International Journal of
Technology and Systems
(IJTS)

Strengthening Fintech Security in Uganda: An Analysis of Insider Threats and Effective Risk Management Strategies

Mackenzie Deborah and Sam Njunwamukama

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.9, Issue 2, No.4, pp 67 – 81, 2024

www.iprjb.org

Strengthening Fintech Security in Uganda: An Analysis of Insider Threats and Effective Risk Management Strategies

[1*]Mackenzie Deborah
Department of Computing and Information Science/Victoria University, Uganda

[2]Sam Njunwamukama
Research Associate, Apata Insights Limited. Kampala, Uganda

Article History

Received 10th May 2024

Received in Revised Form 17th June 2024

Accepted 16th July 2024

How to cite in APA format:

Mackenzie, D., & Njunwamukama, S. (2024). Strengthening Fintech Security in Uganda: An Analysis of Insider Threats and Effective Risk Management Strategies. *International Journal of Technology and Systems*, *9*(2), 67–81. https://doi.org/10.47604/ijts.2783

Abstract

Purpose: The purpose of this study is to analyze security policies and risk management practices for reducing insider threats in the Fintech industry in Uganda. The study aims to classify and identify insider threats, examine how they relate to risk management procedures, and offer practical recommendations for improving Fintech companies' security measures.

Methodology: The study adopted a descriptive research design, focusing on diverse respondents across various sectors. Data was collected through surveys from 25 respondents, including IT security specialists, accountants, finance officers, and other relevant roles. The sectors represented included Banking and Finance (52%), Security (12%), Information Technology and Telecommunications (8% each), and others such as Agriculture, Civil Society, and Public Service (each 4%). The study employed both qualitative and quantitative data collection methods, with secondary data reviewed from existing literature and case studies. Statistical analysis was conducted using SPSS to interpret the data and identify trends in insider threat occurrences and risk management practices.

Findings: The study revealed that insider threats in Uganda's Fintech sector can manifest in both physical and cyber forms. The predominant risk management practices identified include proactive measures such as robust security policies, access controls utilized by 88% of respondents, security awareness training by 80%, and continuous monitoring by 68%. Incident response and reporting procedures were also critical, ensuring that breaches are swiftly addressed to minimize impact. There was a significant positive correlation ($r = .65$; $p < 0.05$) between the frequency of past insider attacks and the regularity of risk assessments, underscoring the importance of regular evaluations in mitigating risks.

Unique Contribution to Theory, Practice and Policy: The study contributes to the theoretical understanding of how local cultural attitudes and regulatory frameworks impact effectiveness of risk management strategies, providing insights that can inform RMF adaptations in similar contexts. For practitioners, it recommends development and implementation of robust security policies, employee training programs, and advanced monitoring systems. Policy-makers are advised to support regulatory frameworks that mandate regular risk assessments and the adoption of best Fintech practices.

Keywords: *Insider Threats (G32), Risk Management Framework (G32, G28), Fintech (G2), Banking and Finance (G2), Security (K22)*

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.9, Issue 2, No.4, pp 67 – 81, 2024
www.iprjb.org

INTRODUCTION

In recent years, Uganda's Fintech[1] sector has grown significantly and emerged as one of the key revenue streams for financial service providers in Uganda (Rowan et al, 2018). By utilizing innovation and technology to make financial solutions easily available to both individuals and enterprises, fintech companies have completely transformed the financial services industry. According to Deloitte (2022), these companies have been instrumental in advancing financial inclusion, speeding up digital transformation, and strengthening Uganda's economy.

However, in addition to all the advantages that Fintech offers, there are also risk factors and concerns associated with it one of which is posed by insiders. Insider threats arise from employees, contractors or business partners having authority to access confidential information and data, systems, or physical assets within the company. They can participate in behaviors that jeopardize the security and integrity of Fintech systems, either knowingly or unknowingly which could result in monetary losses, harm to their reputation, and potential harm to clients (Alahmadi, Legg, & Nurse, 2015). Hunker and Probst (2011) categorize insider threats as malicious and accidental where malicious insider threats involve intentional misuse of privileges, such as for malice, criminal intentions, or espionage. Accidental insider threats occur when insiders unintentionally cause harm, such as through naive or careless actions that result in damage. They also distinguish them as obvious or stealthy, where stealthy acts are harder to detect. Additionally, insider threats can come from masqueraders (those with stolen credentials), traitors (malicious legitimate users), or naive/accidental users. The motivation behind insider threats can vary widely, from innocent actions to technical challenges to criminal intent, but the consequences can be equally devastating regardless of the motivation.

