Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 25 – 38 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

FINTECH RESILIENCE: AN EXPLORATION OF SECURITY RISKS AND RISK MANAGEMENT STRATEGIES

Ali Mwase[1], Ernest Ketcha Ngassam [2], Shawren Singh[3]
[1]Makerere University Business School, Kampala, Uganda
[2]University of South Africa, South Africa

ABSTRACT. The rapid evolution of financial technology (Fintech) has brought about unprecedented opportunities and challenges, particularly in the realm of security. This research paper conducts a thorough exploration of the security landscape within the Fintech sector, with a focus on identifying and understanding the diverse risks that pose threats to the industry's resilience. The study delves into operational, technological, regulatory, and cybersecurity risks, unraveling their complexities and implications for the Fintech ecosystem.

The core of this research lies in the comprehensive examination of risk management strategies employed by Fintech entities to fortify their resilience against the identified security threats. By synthesizing current literature and industry practices, the paper provides valuable insights into innovative risk mitigation approaches, considering the dynamic nature of the Fintech environment. Special attention is given to the integration of advanced technologies, regulatory compliance, and collaborative frameworks that contribute to enhancing the sector's overall resilience.

Furthermore, the study proposes a Fintech Ecosystem Risk Management Metamodel to illustrate the practical application of risk management in addressing security challenges for the sector. The findings aim to equip industry practitioners, policymakers, and researchers with a nuanced understanding of the interconnected dynamics between security risks and effective risk management in the Fintech landscape. Ultimately, this study contributes to the ongoing discourse on fostering resilience within Fintech, ensuring the sustained growth and stability of this transformative sector.

KEYWORDS*:* Fintech, Security risks, Risk management, Cyber security, Risks.

1.0 INTRODUCTION

The Fintech industry has ushered in a new era of financial services, offering innovative solutions that promise convenience, efficiency, and accessibility (Callen-Naviglia & James,2018). However, this digital transformation has brought with it a host of cybersecurity challenges (Dattani, 2016). Because of channel fusion and simplicity, Fintech services are relatively susceptible to security problems (Park & Kim,2015). Fintechs are particularly susceptible to security risks due to the nature of their operations and the sensitive data they handle (Sampat et al, 2023). A Security risk in the context of Fintech is closely related to risks associated with digital technologies due to the heavy deployment of digital components in Fintech solutions and platforms (Kaur et al,2021). Digital security threats like hacking, phishing, virus, and e-fraud could exploit vulnerabilities in digital systems to activate certain risk crystallization (Keong et al,2020). Exposure of or loss of control over customers' personal information, trade secrets, and other confidential information could amount to a potential loss known as a security risk (Keong et al,2020; Razzaque et al,2020). This could consequently result in information theft and degradation of integrity, privacy, confidentiality, authenticity, and accountability of information (Razzaque et al,2020).

A study by Alijoyo (2022) asserts that Fintechs are some of the increasingly high-risk businesses because they provide many online services such as online money lending services. Thus, good risk management is a must for Fintechs. Risk management is the identification, measurement, monitoring,

and evaluation of diverse risks (hazards, disasters, shocks) followed by a coordinated and cost-effective application of resources (prevention, mitigation, preparedness, resilience) to minimize and control the probability and impact of exposure and to try to maximize the realization of possible returns(UN,2021). Risk management further ensures that a company or organization can understand, measure, and monitor various risks and ensure that the policies made can control the various kinds of risks (Alijoyo ,2022). It is postulated that Fintechs can enhance their success in regulated markets by having sound and robust risk management practices. This increases the comfort levels of key stakeholders who value transparency and best practices in risk management (Mehrotra & Menon,2021). Moreover, it is postulated that Risk management in Fintechs is not only essential for protecting against potential threats but also for building trust, ensuring regulatory compliance, and fostering long-term sustainability in a rapidly evolving industry (Fenwick &Erik,2020). The need for risk management in Fintechs is crucial, given the unique challenges and complexities associated with operating in the dynamic intersection of finance and technology (Cernisevs et al,2023). This study therefore aims at investigating the security landscape within the Fintech sector, shed light on effective risk management strategies, and present a metamodel that can guide practitioners and policymakers in fortifying the resilience of the Fintech sector against evolving security threats.

The remaining part of this paper is structured as follows: Section 2 presents the related literature, section 3 covers the methodology adopted by the study, of which the results of our research that present the assets in the Fintech landscape, mapping of potential risks to these assets, mapping of the Fintech Security Risk assessment as well as a proposed Fintech Ecosystem risk management Metamodel are presented in Section 4. Section 4 further presents some existing Risk management strategies. Finally, the conclusion of this work is presented in Section 5.

