International Journal of Multidisciplinary Research and Growth Evaluation.

Human Factors in Fintech Cybersecurity: Addressing Insider Threats and Behavioral Risks

Noah Ayanbode [1], Olumese Anthony Abieba [2], Naomi Chukwurah [3], Olanrewaju Oluwaseun Ajayi [4], Andrew Ifesinachi Daraojimba [5*]

[1] Independent Researcher, Lagos State, Nigeria
[2] Independent Researcher, USA
[3] Independent Researcher, USA
[4] University of the Cumberlands, USA
[5] Signal Alliance Technology Holding, Nigeria

* Corresponding Author: **Andrew Ifesinachi Daraojimba**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 01
January-February 2024
Received: 14-12-2023
Accepted: 10-01-2024
Page No: 1350-1356

Abstract
In the rapidly evolving landscape of financial technology (Fintech), cybersecurity stands as a paramount concern. While technological advancements fortify digital infrastructure, the human element remains critical in mitigating risks. This abstract delves into the intricate interplay of human factors within Fintech cybersecurity, particularly focusing on the challenges posed by insider threats and behavioral risks. Insider threats from within an organization present a formidable challenge in Fintech cybersecurity. These threats can manifest through intentional actions, such as data theft or sabotage, or unintentional negligence, such as falling victim to social engineering tactics. Understanding insiders' motivations and behavioral patterns is crucial in developing effective preventive measures and detection mechanisms. Behavioral risks encompass a wide spectrum of human behaviors that can compromise cybersecurity, including susceptibility to phishing attacks, improper handling of sensitive information, and circumventing security protocols for convenience. Addressing these risks requires a multifaceted approach, incorporating elements of education, training, and technological safeguards. This abstract from psychological and behavioral science frameworks underscores the importance of cultivating a security-centric organizational culture. Promoting awareness, fostering a sense of accountability, and providing continuous training can empower individuals to become proactive defenders against cyber threats. Furthermore, leveraging technological innovations such as artificial intelligence and machine learning holds promise in detecting anomalous behaviors and preempting potential breaches. However, these solutions must be complemented with human oversight to discern nuanced contextual cues that automated systems may overlook. Effective Fintech cybersecurity necessitates a holistic approach that acknowledges and addresses the complexities of human factors. By integrating behavioral insights with technological solutions, organizations can fortify their defenses against insider threats and mitigate the inherent risks posed by human behavior in the digital realm.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.1.1350-1356

Keywords: Human Factor; Fintech; Cybersecurity; Behavioural; Risks; Insider Threats; Review

1. Introduction

In today's digital age, the convergence of finance and technology, commonly referred to as Fintech, has fundamentally transformed the way financial services are delivered and consumed. Digital platforms have become the backbone of modern financial transactions, offering consumers and businesses unprecedented convenience, accessibility, and efficiency (George, 2024). The proliferation of online banking, digital wallets, cryptocurrency transactions, and algorithm-driven investment platforms has redefined traditional financial ecosystems. However, as Fintech continues to evolve, so too do the risks associated with cybersecurity. The need to protect sensitive financial data, prevent fraudulent activities, and ensure the integrity of digital transactions has never been more critical. Both financial institutions and consumers depend on robust security measures to

safeguard their financial assets and maintain trust in Fintech platforms (Pal, 2022).

While significant advancements have been made in cybersecurity technologies—including encryption, multi-factor authentication, and artificial intelligence-driven fraud detection—one often overlooked yet equally crucial element in Fintech security is the human factor (Arcot, Sayed, Parekh, Balasubramanian, & Sudheer, 2024). Cybersecurity is not solely a technological issue; it is also deeply influenced by human behavior, decision-making, and awareness. Even the most sophisticated security systems can be rendered ineffective if human users, whether employees within financial institutions or individual consumers, inadvertently compromise security. This vulnerability makes it imperative to explore the role of human factors in Fintech cybersecurity, particularly in relation to insider threats and behavioral risks (Pollini *et al*, 2022).

Human behavior can impact cybersecurity in numerous ways, both intentional and unintentional. On one hand, external threats such as phishing scams, social engineering attacks, and malware infections often rely on human error to bypass security defenses (Corman, 2023). Cybercriminals exploit psychological tendencies, such as trust, urgency, and curiosity, to manipulate individuals into divulging sensitive information or clicking on malicious links. Many security breaches occur because individuals fail to recognize these deceptive tactics, underscoring the importance of cybersecurity awareness and education. Even in organizations with strict security policies, employees may unknowingly compromise systems by using weak passwords, reusing credentials across multiple accounts, or failing to follow established protocols (Siddiqi, Pak, & Siddiqi, 2022).