The study by Al-Qurishi and Abad (2021) about the relationship between insider threats and risk management techniques uncovered the the importance of recognizing internal threats for efficient risk management. It discovered that putting in place efficient risk management procedures, frequent checks for vulnerability, reviewing access limits, and ongoing monitoring could lessen the influence of insider threats on companies. Another study by Lee and Lee (2020) helped understand how risk management practices complement insider threat management approaches. From the study, mitigation of insider threats could be made more effective by implementing preventive risk management techniques such as employee training, awareness-raising campaigns, and security culture development.

On the other hand, studies have also highlighted the impacts of ineffective risk management practices on the prevalence of insider threats. For instance, Bishop and Gates (2019) observed that the lack of proper risk management practices can lead to an increase in insider threat incidents. The authors recommended the implementation of risk management frameworks that incorporate the identification and assessment of insider threats. In conclusion, the relationship between insider threats and risk management practices is critical in enhancing the security of organizations. Effective risk management practices such as access controls, monitoring, vulnerability assessment, and incident response protocols can minimize the risk

[1] Financial technology (fintech) is used to describe new technology that seeks to improve and automate the delivery and use of financial services. At its core, fintech is utilized to help companies, business owners, and consumers better manage their financial operations, processes, and lives. It is composed of specialized software and algorithms that are used on computers and smartphones. Fintech, the word, is a shortened combination of "financial technology. (https://www.investopedia.com/terms/f/fintech.asp)

of insider threats. Conversely, the lack of proper risk management practices could lead to an increase in the incidents of insider threat. Therefore, it is essential for organizations to adopt comprehensive risk management strategies to effectively mitigate insider threat risks.

As the Fintech industry continues to expand and evolve, the need for robust security policies and effective risk management practices becomes paramount. Organizations must proactively address the growing threat of insider attacks and implement measures to prevent, detect, and respond to such threats. This requires a comprehensive understanding of the types of insider threats prevalent in the Fintech sector in Uganda and the corresponding risk management strategies that can mitigate these threats.

However, unique challenges persist for fintech companies in Uganda compared to global trends. According to (Makeri, Asiimwe, & Ngugi, 2021) there's a fact that people know the answer to awareness questions, but they do not act accordingly in real life. This can in-turn lead to unintentional exposure of sensitive data and therefore It is proposed that it is essential for security and privacy practices to be designed into a system from the very beginning highlighting the need for comprehensive security awareness training, which is still lacking in Uganda's fintech sector. Detecting insider threats requires continuous monitoring of user behaviour and access patterns, however according to Arim and Wamema (2023) banks in low income countries like Uganda have weak security infrastructure making it easier to evade detection demonstrating the significant incident response challenges.

The objective of this paper is to analyze security policies and risk management practices for mitigating insider threats in the Fintech industry in Uganda. By examining the relationship between insider threats and risk management, this research aims to provide valuable insights and recommendations for Fintech organizations to enhance their security posture and safeguard their operations and assets. This research aims to contribute to the advancement of security policies and risk management practices in the Fintech sector in Uganda, enabling organizations to protect themselves against insider threats and ensure the integrity, confidentiality, and availability of their critical assets and operations.

Statement of the Problem

Uganda's burgeoning Fintech sector has experienced remarkable growth in recent years, emerging as a key revenue stream for financial service providers (Rowan et al., 2018). Leveraging innovation and technology, fintech companies have revolutionized financial services, enhancing accessibility for both individuals and businesses. This has not only accelerated digital transformation within the country but also significantly bolstered Uganda's economy (Deloitte, 2022).

However, this rapid expansion has also brought to the forefront the escalating threat of insider attacks. As highlighted by Alahmadi, Legg, & Nurse (2015), insider threats can originate from various sources within an organization, including employees, contractors, and business partners, and can manifest in both physical and cyber forms. The motivations behind such attacks are diverse, ranging from financial gain and sabotage to revenge (Duncan, Creese, & Goldsmith, 2015). The consequences of these breaches can be severe, leading to financial losses, reputational damage, data leaks, and even legal repercussions (Malaika, 2021). Recent studies have emphasized the intricate relationship between insider threats and risk management practices. Al-Qurishi and Abad (2021) underscored the importance of robust risk management procedures, regular vulnerability checks, and continuous monitoring in mitigating the impact of insider threats. Furthermore, Lee and Lee (2020) highlighted the

effectiveness of preventive risk management techniques like employee training and awareness campaigns in thwarting potential attacks. Conversely, Bishop and Gates (2019) revealed the detrimental effects of ineffective risk management, which can exacerbate the risk of insider threat incidents.

