Common Market for
Eastern and Southern Africa

COMESA

COMESA Monetary Institute

SPECIAL REPORT
March 2025

Cyber Security and Digital Banking: Opportunities and Challenges for the Banking Sector in the COMESA Region

Lucas Njoroge, Director COMESA MONETARY INSTITUTE

Contents

Lucas Njoroge
Director, COMESA Monetary Institute

Executive Summary

This article examines opportunities and challenges of digitization and cyber security in the banking sector, in the COMESA region. The article also examines the future of digital banking and cyber security and provides some lessons for banks in the region.

The article observes that rapid digitization has transformed banking from brick-and-mortar branches, into more cost-saving, user friendly and branchless entities, characterized by enhanced convenience, accessibility and great efficiency. However, digital transformation has come with serious cyber risks. Cyber exposure and attacks have increased due to advancement in technology, increased use of computers and mobile phones, and the spread of internet access by customers, among others, across the COMESA region. The frequency and severity of cyber-attacks have also been increasing, leading to greater concerns about the ability of banks in the region, to cope and mitigate these threats. The evolving nature and sophistication of these threats make them even more challenging for banks. The consequences of these cyber risks when they materialize can be devastating and include, among others, huge financial losses, reputational damage, lost relationships and sometimes-legal liability. The deployment of new technologies such as artificial intelligence (AI) by banks in the region has introduced new sources and transmission channels of cyber risks. AI is playing a critical role in both perpetuating and preventing cyber threats, making it a pivotal element for the future of cyber security strategies of banks and financial institutions.

The article notes that banks in the COMESA region cannot avoid competing in the digital space since that is where they can remain profitable. Hence, they face a delicate balance between innovation and cyber security, requiring constant adaptation and investment in robust cyber security technologies. Banks should ensure that cyber security evolves in tandem with technological advances and market demand. This will ensure they can safeguard the trust and reputation that reinforce their role as reliable custodians of both physical and digital financial assets.

The article concludes that collaboration and information sharing, both within a country and internationally, including with technology companies, is essential for cybersecurity. This cooperation enables the early detection of emerging threats and the adoption of best practices, which are critical for mitigating potential cyber risks.

Introduction

All spheres of human life are experiencing the impact of digital transformation. From baby monitors, doorbells, security cameras, smart home assistant, smart watches/toys to WIFI routers, digitization is almost everywhere, with many diverse products connected to the internet. In banking, rapid digital transformation has ushered in a paradigm shift, resulting in enhanced convenience, accessibility and great efficiency. Digitization has transformed banking from brick-and-mortar branches into more cost-saving, customer friendly and branchless entities. From the comfort of a mobile phone, digitization has enabled customers to perform nearly any banking transaction, from sending and receiving, to borrowing and saving money. More and more transactions are taking place online as people go cashless, and the use of digital money like debit or credit cards, internet banking or use of digital wallets, are spontaneously increasing. Currently, it is almost normal to withdraw or deposit money from and or to the bank to and or from a digital wallet, or pay bills online, which was impossible a decade or so ago. The potential array of banking services that can be available through digitization is growing daily, setting the stage for limitless possibilities. The consequence of this increased digitization is infinite possibilities for enhanced customer experience and new revenue streams for banks.

However, digital transformation has come with serious cyber risks. Whether a digital only bank or a bank with physical branches, the challenge of cyber risk is real. Cyber exposure and attacks are increasing due to among other reasons, banks increasing reliance on technology to do business, increased use of computers and mobile phones and the spread of internet access by customers across almost all jurisdictions in the COMESA region. The increasing cyber risks, which refers to the potential threats and vulnerabilities faced by banks in the digital space, must be mitigated or contained, by ensuring cyber security. Cyber security entails a set of technologies and methods designed to protect against unauthorized access, cyber-attacks and data breaches. The primary goal of cyber security is to safeguard customer assets, banks intangible assets such as goodwill, among others (Interpol, 2024).

The evolving nature and sophistication of these threats make them even more challenging for banks. In addition, the frequency and severity of cyber-attacks

have been increasing, leading to greater concerns about the ability to cope and mitigate these threats by protecting banks systems and customer data. The consequences of these cyber risks, when they materialize, can be devastating. They include, among others, huge financial losses, reputational damage, lost relationships and sometimes-legal liability. For instance, the February 2016 Central Bank of Bangladesh heist where hackers exploited the vulnerabilities of SWIFT electronic payment processing system, attempting to steal US dollars 1 billion and got away with US dollars 101 million (Etoom, 2023).