On the other hand, insider threats represent an even more complex challenge in Fintech cybersecurity. Unlike external attacks, insider threats originate from within an organization, involving employees, contractors, or business partners who have authorized access to sensitive systems and data. Insider threats can take various forms, including intentional malicious actions such as data theft, financial fraud, sabotage, and unintentional errors that expose vulnerabilities (Kaur *et al*, 2021). In some cases, disgruntled employees or individuals with financial motives deliberately exploit their access privileges to compromise systems for personal gain. In other instances, well-meaning employees may inadvertently expose critical data due to negligence or a lack of awareness. These insider risks highlight the necessity of implementing behavioral analytics, continuous monitoring, and strict access controls to detect and prevent potential security breaches (Despotović, Parmaković, & Miljković, 2023).

Fintech organizations must adopt a holistic approach that combines technological solutions with human-centric strategies to mitigate the cybersecurity risks posed by human factors. Employee training and cybersecurity awareness programs play a vital role in strengthening security resilience. By educating employees about the latest threats, social engineering tactics, and best security practices, organizations can significantly reduce the likelihood of human errors leading to breaches. Additionally, fostering a culture of cybersecurity accountability within organizations can encourage employees to be more vigilant and proactive in identifying potential threats.

Beyond awareness and training, the implementation of advanced technologies can enhance security by mitigating human-related risks. Behavioral analytics powered by artificial intelligence can help detect anomalies in user behavior, identifying suspicious activities that may indicate insider threats or compromised accounts. Role-based access controls and zero-trust security models can minimize the risk of unauthorized access, ensuring that employees only have access to the data and systems necessary for their roles. Continuous monitoring and real-time threat detection mechanisms can further strengthen Fintech cybersecurity by swiftly identifying and responding to potential security incidents.

Cybersecurity in Fintech cannot be addressed solely through technological advancements. The human element remains a critical factor in ensuring the security and integrity of financial systems. By acknowledging the role of human behavior in cybersecurity and implementing targeted strategies to address insider threats and behavioral risks, Fintech organizations can bolster their defenses against evolving cyber threats. A well-rounded security approach that integrates technological innovations with human-focused interventions is essential to maintaining consumer trust, regulatory compliance, and the long-term stability of digital financial ecosystems.

2. Insider threats in fintech cybersecurity

In the field of cybersecurity, insider threats pose a significant and often underappreciated risk, particularly within the fast-evolving sector of financial technology (Fintech). These threats are uniquely challenging due to the trust placed in individuals who have privileged access to critical systems and sensitive data. Insider threats refer to security risks that arise from individuals within an organization, such as employees, contractors, or partners, who misuse their authorized access for malicious purposes or unintentionally compromise security through negligent actions (Onyebuchi, Onyedikachi, & Emuobosa, 2024c).

Insider threats can be classified into several categories based on the intent and actions of the perpetrators. Malicious insiders intentionally exploit their access to steal sensitive data, commit fraud, sabotage systems, or engage in other illicit activities for personal gain or revenge. On the other hand, while not malicious in intent, negligent insiders still present a significant security risk due to careless or uninformed actions. These can include falling victim to phishing scams, mishandling confidential information, or bypassing security protocols for convenience. In some cases, insiders may even unwittingly assist external threat actors by unknowingly exposing vulnerabilities or being coerced into supporting malicious activities (Uchendu, Omomo, & Esiri, 2024; Umoh, Nwasike, Tula, Ezeigweneme, & Gidiagba, 2024).

Understanding the motivations behind insider threats is crucial for mitigating their risks. One of the most common driving forces is financial gain. Insiders may be motivated to steal financial data, manipulate accounts, or engage in unauthorized transactions to enrich themselves. Disgruntled employees, meanwhile, may resort to malicious actions as a form of retaliation against their employer or colleagues (Ekeh, Apeh, Odionu, & Austin-Gabriel). These acts of vengeance may include sabotaging systems, leaking confidential information, or disrupting operations. Another key motivator for insider threats is espionage or the desire to gain a competitive edge, often by stealing intellectual property, trade secrets, or proprietary information. Some insiders may also act on ideological or political motives to disrupt financial systems or undermine institutions aligned with opposing views (Apeh, Odionu, & Austin-Gabriel).

Numerous high-profile case studies underscore the real-world consequences of insider threats in Fintech cybersecurity. For example, a former employee at a major

financial institution exploited their privileged access to siphon off millions of dollars from customer accounts, highlighting the devastating impact of insider malfeasance. Additionally, the Equifax data breach, which compromised the personal information of millions, was partially attributed to the actions of an insider who failed to patch a known vulnerability despite awareness of the risks involved (Nwaozomudoh *et al*).