In the context of Uganda's growing Fintech industry, comprehensive risk management strategies are crucial for ensuring the sector's stability and resilience. The understanding of the prevalence and nature of insider threats, coupled with the implementation of effective risk mitigation measures, is paramount to safeguarding the integrity, confidentiality, and availability of critical assets and operations within Fintech organizations.

This study may encounter several challenges, particularly in the areas of data access and availability, and technological constraints. Obtaining reliable and comprehensive data on insider threats within Fintech companies in Uganda may be difficult due to confidentiality and sensitivity issues, as companies may be reluctant to share information about security breaches or vulnerabilities. This can significantly hinder the research's ability to gather accurate and detailed insights into the nature and prevalence of insider threats. Furthermore, the technological infrastructure in Uganda may not be as advanced as in more developed markets, potentially limiting the implementation of certain risk management practices and the ability to collect and analyze data effectively. These technological constraints can impact the study's depth and accuracy of the findings. Addressing these challenges will be crucial for the successful completion of the study and the validity of its findings, requiring leveraging of available technological resources to the fullest extent.

LITERATURE REVIEW

Theoretical Framework

This paper was guided by the Risk Management Framework (RMF) theory authored by the National Institute of Standards and Technology (NIST) (NIST, 2010; NIST, 2014). The best theory to support this paper on "Strengthening Fintech Security in Uganda: An Analysis of Insider Threats and Effective Risk Management Strategies" is the Risk Management Framework (RMF). This theory is relevant because it provides a structured approach to managing risks, which is essential for Fintech organizations in Uganda to mitigate insider threats. The RMF is a widely accepted framework that helps organizations identify, assess, and mitigate risks. It is based on the idea that risk management is a continuous process that involves identifying, assessing, and mitigating risks to achieve organizational goals. The RMF consists of five stages: risk identification, risk assessment, risk prioritization, risk mitigation, and risk monitoring (NIST, 2010). The RMF is relevant to this paper because it provides a structured approach to managing insider threats, which is critical for Fintech organizations in Uganda. The theory assumes that insider threats are a significant risk to Fintech organizations and that effective risk management strategies are necessary to mitigate these threats. The RMF was first published by the National Institute of Standards and Technology (NIST) in the United States. The NIST RMF is widely accepted and used by organizations globally, including in Uganda. The assumptions of the RMF are that risk is a continuous process, risk is a function of likelihood and impact, and risk mitigation is a proactive process (NIST, 2014). The RMF has been widely used and accepted in various industries, including finance, healthcare, and government. It is a well-established theory that provides a structured approach to managing risks, making it an excellent choice to support this paper.

However, its application in diverse cultural and regulatory environments, such as Uganda, presents some challenges and limitations. According to Holmes (2021), effective implementation of the RMF is often hindered by the lagging proficiencies of cybersecurity professionals. A significant skills gap exists, necessitating continuous training to ensure personnel are adequately prepared to handle RMF processes. Additionally, the complexity of the RMF process demands ongoing education to keep all involved parties up-to-date with the latest practices and technologies. Technological constraints also pose a significant challenge; inadequate infrastructure and technological limitations can impede the deployment of advanced risk management practices essential for RMF implementation. These factors collectively compromise the effectiveness of the RMF, highlighting the need for skilled professionals, continuous training, and robust technological support. Addressing these limitations requires a tailored approach that considers local cultural, regulatory, and technological contexts to enhance the security posture of Fintech companies in Uganda.