The cyber security threat across many jurisdictions is not a matter of if it will happen but when it will happen, especially given the ever-evolving sophistication of cyber risks. To the extreme, there are concerns that a major cyber incidence can lead to a system-wide financial instability. The Financial Stability Board for instance, warned, "a major cyber incidence, if not properly contained, could seriously disrupt financial systems including critical financial infrastructure leading to broader financial stability implications" (Maurer and Nelson, 2021). A number of studies conducted in this area find that cyber risks significantly affect financial performance and reputation of banks. Bouveret (2018) finds that cyber-attacks lead to reputational damage and loss of customer trust, while Adria and Ferreira (2023) find cyber-attacks in banks were increasing significantly leading to decline in financial performance of banks.

This article examines opportunities and challenges of digitization and cyber security in the banking sector, in the COMESA region. The article also examines the future of digital banking and cyber security, and provides some lessons for banks in the region.

Key Drivers of Digitization and Cyber Risks

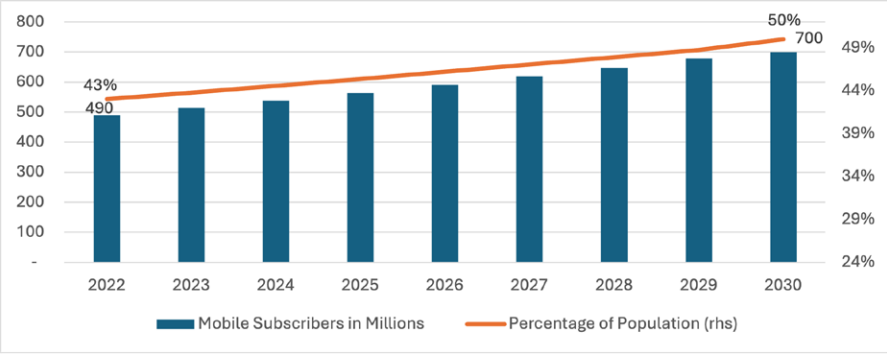
Advances in technology, increased use of computers and gadgets connected to the internet are the main drivers of digital transformation in banks. The resultant interconnectedness between people, machines and the internet imply that the majority of today's data breaches result from human error, making cyber security a people centered problem as well as a technology issue. Unprotected mobile applications and computers or unencrypted data are sources of vulnerability to cyber-attacks. In addition, regulators' intensified focus on consumer data protection and the rising value of non-physical assets

are also driving digitization.

Intense competition to innovate is also driving digital transformation where banks compete with technology companies and technology companies compete with banks. At the same time, malicious actors and hackers are also taking advantage of this digital transformation, trying to innovate and stay ahead with the technology, posing serious cyber security risks. In addition, when digital developments progress faster than adoption and implementation of cyber security laws and regulations, cyber criminals exploit this lacuna, significantly increasing cyber risk.

Advancement in technology and the subsequent digitization of banking has seen banks change their business models to bring on board new types of interactions with customers and other stakeholders, expanding business opportunities and growth. Digital transformation in banking is being driven, by among others, the improved mobile connectivity across the sub-Saharan Africa (SSA) in general, and in the COMESA region in particular. There has been a steady growth of mobile subscribers in SSA for the past 7 years and it is projected to reach over 700 million people, with a mobile penetration of over 50 percent by 2030 (Figure 1).

Figure 1: SSA mobile subscribers and penetration, millions, % of population



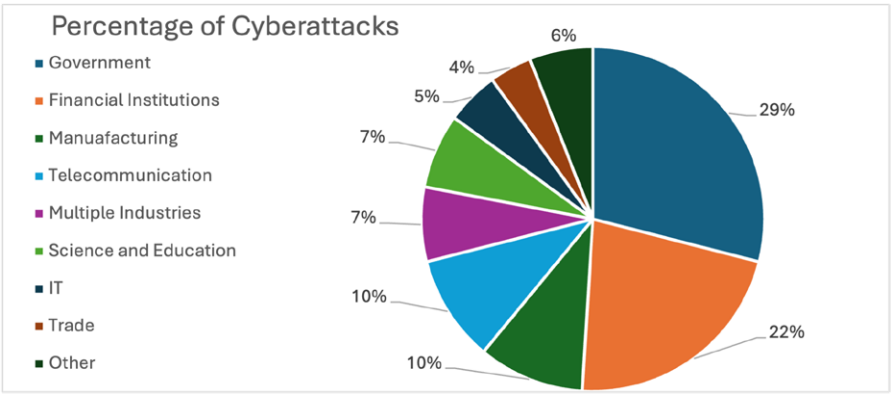
Source: The Mobile Economy SSA (2023), GSMA Intelligence

The subsequent digital transformation has meant that the amount of valuable and sensitive information stored and transmitted digitally has increased

tremendously, making banks prime targets for cyber criminals. For COMESA region, less attention is paid to the growing number of attacks on softer targets, yet digitization is playing a phenomenal role for the push towards greater financial inclusion, with countries making great strides through digital financial services such as mobile payment systems.