Mitigating insider threats requires more than just technological defenses; it demands a deep understanding of human behavior and psychology. Cognitive biases, emotional triggers, and social engineering tactics can all play a pivotal role in shaping an insider's actions, making it essential for organizations to incorporate psychological insights into their cybersecurity strategies. By utilizing knowledge from behavioral science, companies can design more effective training programs, strengthen access control systems, and foster a culture of security awareness that encourages employees to recognize and report suspicious behavior (Nzeako, 2020; Ogunyemi & Ishola).

3. Behavioral risks in fintech cybersecurity

In the constantly evolving landscape of Fintech cybersecurity, behavioral risks represent a significant and often overlooked threat. This section explores the definition and examples of behavioral risks, common vulnerabilities in Fintech, the impact of human behavior on cybersecurity breaches, and the role of social engineering in exploiting behavioral weaknesses (Adewoyin, 2022). Behavioral risks in Fintech cybersecurity encompass a wide range of human actions that can compromise the security of financial systems and data. These risks include phishing attacks involving deceptive emails, messages, or websites designed to trick individuals into revealing sensitive information such as passwords, account numbers, or personal details. Phishing exploits human trust and curiosity, often leading unsuspecting users to click on malicious links or download malware (Adewoyin, 2021; Odio *et al*, 2021).

Social engineering, another significant threat, exploits psychological manipulation to deceive individuals into divulging confidential information, performing unauthorized actions, or compromising security protocols. Common social engineering tactics include pretexting, baiting, and impersonation, which rely on human gullibility and susceptibility to persuasion (Akpukorji *et al*, 2024). Although insider threats were discussed separately, they also fall under the category of behavioral risks, as insiders with privileged access may intentionally or inadvertently compromise security through malicious actions or negligent behavior. Human error is another critical source of behavioral risk in Fintech cybersecurity. Careless or uninformed actions such as using weak passwords, sharing credentials, or failing to update software can expose systems to exploitation by cyber attackers (Abiola, Okeke, & Ajani, 2024; Adegbite *et al*, 2023).

Several common behavioral vulnerabilities make individuals and organizations in the Fintech sector particularly susceptible to cyber threats. A lack of awareness regarding cybersecurity best practices is a key vulnerability, making individuals more susceptible to phishing scams, social engineering attacks, and other forms of cybercrime (Apeh, Odionu, Bristol-Alagbariya, Okon, & Austin-Gabriel, 2024b). Overconfidence in one's ability to detect and respond to cyber threats can also lead individuals to underestimate the risks and fall victim to sophisticated attacks. In the fast-paced world of Fintech, convenience often takes precedence over security. Users may prioritize speed and efficiency over robust security measures, making compromises that leave them vulnerable to exploitation. Furthermore, excessive trust in technology can lead individuals to overlook potential risks and vulnerabilities, assuming that automated systems will protect them from harm (Apeh, Odionu, Bristol-Alagbariya, Okon, & Austin-Gabriel, 2024a; Biu, Nwasike, Nwaobia, Ezeigweneme, & Gidiagba, 2024).

Human behavior plays a significant role in determining the success or failure of cybersecurity measures and has a profound impact on the likelihood and severity of cyber breaches. Poor password hygiene, such as using easily guessable passwords or reusing the same password across multiple accounts, makes it easier for attackers to gain unauthorized access to systems and data. Neglecting to apply security patches and updates leaves systems vulnerable to known vulnerabilities that cyber attackers can exploit (Daramola, Apeh, Basiru, Onukwulu, & Paul, 2024). Phishing attacks rely on human gullibility and susceptibility to deception. Failure to recognize and respond to phishing emails can lead to the unauthorized disclosure of sensitive information or the installation of malware. Social engineering exploits human psychology and emotions to manipulate individuals into divulging confidential information or performing unauthorized actions. By exploiting trust, fear, or urgency, attackers can bypass technical controls and gain access to sensitive systems and data (Apeh, Odionu, Bristol-Alagbariya, Okon, & Austin-Gabriel, 2024c; Biu, Nwasike, Tula, Ezeigweneme, & Gidiagba, 2024).

