African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 9, Issue 3, 2026 (pp. 19-38)

www.abjournals.org

EMERGING CYBERSECURITY THREATS, ORGANIZATIONAL VULNERABILITIES, AND FRAUD RISK IN DIGITAL WORK ENVIRONMENTS

Evans O. N. D. Ocansey and Emmanuel Peprah

Department of Accounting & Finance, Valley View University, Oyibi, Accra, Ghana.

Cite this article:

Evans O. N. D. Ocansey, Emmanuel Peprah (2026), Emerging Cybersecurity Threats, Organizational Vulnerabilities, and Fraud Risk in Digital Work Environments. African Journal of Accounting and Financial Research 9(3), 19-38. DOI: 10.52589/AJAFR-3N2DOPIH

Manuscript History

Received: 30 May 2026

Accepted: 2 Jul 2026

Published: 15 Jul 2026

ABSTRACT: *The rapid digital transformation of organizations has increased operational efficiency while simultaneously exposing organizations to sophisticated cybersecurity threats and cyber-enabled fraud. Although numerous studies have examined these issues, the evidence remains fragmented across disciplines. This study conducts a systematic literature review (SLR) to synthesize existing knowledge on the relationship between emerging cybersecurity threats and organizational fraud risk. Guided by the PRISMA 2020 reporting framework, relevant studies published between 2013 and 2025 were identified through searches of Scopus, Web of Science, Google Scholar, IEEE Xplore, ScienceDirect, and SpringerLink. Following predefined inclusion and exclusion criteria, 32 studies were selected for qualitative synthesis. The findings identify four key moderating factors that shape organizational vulnerability to cyber-enabled fraud: organizational cybersecurity culture, regulatory and compliance environments, remote work policies and technological infrastructure, and employee psychological well-being. The review demonstrates that effective cybersecurity resilience depends on integrating technological safeguards with organizational, regulatory, and human-centred strategies. The study contributes an integrated conceptual framework that advances understanding of cyber-enabled fraud and provides practical recommendations for policymakers, organizational leaders, and cybersecurity professionals seeking to strengthen organizational resilience in increasingly digital work environments.*

KEYWORDS: Cybersecurity threats; Cyber-enabled fraud; Organizational resilience, Cybersecurity culture, Regulatory compliance, Employee well-being.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 9, Issue 3, 2026 (pp. 19-38)

INTRODUCTION

The rapid digital transformation of organizations has fundamentally altered the global business landscape, creating unprecedented opportunities for innovation, operational efficiency, and connectivity. The widespread adoption of cloud computing, artificial intelligence (AI), Internet of Things (IoT) technologies, big data analytics, and remote working arrangements has enabled organizations to operate across geographically dispersed environments while maintaining high levels of productivity and collaboration. However, these technological advancements have simultaneously expanded the cyber threat landscape, exposing organizations to increasingly sophisticated forms of cybercrime and fraud (Franke & Brynielsson, 2014; Javaid et al., 2023).

Cybersecurity threats have evolved substantially over the past decade, extending beyond traditional malware attacks to include ransomware, phishing campaigns, business email compromise (BEC), credential theft, social engineering attacks, insider threats, and AI-enabled cybercrime. These threats pose significant financial, operational, reputational, and legal risks to organizations across all sectors. Recent reports indicate that cyber-enabled fraud has become one of the most pervasive forms of organizational crime, resulting in substantial economic losses and compromising stakeholder trust worldwide (Aldawood & Skinner, 2019; Zaid & Garai, 2024). The convergence of digital technologies and cybercriminal innovation has therefore intensified the need for organizations to adopt comprehensive cybersecurity and fraud prevention strategies.

The expansion of remote and hybrid work arrangements following the COVID-19 pandemic has further complicated organizational cybersecurity management. While remote work has increased organizational flexibility and business continuity, it has also introduced new vulnerabilities associated with unsecured home networks, personal devices, weak authentication practices, and reduced organizational oversight (Okereafor et al., 2020; Bispham et al., 2021). Consequently, cybercriminals have increasingly exploited human and technological weaknesses to facilitate fraudulent activities, highlighting the interconnected nature of cybersecurity and fraud risks in contemporary organizations.

Although cybersecurity and fraud have traditionally been examined as separate research domains, emerging evidence suggests that these phenomena are closely interconnected. Cybersecurity breaches frequently serve as enablers of financial fraud, identity theft, data manipulation, and insider misconduct. At the same time, fraud prevention efforts increasingly depend on effective cybersecurity governance, employee awareness, and organizational resilience. Existing studies have examined various dimensions of this relationship, including cybersecurity culture, regulatory compliance, technological safeguards, and human behavioral factors. However, the literature remains fragmented across disciplines, industries, and methodological approaches, limiting the development of a comprehensive understanding of how these factors jointly influence cyber-enabled fraud outcomes (Alshaikh, 2020; Flores & Ekstedt, 2016).

A growing body of research emphasizes that technological controls alone are insufficient to mitigate cyber-enabled fraud risks. Human factors such as employee awareness, organizational culture, leadership commitment, psychological well-being, and compliance behavior significantly influence cybersecurity outcomes. Likewise, regulatory frameworks and governance mechanisms shape organizational preparedness and accountability in responding

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

to evolving cyber threats (Hiller & Russell, 2019; Williamson & Prybutok, 2024). These findings suggest that cybersecurity resilience emerges from the interaction of technological, organizational, regulatory, and behavioral factors rather than from technical solutions alone.

Despite increasing scholarly attention to cybersecurity and fraud, there remains a lack of systematic synthesis examining how these multidimensional factors moderate the relationship between emerging cybersecurity threats and organizational fraud risk. Previous studies have largely focused on individual sectors, specific technologies, or isolated risk factors, resulting in limited theoretical integration and practical guidance for organizations operating in increasingly digital environments. Furthermore, the rapid evolution of cyber threats necessitates continuous evaluation of existing evidence to identify emerging trends, research gaps, and effective mitigation strategies.