Cyber criminals are constantly developing new and more sophisticated methods to circumvent security measures, posing an ever-fluid security situation, which banks find challenging to cope with. Cyber-attacks are therefore becoming more frequent and are growing in volume and scale, threatening every aspect of banking (Bouveret, 2018). In Africa, financial institutions and especially banks that constitute the largest segment of the financial systems are the key targets of cyber-attacks after the governments (Figure 2). Breaches can lead to significant financial losses, identity theft, and the disruption of critical services such as online banking, payments, and trading platforms. Additionally, the interconnectedness of global financial markets means that a single successful attack on one institution can have a ripple effect, potentially leading to systemic risks.

Figure 2: Africa's categories of victim organization Q1 2023 to Q3 2024



Source: https://global.ptsecurity.com/analytics/cyber security-threatscape-2024-q3

The motives for cyber-attacks are diverse and include the following, among others: Financial gain remains a major motive with criminals moving from the streets to cyber-attacks and ransom demands. Besides making money, some threats actors/criminals are purely engaging in the vice to cause disruptions and destruction, while others who steal also learn about financial system's

networks and operations, which give them an upper hand to even cause more harm in the future or sell such knowledge and capabilities to others. In other cases, some states and states sponsored actors motivated by geopolitical and ideological reasons may cause disruption, destruction, damage, espionage or even financial gain. In other cases, terrorist groups, hacktivists or insider threats may be motivated by either ideological or discontentment, or simply the need to cause mayhem. This rapidly evolving risk landscape is putting banks under enormous pressure to put hackers/criminals at bay. Political conflicts are also leading to a rise in cyber-attacks as warring factions attempt to outsmart each other in cyber space in order to cause harm and disruption of services.

Types of Cyber Security Risks

Digitization has expanded the need for security, continuity and resilience especially for banks where IT is a top priority and at the center of almost all operations. Security considerations range from preserving data confidentiality, maintaining core applications and networks to managing organization risk and exposure including cyber resilience and readiness to face attacks, to concerns about systemic risks that could threaten overall financial stability and the economy. Digitization also presents new risks as financial sector players compete for visibility across their traditional and cloud environment, requiring extremely well-defined access controls and owners. Digitization enables new types of interactions in banks with customers, partners and other stakeholders. Together with unsafe internet connections, these new connections also mean new external threats and elevated cyber risks.

Cyber risks can range from cyber-attacks on banks infrastructures and networks to data breaches, phishing attacks, malware, to theft of sensitive customers information. Cyber-attacks can target internal systems through for example, ransomware or external infrastructures damaging interbank online services. Outsourcing to service providers who sometimes operate for many other institutions can become vectors of contamination in the event of a cyber-incidence. The main cyber security risks that bear the biggest threats to the banking sector are summarized in Figure 3 and a brief on each provided below:

Malware and ransomware are cyber risks where attackers infect computers with malicious software and restrict access to some data using encryption. Then,

they ask for money that the bank must pay to earn access to the restricted data.

Figure 3: Threats to cyber security of banks

Spoofing consists of creating a fraudulent version of an actual domain or website appearing legitimate meant to trick users into giving away login credentials and personal information. Phishing and social engineering aims at extracting confidential information such as passwords and credit card numbers by posing as a reliable entity, and entails spread of malicious software through persuasive tricks requesting unsuspecting computer users to install the software under false pretense that it is an official bank correspondence. Through phishing, attackers use disguised emails or domain to trick individuals into downloading infected software or to give away personal credentials. Through social engineering, individuals are tricked into giving very sensitive details and credentials to attackers or through sending bogus invoices that purport to be from trusted sources. Through the two approaches, criminals are able to access financial information and steal money from customers' accounts. Similarly, cyber criminals may get hold of login credentials that provide access to insider information including customer data. Third parties' breaches refer to cases where hackers target less secure shared banking systems and third parties, to gain unauthorized access.