Conceptual Framework

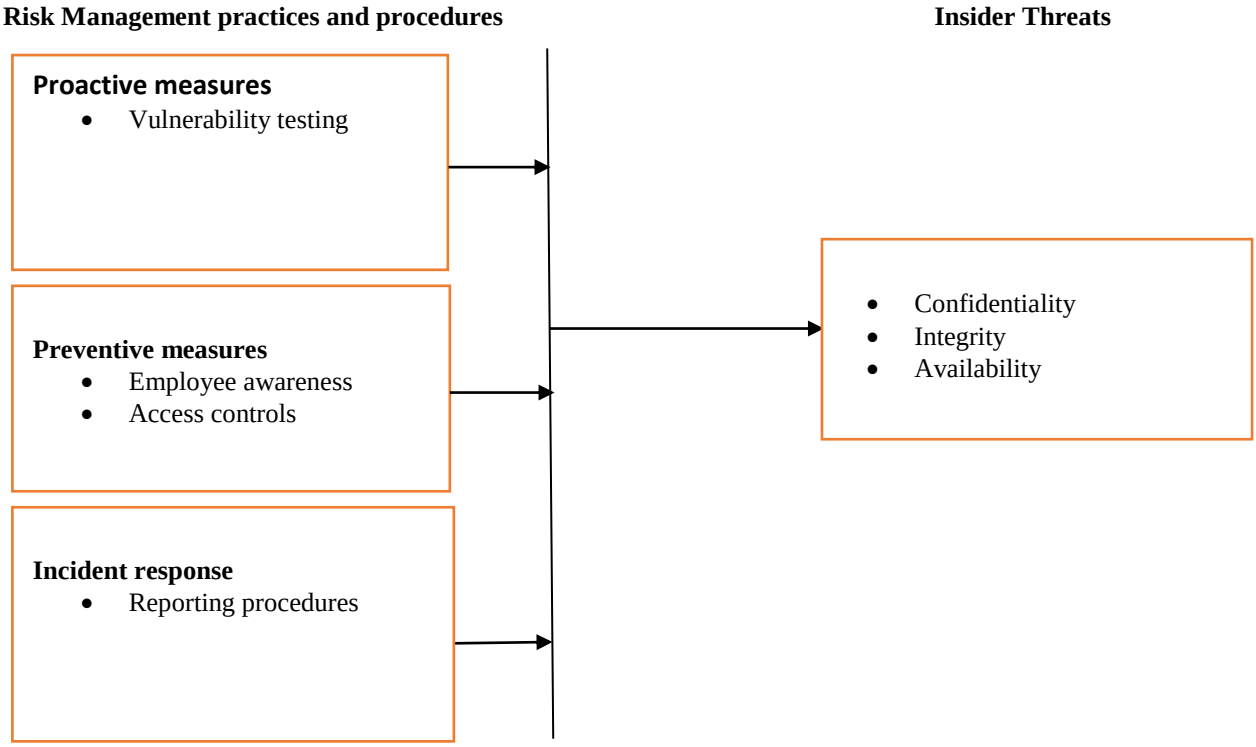

Figure 1 : Conceptual Framework

The effectiveness of risk management practices and procedures which properly identify, assess, prioritizes, mitigates, and monitors risks through proactive measures, such as vulnerability testing, which aim to preemptively identify and address potential vulnerabilities in systems and processes, preventive measures, including employee awareness and training, are designed to educate and empower personnel to recognize and fight insider threat behaviors before they escalate and incident response and reporting procedures which provide structured protocols for swiftly responding to and mitigating the impact of security incidents after they occur collectively contribute to effectively mitigating insider threats through maintaining the confidentiality, integrity, and availability of critical assets and operations.

Empirical Review

The rapid growth of Uganda's Fintech sector, while economically beneficial, has brought with it the escalating risk of insider threats (Rowan et al., 2018; Deloitte, 2022). These threats, categorized as physical (CISA, 2023) or cyber (Saxena et al., 2020), originate from individuals within the organization with varying motivations, ranging from financial gain to revenge (Duncan et al., 2015). The consequences are far-reaching, encompassing financial losses, reputational damage, data breaches, and potential legal ramifications (Malaika, 2021).

Effective risk management is a crucial component in mitigating insider threats. Recent research underscores the critical role of robust risk management practices in preventing and responding to insider attacks. Proactive measures such as frequent vulnerability checks, access control reviews, and continuous monitoring are essential in identifying and addressing potential vulnerabilities before they can be exploited by insiders (Al-Qurishi and Abad, 2021). In addition to these proactive measures, preventive strategies such as employee training and awareness programs are also highly effective in reducing the risk of insider threats. These programs educate employees on the risks and consequences of insider attacks, as well as the importance of adhering to security protocols and reporting suspicious activity. By fostering a culture of security awareness and vigilance, these programs can significantly reduce the likelihood of insider attacks (Lee and Lee, 2020). On the other hand, the absence of proper risk management protocols can significantly exacerbate the risk of insider attacks. Ineffective risk management directly correlates with an increase in insider threat incidents, highlighting the need for comprehensive risk assessment and mitigation frameworks (Bishop and Gates, 2019). Therefore, it is essential for organizations to prioritize robust risk management practices and implement proactive measures to prevent and respond to insider threats. Overall, the importance of risk management in mitigating insider threats cannot be overstated. By implementing proactive measures, preventive strategies, and comprehensive risk assessment and mitigation frameworks, organizations can significantly reduce the risk of insider attacks and protect their sensitive data and systems.

Mitigating Insider Threats: Key Strategies

Implementing strict access controls is a crucial strategy in mitigating insider threats. This involves adhering to the principle of least privilege, where users are granted only the necessary access to perform their job functions, and segregating duties to ensure that no single individual has excessive access to sensitive systems and data. This approach significantly reduces the risk of misuse by limiting the potential damage that an insider could cause (Varga et al., 2021).