2.0 RELATED WORKS

2.1 Definition of Risk and Risk Management

A risk is an uncertain event with a probability of happening and impacting an organization's strategic, operational, and financial objectives (Kure et al,2018). In a business context, risks are any threat to a vulnerable asset that will cause harm to reach business objectives(Vellani,2006). Risks can be divided into proactive and reactive risks. Risks are characterized by the likelihood of the event occurring and the impact of the event. The risk formula can be used to calculate the value of a risk: Risk (Expected Loss) = likelihood multiplied by impact. Risk management involves identifying, analyzing, and controlling risks in an organization's information assets and infrastructure to increase effectiveness and efficiency (Alijoyo, 2022).

2.2 Cyber Risk Assessment

Cyber risk assessments are essential for organizations to identify, estimate, and prioritize risks arising from information systems operations and use (Tunggal,2023).They evaluate threats to IT systems and data, enabling organizations to prioritize improvements, communicate risks to stakeholders, and make informed decisions on resource deployment to mitigate security risks (Cobb,2022).Conducting a cybersecurity risk assessment helps organizations understand the magnitude of risks and manage them effectively. Mitigating identified risks can prevent and reduce costly security incidents and data breaches, while avoiding regulatory and compliance issues(Cobb,2022).Cyber risks include ransomware, data leaks, phishing, malware, insider threats, cyberattacks, infrastructure attacks, intellectual property theft, insecure supply chain partners, and aggressive insider behavior(Tunggal,2023).

2.3 Cyber Security

Cyber security is the protection of information and communication networks from cyber-attacks and threats in the cyberspace or network (Li & Liu,2021). It involves the collection of tools, policies, security safeguards, guidelines, risk management approaches, training, best practices, assurance, and technologies used to protect the cyber environment and organizations' assets(Armenia et al,2021).Cybersecurity encompasses both human and non-human entities, and focuses on three key

factors: methods of protecting IT, data processing and transmission, level of protection obtained, and professional aspects. Cybersecurity investment has become an increasingly important issue due to advanced technology and cyber attackers (Dunn Cavelty,2014). Fintech organizations must prioritize cybersecurity measures to protect their IT infrastructure, including secure APIs and cloud servers. By addressing the range and scope of cyber-attacks, organizations can reduce vulnerability across relevant weaknesses and ensure the overall security of their IT infrastructure.

3.METHODOLOGY

We conducted a systematic literature review using a six-step approach, which consists of selecting a topic, looking for pertinent articles, creating arguments, reviewing, assessing, and publishing the literature (Machi & McEvoy, 2016).

In order to explore the state of the art of the Fintech security landscape through various combinations of the keywords that are specified before the introduction, we therefore searched databases such as google

scholar, Science Direct, Wiley database, Sage database, IEEE database, ACM, MDPI, Springer, and Emerald. Thereafter, we selected papers from fifteen peer-reviewed Information Systems and computer security journals with specific publications on Fintech security risk related articles. They are all ranked highly in the 2020 SJR Journal ranking charts. The articles that were selected for examination were published over the last eleven years, from 2011 to 2021. Even so, older papers were included if they included relevant information about the topic of the study. We looked through up to five volumes in each of these journals to locate a maximum of five articles, pausing when we had located the five volumes or five articles, whichever comes first. According to the Krejcie & Morgan (1970) table for calculating sample size for a given population (Krejcie & Morgan, D1970), this produced a total of 50, and a matching sample size of 44.

The final selection consisted of 44 papers, 24 from computer security journals and 20 from information systems journals. We decided to use open coding. Multiple category names that had the same meaning were consolidated into one without taking that differentiation into account. To resolve any remaining differences regarding classification, the researchers studied the pertinent papers; this iterative approach aided in reaching a consensus. The results section below contains the presentation of the findings.

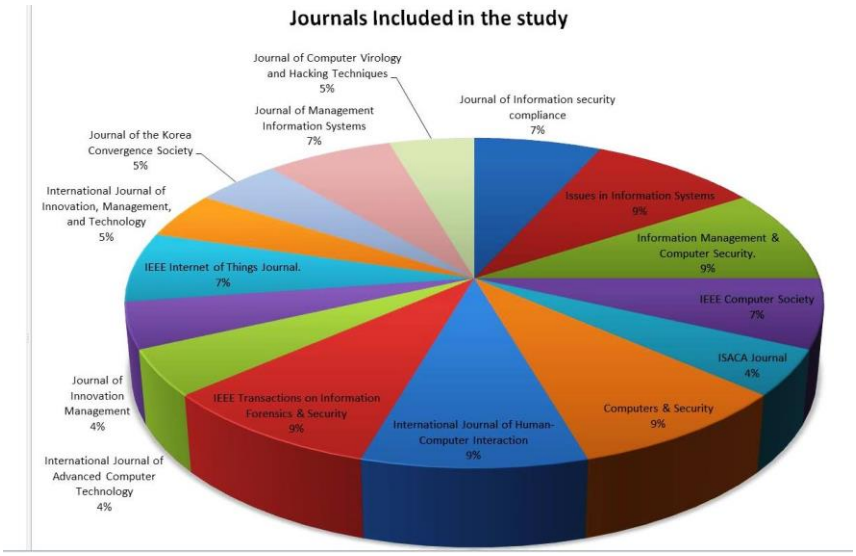

Fig. 1. Information Systems and Computer Security journals included in the study

4. RESULTS AND DISCUSSIONS

After analyzing the data, comparisons were drawn on parameters judged to be essential in the process of understanding and combating security risks in the fintech landscape. These are presented in the next sections 4.1 to 4.3 below.