Social engineering plays a pivotal role in exploiting behavioral weaknesses and circumventing traditional cybersecurity defenses. By leveraging psychological manipulation and deception, attackers can trick individuals into divulging sensitive information, performing unauthorized actions, or compromising security protocols. Common social engineering tactics include phishing attacks, which typically involve deceptive emails, messages, or websites that trick individuals into revealing sensitive information such as passwords or personal details (Ezeigweneme, Nwasike, Adekoya, Biu, & Gidiagba, 2024; Ishola, Odunaiya, & Soyombo, 2024). These phishing emails often mimic legitimate communications from trusted sources, making them difficult to detect. Pretexting involves creating a false scenario to elicit information from individuals. This may involve impersonating a trusted authority figure, such as a bank representative or IT technician, and using persuasion or manipulation to extract sensitive information. Baiting attacks entice individuals with the promise of a reward or incentive, such as a free download or discount offer, luring them into clicking on malicious links or downloading malware. Baiting exploits human curiosity and the desire for instant gratification, leading unsuspecting users to compromise their security in exchange for a perceived benefit. Impersonation attacks involve deceiving victims by pretending to be trusted individuals or organizations. This may include spoofing email addresses or phone numbers to mimic legitimate communications, making it difficult for victims to distinguish between genuine and fraudulent messages (Ezeigweneme, Daraojimba, Tula, Adegbite, & Gidiagba, 2024; Kokogho, Odio, Ogunsola, & Nwaozomudoh, 2024a).

4. Addressing insider threats

Insider threats pose a significant risk to Fintech cybersecurity, requiring organizations to adopt proactive measures to mitigate these risks effectively. This section explores various strategies for addressing insider threats, including implementing access controls and least privilege

principles, monitoring and auditing employee activities, conducting regular employee training and awareness programs, and establishing a culture of transparency and accountability.

One of the most effective ways to mitigate insider threats is by implementing robust access controls and adhering to the principle of least privilege. This involves restricting access to sensitive systems, data, and resources only to those individuals who need it to perform their job functions. By limiting employee privileges, organizations can minimize the potential damage caused by insider threats and prevent unauthorized access to critical assets (Kokogho, Odio, Ogunsola, & Nwaozomudoh, 2024b). Access controls should be tailored to each individual's specific needs and responsibilities, ensuring that employees only have access to the information and resources necessary for their job duties. This can be achieved through the use of role-based access controls (RBAC), which assign permissions based on predefined roles and responsibilities within the organization. Additionally, organizations should regularly review and audit user access rights to identify and address any unnecessary or excessive privileges. This helps ensure that employees only have access to the information and resources required to perform their job functions, reducing the risk of insider threats (Kokogho, Odio, Ogunsola, & Nwaozomudoh, 2024c; Lottu, Ezeigweneme, Olorunsogo, & Adegbola, 2024).

Monitoring and auditing employee activities are essential components of an effective insider threat detection and prevention strategy. By closely monitoring user behavior and activities, organizations can identify suspicious or anomalous behavior indicative of insider threats and take appropriate action to mitigate the risk. This can involve implementing user activity monitoring tools and technologies that track and log employee actions across various systems, applications, and networks. These tools can provide valuable insights into user behavior, including login attempts, file accesses, system changes, and data transfers, allowing organizations to identify and investigate potential insider threats in real-time. In addition to monitoring employee activities, organizations should conduct regular audits and reviews of system logs, access controls, and user permissions to identify discrepancies or unauthorized activities. This helps ensure that employees are adhering to established security policies and procedures and provides an opportunity to identify and address any potential insider threats before they escalate (Odionu, Bristol-Alagbariya, & Okon, 2024; Ogunyemi & Ishola, 2024).

Employee training and awareness are critical components of any insider threat prevention strategy. By educating employees about the risks and consequences of insider threats, organizations can empower them to recognize and report suspicious behavior, adhere to security best practices, and effectively mitigate the risk of insider threats. Training programs should cover a range of topics, including the types and motivations of insider threats, common behavioral indicators of insider threats, and best practices for protecting sensitive information and systems. Employees should also receive training on identifying and responding to phishing attacks, social engineering tactics, and other common forms of cyber threats (Okedele, Aziza, Oduro, & Ishola, 2024a, 2024b).

In addition to formal training sessions, organizations should promote a culture of security awareness by regularly communicating security policies and procedures, providing updates on emerging threats and vulnerabilities, and encouraging employees to remain vigilant and proactive in their efforts to protect sensitive information and systems.

Finally, establishing a culture of transparency and accountability is essential for effectively addressing insider threats. By fostering an environment where employees feel comfortable reporting suspicious behavior and raising security concerns, organizations can create a strong line of defense against insider threats and ensure that potential risks are identified and addressed promptly. This can involve implementing anonymous reporting mechanisms, such as hotlines or online reporting portals, where employees can report insider threats or security incidents without fear of retaliation (Okedele, Aziza, Oduro, & Ishola, 2024d). Organizations should also establish clear communication channels for reporting security concerns to management, IT security teams, or other relevant stakeholders, ensuring that potential threats are investigated and addressed promptly. Additionally, organizations should hold employees accountable for their actions and adherence to security policies and procedures. This can involve implementing consequences for violating security policies, such as disciplinary action or termination of employment, to deter malicious behavior and reinforce the importance of security awareness and compliance (Okedele, Aziza, Oduro, & Ishola, 2024c; Onyebuchi, Onyedikachi, & Emuobosa, 2024b).