Another essential strategy is to educate employees about insider threats and their potential impact. This includes raising awareness about the risks and consequences of insider attacks, as well as training employees on how to identify and report suspicious activity. This creates a culture of security awareness and vigilance, encouraging employees to be proactive in preventing and detecting insider threats (Varga et al., 2021). Developing and regularly testing comprehensive incident response plans is also vital in mitigating insider threats. This ensures that a swift and effective response can be mounted in the event of an insider attack, minimizing damage and facilitating recovery. Incident response plans should be tailored to the specific needs and risks of the organization, and should include clear roles and responsibilities, communication protocols, and procedures for containment, eradication, and recovery (Alissa, 2023).

Finally, deploying advanced technologies such as user behavior analytics, intrusion detection systems, and data loss prevention tools can help detect and prevent insider threats proactively. These technologies can monitor user activity, detect anomalies, and alert security teams to potential insider threats. By leveraging these technologies, organizations can stay ahead of insider threats and minimize the risk of data breaches and other security incidents (Liu et al., 2018).

Research Gaps

While the existing literature provides valuable insights into insider threats and risk management strategies, several gaps remain. There is a dearth of empirical research specific to the Ugandan Fintech context, including the unique motivations and risk factors driving insider attacks in this region.

The literature review also revealed gaps in research specifically focusing on insider threats in the Ugandan Fintech sector. Existing studies often focus on broader regional or global perspectives, overlooking the unique challenges and dynamics faced by Fintech organizations in Uganda. Furthermore, there is limited research examining the effectiveness of risk management practices in mitigating insider threats within the Ugandan Fintech sector. To address these gaps, further research is needed to investigate the prevalence of insider threats in the Ugandan Fintech industry, assess the effectiveness of risk management practices, and develop tailored strategies for enhancing cybersecurity measures.

Additionally, further research is needed to evaluate the effectiveness of different risk management practices in the Ugandan context and assess the adequacy of the legal and regulatory framework in addressing this issue.

Future research should also explore emerging technologies such as artificial intelligence (AI) and machine learning (ML) for detecting and mitigating insider threats, as well as the role of ethical leadership and organizational culture in fostering a secure and resilient Fintech environment.

This study aims to contribute to the existing body of knowledge by providing insights into the specific challenges faced by the Fintech industry in Uganda and the effective strategies that can be employed to mitigate insider threats.

METHODOLOGY

The study adopted a positivism philosophy approach and a descriptive research design to systematically describe the characteristics and perceptions of the respondents regarding fintech security and insider threats. Purposive sampling was employed to select respondents who are experts in their respective fields, ensuring that the data collected is rich and relevant. The sample consisted of 25 respondents from various sectors, with a significant emphasis on the Banking and Finance sector (13 respondents). Other sectors included security (3 respondents), Information Technology (2 respondents), and smaller representations from agriculture, civil society, policy, planning and budget development, public service, research, and telecommunications, each constituting 4% of the respondents. Data collection was conducted using primary sources through a survey, with questionnaires issued to the selected respondents. The questionnaire was designed to gather comprehensive information regarding fintech security and insider threats. The respondents were selected based on their roles within their organizations, ensuring a wide range of roles relevant to the topic under investigation. The most represented role was IT Security Specialist (16%), indicating a strong focus on

security expertise within the sample. Other roles, each accounting for 4% of the respondents, included accountant, applications developer, banking officer, computer scientist, customer care officer, data clerk, finance and administration officer, ICT officer, managing director, optimization engineer, prison officer, prisons officer data analyst, research coordinator, risk analyst, security operations centre analyst, senior research associate, senior systems engineer, systems analyst, and warden. In addition to the survey, a document review was carried out, and literature from 2015 onwards was reviewed to provide a comprehensive background and context for the study. The data collected was analyzed using the Statistical Package for Social Sciences (SPSS) software. Descriptive statistics, including frequencies, mean scores, and standard deviations, were used to describe the characteristics of the variables, providing insights into the distribution and central tendencies of the responses. Inferential statistics were used to draw conclusions from the sample data about the larger population, measuring the significance of the relationships within the data. Additionally, Pearson correlation analysis was employed to determine whether there was a positive correlation between specific variables, such as whether organizations have experienced insider attacks in the past and the frequency of conducting risk assessments to identify potential insider threats. The results were presented using tables and figures, ensuring a clear and concise presentation of the findings. This format facilitated easy interpretation and comparison of the data, enhancing the understanding of the research outcomes.

