., Mahmudul, I., Shifa, T., Mahfuza, T., & Shima Ali, S. (2022). Exploring The Potential of Visual Narratives and Interactive Gamified Communication Systems to Prevent Disease, Counter Health Misinformation,

And Strengthen Public Trust in Low-Literacy Communities: A Literature Review. *American Journal of Interdisciplinary Studies*, *3*(02), 165-220. https://doi.org/10.63125/zmqs4n64

[46]. Maishar Mostari, Z. (2025). Impact of Deep Learning on Real-Time Network Intrusion Detection: A Quantitative Evaluation Using Benchmark Datasets. *Review of Applied Science and Technology*, *4*(04), 296–338. https://doi.org/10.63125/tnaksd40

[47]. Mashfiqur, R. (2025). Multivariate Time-Series Forecasting of Working Capital Requirements for Improving Cash-Flow Stability in Export-Oriented Manufacturing. *American Journal of Data Science and Analytics*, *6*(12), 217-249. https://doi.org/10.63125/ty3dtt46

[48]. Mashfiqur, R. (2026). Explainable Artificial Intelligence for Supplier Cost-Risk Assessment and Margin Optimization in Global Manufacturing Supply Chains. *American Journal of Interdisciplinary Studies*, *16*(08), 01-37. https://doi.org/10.63125/np6bw920

[49]. Mashfiqur, R., & Md, A. (2022). Monte Carlo Simulation and Stochastic Cash-Flow Modeling for Reducing Liquidity Risk in Project-Based Enterprises. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 382–431. https://doi.org/10.63125/zf3fwv21

[50]. Mashiat, N. (2024). Reducing Telecommunications Service Interruptions Through Predictive Root-Cause Analytics of Multivariate System Telemetry. *International Journal of Scientific Interdisciplinary Research*, *14*(11), 01-37. https://doi.org/10.63125/nqjh0c29

[51]. Mashiat, N. (2025). Improving Enterprise Data Integrity Through Automated Validation and Schema-Drift Detection in Large-Scale Data Integration Systems. *Review of Applied Science and Technology*, *4*(02), 889–934. https://doi.org/10.63125/21zzkk04

[52]. Mashiat, N. (2026). Accelerating Incident Diagnosis and Service Recovery Through Generative AI-Assisted Failure Intelligence in Critical Digital Infrastructure. *American Journal of Data Science and Analytics*, *7*(06), 702-740. https://doi.org/10.63125/61etqg30

[53]. Mashiat, N., & Md Anisur Rahman, M. (2022). Machine Learning Approaches to Credit Risk Scoring and Default Prediction in Small-Business Lending: Empirical Evidence from Lending Portfolio Data. *American Journal of Data Science and Analytics*, *3*(06), 137-182. https://doi.org/10.63125/j256rs96

[54]. Md, A., & Gazi Yeasin, A. (2022). Machine Learning Enhanced Spatial-Data Workflow Redesign: A Quantitative Evaluation of Task Success and Operational Cost Reduction in Enterprise LiDAR Platforms. *American Journal of Data Science and Analytics*, *3*(06), 80-136. https://doi.org/10.63125/0den7c02

[55]. Md Anisur Rahman, M. (2023). Development of AI-Driven Business Intelligence Frameworks for Financial Risk and Liquidity Monitoring in Real Time. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 152–203. https://doi.org/10.63125/jm55ca64

[56]. Md Arif Uz, Z., Sharmin, S., & Md Abdur, R. (2025). Factors Influencing Behavioural Intention to Use he Innovative Open And Distance Learning Systems With The Role Of Continuance Intention. *American Journal of Scholarly Research and Innovation*, *4*(01), 202-220. https://doi.org/10.63125/pbjxp014

[57]. Md Ashfaq, S., & Abdullah Mohammad, S. (2022). CNT/PANI Composite Electrodes for Flexible Fiber-Shaped Dye-Sensitized Solar Cells: Synthesis, Characterization, and Photovoltaic Performance. *American Journal of Interdisciplinary Studies*, *3*(02), 221-274. https://doi.org/10.63125/m334mf41

[58]. Md Asif Ali Sheak, A., & Tahmedur, R. (2023). A Data-Driven Framework for Engineering Project Risk Assessment Under Schedule and Cost Uncertainty. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 204–251. https://doi.org/10.63125/kq4zzh16