To address this gap, this study conducts a systematic literature review of empirical and theoretical research published between 2013 and 2025. The review synthesizes evidence concerning four critical moderating dimensions: organizational cybersecurity culture, regulatory and compliance environments, remote work policies and technological infrastructure, and employee psychological factors. By integrating findings across diverse industries and contexts, the study seeks to develop a comprehensive understanding of how these factors influence organizational vulnerability to cyber-enabled fraud.

The review is guided by the following research questions:

1. What emerging cybersecurity threats are most frequently associated with organizational fraud in contemporary digital work environments?
2. How do organizational, regulatory, technological, and psychological factors moderate the relationship between cybersecurity threats and fraud risk?
3. What evidence exists regarding the effectiveness of current cybersecurity and fraud prevention strategies?
4. What research gaps and future directions emerge from the existing body of literature?

This systematic literature review contributes to the growing cybersecurity and fraud literature in three important ways. First, it consolidates fragmented evidence across multiple disciplines into a unified analytical framework. Second, it identifies key moderating factors that influence the effectiveness of organizational responses to cyber-enabled fraud. Third, it provides evidence-based insights for policymakers, organizational leaders, cybersecurity professionals, and researchers seeking to strengthen resilience against emerging cyber threats in an increasingly digital economy.

Theoretical Framework

This review is grounded primarily in Socio-Technical Systems Theory (STS) and Institutional Theory, which together provide a comprehensive lens for understanding how cybersecurity threats translate into organizational fraud risk.

Socio-Technical Systems Theory argues that organizational performance is shaped by the interaction between technical systems and social systems rather than by technology alone. In cybersecurity contexts, technical controls such as firewalls, endpoint protection, encryption,

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

and multi-factor authentication are only effective when complemented by supportive organizational cultures, leadership commitment, employee awareness, and appropriate work practices. This perspective explains why organizations with comparable technological resources often experience different cybersecurity outcomes depending on employee behaviour and organizational culture.

Within this review, STS Theory explains how organizational cybersecurity culture, remote work infrastructure, and employee psychological well-being jointly moderate the relationship between cybersecurity threats and cyber-enabled fraud.

Institutional Theory proposes that organizational behaviour is influenced by external institutional pressures, including regulations, legal requirements, professional standards, and stakeholder expectations. Organizations often adopt cybersecurity practices to comply with regulatory frameworks such as data protection legislation, industry standards, and governance requirements. This theory therefore explains the role of regulatory compliance and governance mechanisms in strengthening organizational resilience against cyber-enabled fraud. Organizations operating within stronger institutional environments are generally more likely to implement comprehensive cybersecurity controls and fraud prevention mechanisms.

The integration of Socio-Technical Systems Theory and Institutional Theory provides the theoretical foundation for this review. While STS explains the interaction between technological and human factors, Institutional Theory explains how regulatory and governance environments shape organizational cybersecurity practices. Together, these theories support the proposed conceptual framework by demonstrating that organizational fraud risk emerges from the interaction of technological, organizational, regulatory, and behavioural factors rather than from isolated cybersecurity controls.

METHODOLOGY

Research Design

This study adopted a Systematic Literature Review (SLR) approach to synthesize existing knowledge on the relationship between emerging cybersecurity threats, organizational vulnerability, and fraud risk. A systematic review was selected because it provides a rigorous, transparent, and replicable process for identifying, evaluating, and synthesizing relevant literature within a specific research domain (Tranfield et al., 2003; Page et al., 2021). The review focused on understanding how organizational, regulatory, technological, and psychological factors influence organizational vulnerability to cyber-enabled fraud in contemporary digital environments.

The review was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines to ensure methodological transparency and consistency throughout the search, screening, eligibility assessment, and inclusion stages.

Search Strategy

A comprehensive literature search was conducted across major academic databases, including Google Scholar, Crossref, Scopus, Web of Science, IEEE Xplore, ScienceDirect, and

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

SpringerLink. These databases were selected because they provide extensive coverage of cybersecurity, information systems, fraud management, organizational behavior, and regulatory compliance research.

The search focused on peer-reviewed journal articles published between January 2013 and March 2025. This period was selected to capture contemporary developments in cybersecurity threats, digital transformation, remote work environments, and cyber-enabled fraud.

The search strings combined keywords related to cybersecurity threats and fraud risks with moderating organizational factors. Examples of search terms included: "cybersecurity threats" AND fraud, "cyber-enabled fraud" AND organizations, "cybersecurity culture" AND fraud prevention, "regulatory compliance" AND cybersecurity risk, "remote work security" AND cybercrime, "employee stress" AND cybersecurity, "social engineering" AND organizational vulnerability, "insider threats" AND fraud risk, and "cyber resilience" AND organizational security. Boolean operators (AND, OR) and truncation techniques were used to maximize search sensitivity while maintaining relevance.

Inclusion and Exclusion Criteria

To ensure consistency and relevance, studies were evaluated using predefined inclusion and exclusion criteria.

Inclusion Criteria

Studies were included if they: were published in peer-reviewed journals, conference proceedings, or reputable academic publications; were written in English; were published between 2013 and 2025; and examined cybersecurity threats, cybercrime, cyber-enabled fraud, or related organizational risks. The study also included papers that investigated at least one moderating factor, including organizational cybersecurity culture, regulatory compliance, remote work infrastructure, or employee psychological factors, and reported empirical, theoretical, conceptual, or review-based findings relevant to the study objectives.

Exclusion Criteria

Studies were excluded if they focused exclusively on technical system design without organizational implications and were opinion pieces, editorials, blogs, or non-scholarly publications. Those that did not address cybersecurity or fraud-related outcomes, had duplicate records across databases, and lacked sufficient methodological detail or relevance to the review objectives were also excluded.

Study Selection Process

The study selection process followed four stages based on the PRISMA framework: identification, screening, eligibility assessment, and inclusion. The initial database search yielded more than 1,000 records. Additional studies were identified through backward and forward citation tracking of highly relevant publications. Titles and abstracts were screened to determine their relevance to the review objectives. Duplicate records were removed prior to screening. Full-text articles that met the screening criteria were evaluated against the inclusion and exclusion criteria. Studies were assessed for methodological quality, relevance, publication credibility, and contribution to understanding cybersecurity-fraud relationships. Following the eligibility assessment, 32 studies were retained for final synthesis. These studies represented

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

diverse sectors, including finance, healthcare, education, manufacturing, information technology, hospitality, and public administration.