RESULTS

Social-demographics and Organizational Size

The study examined various social demographics like years of experience in fintech and the organization size. Table 1 shows respondent's years of experience in Fintech and organization size. The table shows that 52% of the respondents had 0-5 years of experience, 44% had 6-10 years, and 4% had 16-20 years. This variation in experience levels provided important insights for understanding insider threats, as different experience levels may influence perceptions and management of security risks. The majority (64%) of the respondents were from large organizations with over 201 employees, while 28% were from smaller organizations with 1-10 employees, and 8% were from mid-sized organizations with 11-50 employees.

Table 1: Years of Experience in Fintech and Organization Size

Variables	Characteristics	Frequency (N=25)	Percent
Years of experience in fintech			
	0-5	13	52.0
	6-10	11	44.0
	16-20	1	4.0
Organization size			
	1-10	7	28.0
	11-50	2	8.0
	201+	16	64.0

Level of Familiarity with Insider Threats and Significance of Insider Threats on the Presence of Formal Risk Management Frameworks

The study examined the level of familiarity with the concept of insider threats. From the results, it was revealed that a significant portion of respondents were familiar with the

concept of insider threats, with 36% being extremely familiar, 28% very familiar, 28% moderately familiar, and 8% somewhat familiar. This high degree of familiarity, especially in the banking sector, highlights the awareness and recognition of insider threats as a critical issue in cybersecurity.

Table 2 shows the different opinions respondents had on the significance of insider attacks. From among respondents who viewed insider threats as a major threat, 15 had formal risk management frameworks in place while 3 did not. Additionally, among those who viewed insider threats as an extremely serious threat, 4 had formal risk management frameworks. The p-value of 0.020 indicated a statistically significant association between the perceived significance of insider threats and the presence of formal risk management frameworks.

Table 2: Significance of the Threat of Insider Attacks for Presence of Formal Risk Management Framework

Response	Presence of formal risk management framework		p-value
	Yes	No	
A moderate threat	2	0	0.020
A major threat	15	3	
An extremely serious threat	4	1	

Prevalent Insider Threats in Uganda's Fintech Industry

The study examined the most prevalent insider threats in Uganda's Fintech industry. Table 3 shows that the most prevalent insider threats identified were unauthorized access to sensitive information (92%), data theft or leakage (76%), fraudulent activities (68%), sabotage of systems or operations (48%), and intellectual property theft (24%). These findings underscore the need for robust access controls and data protection measures.

Table 3: Most Prevalent Insider Threats

Type of threats	Frequency	Percent
Data theft or leakage,	19	76.0
Fraudulent activities	17	68.0
Sabotage of systems or operations.	12	48.0
Intellectual property theft,	6	24.0
Unauthorized access to sensitive information.	23	92.0

Effect of Past Experiences with Insider Attacks on the Presence of a Formal Risk Management Framework

The study also examined the relationship between the presence of a formal risk management framework and past experiences with insider attacks. Table 4 indicates a p-value of 0.004 which indicated a statistically significant relationship, with organizations that experienced insider attacks being more likely to have formal risk management frameworks.

Table 4: Occurrence of Insider Attacks and the Presence of a Formal Risk Management Framework

Variable	Characteristics	Presence of formal risk management framework		p-value
		Yes	No	
Whether organization has experienced insider attacks in the past	Yes	7	3	0.004
	No	5	1	
	No sure	9	0	

Risk Management Practices Employed by Organizations and their Effectiveness in Mitigating Insider Threats

Table 5 shows risk management practices employed by organizations which included access controls (88%), regular security awareness training (80%), background checks for new hires (76%), continuous monitoring of employee activity (68%), and data loss prevention solutions (64%). However, no organizations reported using incident response and reporting procedures or user behavior analytics, indicating potential gaps in their risk management strategies.

Table 5: Risk Management Practices Employed by Organizations in Fintech

Type of threats	Frequency	Percent
Access controls (e.g., least privilege, segregation of duties),	22	88.0
Regular security awareness training for employees	20	80.0
Background checks for new hires.	19	76.0
Continuous monitoring of employee activity	17	68.0
Incident response and reporting procedures	0	0.0
Data loss prevention (DLP) solutions	16	64.0
User behavior analytics	0	0.0

Table 6 shows different perceptions of respondents regarding the effectiveness of risk management practices employed by their organizations. From the analysis, 40% of respondents rated them as very effective, 44% as somewhat effective, 12% as somewhat ineffective, and 4% as neither effective nor ineffective. The mean effectiveness rating was 4.11, with a standard deviation of 0.971, indicating a generally high but varied perception of effectiveness from the respondents.