4.1 Assets in the Fintech Ecosystem

Assets are defined as tangible or intangible entities that are necessary and have value to the Fintech organization (Kure et al,2018). Identification of key assets, and putting a value on each key asset, is an important process of risk management. These key assets could be people, services, facilities, processes, etc. It is important to identify critical assets as well as estimate their critical failure modes or the impact of the loss. An asset has two features: (i) criticality and (ii) category. Criticality is defined as a measure of the consequences associated with the degradation or loss of an asset. It is the major indicator used by organizations to determine which asset is of more value to business continuity. Category classifies assets according to their level of sensitivity and security requirements. The criticality of an asset category can be high, medium, or low, which means that assets with high ratings are the most valuable to the organization (Kure et al,2018).

To determine the key assets and role players in the Fintech ecosystem, we consider each aspect of the Fintech ecosystem. This was followed by determining the potential risks associated with these assets and further doing some classification of such risks in terms of business risk, technological risks, etc. The key assets and role players are summarized in table 1 below.

Tab. 1. Key assets and role players in the Fintech ecosystem

Stakeholders/ Role players	Assets	Systems components
• Fintech Companies • Financial Institutions • Venture Capital Firms • Incubators/Accelerators • Legal Advisors • Consultancy Firms • Research (Academia) • International Knowledge Partners • Regulatory Authorities • Industry Associations • Intermediary Organizations • The Financial Consumers • Incumbent Banks • Insurers • Software Companies • Technology Hubs	• Computer hardware • Computer software • Telecommunication devices • WLANS • LANS • Networking Cables • Mobile computing devices • Data Centers(Servers) • Database • Automated Teller Machines(ATM) • Crypto Assets • People • Transactions • Robo Advisors(AI) • Money	• Online platforms • Mobile Apps • Bank Accounts • ATM Cards • Financial Cards • Digital Wallets • Smart Contracts • Mobile point-of-sale systems

4.2 Fintech Assets and potential Risks

Determining and classifying potential risks associated with assets in the Fintech landscape is crucial. Indeed, a study by AFI (2020) posits that Fintechs pose potential risks to financial stability (Vučinić, 2020). Furthermore, a special report by Alliance for Financial Inclusion (AFI) (AFI,2020).Creating Enabling Fintech Ecosystems: observes that the rise of digital financial services and Fintech products

present new risks and threats, such as those stemming from opaque data privacy practices or systemic vulnerabilities from cybersecurity threats(AFI,2020).

It is observed that technology may lead to new types of risk or exacerbate existing ones. There is a need to explore risks such as the cyber risks in Fintech. This is because there is an increasing concentration of infrastructure at a limited number of participants (e.g., banks and broker-dealers providing trading technology and infrastructure to others), or central counterparties (Gomber et al,2018).

Risk identification entails examining an organization's current information technology security situation, Risk assessment involves determining the extent to which the assets are exposed or at risk, and Risk control focuses on applying controls to reduce risks to an organization's data and information systems (Whitman & Mattord,2021).

It is stated that the surge of adoption of sophisticated systems of Fintech among financial institutions, has highlighted the prominence of operational risk. An effective operational risk management process includes the identification and measurement of operational risk, which should lead to an understanding of the specific causes and events embedded in the adoption of Fintech, which may expose a Fintech company to operational risks (Khalil & Alam,2020).

Risks can be both internal and external to the firm. Risks are of various types namely; business risk, financial risk, operational risk, technology risk, security risk, compliance risk, availability risk, and strategic risk (Vellani, 2006). Others are; Systemic, Reputation, Legal, Liquidity, and Fraud(Lake,2013). The key risk areas for the Fintech Ecosystem are presented in table 2 below.

Tab. 2. Key risk areas for the Fintech Ecosystem

ASSETS	Potential Risks	Author	Risks Classification
• Computer hardware • Computer software	Security misconfigurations. Insufficient Logging & Monitoring. Deliberate hardware destruction	Akanksha(2022); Gurdip&Arash(2021)	Technological risk Security Risk
• People	Broken User Authentication. Sensitive data exposure and privacy incidents. Digital Identity risks. Credit card fraud. Accounting hijacking Imprudent lending.	Akanksha(2022); Gurdip&Arash(2021) ;Govindraj(2022); World Bank(2021)	Technological risk Security Risk Fraud risk
• Transactions	Broken Function Level Authorization. Insecure interfaces and API.	Akanksha(2022); Govindraj(2022)	Technological risk Security Risk Operational Risk
• Mobile computing devices	Application security risks. Hacktivists. Cybercriminals. Script kiddies. Cyber terrorists. Insecure interfaces and API's. Remote nature of digital channels and the rapid speed	Gurdip&Arash(2021) ;Govindraj(2022 World Bank(2021); Muhn,(2020)	Technological risk Security Risk Fraud risk Operational Risk