Quality Assessment

To enhance the reliability of the review, each selected study underwent a quality appraisal process. Studies were evaluated according to research design and methodological rigor; clarity of objectives and theoretical grounding; data collection and analytical procedures; validity and reliability considerations; relevance to the review questions; and citation impact and publication quality. Studies demonstrating strong methodological quality and direct relevance to the review objectives were prioritized during the synthesis process.

Data Extraction

A structured data extraction protocol was used to ensure consistency across studies. The following information was extracted from each article: author(s) and publication year; country or geographical context; industry or sector studied; research methodology; sample characteristics; type of cybersecurity threat examined; fraud-related outcomes; key findings; moderating factors identified; and implications for organizational cybersecurity and fraud prevention. The extracted information was organized into a review matrix to facilitate comparison across studies.

Data Synthesis and Analysis

A thematic synthesis approach was employed to analyze and integrate findings across the selected studies. Thematic analysis was considered appropriate because the literature included qualitative, quantitative, conceptual, and mixed-methods research designs. The synthesis process involved three stages: initial coding of findings related to cybersecurity threats and fraud risks; identification of recurring themes and patterns across studies; and development of higher-order categories representing major moderating factors.

Four dominant themes emerged from the analysis: organizational cybersecurity culture, regulatory environment and compliance enforcement, remote work policies and technological infrastructure, and employee psychological factors (stress, burnout, and job satisfaction). These themes formed the analytical framework used to examine how organizational vulnerabilities influence the relationship between emerging cybersecurity threats and fraud outcomes.

Reliability and Validity

To improve the credibility of the review findings, the study employed transparent search procedures, clearly defined selection criteria, and systematic data extraction protocols. The use of multiple databases reduced the likelihood of publication bias and improved coverage of interdisciplinary research. Furthermore, adherence to PRISMA guidelines enhanced methodological transparency and reproducibility.

Ethical Considerations

This study relied exclusively on publicly available secondary data from published academic sources and therefore did not require formal ethical approval. All sources were appropriately acknowledged and cited in accordance with academic research standards.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

African Journal of Accounting and Financial Research
ISSN: 2682-6690
Volume 9, Issue 3, 2026 (pp. 19-38)
www.abjournals.org

PRISMA Flow Diagram and Study Selection

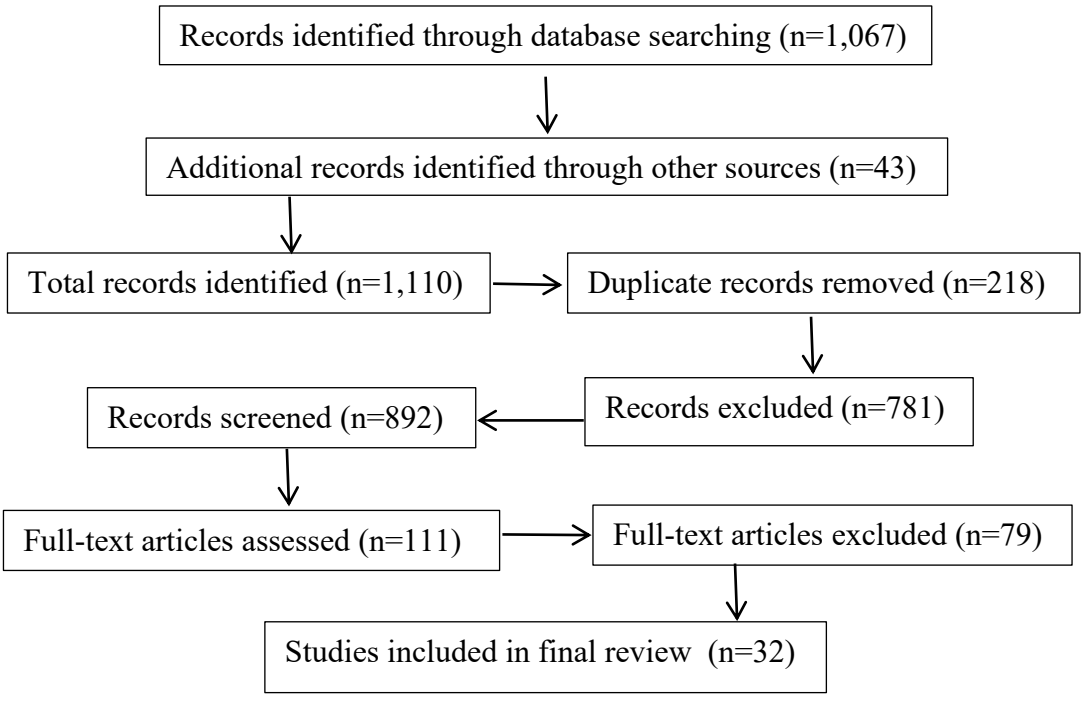
The study selection process followed the PRISMA 2020 framework to ensure transparency and methodological rigor throughout the review process. The identification stage consisted of an initial search across Google Scholar, Crossref, Scopus, Web of Science, ScienceDirect, IEEE Xplore, and SpringerLink, yielding 1,067 records. An additional 43 records were identified through citation tracking and manual searches of reference lists. The total number of records identified was 1,110.

The screening stage was conducted by removing duplicate records (n = 218), and 892 studies remained for title and abstract screening. During this stage, 781 studies were excluded because they did not focus on cybersecurity threats, cyber-enabled fraud, organizational vulnerabilities, or related moderating factors. The records screened were **892, and** records excluded were **781.**

The eligibility stage assessed the remaining 111 full-text articles. Of these, 79 studies were excluded for one or more of the following reasons: limited relevance to organizational fraud (n = 24), insufficient methodological detail (n = 18), technical focus without organizational implications (n = 21), non-peer-reviewed sources (n = 9), and duplicate reporting of findings (n = 7). The full-text articles assessed were **111, and** full-text articles excluded were **79.** A total of **32 studies** met all inclusion criteria and were included in the final qualitative synthesis.