[59]. Md Kaium, H. (2023). A GIS-Based Multi-Criteria Decision-Support and Land-Suitability Optimization Framework for Climate-Resilient Urban and Regional Planning. *American Journal of Data Science and Analytics*, *4*(06), 43–103. https://doi.org/10.63125/wvq0sx87

[60]. Md Kaium, H. (2024). Machine Learning Enhanced GIS And AHP Modeling for High-Resolution Flood-Susceptibility Prediction, Vulnerability Assessment, and Risk Classification. *Review of Applied Science and Technology*, *3*(02), 92–140. https://doi.org/10.63125/fz8hv245

[61]. Md Kaium, H. (2025). Integrating Artificial Intelligence, Semantic Indoor Geospatial Modeling, And Network-Based Routing for High-Precision NG911 Emergency Location Intelligence. *International Journal of Scientific Interdisciplinary Research*, *6*(1), 616–670. https://doi.org/10.63125/5hc1xx56

[62]. Md Kaium, H. (2026). An Artificial Intelligence Integrated Geospatial Decision-Support Framework for Scenario-Based Climate-Adaptive Land-Use Optimization and Environmental Risk Reduction. *American Journal of Data Science and Analytics*, *7*(06), 425-483. https://doi.org/10.63125/nyc7sh45

[63]. Md Mahamud Pervaz, P. (2023). Integration of MES, SAP, And PI Historian Platforms for Real-Time Industrial Asset Performance Management. *Review of Applied Science and Technology*, *2*(04), 393–445. https://doi.org/10.63125/9ebtas97

[64]. Md Mahamud Pervaz, P. (2025). Development of a CMMS-Integrated Predictive Maintenance Framework for Industrial PLC and Drive Systems. *American Journal of Scholarly Research and Innovation*, *4*(01), 894–942. https://doi.org/10.63125/j33gtf31

[65]. Md Mahamud Pervaz, P. (2026). Implementation of an OSHA-Compliant Lockout/Tagout and Arc-Flash Hazard Mitigation Framework for U.S. Industrial Maintenance Operations. *American Journal of Interdisciplinary Studies*, *7*(02), 73-119. https://doi.org/10.63125/8ky04n07

[66]. Mikalef, P., Krogstie, J., Pappas, I. O., & Pavlou, P. A. (2020). Exploring the relationship between big data analytics capability and competitive performance: The mediating roles of dynamic and operational capabilities. *Information & Management*, *57*(2), 103169. https://doi.org/10.1016/j.im.2019.05.004

[67]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning–Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, *3*(02), 33-77. https://doi.org/10.63125/y3yfxa92

[68]. Molla Al Rakib, H., & Mohammad Towhidul, I. (2023). Cyber-Resilient Marketing Intelligence Systems for Fraud Detection and Data Integrity in Digital Campaigns. *American Journal of Scholarly Research and Innovation*, *2*(02), 485–518. https://doi.org/10.63125/b53pgr11

[69]. Mst Kaniz, F., & Jahanara, A. (2022). Lean Six Sigma Implementation in Home Health Administrative Operations: A DMAIC Case Study of Managerial Workflow Redesign and Error Reduction. *International Journal of Scientific Interdisciplinary Research*, *12*(04), 01–60. https://doi.org/10.63125/xchca204

[70]. Mst Shamima, A. (2026). Enhancing Financial Accountability and Cost Control in North American Outpatient Clinics Through Data Science: A Mixed-Methods Healthcare Administration Study. *American Journal of Data Science and Analytics*, *7*(05), 01-41. https://doi.org/10.63125/wksgy749

[71]. Mukut Kanti, B. (2023). Importance of the Sustainable growth in the Testing, Inspection and Certification (TIC) industries through AI tools and techniques. *Review of Applied Science and Technology*, *13*(07), 50–75. https://doi.org/10.63125/0aagev30

[72]. Mukut Kanti, B. (2024). AI-Enabled Predictive Asset Integrity Monitoring for Industrial Equipment in Oil & Gas and Energy Sector Facilities. *International Journal of Scientific Interdisciplinary Research*, *5*(2), 746–791. https://doi.org/10.63125/3mjcah04