	of transactions. Platform/technology unreliability or vulnerability.		
• Crypto Assets	Insecure interfaces and API's. Unrecognized and illegal cryptocurrency trading Activity. Blockchain Security. Platform/technology unreliability or vulnerability.	Govindraj(2022); NSFOCUS(2018)	Technological risk Security Risk Fraud risk Operational Risk
• Robo Advisors(AI)	Cyber terrorists	Gurdip&Arash(2021)	Technological risk Security Risk Fraud risk Operational Risk
• Automated Teller Machines(ATM)	Denial of service Fraudulent transactions Cyber terrorists Compromising ATM infrastructure	Gurdip&Arash(2021) ; Lukonga(2018)	Reputation risks Technological risk Security Risk Fraud risk Operational Risk
• Telecommunication devices • WLANS • LANS • Networking Cables	Deliberately hardware destruction System outages. Surging Traffic. Web security threats	Gurdip&Arash(2021) ; Lukonga(2018); Wang(2021);NSFOCUS(2018).	Reputation risks Technological risk Security Risk Fraud risk Operational Risk
• Data Centers(Servers) • Database	Information theft. Injections. Data breaches. Hacking through third-party vendors.	Akanksha(2022); Lukonga(2018)	Reputation risks Technological risk Security Risk Fraud risk Operational Risk

4.3 Approaches to Cyber Risk Assessment

Risk assessment entails a systematic process for risk identification, consequences analysis, and risk management (Aagedal et al,2002). Risk assessment needs to identify potential causes, events, and effects that could materialize in the future, and it needs to make use of suitable tools for representing or expressing uncertainties (Amundrud et al,2017). There are several approaches to cyber risk assessment and these involve understanding security posture, collecting data, modeling potential attacks, and prioritizing mitigation actions(CYE,2022).

The compliance-driven approach to cyber risk assessment compares an organization's security controls with cybersecurity and regulatory frameworks like NIST, ISO/IEC, and the European Union. These frameworks provide credible guidelines for compliance activities and basic security practices(CYE,2022).

Threat modeling approach which is a process used to identify and prioritize risks in a business context. It involves analyzing potential threats, identifying assets and access points, and identifying threats [92].Threat modeling uses approaches, like Attack Trees, STRIDE, Abuser Stories, Agile

modeling, T-MAP, CORAS, fuzzy logic, SDL Threat Modelling Tool, and Application Threat Modelling (TAM) Tool. Threat modeling can be either proactive or reactive, with reactive approaches protecting against adversarial attacks and proactive approaches defending FinTech institutions against cyber-attacks (Gurdip & Arash,2021).

Attack route analysis approach involves gathering information about likely threats and key assets, using real attackers' techniques and thought processes(CYE,2022). This helps security teams build a graph of attack routes between threats and key assets, including systems, networks, and cloud platforms. This graph helps security teams focus on real dangers and prioritize vulnerabilities that are not on an attack route leading to a critical asset or are blocked by existing controls. This approach simplifies communication with non-technical managers, allowing them to understand how threats operate and how to neutralize them by removing vulnerabilities or adding controls(CYE,2022).

Lastly, the five-step framework for conducting a cybersecurity risk assessment is as follows: scoping, risk identification, risk analysis, risk evaluation, and documentation(Cobb,2022). The first step involves determining the scope of the assessment, which can be the entire organization, business unit, location, or specific aspect of the business. The second step involves identifying cyber security risks, creating an inventory of all physical and logical assets within the scope, and identifying the consequences of an identified threat exploiting vulnerability. The third step involves analyzing risks and determining potential impact. The fourth step involves risk evaluation, prioritizing risks using a risk matrix.

The fifth step involves documenting all identified risk scenarios in a risk register, which should be regularly reviewed and updated to ensure management has an up-to-date account of its cybersecurity risks(Cobb,2022).

4.3.1 Fintech Ecosystem risk management Metamodel

The Risk Management (RM) process comprises coordinated activities aimed at guiding and controlling an organization as far as risks are concerned. These activities encompass the definition of the context of analysis, assessment, treatment, and acceptance, as well as the communication and monitoring of information security risks(Mayer&Fagundes,2009). Risk management ascertains that procedures are defined for ensuring that risks have been sufficiently managed, as well as including assessing the risk factors of IT investments (Asgarkhani,Correia,& Sarkar,(2017). Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment (Stoneburner,Goguen &Feringa,2002).In a similar study, Haneef et al (2012) argue that Risk Management encompasses risk identification, assessment, measurement, monitoring and controlling all risks inherent in the business processes.

According to Fintech Global (2021), Fintechs continue to evolve, it is essential that they prioritize risk assessment to maintain trust and credibility with their customers and regulators as well as prevent fraud.