Unencrypted data is when sensitive financial information is exposed to interception and exploitation by cybercriminals. Without encryption, data

transmitted between users and banking platforms, such as account details, passwords, and transaction history, can be easily accessed, manipulated, or stolen. This exposes both customers and financial institutions to fraud, identity theft, and unauthorized access, undermining trust in the digital banking system. As more people rely on online banking services, the importance of securing data through robust encryption methods becomes increasingly crucial to safeguarding financial assets and ensuring the privacy of personal information. One form or the other of these attacks have happened in different jurisdictions in the COMESA regions. A brief on a few examples of cyber-attacks in the region are contained in Table 1:

Table 1: Cyber-attacks examples in the region

Date	Source	Country	Effect
1. February 2024	DDoS (distributed denial of services) attack on the largest mobile networks, MTN and Airtel	Uganda	Caused a major disruption of operations
2. First half 2024	4,623 attempted cyber-attacks both on government and private enterprises	Ethiopia	Causing disruptions of activities on Government and private enterprises
3. July 2023	Government online platform - eCitizen suffered a DDoS attack	Kenya	Key services were unavailable, including those related to obtaining passports, visas, driver's licences etc.
4. November 2023	Cyber-attack on Fawry – a leading provider of e-payment and digital financial solutions	Egypt	Resulted in leak of personal data on the company's clients, including addresses, phone numbers, date of births etc.

Source: Author's compilation from various sources

At the continental level, over the past five years, Africa has experienced a significant increase in cyber-attacks, both in volume and in terms of financial impact. According to Interpol, nearly half of the African countries reported ransomware attacks against their critical infrastructure in 2023 (Interpol, 2023). In addition, Check Point showed a 20% increase in cyber-attacks on enterprises in Africa during the first quarter of 2024 compared to the first quarter in 2023 (Check Point, 2024).

The financial repercussions of cyber-attacks can be severe. Interpol indicated that the average cost of a ransomware attack globally reached USD 5.13 million in 2023, a 13% increase from 2022. The United Nations Economic Commission for Africa (UNECA) also reported that the continent's inadequate preparedness for cyber threats resulted in an average loss equivalent to 10% of GDP per country (UNECA, 2022). Similarly, at an industrial level, a large-scale cyber incidence in the banking sector can have significant systemic implications, potentially leading to economy-wide financial disruption and financial instability (Kopp *et al*, 2017). These statistics highlight the pressing need for enhanced cyber security measures across Africa, inclusive of the COMESA region.

The Key Challenges to Cyber Security

Cyber risks pose a potential threat to security, resilience and trust underpinning the credibility of the banking system. Some of the challenges for cyber security for digital banking include the following:

Cyber criminals are employing increasingly sophisticated cyber-attacks to breach banking systems by ensuring that they stay ahead as regulations lag behind cyber security innovations. Another challenge relates to third party risks brought about by the interconnected nature of modern banking system where banks must collaborate with third-party vendors, fin-tech companies and other partners. This interconnectedness introduces additional cyber security challenge where weakness in the security practices of third-party entities become the point of vulnerability for cyber-attack for the entire system. It is therefore a daunting and complex task to ensure third-party entities adhere to stringent security standards and best practices. Digital banking has also come with new demands requiring banks to navigate complex compliance requirements including data protection, Anti-Money laundering/Countering the Financing of Terrorism (AML/CFT) laws, and customer authentication protocols. Non-compliance by banks leads to penalties, eroding customer trust and loss of reputation.

Another challenge relates to inadequate user authentication where the traditional methods like use of usernames and passwords are increasingly vulnerable to cyber-attacks, forcing banks to adopt multi-factor authentication (MFA) to deal with unauthorized access to bank systems. However, MFA may not have the best user experience for the customers, calling for striking the right

balance between security and user experience. Banks also face insider threats where employees with access to sensitive systems and data inadvertently cause security breaches.

Integration of emerging technologies such as artificial intelligence (AI) present opportunities including enhanced customer experience and operational efficiency. However, these technologies pose serious cyber security challenges, with criminals being able to manipulate AI to get sensitive information from unsuspecting customers. In addition, the demand for skilled cyber security professionals far outpaces the supply, which complicates efforts to maintain robust cyber security defenses, to deal with the ever evolving and complex cyber security space. Lack of the necessary infrastructure and technical capabilities to effectively monitor and respond to cyber threats, hinders the ability to implement and maintain robust security measures. In addition, limited understanding of cyber risks among individuals and businesses leads to vulnerabilities. Finally, there is lack of comprehensive and harmonized cyber security laws across the African continent, which makes rapid response to cyber-attack challenging. Another challenge facing banks is the need to keep up with the rapid pace of technological change in the cyber security space, as threats evolve on a continuous basis.