5. Addressing behavioral risks

Behavioral risks present significant challenges in Fintech cybersecurity, but they can be effectively addressed through a combination of technological solutions and human interventions. This section explores strategies for addressing behavioral risks, including providing employee cybersecurity awareness training, implementing multi-factor authentication and encryption, developing user-friendly security policies and procedures, and leveraging behavioral analytics and AI for threat detection.

One of the most critical steps in addressing behavioral risks is providing employees comprehensive cybersecurity awareness training. This training should cover a wide range of topics, including recognizing phishing emails and other social engineering tactics, using strong passwords and implementing good password hygiene, identifying and reporting suspicious behavior or security incidents, understanding the importance of data protection and privacy, and adhering to security policies and procedures. By educating employees about the risks and best practices for cybersecurity, organizations can empower them to recognize and mitigate potential threats effectively.

Multi-factor authentication (MFA) and encryption are essential tools for mitigating behavioral risks in Fintech cybersecurity. MFA adds an extra layer of security by requiring users to provide multiple forms of identification, such as a password and a one-time code sent to their mobile device, before accessing sensitive systems or data. This helps prevent unauthorized access, even if an attacker has obtained a user's password through phishing or other means. Encryption, on the other hand, protects data by encoding it in such a way that only authorized parties can access it. By encrypting sensitive information both in transit and at rest, organizations can ensure that even if data is intercepted or compromised, it remains unintelligible to unauthorized parties (Okedele, Aziza, Oduro, Ishola, *et al*, 2024; Okon, Odionu, & Bristol-Alagbariya, 2024).

Implementing MFA and encryption strengthens the security posture of Fintech systems and reduces the risk of data breaches resulting from human error or malicious activity. User-friendly security policies and procedures are also essential for encouraging compliance and reducing the likelihood of human error or negligence. Complex or overly

restrictive security measures can lead to frustration and resistance among employees, increasing the risk of non-compliance or circumvention of security protocols. To address this challenge, organizations should develop clear, concise, and easy-to-understand security policies and procedures (Okedele, Aziza, Oduro, Ishola, *et al*, 2024; Okon *et al*, 2024). Policies should be tailored to employees' specific needs and responsibilities, providing practical guidance on how to adhere to security best practices without impeding productivity or efficiency. Additionally, organizations should provide ongoing training and support to ensure that employees understand and comply with security policies and procedures. By fostering a security awareness and compliance culture, organizations can reduce the likelihood of behavioral risks and strengthen their overall security posture (Onyebuchi, Onyedikachi, & Emuobosa, 2024a).

Behavioral analytics and artificial intelligence (AI) can play a crucial role in identifying and mitigating behavioral risks in Fintech cybersecurity. These technologies analyze user behavior and network activity to identify anomalies and potential security threats, enabling organizations to detect and respond to threats in real-time. Behavioral analytics uses machine learning algorithms to identify patterns and deviations from normal behavior, allowing organizations to detect suspicious activities such as unauthorized access attempts, data exfiltration, or insider threats. Similarly, AI-driven threat detection systems can analyze vast amounts of data to identify emerging threats and vulnerabilities, enabling organizations to mitigate risks before they escalate proactively. By leveraging behavioral analytics and AI for threat detection, organizations can augment their existing security measures and better protect against behavioral risks in Fintech cybersecurity (Onyebuchi *et al*, 2024b, 2024c).

6. Integration of technological solutions and human oversight in fintech cybersecurity

The integration of technological solutions and human oversight is essential for effectively addressing behavioral risks and strengthening Fintech cybersecurity. This approach combines the strengths of both automated systems and human intervention, ensuring that organizations can detect, prevent, and respond to security threats in a comprehensive and adaptive manner. While technological solutions such as multi-factor authentication, encryption, and behavioral analytics offer significant benefits, they also have limitations that must be addressed through effective human oversight.

Technological solutions provide organizations with critical tools for managing behavioral risks. Multi-factor authentication (MFA) adds an extra layer of security by requiring multiple forms of identification to access sensitive systems or data. Encryption ensures that even if data is intercepted or compromised, it remains unreadable to unauthorized parties. Behavioral analytics and AI-driven threat detection systems use machine learning to identify anomalies in user behavior, allowing organizations to detect suspicious activities such as unauthorized access attempts or insider threats in real-time. These solutions enable organizations to respond swiftly to emerging threats but are not without challenges. False positives generated by behavioral analytics can lead to unnecessary alerts or disruptions, and the management of these technologies can be resource-intensive, requiring specialized expertise. Additionally, the rapidly evolving tactics of cyber attackers present a constant challenge for technological solutions to keep up.