The review followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines, an internationally recognised framework designed to improve the transparency, completeness, and reproducibility of systematic reviews. PRISMA 2020 outlines four sequential stages—identification, screening, eligibility assessment, and inclusion—which guide researchers in documenting the study selection process. Adherence to these guidelines enhances methodological rigour and enables readers to evaluate the comprehensiveness of the review. Figure 1 presents the PRISMA flow diagram illustrating the study selection process.

Figure 1. PRISMA 2020 Flow Diagram of Study Selection



Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

The review matrix was used as the primary data extraction tool during the synthesis process. Table 1 presents a summarized version of the review matrix, highlighting the characteristics of the included studies.

Table 1. Summary of Included Studies' Characteristics

Author(s)	Year	Sector	Focus Area	Key Findings
Franke & Brynielsson	2014	Cybersecurity	Situational Awareness	Cyber awareness strengthens threat detection capabilities.
Ifinedo	2014	Information Systems	Security Compliance	Organizational influence improves policy compliance.
Khamisa et al.	2015	Healthcare	Stress and Burnout	High stress increases vulnerability to errors and security lapses.
Wagaman et al.	2015	Social Work	Employee Well-being	Empathy reduces burnout and improves resilience.
Hayes et al.	2015	Healthcare	Job Satisfaction	Burnout negatively affects organizational performance.
Öğütçü et al.	2016	Information Security	Security Awareness	User awareness influences secure behavior.
Ani et al.	2016	Manufacturing	Critical Infrastructure Security	Human and technical controls are jointly required.
Flores & Ekstedt	2016	Business	Security Culture	Leadership influences resistance to social engineering.
Hendrix et al.	2016	Education	Cybersecurity Training	Serious games improve awareness outcomes.
Souppaya & Scarfone	2016	Technology	Remote Work Security	BYOD policies require structured controls.
Hiller & Russell	2019	Law and Policy	Cybersecurity Regulation	Strong regulation reduces organizational vulnerabilities.
Aldawood & Skinner	2019	Cybersecurity	Social Engineering	Awareness programs reduce cyber manipulation risks.
Carter	2019	Genomics	Data Privacy	Regulatory compliance supports secure data management.
Alshaikh	2020	Business	Cybersecurity Culture	Security culture influences employee behavior.
Okereafor et al.	2020	Remote Work	Telecommuting Security	Remote work introduces new cyber vulnerabilities.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

Evangelakos	2020	Business	Remote Security	Distributed work requires stronger security governance.
Shah & Nazir	2020	Information Security	Remote Work Risks	Cyber risks increased significantly during remote work adoption.
Bispham et al.	2021	Technology	Work-from-Home Security	Cybersecurity practices support sustainable remote work.
Wylde et al.	2022	Blockchain	Data Privacy	Blockchain improves integrity but requires regulatory support.
Javaid et al.	2023	Healthcare	Healthcare Cybersecurity	Cyberattacks increasingly target healthcare systems.
Dhirani et al.	2023	Emerging Technologies	Ethics and Privacy	Regulatory gaps create cybersecurity risks.
Chauhan & Shiaeles	2023	Cloud Computing	Cloud Security	Security frameworks improve cloud resilience.
Bello et al.	2024	SMEs	Financial Compliance	Compliance systems reduce operational risks.
Walter	2024	Artificial Intelligence	AI Governance	Regulatory harmonization remains limited.
Williamson & Prybutok	2024	Healthcare AI	Privacy and Security	Strong governance improves trust and compliance.
Zaid & Garai	2024	Cybersecurity	Emerging Threats	Threat landscape continues to evolve rapidly.
Moore et al.	2016	Financial Crime	Employee Stress	Workplace stress contributes to fraud risk.
Younglove	2000	Technology	VPN Security	VPNs remain fundamental for secure remote access.
Upadyaya et al.	2016	Occupational Psychology	Burnout and Engagement	Employee engagement reduces negative outcomes.
Cheng & O-Yang	2018	Hospitality	Job Crafting	Organizational support improves employee resilience.
Williams	2016	International Business	Cybersecurity Regulation	Regulatory frameworks influence security practices.
Additional cross-sector synthesis studies	2013–2025	Multiple	Cybersecurity and Fraud	Integrated approaches are most effective.

Source: *Compiled by the authors from the studies included in the systematic literature review (2025)*

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

RESULTS AND DISCUSSION

Results and Discussion

Overview of Included Studies

The systematic review synthesized evidence from 32 studies published between 2013 and 2025 as indicated in Table 1. The selected studies represented a diverse range of sectors, including healthcare, information technology, manufacturing, financial services, hospitality, education, social work, and public administration. This diversity demonstrates that cybersecurity threats and cyber-enabled fraud are not sector-specific challenges but increasingly pervasive organizational risks affecting both public and private institutions.

The reviewed studies consistently identified four major themes influencing organizational vulnerability to cyber-enabled fraud. The themes are organizational cybersecurity culture, regulatory environment and compliance enforcement, remote work policies and technological infrastructure, and employee psychological factors. These themes emerged as critical moderating factors shaping the extent to which cybersecurity threats translate into successful fraud incidents.

Organizational Cybersecurity Culture

One of the most prominent findings across the reviewed literature is the importance of organizational cybersecurity culture in mitigating fraud risk. Studies consistently indicate that organizations with strong cybersecurity cultures exhibit higher levels of employee vigilance, policy compliance, and resistance to social engineering attacks.

Aldawood and Skinner (2019) found that cybersecurity awareness programs significantly improve employees' ability to recognize manipulation tactics commonly used in phishing and social engineering campaigns. Similarly, Alshaikh (2020) argued that cybersecurity culture extends beyond technical controls and encompasses shared values, norms, and behavioral expectations that influence organizational security outcomes.

Leadership commitment emerged as a particularly important determinant of cybersecurity culture. Flores and Ekstedt (2016) demonstrated that transformational leadership positively influences employee intentions to resist social engineering attacks through the development of a strong information security culture. These findings suggest that organizational leaders play a critical role in embedding cybersecurity values throughout the organization.