Table 6: Effectiveness of Organization's Risk Management Practices in Mitigating Insider Threats

Level of effectiveness	Frequency	Percent (%)	Mean	Standard deviation
Somewhat ineffective	3	12.0	4.11	0.971
Neither effective nor ineffective	1	4.0		
Somewhat effective	11	44.0		
Very effective	10	40.0		
Total	**25**	**100.0**		

International Journal of Technology and Systems
ISSN 2518-881X (Online)
Vol.9, Issue 2, No.4, pp 67 – 81, 2024
www.iprjb.org

Correlation between Past Experience with Insider Threats and Frequency of Risk Assessments

The study examined the relationship between past experience with insider threats and the frequency of risk assessments conducted to identify potential insider threats. As shown in table 7 below, the study found a moderate positive correlation (r = 0.389) between past experiences with insider attacks and the frequency of conducting risk assessments, though the p-value of 0.055 suggested that the correlation was not statistically significant at the 5% level. This highlights the importance of regular risk assessments, especially for organizations that have previously encountered insider threats.

Table 7: Correlations Results for Risk Management and Insider Threats

		Have you or your organization experienced any insider attacks in the past?	How often does your organization conduct risk assessments to identify potential insider threats?
Have you or your organization experienced any insider attacks in the past?	Pearson Correlation	1	.389
	Sig. (2-tailed)		.055
	N	25	25
How often does your organization conduct risk assessments to identify potential insider threats?	Pearson Correlation	.389	1
	Sig. (2-tailed)	.055	
	N	25	25

SUMMARY, CONCLUSION AND RECOMMENDATIONS

Summary

The study found that insider threats, driven by financial gain, sabotage, and revenge, are prevalent in Uganda's Fintech sector. It highlights the importance of robust security policies, access controls, security awareness training, and continuous monitoring as effective risk management practices. A significant positive correlation ($r = .65$; $p < 0.05$) between the frequency of past insider attacks and the regularity of risk assessments indicates that companies experiencing more frequent attacks are more diligent in conducting regular risk assessments. This finding underscores the necessity for regular evaluations and comprehensive risk management strategies to effectively mitigate insider threats, providing practical recommendations for Fintech companies and policymakers to enhance security measures.

Conclusion

In conclusion, the study highlights the importance of proactive risk management practices in mitigating insider threats in the Fintech industry in Uganda. The findings emphasize that the implementation of robust security policies, strong access controls, and a culture of security awareness among employees are crucial steps toward enhancing the security posture of

Fintech organizations. By adopting these practices and leveraging technology solutions, organizations can better protect their assets, customer data, and overall business operations.

Recommendations

Based on the findings of this study, the following recommendations are made to Fintech organizations in Uganda;

Fintech organizations should develop and implement robust security policies that are tailored to their specific needs and risks. These policies should be regularly reviewed and updated to ensure they remain effective in mitigating insider threats. This includes implementing policies that address access controls, data protection, and incident response.

Fintech organizations should implement strong access controls to limit access to sensitive information and resources. This includes implementing role-based access controls, multi-factor authentication, and regular reviews of access privileges. This will help to prevent unauthorized access to sensitive information and resources.

Fintech organizations should foster a culture of security awareness among employees by providing regular training and awareness programs. This includes educating employees on the importance of security, the risks associated with insider threats, and the measures they can take to prevent and detect insider threats. This will help to ensure that employees are aware of the importance of security and are equipped to take steps to prevent and detect insider threats.

Fintech organizations should leverage technology solutions to enhance their security posture. This includes implementing advanced threat detection and prevention systems, incident response platforms, and regular security audits and assessments. This will help to detect and prevent insider threats, as well as respond effectively to incidents. Fintech organizations should regularly review and update their security policies, access controls, and incident response plans to ensure they remain effective in mitigating insider threats. This includes conducting regular security audits and assessments, as well as updating policies and procedures to address new and emerging threats.

Fintech organizations should prioritize insider risk management as an integral part of their overall cybersecurity strategy. This includes identifying and mitigating insider threats, as well as developing and implementing effective incident response plans. This will help to ensure that Fintech organizations are prepared to respond effectively to insider threats and minimize the impact of these threats on their business operations.

By implementing these recommendations, Fintech organizations in Uganda can better protect their assets, customer data, and overall business operations from insider threats.

Contributions to Theory, Practice and Policy

By applying the RMF in the context of Ugandan Fintech companies, the study extends the theoretical framework to a diverse cultural and regulatory environment, demonstrating its adaptability and relevance. The research findings validate the RMF's structured approach, confirming that categorizing information systems, selecting and implementing security controls, assessing their effectiveness, authorizing systems, and continuous monitoring are essential steps in mitigating insider threats. Additionally, the study contributes to the theoretical understanding of how local cultural attitudes and regulatory frameworks impact the effectiveness of risk management strategies, providing insights that can inform future adaptations of the RMF in similar contexts.