[73]. Mukut Kanti, B. (2026). Digital-Twin And IOT-Based Condition Monitoring for Rotating Machinery and Process Equipment in Petrochemical and Industrial Environments. *American Journal of Scholarly Research and Innovation*, *5*(01), 382–428. https://doi.org/10.63125/mwdnjv55

[74]. Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex & Intelligent Systems*, *8*, 1763-1780. https://doi.org/10.1007/s40747-021-00494-8

[75]. Nishat, J. (2023). Communicable Disease Prevention in a Post-Pandemic Era: A Global Review of Public Health Education, Surveillance, and Community-Level Interventions. *International Journal of Scientific Interdisciplinary Research*, *4*(4), 630–678. https://doi.org/10.63125/mnqefj36

[76]. Nuzhat Sadia, P. (2023). A Multi-Criteria Decision-Support Framework For ERP-Based Business Process Optimization in Mid-Sized Manufacturing Enterprises. *American Journal of Scholarly Research and Innovation*, *2*(02), 519–573. https://doi.org/10.63125/j58k5d55

[77]. Palash Chandra, D. (2025). Advanced Composite and Geopolymer Materials for Durable Water Supply and Sanitation Infrastructure: Performance, Sustainability, and Lifecycle Assessment. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 1887–1921. https://doi.org/10.63125/z64akr77

[78]. Pavlou, P. A., & El Sawy, O. A. (2011). Understanding the elusive black box of dynamic capabilities. *Decision Sciences*, *42*(1), 239-273. https://doi.org/10.1111/j.1540-5915.2010.00287.x

[79]. Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. *Computers & Security*, *67*, 35-58. https://doi.org/10.1016/j.cose.2017.02.005

[80]. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, *86*, 147-167. https://doi.org/10.1016/j.cose.2019.06.005

[81]. Risha, A., & Mst Shurovi, A. (2023). Cloud-Based Accounting Systems and Cybersecurity Frameworks for Financial Data Protection in Emerging Economies: A Meta-Analysis. *International Journal of Business and Economics Insights*, *3*(4), 26–64. https://doi.org/10.63125/zb0h3n85

[82]. Rony, S., & Md, A. (2026). Multi-Agency Coordination in Sustained Healthcare Supply Shortages: Lessons from Covid-19, Drug Shortages, and Critical Medical Supply Disruptions. *American Journal of Data Science and Analytics*, *7*(01), 181-221. https://doi.org/10.63125/5v6t8515

[83]. Sadia, Z., & Maishar Mostari, Z. (2022). The Impact of Interactive Dashboard Visualization on Data-Driven Decision Making in Financial Services: A Qualitative Evaluation. *International Journal of Scientific Interdisciplinary Research*, *12*(03), 01–35. https://doi.org/10.63125/3jstsv75

[84]. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, *23*(16), 7273. https://doi.org/10.3390/s23167273

[85]. Samtani, S., Chai, Y., & Chen, H. (2022). Linking exploits from the Dark Web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep structured semantic model. *MIS Quarterly*, *46*(2), 911-946. https://doi.org/10.25300/misq/2022/15392

[86]. Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the artificial intelligence for cybersecurity discipline: A multi-disciplinary research roadmap. *ACM Transactions on Management Information Systems*, *11*(4), Article 17, 11-19. https://doi.org/10.1145/3430360

[87]. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*, Article 41. https://doi.org/10.1186/s40537-020-00318-5

[88]. Schlette, D., Böhm, F., Caselli, M., & Pernul, G. (2021). Measuring and visualizing cyber threat intelligence quality. *International Journal of Information Security*, *20*, 21-38. https://doi.org/10.1007/s10207-020-00490-y

[89]. Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, *97*, 101996. https://doi.org/10.1016/j.cose.2020.101996

[90]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, *3*(04), 1-31. https://doi.org/10.63125/negjw373

[91]. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41-50. https://doi.org/10.1109/tetci.2017.2772792

[92]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305-316. https://doi.org/10.1109/sp.2010.25

[93]. Stabak, D., & Md Shahid, N. (2022). Empirical Assessment of Uncertainty-Aware Real-Time Decision-Making for Reliable and Resilient Cyber-Physical Systems. *International Journal of Scientific Interdisciplinary Research*, *1*(01), 432–477. https://doi.org/10.63125/q3r4kk16