Moreover, it is pointed out that risk assessments support organisations to navigate amid chaos and meet their strategic objectives. Thus, the process must be baked into every step of the digital transformation journey to achieve long-term success (Fintech Global,2021).

Therefore, in this study, we propose that the designed Fintech Ecosystem risk management Metamodel is beneficial in mapping and mitigating risks.

We adopt Innerhofer-Oberperfler and Breu (2006) security information meta-model as the cornerstone of the security management process to conduct a risk assessment in the Fintech ecosystem. The study adds security-relevant information to the security information meta-model by connecting the model's elements to security artifacts like Fintech Assets, Fintech Risks, threats, security incidents, and security controls. This information reflects the state of the entire Fintech ecosystem's security process.

As shown in Figure 2, the Fintech Ecosystem Risk Management Metamodel is modeled using a series of UML diagrams to represent the various aspects and demonstrate the relationships maintained between one another. A set of design notations called the Unified Modelling Language (UML) offers a number of valuable capabilities, including numerous interconnected design views. The Metamodel is illustrated in Figure 2 below.

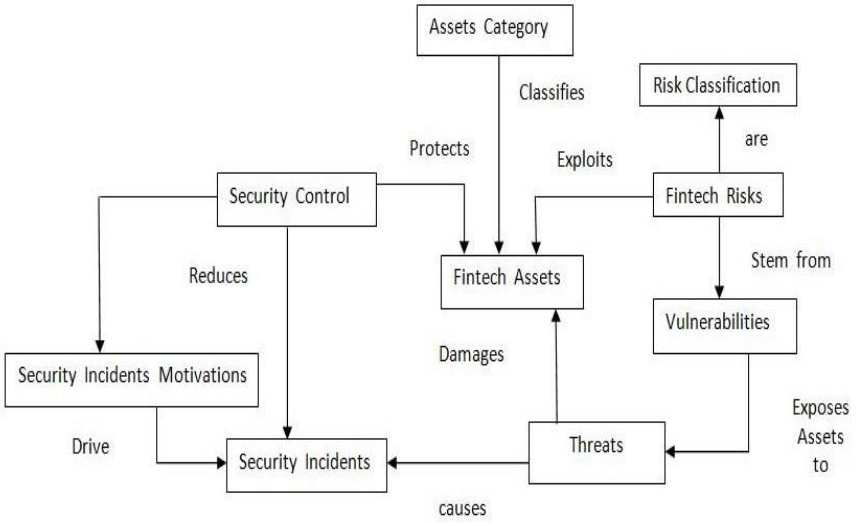

Fig. 2. Fintech Ecosystem risk management Metamodel

The Fintech Ecosystem risk management Metamodel presented in figure 2 above is explained as follows;

Fintech Assets: The central element of the Fintech Ecosystem risk management Metamodel is the concept of Fintech Assets. Fintech Assets act as a place-holder for any type of tangible or intangible entities which are necessary and have value to the Fintech organization. These key assets could be people, services, facilities, processes, etc.

Assets Category: classifies assets according to their level of sensitivity and security requirements. The criticality of an asset category can be high, medium, or low, which means that assets with high ratings are the most valuable to the organization.

Fintech Risk: these are any threats to a vulnerable asset that will cause harm to reaching business objectives.

Vulnerability: Vulnerability is the weakness in an organization's security program that is exploited by a threat to gain unauthorized access to an asset. It has three properties. i.e., impact, type, and weight score.

Threats: The concept of threat describes anything that can cause damage to an asset. The threats can be natural and political disasters, intentional actions, and unintentional actions. A threat is always related to a specific Fintech Asset. A threat is evaluated by measuring its probability and potential impact resulting in a measurement of its risk.

Risk Classification: Identifying risks and their categorization into suitable risk categories are fundamental to enterprise risk management procedures. Risk Classification enables the grouping of the resources or Fintech assets exposed to risk such as physical, human, and financial resources. Risk categorization evaluates inherent and residual risks for various processes and activities possible. Risk must be categorized based on its type, nature, and complexity.

Security incidents: A security incident is an event that may indicate that a Fintech organization's asset has been compromised or that measures put in place to protect them have failed. Security incidents are usually distinguished by the degree of severity and the associated potential risk to the organization.

Security Control: This activity identifies the possible control measures that could mitigate and eliminate identified Fintech risks related to the Fintech assets. No system is risk-free, therefore, to reduce security breaches to protect assets from the various types of threats and vulnerabilities, effective controls must be applied.

Security incidents Motivation: The number of cyber security incidents is growing rapidly. To curb these incidents, it is imperative to understand what motivations drive these cyber incidents.

In addition, the designed Fintech Ecosystem risk management Metamodel can be exploited from both a human and technology perspective. It can be leveraged as follows;

a) From a Human Perspective:

Standardization and Consistency: The metamodel provides a standardized framework for representing and organizing security-related concepts, relationships, and behaviors. By leveraging a common metamodel, Fintechs can ensure consistency in understanding and implementing security measures across human stakeholders. This reduces the chances of miscommunication, gaps in security, and inconsistencies in risk mitigation efforts.