The evidence therefore supports the argument that cybersecurity resilience is not solely a technological issue but also a cultural and behavioral challenge. Organizations that invest in continuous awareness training, leadership engagement, and security-conscious workplace cultures are better positioned to prevent cyber-enabled fraud.

Regulatory Environment and Compliance Enforcement

The second major theme concerns the role of regulatory frameworks in reducing organizational exposure to cybersecurity threats and fraud. The literature consistently indicates that strong regulatory environments improve organizational accountability, strengthen governance mechanisms, and encourage proactive cybersecurity investments.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

Studies examining GDPR implementation, financial compliance systems, cloud security standards, and AI governance frameworks suggest that regulatory compliance serves as both a deterrent and a protective mechanism against cybercrime. Hiller and Russell (2019) found that jurisdictions with mature cybersecurity regulations demonstrate greater resilience against cyber threats than those with fragmented legal frameworks.

Recent studies also emphasize the challenges associated with emerging technologies. Dhirani et al. (2023) and Walter (2024) highlight regulatory uncertainty surrounding artificial intelligence, while Williamson and Prybutok (2024) emphasize privacy concerns in AI-driven healthcare systems. These findings suggest that regulatory systems must evolve continuously to address emerging technological risks. In all, the review indicates that effective regulatory enforcement reduces opportunities for cyber-enabled fraud by establishing clear standards, increasing accountability, and promoting organizational preparedness.

Remote Work Policies and Technological Infrastructure

The third major theme emerging from the review concerns the role of remote work policies and technological infrastructure in moderating organizational exposure to cybersecurity threats and fraud. The rapid transition to remote and hybrid work arrangements following the COVID-19 pandemic fundamentally altered organizational security environments. While remote work improved flexibility and business continuity, it simultaneously expanded the attack surface available to cybercriminals.

Several studies identified inadequate remote work governance as a significant contributor to cybersecurity vulnerabilities. Okereafor et al. (2020) observed that employees working from home frequently relied on personal devices, unsecured Wi-Fi networks, and consumer-grade communication tools, increasing organizational exposure to cyberattacks. Similarly, Shah and Nazir (2020) found that remote work environments created opportunities for phishing, credential theft, ransomware attacks, and unauthorized access to corporate systems.

The reviewed literature consistently highlights the importance of secure technological infrastructure in mitigating these risks. Souppaya and Scarfone (2016) emphasized that remote work security requires comprehensive policies governing device management, secure authentication, network access controls, and endpoint protection. Organizations implementing structured Bring Your Own Device (BYOD) policies, multi-factor authentication (MFA), endpoint detection and response (EDR) systems, and regular software updates demonstrated greater resilience against cyber threats.

Virtual Private Networks (VPNs) emerged as one of the most frequently cited technological safeguards. Younglove (2000) noted that VPNs facilitate secure communication channels between remote employees and organizational networks by encrypting data transmissions and restricting unauthorized access. Although VPN technologies are not new, their importance has increased substantially in the era of remote work and distributed operations.

Cloud computing infrastructure also plays a critical role in organizational cybersecurity. Chauhan and Shiaeles (2023) found that organizations adopting recognized cloud security frameworks, including ISO 27001, NIST, CSA STAR, and AWS Well-Architected Frameworks, were better positioned to manage emerging cyber risks. These frameworks provide structured approaches to access control, incident response, data protection, and continuous monitoring.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

An important insight emerging from the literature is that cybersecurity should not be viewed as a barrier to remote work but rather as an enabler of sustainable digital transformation. Bispham et al. (2021) argued that robust cybersecurity practices allow organizations to maintain flexible work arrangements while preserving operational resilience. This finding challenges earlier assumptions that remote work inherently increases organizational vulnerability and instead suggests that risk outcomes depend largely on the quality of governance and technological safeguards implemented.

In all, the evidence demonstrates that remote work policies and technological infrastructure significantly influence whether cybersecurity threats evolve into successful fraud incidents. Organizations that invest in secure technologies, formal governance structures, and continuous monitoring mechanisms are better equipped to protect digital assets and reduce cyber-enabled fraud risks.

Employee Psychological Factors

The fourth major theme concerns the influence of employee psychological factors on cybersecurity outcomes and fraud vulnerability. Across multiple sectors, including healthcare, hospitality, social work, and information technology, the literature demonstrates that employee well-being is closely associated with organizational security performance.

High levels of stress, burnout, and job dissatisfaction were consistently linked to increased vulnerability to both external cyberattacks and insider-related fraud. Khamisa et al. (2015) found that occupational stress and burnout negatively affect employees' attention, decision-making, and adherence to organizational procedures. These conditions increase the likelihood of security errors, policy violations, and susceptibility to manipulation by cybercriminals.

Similarly, Hayes et al. (2015) reported that burnout among healthcare professionals contributed to reduced performance and increased operational risks. Although the study focused on healthcare settings, its findings have broader implications for cybersecurity management because human error remains one of the most common causes of security breaches.

Research by Wagaman et al. (2015) further demonstrates that psychological resilience and empathy can serve as protective factors against workplace stress and burnout. Employees experiencing higher levels of emotional well-being were more likely to demonstrate vigilance, engagement, and responsible behavior. These findings suggest that employee wellness initiatives may indirectly strengthen organizational cybersecurity defenses.

The relationship between organizational support and employee well-being also emerged as an important factor. Cheng and O-Yang (2018) found that perceived organizational support moderates the effects of job stress and burnout. Employees who feel supported by their organizations exhibit higher levels of engagement and job satisfaction, reducing behaviors associated with negligence and non-compliance.

Longitudinal evidence presented by Upadyaya et al. (2016) indicates that work engagement serves as a buffer against burnout and psychological distress. Employees who are engaged and satisfied with their work are more likely to follow security procedures, participate in cybersecurity initiatives, and contribute positively to organizational resilience.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

The reviewed literature therefore suggests that cybersecurity should not be viewed solely through a technological lens. Human behavior, emotional well-being, and workplace conditions substantially influence organizational security outcomes. Consequently, cybersecurity strategies that integrate employee wellness programs, supportive leadership practices, and psychological resilience initiatives may be more effective than purely technical interventions.