Future of Digital Banking and Cyber Security

The current advances in computing, data storage power and application of big data has seen the deployment of Artificial Intelligence (AI) in many spheres of life including digital banking and cyber security (Doerr, *et al*. 2021). The deployment of AI in the banking sector can facilitate gains in efficiency, cost saving, enhance forecasting accuracy and better monitoring of market sentiments, and improved risk management and compliance. AI has the potential to strengthen monetary and prudential oversight, help improve understanding of economic and financial developments, strengthen systemic monitoring and help predict the buildup of systemic risks and speed up crisis response. AI can ensure better internal controls including better monitoring of internal operations and more efficient resource allocations. However, risks of AI application abound. They include embedded bias and inherent opaqueness, creating new sources and transmission channels of systemic risks including greater homogeneity in risk assessment and credit decisions and rising interconnection that could amplify

shocks. Other serious limitations of AI include data biases and concerns that sudden structural shift in data from unforeseen events could lead to unreliable predictions by AI systems.

AI adoption also comes with new unique cyber risks that exploits inherent limitations of AI algorithms. Attackers attempt to evade detection and prompt AI to extract wrong information. This undetected data poisoning entails adding wrong information at the training stage of AI algorithms, which leads to wrong analysis and projections. Such outcomes undermine the financial sector's capacity to accurately assess, price and manage risks, which could lead to the buildup of unobserved systemic risks. Besides, AI systems are also vulnerable to cyber-attacks, where attackers can gain access to sensitive financial and personal information, just like any other IT (information technology) system. Ultimately, this erodes the integrity and trust of the AI system application and use, leading to reputational and financial losses for financial institutions (McKinsey, 2020).

AI can support sophisticated cyber-attacks with attackers leveraging its potential for social engineering and phishing, reconnaissance and exploitation. For instance, cyber-attackers are able to come up with more convincing phishing emails/messages to improve their hacking. The attackers can even be able to reverse-engineer AI models, circumventing their guardrails and utilizing

them with malicious intent to conduct successful operations. On the contrary, also, AI can help in creating cyber resilience and counter cyber-attacks very effectively. For instance, AI can support threat intelligence in collecting and analyzing data to prevent and detect cyber-attacks by identifying anomalies in user system and network behaviors in real time (ECB, 2024). AI is hence playing a critical role in both perpetuating and preventing cyber threats, making it a pivotal element for the future of cyber security strategies of banks and financial institutions.

A delicate balance between innovation and cyber security will therefore shape the future of digital banking, as cyber-attacks continue to pose significant threats. As financial institutions expand their digital offerings, they must invest in robust cyber security measures to safeguard sensitive customer data and financial transactions. For instance, Wilson et al (2019) finds that regulatory frameworks with inbuilt penalties for non-compliance can incentivize banks to invest in cyber security. AI technology will play a key role in this evolution, providing advanced tools for real-time threat detection, fraud prevention, and personalized customer services. AI will help identify unusual patterns, detect vulnerabilities, and respond to threats quickly, reducing human error and response times. However, the increasing sophistication of cyber-attacks will require constant adaptation and investment in AI-driven solutions to stay ahead of criminals. Overall, the integration of AI will not only enhance operational efficiency but will also be critical in securing the digital landscape of banking, fostering trust among customers.

Policy Implications and Lessons for COMESA Member Central Banks

Banks in the COMESA region cannot avoid competing in the digital space since that is where they can remain profitable. However, the implied eminent cyber security risks that come with digital transformation require banks to strike a balance of risk versus opportunity. Digitization requires banks in the COMESA region to change and consider (if they have not already) embracing the following, among others:

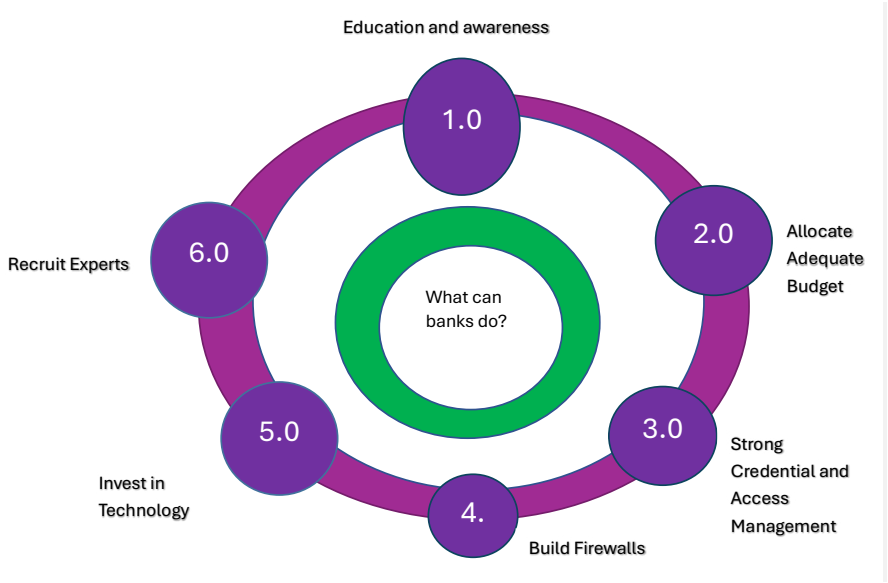
On a continuous basis, banks need to conduct security audits to identify vulnerabilities within their existing systems and pave the way for the deployment of enhanced firewalls, update of antivirus, automatic logout features and anti-malware applications that would effectively create a robust barrier against cyber-

attacks. Banks need to adopt integrated advanced technologies, implement robust security measures and ensure enhanced awareness of regulatory requirements. They need to implement MFA such as, use of passwords, fingerprints or security tokens, to access sensitive information and systems.

Banks should also encrypt all sensitive data to protect it from unauthorized access. Adoption of MFA and biometrics can provide another layer of technology solution of security firewalls. They need to adapt and innovate cyber security defenses that will keep them ahead of the cyber criminals. Banks must ensure that cyber security evolves in tandem with technological advances and market demand. This will ensure that banks can safeguard the trust and reputation that reinforce their role as reliable custodians of both physical and digital financial assets.

Further, banks need to implement a robust cyber security framework covering all aspects of their operations, from network security to incidence response based on the industry standards and best practice such as ISO 27001. They also need to keep updating, testing and monitoring their security systems and protocols to stay ahead of security incidents. Since effectiveness of any measures depends on a bank's ability to respond to potential threats in real-time, banks need to continuously invest in cyber security technologies such as building firewalls, intrusion detection systems and encryption technologies. Banks need to adopt cloud solutions for better scalability and operational efficiency. Enhanced cloud security protocols and hybrid architectures need to be developed, to protect sensitive data outside traditional banking infrastructure. A summary of some solutions that banks in COMESA can implement to prevent cyber-attacks are in figure 4:

Figure 4: Key solutions to cyber security by banks



There is a need to build an effective risk management framework that can identify, assess and manage cyber risks. The framework should have a risk mitigation plan that includes, among others measures, technical controls, security policies and procedures, incident response plans and where possible, cyber security insurance to mitigate the financial impact of cyber incidence. All such measures require adequate budget allocation. Banks need to have a thorough vender evaluation program to ensure that third party venders comply with banks' stringent security standards.

The solution to cyber security goes beyond Information Technology (IT) systems and involves changing people's culture driven by continuous awareness and education programs, prioritizing secure actions and decisions and making employees and customers aware. Banks should make employees understand why cyber security matters to them and to the institution, and why it is to their benefit. Hence, an effective cyber security program needs to, among others, change employee's behavioral psychology through persuasive tactics and techniques that get employees invest in cyber security, make them more receptive to the learning or increase awareness of activities being implemented, which will effectively deal with insider cyber security threats.

The priority should be to cultivate a culture of cyber security awareness, to be able to recognize and avoid risky situations and take action to mitigate cyber threats. These measures will result in a strong security posture and early recognizing potential threats. In addition, customers have an equally important responsibility for ensuring cyber security. Reusing passwords or opening suspicious emails can result in losing financial data. Through awareness programs, banks should make both employees and customers to be cyber security agents, in order to create a formidable human firewall capable of spotting and preventing even the most sophisticated cybercrime attempts and breaches, putting at bay 95 percent cyber threats associated with human error.