Knowledge Sharing and Training: The metamodel can be used as a training resource for educating human stakeholders on security principles, standards, and guidelines. By promoting awareness and understanding of the metamodel, organizations can enhance the security knowledge and competence of their workforce, empowering them to identify and address security risks effectively.

Risk Assessment and Decision Making: The metamodel facilitates the identification and analysis of security risks. Human stakeholders can use the metamodel to assess risks, evaluate their potential impact, and make informed decisions regarding risk mitigation strategies. The metamodel provides a structured framework for considering various security dimensions, dependencies, and relationships, helping stakeholders prioritize and allocate resources appropriately.

b) From a Technology Perspective:

System Design and Architecture: The metamodel can guide the design and architecture of technology systems. By incorporating security considerations from the metamodel, organizations can ensure that security requirements and controls are embedded into the technology infrastructure. The metamodel can provide guidelines for secure system configurations, access controls, encryption mechanisms, and other technical security measures, reducing vulnerabilities and potential attack surfaces.

Security Controls and Monitoring: The security metamodel can be leveraged to identify and select appropriate security controls and monitoring mechanisms for technology systems. It helps in mapping security requirements to specific controls, ensuring comprehensive coverage of security risks. The metamodel can also guide the implementation of security monitoring and incident response mechanisms, enabling timely detection and mitigation of security incidents.

Integration and Interoperability: security metamodel provides a structured approach to ensure the harmonious integration of security components and their interoperability across various technology systems in complex technology environments by leveraging the metamodel, organizations can establish consistent security interfaces, data formats, and protocols, enhancing the overall effectiveness of security measures.

4.3.2 Risk Management Frameworks

Stoneburner, Goguen and Feringa (2002) asserts that a Risk Management Framework is a template and guideline used by companies to identify, eliminate and minimize risks. The literature presents a wide range of risk management frameworks. These include;

a) Enterprise Risk Management Integrated Framework

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is a structured and flexible approach for managing security and privacy risks. It includes information security categorization, control selection, implementation, assessment, system and common control authorizations, and continuous monitoring(Prewett&Terry,2018). The RMF can be applied to new and legacy systems, any type of system or technology, and any organization regardless of size or sector. The framework consists of seven steps: preparing the organization, categorizing the system and information, selecting the set of controls, implementing the controls, assessing the controls, approving the system, and continuously monitoring control implementation and risks. The Enterprise Risk Management Integrated Framework from ICOSO is composed of five interrelated components: governance and culture, strategy and objective setting, performance, review and revision, and information, communication, and reporting. These frameworks help organizations identify, manage, and support the achievement of objectives while ensuring a safe and secure environment.

b) The National Institute Of Standards And Technology [NIST] Risk Management Framework (RMF)

The Risk Management Framework (RMF) is a structured and flexible approach for managing security and privacy risks. It involves categorizing information, selecting controls, implementing them, assessing their effectiveness, appointing system and common control authorities, and continuously monitoring. The RMF promotes near-real-time risk management and accountability for controls implemented within an organization's information systems. It can be applied to new and legacy systems, regardless of size or sector. The NIST Risk Management Framework (RMF) consists of seven steps (Stoneburner, Goguen and Feringa,2002). These are:

(1) It starts with essential activities to prepare the organization to manage security and privacy risks

(2) Categorize the system and information processed, stored, and transmitted based on an impact analysis

(3) Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)

(4) Implement the controls and document how controls are deployed

(5) Assess to determine if the controls are in place, operating as intended, and producing the desired results

(6) Senior official makes a risk-based decision to authorize the system (to operate)

(7) Continuously monitor control implementation and risks to the system

c) The ISO 31000 standard Risk management approach

The ISO 31000 is an international standard that provides principles and guidelines for effective risk management. It is applicable to various types of risks, including financial, safety, and project risks, and can be used by any organization (ISO,2002). ISO 31000 offers a centralized and integrated risk management approach, allowing organizations to improve, coordinate, and interoperate their risk management activities. The six-part risk management process includes communication and consultation, scope, context, criteria, risk assessment, risk treatment, monitoring, review, and reporting. It promotes risk awareness, adapts the overall risk management process, and ensures design

quality and efficiency(ISO,2002). It also encourages documentation of activities, results, and decision-making to further improve risk management activities.

d) EU (ITSRM), IT security risk management methodology V1.2

The IT Security Risk Management Methodology (ITSRM²) was developed by the European Commission to establish a risk-based security model. It involves defining the scope and framework, identifying risks based on assets, security requirements, threats, and existing measures, analyzing and evaluating risks, implementing risk treatment measures, and deciding on risk acceptance(Hutchins,2018). The methodology also includes a continuous monitoring and review process, and a risk communication process for exchanging information about risk with stakeholders.

In a nut shell, the above frameworks can be leveraged by Fintechs in managing cyber security threats, operational disruptions, data breaches, and regulatory changes, aiding in risk identification, assessment, monitoring, and mitigation, aligning with regulations, promoting compliance, and fostering innovation in the industry.