[94]. Stabak, D., & Md Siam, T. (2023). Real-Time Edge Computing for Cyber-Physical Systems: A Meta-Analysis of Energy Efficiency and Fault Tolerance. *American Journal of Scholarly Research and Innovation*, *13*(06), 01–44. https://doi.org/10.63125/g9c9cp41

[95]. Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748-1774. https://doi.org/10.1109/comst.2023.3273282

[96]. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2019). Data-driven cybersecurity incident prediction: A survey. *IEEE Communications Surveys & Tutorials*, *21*(2), 1744-1772. https://doi.org/10.1109/comst.2018.2885561

[97]. Syed Feroz, A. (2023). Quality-Management Systems for Resilient Energy Infrastructure Fabrication. *International Journal of Scientific Interdisciplinary Research*, *13*(10), 37–91. https://doi.org/10.63125/mbhhrm88

[98]. Syed Feroz, A. (2024). AI-Assisted NDT Analytics for Early Crack Detection in Energy-Infrastructure Pressure Vessels Using Advanced Manufacturing Data. *Review of Applied Science and Technology*, *14*(07), 01-52. https://doi.org/10.63125/8bdqs538

[99]. Syed Feroz, A. (2025). Intelligent Process Monitoring for Enhancing Weld Integrity and Reliability in Advanced Manufacturing of LPG Energy Infrastructure. *American Journal of Interdisciplinary Studies*, *6*(3), 394-441. https://doi.org/10.63125/p3b5mb44

[100]. Syed Feroz, A., & Md Mahamud Pervaz, P. (2022). Root-Cause Analysis and FMEA-Driven Reliability Improvement in Gas Production Facilities: A Multi-Year Empirical Study. *International Journal of Scientific Interdisciplinary Research*, *12*(10), 01–53. https://doi.org/10.63125/70msp878

[101]. Tahmedur, R., & Rifat, C. (2023). Critical Path Analysis and Resource-Leveling Optimization for Multi-Project Engineering Portfolios. *American Journal of Interdisciplinary Studies*, *13*(12), 01-47. https://doi.org/10.63125/8eqnea46

[102]. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. *Strategic Management Journal*, *28*(13), 1319-1350. https://doi.org/10.1002/smj.640

[103]. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212-233. https://doi.org/10.1016/j.cose.2017.09.001

[104]. Tsen, E., Ko, R. K. L., & Slapnicar, S. (2022). An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce*, *32*(2), 153-174. https://doi.org/10.1080/10919392.2022.2068906

[105]. Uddin, H. M. M., & Risha, A. (2024). Hybrid Cloud Security and Compliance in U.S. Enterprises: Addressing Data Privacy Risks and Governance Challenges. *American Journal of Scholarly Research and Innovation*, *3*(01), 153–197. https://doi.org/10.63125/qcy0cj46

[106]. Vasudevan, S., Piazza, A., & Carr, M. (2022). Qualitative factors in organizational cyber resilience. *2022 International Conference on Cyber Resilience (ICCR)*, 1-5. https://doi.org/10.1109/iccr56254.2022.9995762

[107]. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, *7*, 41525-41550. https://doi.org/10.1109/access.2019.2895334

[108]. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, *87*, 101589. https://doi.org/10.1016/j.cose.2019.101589

[109]. Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. *Journal of Business Research*, *70*, 356-365. https://doi.org/10.1016/j.jbusres.2016.08.009

[110]. Wilden, R., Gudergan, S. P., Nielsen, B. B., & Lings, I. (2013). Dynamic capabilities and performance: Strategy, structure and environment. *Long Range Planning*, *46*(1-2), 72-96. https://doi.org/10.1016/j.lrp.2012.12.001

[111]. Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365-35381. https://doi.org/10.1109/access.2018.2836950

[112]. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, *5*, 21954-21961. https://doi.org/10.1109/access.2017.2762418

[113]. Zibak, A., Sauerwein, C., & Simpson, A. (2021). A success model for cyber threat intelligence management platforms. *Computers & Security*, *111*, 102466. https://doi.org/10.1016/j.cose.2021.102466

[114]. Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. *Journal of*.