Banks should invest in training and mentorship programs to develop a skilled cyber security workforce while implementing robust cyber security frameworks and legislation that can deter cybercrime. Regular staff training to raise awareness on how to identify and prevent security threats and respond to potential cyber threats is critical. In addition, there is need to build the capacity of the cyber security workforce with the requisite advanced cyber security technology both at the level of banks and sector-wide to expand the entire financial sector's cyber security capacity and safeguard gains in financial inclusion that have resulted from the digital transformation. Maintaining progress in financial inclusion requires strengthening connections between financial inclusion and cyber security by among others, establishing teams of experts focusing on both.

At country or institutional level, even when banks have the financial resources to build the requisite firewalls, implement technical solutions and abide with necessary regulations, these measures may not be enough to fight cyber risks and serve as a guarantee against the growing cyber risks. Cooperation between institutions in a country including technology companies on cyber security will overcome the concerns that individual banks or institutions working in silos and in a fragmented nature. With the banking sector constituting the largest segment of the financial sector in most countries in the COMESA region, national intelligence gathering should include cyber threats to this sector and should be shared with all stakeholders in a country. Banks also need to collaborate with the regulator and other stakeholders in order to remain current on any new threats and regulations related to cyber security. For instance, Etoom (2023) finds that collaboration between banks, regulators and other stakeholders,

and implementing comprehensive cyber security framework including regular assessments and employee training are essential for effectively combating cyber threats and significantly reducing the impact of cyber risks on banks.

'Central Banks in the region could consider developing regional cybersecurity standards and establishing information sharing mechanisms', COMESA Committee of Central Banks' Governors

The COMESA Committee of Central Banks echoed similar sentiments during their symposium in 2024. Governors noted that Central Banks in the region could consider developing regional cybersecurity standards and establishing information sharing mechanisms. This is in addition to building cyber resilience through continuous monitoring and testing, e.g. establishing a COMESA Cyber Threat Intelligence Center and harmonized regulatory framework for fintech and digital banking. They also observed the need to foster innovation while managing risks through creating regulatory sandboxes and innovation hubs, balanced approach to fintech regulation and encouraging responsible innovation, and strengthening digital capabilities through capacity building of staff in cybersecurity, investing in advanced data analytics and incrementally modernizing IT infrastructure. In addition, governors observed the need for adopting collaborative approaches with regulated financial institutions at regional and international levels on digital banking policies and Public Private Partnerships for cybersecurity; and the need for carrying out a collaborative benchmarking exercise to identify IT and cybersecurity skills gaps in the region, to facilitate possible exchange programmes[1].

At the international level, there is a need for collaboration and sharing of information to ensure early detection of emerging threats and best practices, critical for mitigating potential cyber risks. There is need for cooperation between African nations that can lead to sharing of expertise, best practices, and coordinated responses to cyber threats. To this end, the recent declaration by African leaders emphasizing the importance of cybersecurity and commitments to strengthening regional cooperation in combating cybercrime and the African Union Convention on Cyber security and Personal Data Protection (Malabo Convention) that advocates for a legal framework to promote cyber security standards across Africa, are significant steps in the right direction (Nathaniel, 2021).

1 Report of the 2024 Symposium of Governors of COMESA Central Banks.

On the role of AI in digital banking and cybersecurity, AI is playing a dual role, through cybercriminals launching sophisticated attacks and cybersecurity experts countering these threats. Hackers and criminals are leveraging on AI to cause more serious and sophisticated cyber-attacks. Thus, banks need to continue investing in AI for better threat detection and collaborating with the regulator to comply with cybersecurity standards. Banks should also maintain vigilance and adopt AI strategies that will ensure they stay ahead of cybercriminals. The deployment of AI will help detect unusual patterns and behaviors that indicate potential threats. AI is proving invaluable in real-time monitoring, predictive analysis and automated responses to security incidences, significantly reducing the response time and the potential for human error.

Conclusion

Banks digital transformation has made the relationship between innovation and responsibility strikingly evident. Banks in the COMESA region therefore need to remain steadfastly vigilant, unfailingly adaptable and perpetually innovative to protect customer data from cyber-attacks. They should adhere to stringent regulatory frameworks and safeguard the bedrock of trust upon which banks reputation is built. This calls for a robust cybersecurity strategy that prioritizes a multifaceted approach, continuously investing and implementing innovative technologies and solutions and nurturing talent, to ensure an invisible fortress against the ceaseless waves of cyber threats. Banks also need to address cybersecurity risk more holistically, more aggressively integrating it into their risk management frameworks. Banks have an obligation to ensure that they can withstand, respond to and recover from all types of information and communication technology (ICT) related cybersecurity threats.