While technological solutions play a crucial role in mitigating behavioral risks, human oversight is indispensable for interpreting the behavioral cues detected by automated systems. Human analysts bring valuable context and insight, distinguishing between legitimate user behavior and suspicious or malicious activity. This interpretation helps reduce the risk of false positives and prevents unnecessary disruptions to operations. Human involvement is also vital for adapting to new and emerging threats that may not yet be accounted for by automated systems. Analysts can make informed decisions based on a broader understanding of the organizational context and the evolving threat landscape.

Organizations must adopt a holistic approach to integrate technological solutions and human oversight effectively. This approach should combine automated systems for real-time threat detection and response with human analysts for decision-making and interpretation. Continuous training and support for analysts are necessary to ensure they have the expertise to interpret behavioral cues effectively and respond to security threats appropriately. Establishing clear communication channels and workflows between automated systems and human analysts enables seamless coordination, enhancing the organization's ability to respond quickly and efficiently to potential threats. Regularly evaluating the effectiveness of both technological solutions and human intervention ensures that the strategies remain agile and adaptable to the evolving cybersecurity landscape.

The future of Fintech cybersecurity will likely see increasing reliance on AI and machine learning technologies, enabling more sophisticated threat detection and response. However, as new technologies like quantum computing emerge, they bring both opportunities and challenges. While quantum computing holds the potential to revolutionize encryption and data security, it also introduces new vulnerabilities that organizations must address. As Fintech continues to disrupt traditional financial services, regulators will likely place greater emphasis on cybersecurity practices and data protection measures. Organizations will need to stay ahead of regulatory changes and compliance standards to maintain a robust cybersecurity posture.

In response to the rise of remote work and cloud-based services, organizations are increasingly adopting zero-trust architecture, which requires continuous authentication and authorization, bolstering security in an increasingly decentralized and interconnected digital environment. As insider threats remain a significant concern, organizations are investing in behavioral analytics and insider threat detection to identify and mitigate internal security risks. In this dynamic environment, the integration of technological solutions with human oversight will be crucial for Fintech organizations to remain agile, proactive, and resilient against the evolving cybersecurity threat landscape.

7. Recommendations and conclusion

Throughout this discussion, we have explored the critical role that human factors play in Fintech cybersecurity, particularly in addressing insider threats, behavioral risks, and the strategies required to mitigate these challenges. It has been emphasized that understanding human behavior, implementing effective technological solutions, and fostering a culture of security awareness are essential components in defending against cyber threats. Human factors are central to the success of cybersecurity practices in the Fintech sector, influencing how well technological solutions are adopted and how security policies are implemented across the organization.

Organizations must recognize and address the complexities of human behavior to mitigate insider threats and behavioral risks. By doing so, they can enhance the effectiveness of their

cybersecurity measures, ensuring stronger defenses against data breaches, unauthorized access, and other security incidents. Building a proactive and security-conscious workforce, supported by robust technological systems, can significantly reduce the likelihood of cybersecurity breaches caused by human error or malicious intent.

Looking ahead, several areas of Fintech cybersecurity warrant further research and development. There is a growing need for more sophisticated behavioral analytics and AI-driven systems to identify emerging risks and improve response times. These technologies can help pinpoint anomalous behavior more accurately, enabling faster detection and mitigation of potential threats.

While automated systems are invaluable for threat detection, human oversight remains essential for interpreting complex situations. Future developments should focus on refining the integration of automated systems with human intervention, ensuring that both elements work seamlessly together to enhance cybersecurity response strategies.

The rise of quantum computing and blockchain presents both opportunities and challenges for Fintech cybersecurity. The implications of these technologies on encryption, data protection, and security strategies need to be carefully examined to safeguard against new vulnerabilities that may arise. The Fintech sector faces an ever-changing regulatory environment, with increased scrutiny on cybersecurity practices and data protection. Organizations must stay informed about new compliance requirements to ensure that they align their security strategies with the latest regulatory expectations.