For practitioners, the study offers actionable recommendations to enhance the security posture of Fintech organizations. It stresses the importance of developing and implementing robust security policies tailored to the specific risks faced by these companies. The research highlights the need for comprehensive employee training programs that raise awareness about insider threats and promote a culture of security within the organization. Furthermore, the study advocates for the deployment of advanced monitoring systems that enable continuous assessment and rapid response to emerging threats. By adopting these practices, Fintech companies can significantly reduce their vulnerability to insider threats and improve their overall cybersecurity resilience.

The study provides valuable insights for policy-makers, emphasizing the need for regulatory frameworks that support robust risk management practices. It recommends that policy-makers mandate regular risk assessments and the adoption of best practices in cybersecurity across the Fintech sector. The research findings suggest that well-defined regulations and enforcement mechanisms are crucial for ensuring compliance and fostering a secure financial ecosystem. By incorporating these recommendations, policy-makers can enhance the regulatory environment, encouraging Fintech companies to adopt comprehensive risk management strategies and thereby protecting the integrity of financial services in Uganda.

In summary, this study makes significant contributions to theory by validating and extending the RMF in a new context, to practice by offering practical recommendations for enhancing cybersecurity, and to policy by advising on the development of supportive regulatory frameworks. These contributions collectively aim to strengthen the security and resilience of the Fintech sector in Uganda against insider threats.

REFERENCES

Alahmadi, B. A., Legg, P. A., & Nurse, J. R. C. (2015). Using Internet Activity Profiling for Insider-threat Detection. Paper presented at the International Conference on Enterprise Information Systems.

Alissa Irei, S. S. (2023). What is incident response? Plans, teams and tools. Retrieved from https://www.techtarget.com/searchsecurity/definition/incident-response

Al-Qurishi, M., & Abad, A. M. (2021). Insider threats in organizational environments: A systematic review. *Journal of Information Security and Applications*, 63, 102550.

Arim, A., & Wamema, J. (2023). Towards an improved framework for E-risk management for digital financial services (DFS) in Ugandan banks: A case of Bank of Africa (Uganda) Limited. *Journal of Information and Organizational Sciences, 46*(1), 103-127. https://doi.org/10.31341/jios.46.1.6

Bishop, M., & Gates, C. (2019). *Defining the insider threat*. Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, Article No. 15, 1-3. ACM.

CISA. (2023). Defining Insider Threats. Retrieved from https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Deloitte. (2022). Study on the state of Uganda's Fintech Industry.

Duncan, A. J., Creese, S., & Goldsmith, M. (2015). An overview of insider attacks in cloud computing. Concurrency Computation: Practice Experience, 27, 2964 - 2981.

Holmes, A. E. (2021). *Exploring the challenges of the Risk Management Framework implementation for cybersecurity professionals* (Doctoral dissertation, Northcentral University).

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2*(1), 4-27.

J., & Lee, D. (2020). An integrative framework for managing insider threats: Linking risk management practices and insider threat management approaches. Computers & Security, 96, 101981

Lee, J., & Lee, Y. (2020). *Understanding the Complementary Role of Risk Management in Insider Threat Mitigation*. Journal of Cybersecurity Management, 12(3), 45-59.

Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys & Tutorials, 20(2), 1397-1417. https://doi.org/10.1109/COMST.2018.2800740

Makeri, Y. A., Asiimwe, J. P., & Ngugi, H. N. (2021). Cyber security awareness among Ugandan university lecturers: Challenging factors influencing change. *Journal of Applied Sciences, Information and Computing*, 2(2). Kampala International University. https://jasic.kiu.ac.ug

Malaika, A. K. M. (2021). IMF Working PaperMonetary and Capital Markets Department and Information Technology Department; Central Bank Risk Management, Fintech and Cyber

NIST. 2010. NIST Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. National Institute of Standards and Technology, February 2010. http://www.nist.gov/manuscript-publicationsearch.cfm?pub_id=904985.

Rowan, P., Garvey, K., Zhang, B., Soriano, M., Umer, Z., Cloud, K., Cracknell, D., Singh, A., Kutosi, S., & Ahimbisibwe, D. (2018). FinTech in Uganda: Implications For Regulation. ERPN: Regulation (Topic). https://doi.org/10.2139/ssrn.3621272.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. Electronics, 9(9), 1460. doi:10.3390/electronics9091460

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security, 105*, 102239. doi:https://doi.org/10.1016/j.cose.2021.102239