Integrated Discussion and Conceptual Framework

Integrated Discussion

The findings of this systematic literature review reveal that cyber-enabled fraud is a multidimensional phenomenon influenced by the interaction of technological, organizational, regulatory, and human factors. Rather than operating independently, these factors collectively determine organizational vulnerability and resilience.

The reviewed studies consistently demonstrate that strong cybersecurity cultures, effective regulatory frameworks, secure technological infrastructures, and psychologically healthy workforces reinforce one another in reducing fraud risk. Organizations that excel in one dimension but neglect others may remain vulnerable despite substantial investments in cybersecurity technologies.

The findings align with socio-technical systems theory, which argues that organizational outcomes emerge from the interaction of social and technical subsystems. Cybersecurity effectiveness depends not only on technological controls but also on organizational structures, leadership practices, employee behaviors, and regulatory environments. Similarly, the results support institutional theory by demonstrating that regulatory pressures influence organizational security practices and fraud prevention strategies.

The review also highlights the growing convergence of cybersecurity and fraud management. Historically treated as separate domains, contemporary evidence suggests that cyber threats frequently serve as mechanisms through which fraudulent activities occur. Consequently, organizations should adopt integrated risk management approaches that simultaneously address cybersecurity and fraud prevention.

The synthesis further indicates that human factors remain the most significant source of organizational vulnerability. While technological defenses continue to advance, cybercriminals increasingly exploit behavioral weaknesses through phishing, social engineering, and insider manipulation. This reinforces the need for comprehensive security strategies that balance technological investments with human-centered interventions.

Conceptual Framework for Understanding Cyber-Enabled Fraud Risk

Based on the synthesis of the reviewed literature, this study proposes a conceptual framework illustrating the relationship between emerging cybersecurity threats and organizational fraud risk. The framework positions emerging cybersecurity threats as the primary risk drivers and organizational fraud risk as the outcome variable. The relationship between these variables is moderated by four interconnected dimensions: organizational cybersecurity culture, regulatory environment and compliance enforcement, remote work policies and technological infrastructure, and employee psychological factors.

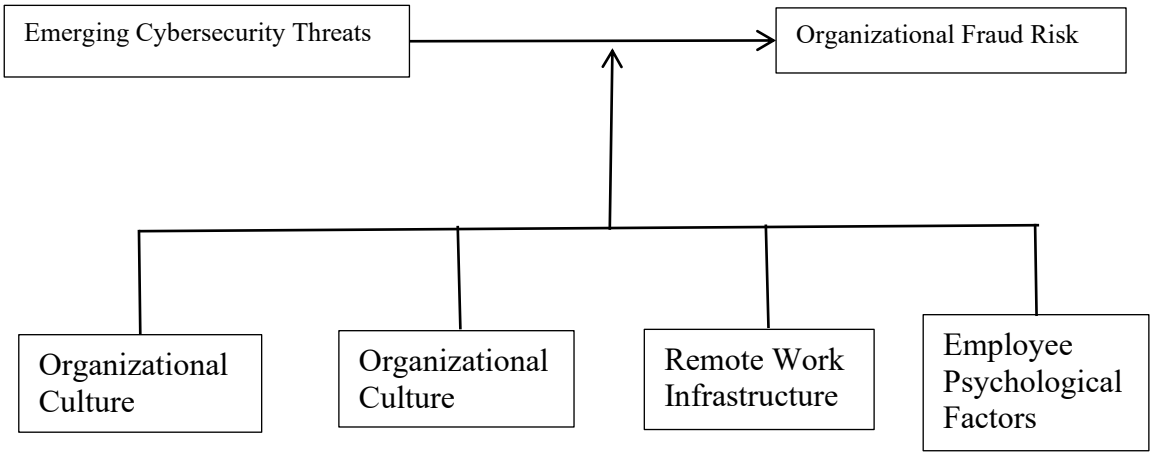
Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

The emerging cybersecurity threats include phishing attacks, social engineering schemes, ransomware attacks, insider threats, credential theft, business email compromise (BEC), cloud-based attacks, AI-enabled cybercrime, and data breaches. Organizational Cybersecurity Culture has the following dimensions: leadership commitment, security awareness training, security policy compliance, employee security behavior, and organizational communication.

The regulatory environment and compliance have the following dimensions: data protection regulations, cybersecurity legislation, industry standards, compliance monitoring, and governance mechanisms. The remote work infrastructure covers the following dimensions: virtual private networks (VPNs), multi-factor authentication, endpoint security, cloud security controls, and remote work policies. The employee psychological factors consist of the following dimensions: work-related stress, burnout, job satisfaction, employee engagement, and organizational support. Organizational fraud risk includes financial fraud, identity theft, data manipulation, insider fraud, information misuse, and operational misconduct.

The framework suggests that stronger moderating factors weaken the relationship between cybersecurity threats and fraud risk, while weaknesses in these dimensions strengthen organizational vulnerability. Figure 2 presents the proposed conceptual framework for emerging cybersecurity threats and organizational fraud risk.

Figure 2: Proposed Conceptual Framework



Theoretical Contributions

This study contributes to the cybersecurity and fraud literature in several important ways. First, it integrates fragmented research streams from cybersecurity, fraud management, organizational behavior, regulatory compliance, and occupational psychology into a unified conceptual framework. This interdisciplinary perspective provides a more comprehensive understanding of organizational vulnerability to cyber-enabled fraud. Second, the review identifies four critical moderating factors—organizational cybersecurity culture, regulatory compliance, remote work infrastructure, and employee psychological well-being—that shape the relationship between emerging cyber threats and fraud outcomes. These findings extend existing theoretical discussions by highlighting the interconnected nature of these factors.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

Third, the study advances the emerging concept of cyber-enabled fraud by demonstrating that fraud prevention and cybersecurity resilience should be examined as complementary rather than independent organizational capabilities. Finally, the review proposes a holistic framework that can guide future empirical research examining the interaction between technological and human dimensions of cybersecurity risk.

Policy Implications

The findings of this systematic literature review have important implications for policymakers, regulators, and governmental institutions responsible for strengthening national and organizational cybersecurity resilience. Governments should develop adaptive cybersecurity regulations capable of responding to rapidly evolving technological environments. Traditional regulatory approaches often lag behind technological innovation, creating gaps that cybercriminals can exploit. Policymakers should establish flexible and technology-neutral regulations that can accommodate emerging threats associated with artificial intelligence, cloud computing, and digital platforms.