8. References

1. Abiola OA, Okeke IC, Ajani O. The role of tax policies in shaping the digital economy: Addressing challenges and harnessing opportunities for sustainable growth. International Journal of Advanced Economics. 2024; P-ISSN: 2707-2134.
2. Adegbite AO, Nwasike CN, Nwaobia NK, Gidiagba JO, Enabor OT, Dawodu SO, *et al* Mechatronics in modern industrial applications: Delving into the integration of electronics, mechanics, and informatics. World Journal of Advanced Research and Reviews. 2023;20(3).
3. Adewoyin MA. Developing frameworks for managing low-carbon energy transitions: Overcoming barriers to implementation in the oil and gas industry. [Unpublished manuscript]. 2021.
4. Adewoyin MA. Advances in risk-based inspection technologies: Mitigating asset integrity challenges in aging oil and gas infrastructure. [Unpublished manuscript]. 2022.
5. Akpukorji IS, Nzeako G, Akinsanya MO, Popoola OA, Chukwurah EG, Okeke CD. Theoretical frameworks for regulatory compliance in fintech innovation: A comparative analysis of Africa and the United States. Finance and Accounting Research Journal. 2024;6(5):721-730.
6. Apeh CE, Odionu CS, Austin-Gabriel B. Transforming healthcare outcomes with predictive analytics: A comprehensive review of models for patient management and system optimization. [Unpublished manuscript].
7. Apeh CE, Odionu CS, Bristol-Alagbariya B, Okon R, Austin-Gabriel B. Advancing workforce analytics and big data for decision-making: Insights from HR and pharmaceutical supply chain management. International Journal of Multidisciplinary Research Growth and Evaluation. 2024a;5(1):1217-1222.
8. Apeh CE, Odionu CS, Bristol-Alagbariya B, Okon R, Austin-Gabriel B. Ethical considerations in IT systems design: A review of principles and best practices. [Unpublished manuscript]. 2024b.
9. Apeh CE, Odionu CS, Bristol-Alagbariya B, Okon R, Austin-Gabriel B. Reviewing healthcare supply chain management: Strategies for enhancing efficiency and resilience. International Journal of Research in Science and Innovation. 2024c;5(1):1209-1216.
10. Arcot PP, Sayed G, Parekh B, Balasubramanian J, Sudheer V. The interplay of ethics, culture, and society in the age of finance digital transformation. Journal of Southwest Jiaotong University. 2024;59(2):139-163.
11. Biu PW, Nwasike CN, Nwaobia NK, Ezeigweneme CA, Gidiagba JO. GIS in healthcare facility planning and management: A review. World Journal of Advanced Research and Reviews. 2024;21(1):012-019.
12. Biu PW, Nwasike CN, Tula OA, Ezeigweneme CA, Gidiagba JO. A review of GIS applications in public health surveillance. World Journal of Advanced Research and Reviews. 2024;21(1):030-039.
13. Corman A. The human element in cybersecurity: Bridging the gap between technology and human behaviour. [Unpublished manuscript]. 2023.
14. Daramola OM, Apeh CE, Basiru JO, Onukwulu EC, Paul PO. Environmental law and corporate social responsibility: Assessing the impact of legal frameworks on circular economy practices. [Unpublished manuscript]. 2024.
15. Despotović A, Parmaković A, Miljković M. Cybercrime and cybersecurity in fintech. In: Digital transformation of the financial industry: Approaches and applications. Springer. 2023;255-272.
16. Ekeh AH, Apeh CE, Odionu CS, Austin-Gabriel B. Advanced data warehousing and predictive analytics for economic insights: A holistic framework for stock market trends and GDP analysis. [Unpublished manuscript].
17. Ezeigweneme CA, Daraojimba C, Tula OA, Adegbite AO, Gidiagba JO. A review of technological innovations and environmental impact mitigation. World Journal of Advanced Research and Reviews. 2024;21(1):075-082.
18. Ezeigweneme CA, Nwasike CN, Adekoya OO, Biu PW, Gidiagba JO. Wireless communication in electro-mechanical systems: Investigating the rise and implications of cordless interfaces for system enhancement. Engineering and Science Technology Journal. 2024;5:21-42.
19. George AS. Finance 4.0: The transformation of financial services in the digital age. Partners Universal Innovative Research Publication. 2024;2(3):104-125.
20. Ishola AO, Odunaiya OG, Soyombo OT. Framework for tailoring consumer-centric communication to boost solar energy adoption in US households. [Journal Name Pending]. 2024.
21. Kaur G, Habibi Lashkari Z, Habibi Lashkari A, Kaur G, Habibi Lashkari Z, Habibi Lashkari A. Cybersecurity threats in FinTech. Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends. 2021;65-87.
22. Kokogho E, Odio PE, Ogunsola OY, Nwaozomudoh MO. AI-powered economic forecasting: Challenges and opportunities in a data-driven world. [Unpublished manuscript]. 2024a.
23. Kokogho E, Odio PE, Ogunsola OY, Nwaozomudoh MO. Conceptual analysis of strategic historical perspectives: Informing better decision-making and