5. CONCLUSION

In conclusion, this research paper has delved into the critical realm of Fintech resilience by comprehensively examining security risks and proposing effective risk management strategies. The dynamic landscape of financial technology demands a proactive and vigilant approach to ensure the integrity, continuity, and security of operations. The research paper explores the security landscape within the Fintech sector, identifying and understanding the diverse risks that pose threats to the Fintech Assets.

The paper provides valuable insights into innovative risk mitigation approaches, considering the dynamic nature of the Fintech environment. Special attention is given to the collaborative frameworks that contribute to enhancing the sector's overall resilience.

The study proposes a Fintech Ecosystem Risk Management Metamodel to illustrate the practical application of risk management in addressing security challenges for the sector. By leveraging the metamodel, organizations can establish consistent security interfaces, data formats, and protocols, enhancing the overall effectiveness of security measures. The findings aim to equip industry practitioners, policymakers, and researchers with a nuanced understanding of the interconnected dynamics between security risks and effective risk management in the Fintech landscape. This study recommends that governments and Fintech industry adopt the proposed approach for Fintech risk assessment and management.

FUNDING: This article did not receive any specific grant from funding agencies in the public, commercial or Not for Profit Sectors.

CONFLICT OF INTEREST: AUTHORS DECLARE THAT THEY HAVE NO CONFLICT OF INTEREST.

REFERENCES:

1. Aagedal, J.O., Den Braber, F., Dimitrakos, T., Gran, B.A., Raptis, D. and Stolen, K. (2002).September. Model-based risk assessment to improve enterprise security. In Proceedings. Sixth International Enterprise Distributed Object Computing (pp. 51-62). IEEE.

2. Akanksha, M. (2022).Top 10 Fintech API Security Risks and Challenges. Available at: https://www.valuebound.com/resources/blog/top-10-fintech-api-security-risks-and-challenges.

3. Alijoyo, F.A. (2022). The use ISO 31000: 2018 in Indonesian Fintech Lending Companies: What Can We Learn?. Journal of Business and Management Studies, 4(1), pp.16-22.

4. Alliance for Financial Inclusion(AFI),(2020).Creating Enabling Fintech Ecosystems: The Role Of Regulators.Special Report.

5. Amundrud, Ø., Aven, T. and Flage, R.(2017). How the definition of security risk can be made compatible with safety definitions. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231(3), pp.286-294.

6. Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M.F., (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, p.113580.

7. Asgarkhani, M., Correia, E. and Sarkar, A. (2017). February. An overview of information security governance. In 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (pp. 1-4). IEEE.

8. Callen-Naviglia, J. and James, J.(2018).FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY. Issues in Information Systems, 19(3).

9. Cernisevs, O., Popova, Y. and Cernisevs, D.(2023). Risk-Based Approach for Selecting Company Key Performance Indicator in an Example of Financial Services. In Informatics (Vol. 10, No. 2, p. 54). MDPI.

10. Cobb,M.,(2022).How to perform a cybersecurity risk assessment in 5 steps. Available at: https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

11. CYE.(2022). A Step-By-Step Guide to Cyber Risk Assessment: How to strengthen your security posture and optimize security investments by assessing and prioritizing cyber risks.

12. Dattani, I.(2016).Financial Services and Fintech A review of the Cyber Security threats and implications. Technical Report. Research gate.

13. Dunn Cavelty, M., (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and engineering ethics, 20, pp.701-715.

14. Fenwick, M., and Erik PM V. (2020).Banking and regulatory responses to FinTech revisited-building the sustainable financial service'ecosystems' of tomorrow.: 165-189. Singapore Journal of Legal Studies Mar 2020.

15. Fintech Global (2021).Why risk assessment is important for financial institutions in a digital era. Available at https://fintech.global/2021/03/25/why-risk-assessment-is-important-for-financial-institutions-in-a-digital-era/

16. Gomber,P., Robert J. Kauffman, Chris Parker & Bruce W. Weber.(2018).On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services, Journal of Management Information Systems, 35:1, 220-265, DOI:10.1080/07421222.2018.1440766.

17. Govindraj, B. (2022). Understanding Fintech Security Concerns For A Safer Fintech Ecosystem. Global Business Head Available at: https://www.appsealing.com/fintech-security-concerns/.

18. Gurdip,K., and Arash, H.,L.(2021). Understanding cybersecurity management for FinTech: cybersecurity threats in FinTech (Article 3) Available at: https://www.itworldcanada.com/blog/understanding-cybersecurity-management-for-fintech-cybersecurity-threats-in-fintech-article-3/462547

19. Hamilton.A.(2020). 2020 review:Top five cyberattacks this year. Available at: https://www.fintechfutures.com/2020/12/2020-review-top-five-cyberattacks-this-year/

20. Haneef, S., Riaz, T., Ramzan, M., Rana, M.A., Hafiz, M.I. and Karim, Y. (2012). Impact of risk management on non-performing loans and profitability of banking sector of Pakistan. International Journal of Business and Social Science, 3(7).