Cybercrime is inherently transnational. Cyberattacks frequently cross jurisdictional boundaries, making enforcement difficult when legal frameworks differ significantly across countries. International collaboration through harmonized cybersecurity standards, information-sharing mechanisms, and joint enforcement initiatives is therefore essential. Governments should strengthen cooperation among cybersecurity agencies, law enforcement institutions, financial intelligence units, and international organizations to improve collective cyber resilience.

Small and medium-sized enterprises (SMEs) often face significant cybersecurity challenges due to limited financial and technical resources. Public policy initiatives should provide SMEs with access to affordable cybersecurity training, technical assistance, threat intelligence resources, and compliance support mechanisms. Targeted support programs could significantly reduce vulnerabilities within a sector that frequently lacks dedicated cybersecurity expertise.

Human behavior remains one of the most exploited vulnerabilities in cyber-enabled fraud. Governments should therefore prioritize cybersecurity education initiatives at all levels of society. National awareness campaigns, educational curricula, professional certification programs, and workforce development initiatives can contribute to building a cybersecurity-conscious population capable of recognizing and responding to cyber threats.

The findings suggest that employee stress, burnout, and dissatisfaction contribute indirectly to cybersecurity vulnerabilities. Policymakers and organizational leaders should recognize employee well-being (physical, psychological, and social health of employees) as an important component of cybersecurity resilience. Future cybersecurity policies should incorporate workforce wellness considerations alongside traditional technical and compliance-focused requirements.

Practical Implications

The findings offer several important implications for practitioners, policymakers, and organizational leaders. Organizations should prioritize the development of cybersecurity cultures that promote shared responsibility, continuous learning, and leadership engagement. Security awareness training should move beyond compliance-focused approaches and

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

emphasize behavioral change and resilience. Policymakers should strengthen cybersecurity regulations and encourage greater harmonization of standards across jurisdictions. Consistent regulatory frameworks reduce uncertainty and encourage organizations to adopt proactive security measures.

Investments in remote work infrastructure should remain a strategic priority. Organizations should implement secure authentication mechanisms, endpoint protection systems, cloud security frameworks, and comprehensive remote work policies to address evolving cyber risks. Employee well-being should be integrated into cybersecurity and risk management strategies. Programs addressing stress management, burnout prevention, employee engagement, and psychological resilience can contribute significantly to organizational security outcomes. Finally, organizations should adopt integrated risk management frameworks that address cybersecurity, fraud prevention, governance, and human resource management as interconnected functions rather than isolated activities.

Future Research Directions

Several opportunities for future research emerge from this review. First, longitudinal studies are needed to examine how cybersecurity threats and fraud risks evolve over time as organizations adopt new technologies and work models. Second, future research should develop standardized measures for cybersecurity culture, employee cybersecurity behavior, and cyber-enabled fraud outcomes to improve comparability across studies. Third, more empirical studies are needed in developing economies, where cybersecurity infrastructure, regulatory frameworks, and organizational capabilities may differ significantly from those observed in developed countries. Fourth, future studies should examine the cybersecurity implications of emerging technologies such as artificial intelligence, generative AI, blockchain, quantum computing, and autonomous systems. Fifth, research should investigate the effectiveness of integrated interventions that combine technological safeguards, organizational policies, regulatory compliance mechanisms, and employee wellness initiatives. Finally, comparative cross-sector analyses could provide deeper insights into how industry-specific characteristics influence cybersecurity and fraud risk management practices.

CONCLUSION

This systematic literature review examined the relationship between emerging cybersecurity threats and organizational fraud risk by synthesizing evidence from 32 studies published between 2013 and 2025. The review sought to identify the key factors that influence how cybersecurity threats translate into fraud outcomes and to provide a comprehensive understanding of organizational resilience within increasingly digital and interconnected environments.

The findings reveal that cyber-enabled fraud is a complex and multidimensional phenomenon that cannot be adequately addressed through technological controls alone. Across the reviewed studies, four major moderating factors consistently emerged as influential determinants of organizational vulnerability and resilience: organizational cybersecurity culture, regulatory and compliance environments, remote work policies and technological infrastructure, and employee psychological well-being.

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

Organizations characterized by strong cybersecurity cultures demonstrated greater resistance to cyber threats through enhanced employee awareness, stronger policy compliance, and more effective leadership engagement. Security-conscious organizational environments were associated with lower susceptibility to phishing attacks, social engineering schemes, insider threats, and other forms of cyber-enabled fraud. These findings reinforce the importance of embedding cybersecurity principles into organizational values, practices, and decision-making processes.

The review also highlights the significant role played by regulatory frameworks and compliance mechanisms. Jurisdictions and organizations operating under comprehensive cybersecurity regulations generally exhibited stronger governance structures and more proactive risk management practices. Effective regulatory oversight not only encourages compliance but also promotes accountability, transparency, and continuous improvement in cybersecurity preparedness.

Remote and hybrid work arrangements emerged as another critical consideration. While digital work environments offer substantial operational benefits, they also create new vulnerabilities that can be exploited by cybercriminals. The literature demonstrates that organizations implementing secure remote work infrastructures, including multi-factor authentication, endpoint protection, cloud security controls, and formal governance policies, are better positioned to mitigate cyber risks and prevent fraud.

Furthermore, the review underscores the importance of employee psychological factors. High levels of workplace stress, burnout, and disengagement were consistently associated with increased organizational vulnerability to cyber threats and fraud. Conversely, supportive work environments characterized by employee engagement, organizational support, and psychological well-being contributed positively to cybersecurity resilience. These findings emphasize the need to view cybersecurity as both a technological and human challenge.

Theoretical analysis suggests that organizational cybersecurity outcomes are best understood through integrated socio-technical perspectives that recognize the interaction between technological systems, human behavior, organizational structures, and institutional influences. The review therefore contributes to existing scholarship by providing an interdisciplinary framework that links cybersecurity and fraud research within a unified analytical perspective.