planning for SMEs. [Unpublished manuscript]. 2024b.
24. Kokogho E, Odio PE, Ogunsola OY, Nwaozomudoh MO. Transforming public sector accountability: The critical role of integrated financial and inventory management systems in ensuring transparency and efficiency. [Unpublished manuscript]. 2024c.
25. Lottu OA, Ezeigweneme CA, Olorunsogo T, Adegbola A. Telecom data analytics: Informed decision-making: A review across Africa and the USA. World Journal of Advanced Research and Reviews. 2024;21(1):1272-1287.
26. Nwaozomudoh MO, Odio PE, Kokogho E, Olorunfemi TA, Adeniji IE, Sobowale A. Developing a conceptual framework for enhancing interbank currency operation accuracy in Nigeria's banking sector. [Unpublished manuscript].
27. Nzeako G. Framework to address the digital disability divide in Finland. [Unpublished manuscript]. 2020.
28. Odio PE, Kokogho E, Olorunfemi TA, Nwaozomudoh MO, Adeniji IE, Sobowale A. Innovative financial solutions: A conceptual framework for expanding SME portfolios in Nigeria's banking sector. International Journal of Multidisciplinary Research and Growth Evaluation. 2021;2(1):495-507.
29. Odionu CS, Bristol-Alagbariya B, Okon R. Big data analytics for customer relationship management: Enhancing engagement and retention strategies. International Journal of Scholarly Research in Science and Technology. 2024;5(2):050-067.
30. Ogunyemi FM, Ishola AO. Supporting the green energy transition in US SMEs: A sustainable finance and consulting approach. [Unpublished manuscript].
31. Ogunyemi FM, Ishola AO. Global competitiveness and environmental sustainability: Financing and business development strategies for US SMEs. International Journal of Management and Entrepreneurship Research. 2024;6(11).
32. Okedele PO, Aziza OR, Oduro P, Ishola AO. Assessing the impact of international environmental agreements on national policies: A comparative analysis across regions. [Unpublished manuscript]. 2024a.
33. Okedele PO, Aziza OR, Oduro P, Ishola AO. Carbon pricing mechanisms and their global efficacy in reducing emissions: Lessons from leading economies. [Unpublished manuscript]. 2024b.
34. Okedele PO, Aziza OR, Oduro P, Ishola AO. Climate change litigation as a tool for global environmental policy reform: A comparative study of international case law. Global Environmental Policy Review. 2024c.
35. Okedele PO, Aziza OR, Oduro P, Ishola AO. Integrating indigenous knowledge systems into global climate adaptation policies. International Journal of Engineering Research and Development. 2024;20(12):223-231.
36. Okedele PO, Aziza OR, Oduro P, Ishola AO, Center EL, Center PMHL. Global legal frameworks for an equitable energy transition: Balancing growth and justice in developing economies. International Journal of Applied Research in Social Sciences. 2024;6(12):2878-2891.
37. Okon R, Odionu CS, Bristol-Alagbariya B. Integrating technological tools in HR mental health initiatives. IRE Journals. 2024;8(6):554.
38. Onyebuchi U, Onyedikachi O, Emuobosa E. The concept of big data and predictive analytics in reservoir engineering: The future of dynamic reservoir models. Computer Science & IT Research Journal. 2024a;5(11):2562-2579.
39. Onyebuchi U, Onyedikachi O, Emuobosa E. Strengthening workforce stability by mediating labor disputes successfully. International Journal of Engineering Research and Development. 2024b;20(11):98-1010.
40. Onyebuchi U, Onyedikachi O, Emuobosa E. Theoretical insights into uncertainty quantification in reservoir models: A Bayesian and stochastic approach. International Journal of Engineering Research and Development. 2024c;20(11):987-997.
41. Pal P. The adoption of waves of digital technology as antecedents of digital transformation by financial services institutions. Journal of Digital Banking. 2022;7(1):70-91.
42. Pollini A, Callari TC, Tedeschi A, Ruscio D, Save L, Chiarugi F, Guerri D. Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work. 2022;24(2):371-390.
43. Siddiqi MA, Pak W, Siddiqi MA. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences. 2022;12(12):6042.
44. Uchendu O, Omomo KO, Esiri AE. Conceptual advances in petrophysical inversion techniques: The synergy of machine learning and traditional inversion models. Engineering Science & Technology Journal. 2024;5(11).
45. Umoh AA, Nwasike CN, Tula OA, Ezeigweneme CA, Gidiagba JO. Green infrastructure development: Strategies for urban resilience and sustainability. World Journal of Advanced Research and Reviews. 2024;21(1):020-029.