21. Hutchins, G. (2018).ISO 31000: 2018 enterprise risk management. Greg Hutchins.

22. IBM.(2023).What are security controls?.Available at: https://www.ibm.com/topics/security-controls

23. Innerhofer-Oberperfler, F. and Breu, R. (2006).Using an Enterprise Architecture for IT Risk Management. In ISSA (pp. 1-12).

24. ISO, (2002). Risk management vocabulary. ISO/IEC Guide 73

25. Kaur, G., Lashkari, Z.H. and Lashkari, A.H. (2021).Understanding Cybersecurity Management in FinTech. Springer International Publishing.

26. Keong, O. C., Leong, T. K., & Bao, C. J. (2020). Perceived Risk Factors Affect Intention To Use FinTech. Journal of Accounting and Finance in Emerging Economies, 6(2), 453–463.

27. Khalil, F. and Alam, H.M.(2020).Identification of Fintech Driven Operational Risk Events. Journal of the Research Society of Pakistan, 57(1), p.75.

28. Krejcie, R. V., & Morgan, D. W.(1970). Determining sample size for research activities. Educational and

psychological measurement, 30(3), 607-610.

29. Kure, H.I., Islam, S. and Razzaque, M.A.(2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), p.898.

30. Lake, A.J.(2013). Risk management in Mobile Money: Observed risks and proposed mitigants for mobile money operators. World Bank.

31. Li, Y. and Liu, Q., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, pp.8176-8186.

32. Lukonga,I.(2018). Fintech, Inclusive Growth and Cyber Risks: A Focus on the MENAP and CCA Regions. IMF Working Paper.

33. Machi, L. A., & McEvoy, B. T. (2016).The literature review: Six steps to success.

34. Maseno, E.M.; Ogao, P. Matende, S.(2017).Vishing Attacks on Mobile Platform in Nairobi County Kenya. Int. J.Adv. Res. Comput. Sci. Technol.

35. Mayer, J. and Fagundes, L.L.(2009). A model to assess the maturity level of the risk management process in information security. In 2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops (pp. 61-70). IEEE.

36. Mehrotra, A. and Menon, S. (2021). Second round of FinTech-Trends and challenges. In 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 243-248). IEEE.

37. Muhn, J. (2020).Cybersecurity: The Hidden Risks of Fintech Services" .Available at https://finovate.com/cybersecurity-the-hidden-risks-of-Fintech-services/. Accessed on 25th-June-2020. [108]NSFOCUS.: 2017 Fintech Security Analysis Report. Available at: https://nsfocusglobal.com/2017-fintech-security-analysis-report/.(2018)

38. Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 96, 227-242.

39. NSFOCUS.(2018).2017 Fintech Security Analysis Report. Available at: https://nsfocusglobal.com/2017-fintech-security-analysis-report/.

40. NSFOCUS.(2018).2017 Fintech Security Analysis Report. Available at: https://nsfocusglobal.com/2017-fintech-security-analysis-report/.

41. Park, J. K., & Kim, I. (2015).A Study of Countermeasure against Security Risk of Fintech Services for Financial Innovation. Knowledge Management Research, 16(4), 35-45.

42. Prewett, K., & Terry, A. (2018).COSO's updated enterprise risk management framework—A quest for depth and clarity. Journal of Corporate Accounting & Finance, 29(3), 16-23.

43. Razzaque, A., Cummings, R. T., Karolak, M., & Hamdan, A. (2020).The Propensity to Use FinTech: Input from Bankers in the Kingdom of Bahrain. Journal of Information and Knowledge Management, 19(1), 1–22.

44. Sampat, B., Mogaji, E., & Nguyen, N. P. (2023).The dark side of FinTech in financial services: a qualitative enquiry into FinTech developers' perspective. International Journal of Bank Marketing.

45. Santa, R. and Carlos, H.,(2014). Physical and Infrastructure Security IT. Computer Science.

46. Stoneburner, G., Goguen, A. and Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), pp.800-30.

47. Tunggal,A.,T.(2023). Cybersecurity:How to Perform a Cybersecurity Risk Assessment (2023 Guide). Available at: https://www.upguard.com/blog/cyber-security-risk-assessment

48. UN (2021).CEPA strategy guidance note on Risk management frameworks.

49. Vellani, K.(2006). Strategic security management: a risk assessment guide for decision makers. Elsevier.

50. Vučinić, M.(2020). Fintech and Financial Stability Potential Influence of Fintech on Financial Stability, Risks and Benefits. Journal of Central Banking Theory and Practice, 9(2), pp.43-66.

51. Wang,J.(2021).4 Security Issues Fintech Firms are Facing. Available at: https://www.imc.edu.au/news-archive/4-security-issues-fintech-firms-are-facing.

52. Whitman, M.E. and Mattord, H.J.(2021). Principles of information security. Cengage learning.

53. World Bank.(2021). Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches. World Bank.