From a practical standpoint, the findings indicate that organizations should adopt comprehensive and integrated cybersecurity strategies that combine technological safeguards with investments in leadership development, employee awareness, regulatory compliance, and workforce well-being. Isolated interventions are unlikely to provide sustainable protection against increasingly sophisticated cyber threats.

Although this review provides important insights, several limitations should be acknowledged. The review was restricted to English-language publications and relied primarily on peer-reviewed literature, which may have excluded relevant studies published in other languages or practitioner-oriented sources. Additionally, variations in study designs, contexts, and measurement approaches limited opportunities for direct comparison across studies.

Future research should focus on longitudinal investigations, cross-sector comparisons, and the development of standardized measurement frameworks capable of improving consistency within cybersecurity and fraud research. Further examination of emerging technologies such

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

as artificial intelligence, blockchain, and quantum computing will also be essential as organizations continue to navigate rapidly evolving digital environments.

In conclusion, the evidence demonstrates that protecting organizations from cyber-enabled fraud requires a holistic and adaptive approach that integrates technological defenses, organizational culture, regulatory compliance, secure digital infrastructures, and employee well-being. As cyber threats continue to evolve in scale and sophistication, organizations that adopt integrated and proactive cybersecurity strategies will be better positioned to safeguard their assets, maintain stakeholder trust, and sustain long-term organizational resilience in the digital economy.

REFERENCES

Aldawood, H., & Skinner, G. (2019). Reviewing cybersecurity social engineering training and awareness programs: Pitfalls and ongoing issues. *Future Internet, 11*(3), 73. https://doi.org/10.3390/fi11030073

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology, 1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Navigating financial compliance in small and medium-sized enterprises (SMEs): Overcoming challenges and implementing effective solutions. *World Journal of Advanced Research and Reviews, 23*(1), Article 1984. https://doi.org/10.30574/wjarr.2024.23.1.1984

Bispham, M., Creese, S., Dutton, W. H., Esteve-González, P., & Goldsmith, M. (2021). Cybersecurity in working from home: An exploratory study. *In TPRC 49: The Research Conference on Communication, Information and Internet Policy.* https://doi.org/10.2139/ssrn.3897380

Carter, A. B. (2019). Considerations for genomic data privacy and security when working in the cloud. *The Journal of Molecular Diagnostics, 21*(4), 542–552. https://doi.org/10.1016/j.jmoldx.2018.07.009

Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems, and proposed solutions. *Network, 3*(3), 422–450. https://doi.org/10.3390/network3030018

Cheng, J.-C., & O-Yang, Y. (2018). Hotel employee job crafting, burnout, and satisfaction: The moderating role of perceived organizational support. *International Journal of Hospitality Management, 72*, 78–85. https://doi.org/10.1016/j.ijhm.2018.01.005

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors, 23*(3), 1151. https://doi.org/10.3390/s23031151

Evangelakos, G. (2020). Keeping critical assets safe when teleworking is the new norm. *Network Security, 2020*(7), 5–8. https://doi.org/10.1016/S1353-4858(20)30067-2

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security, 46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game-based cybersecurity training: Are serious games suitable for cybersecurity training? *International Journal of Serious Games, 3*(1), 53–61. https://doi.org/10.17083/ijsg.v3i1.107

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management, 51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications, 1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

Khamisa, N., Oldenburg, B., Peltzer, K., & Ilic, D. (2015). Work-related stress, burnout, job satisfaction, and general health of nurses. *International Journal of Environmental Research and Public Health, 12*(1), 652–666. https://doi.org/10.3390/ijerph120100652

Moore, T., Han, S., & Clayton, R. (2016). The post-economic downturn: Employee stress and fraud risk. *Journal of Financial Crime, 23*(3), 447–460.

Ogutcu, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83–93. https://doi.org/10.1016/j.cose.2015.10.002

Okereafor, K., Manny, P., & Sabri, M. S. (2020). Understanding cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3627805

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). *The PRISMA 2020 statement: An updated guideline for reporting systematic reviews*. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Shah, M. A., & Nazir, M. (2020). Remote working cyber risks: COVID-19 and beyond. *Computers & Security, 99*, 102076.

Souppaya, M., & Scarfone, K. (2016). *Guide to enterprise telework, remote access, and bring your own device (BYOD) security* (NIST Special Publication 800-46 Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-46r2

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management, 14*(3), 207–222. https://doi.org/10.1111/1467-8551.00375

Upadyaya, K., Vartiainen, M., & Salmela-Aro, K. (2016). From job demands and resources to work engagement, burnout, life satisfaction, depressive symptoms, and occupational health. *Burnout Research, 3*(4), 101–108. https://doi.org/10.1016/j.burn.2016.10.001

Wagaman, M. A., Geiger, J. M., Shockley, C., & Segal, E. A. (2015). The role of empathy in burnout, compassion satisfaction, and secondary traumatic stress among social workers. *Social Work, 60*(3), 201–209. https://doi.org/10.1093/sw/swv014

Walter, Y. (2024). Managing the race to the moon: Global policy and governance in artificial intelligence regulation—A contemporary overview and an analysis of socioeconomic

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH

consequences. *Discover Artificial Intelligence, 4,* Article 14. https://doi.org/10.1007/s44163-024-00109-4

Williamson, S. M., & Prybutok, V. (2024). Balancing privacy and progress: A review of privacy challenges, systemic oversight, and patient perceptions in AI-driven healthcare. *Applied Sciences, 14*(2), 675. https://doi.org/10.3390/app14020675

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, data privacy, and blockchain: A review. *SN Computer Science, 3,* Article 127. https://doi.org/10.1007/s42979-022-01020-4

Younglove, R. (2000). Virtual private networks: How they work. *Computing & Control Engineering Journal, 11*(6), 260–262. https://doi.org/10.1049/cce:20000602

Zaid, T., & Garai, S. (2024). Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers. *Blockchain in Healthcare Today, 7,* Article 302. https://doi.org/10.30953/bhty.v7.302

Article DOI: 10.52589/AJAFR-3N2DOPIH
DOI URL: https://doi.org/10.52589/AJAFR-3N2DOPIH