Moreover, banks in the region should endeavor to incorporate cyber risks and other threats into their overall business strategy and not to be seen to have knee jack reactions to the latest cyber "scare". This should entail developing robust cybersecurity frameworks that include regular assessments, employee training, incidence response planning and use of the latest security technologies. The need for collaboration between various actors including the regulator, government intelligence arm, banks and other financial sector players are critical in neutralizing cyber threats effectively. This will ensure that banks remain resilient in the face of cyber threats, ensuring that banks

remain secure and dependable, trusted and reliable amidst the fast-changing digital revolution. It is also important for banks to keep ahead of the game with innovative solutions to counter what criminals are innovating.

Banks in the region need to expand cybersecurity framework requirements to cover AI specific cyber threats and implied mitigation strategies. This includes an assurance that AI algorithms are robust enough to build public trust in AI driven financial system and safeguard financial stability and integrity of the financial system. The use of AI by both banks and hackers adds a layer of complexity, requiring continuous vigilance, relentless efforts and innovation, and adaptation, in this race against time and technology. Banks must thoroughly assess and address the security implications of adopting AI technologies.

Central banks' role in combating cyber threat entails developing clear guidelines and standards for banks to follow, based on international best practice and fostering information sharing between central banks. Central banks should consider collaborating at the regional level in developing regional cybersecurity standards and establishing information sharing mechanisms. They should also consider strengthening digital capacities through skills-development and fostering innovations in the context of balanced regulatory environment to mitigate cyber risks. Regular assessments and updates of guidelines to keep up with the ever-evolving cyber threats should be a priority.

Reference

Adrian, T., Ferreira, C. (2023). "Mounting Cyber Threats Mean Financial Firms Urgently

Need Better Safeguards", *https://www.imf.org/en/Blogs/Articles/2023/03/02*.

Africa Center (2023). https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Tomslin Samme-Nlar (2020)., "Cyberspace Security in Africa – Where do we stand?" *African Academic Network on Internet Policy*, February 12, 2020.

Alonso, C., A. Berg, S. Kothari, C. Papageorgiou, and S. Rehman. (2020)., "Will the AI Revolution Cause a Great Divergence?" *IMF Working Paper 20/184*, International Monetary Fund, Washington, DC.

Bouveret, A. (2018). "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment", *https://www.imf.org/en/Publications/WP/Issues/2018/06/22*.

Check Point. (2024). "*Cyber security Threat-Scape for African Countries: Q1 2023–Q3 2024",* https://global.ptsecurity.com/analytics/cyber security-threatscape-for-african-countries-q1-2023-q3-2024

Doerr, S., L. Gambacorta, and J. M. Serena, (2021). "Big Data and Machine Learning in Central Banking." *BIS Working Paper 930*, Bank for International Settlements, Basel.

ECB (2024). "ECB to stress test banks' ability to recover from cyber-attack", *Press Release, 3, January.*

El Bachir B., Ghiath S., Khaled A., Jose D., Aquiles F., Ebru S., Alin T., and Rangachary R. (2021). "Powering the Digital Economy : Opportunities and Risks of Artificial Intelligence in Finance." *IMF Working Paper DP/2021/024*, International Monetary Fund, Washington, DC.

Etoom, A. (2023). "Strategizing cyber security: Why a risk-based approach is key", *https://www.weforum.org/agenda/2023/04.*

INTERPOL. (2024). *African Cyberthreat Assessment Report 2024. https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf*

Kopp, E., Kaffenberger, L., and Wilson, C. (2017). "Cyber Risk, Market Failures, and Financial Stability", *https://www.imf.org/en/Publications/WP/Issues/2017/08/07.*

Maurer, T., and Nelson, A., (2021). "The Global Cyber Threat", *Finance and Development*, March 2021.

McKinsey. (2020). "AI-Bank of the Future: Can Banks Meet the AI Challenge?" *https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai challenge.*

Nathaniel, A., (2021) "Africa's Evolving Cyber Threats", *Africa Center for Strategic Studies, https://africacenter.org/spotlight/africa-evolving-cyber-threats/*

United Nations Economic Commission for Africa (UNECA). (2022). "*Cyber security in Africa: Challenges and Opportunities", https://www.uneca.org.*

COMESA SECRETARIAT
COMESA Center
Ben Bella Road
P.O. Box 30051
Lusaka Zambia

+260 211 229 725

www.comesa.int

info@comesa.int

facebook.com/ComesaSecretariat/

@comesa_HQ

Comesasecretariat