FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Cyber Threats to the Financial Sector in Africa

An Assessment of the Current Threat and an Analysis of Emerging Trends on the Future Threat Landscape

MARCH 2022

WORLD BANK GROUP

ACKNOWLEDGEMENTS
This report was prepared by Robert Dartnall, Kit Palmer and Wiebe Ruttenberg from Security Alliance, with guidance from Dorothee Delort (World Bank) and the assistance of Renuka Pai, under the leadership of Mahesh Uttamchandani and Harish Natarajan (World Bank Group, Finance, Competitiveness and Innovation Global Practice), in the context of the Financial Inclusion Global Initiative Working Group on cybersecurity (under the Security and Trust Working Group).

The authors thank Zafer Mustafaoglu and Siegfried Zottel (World Bank Group, Finance, Competitiveness and Innovation Global Practice) and Emran Islam (International Monetary Fund) for their review of the paper and their input.

The interpretations and conclusions expressed in this work belong to the authors and do not necessarily reflect the views or positions of either the World Bank Group, its Board of Executive Directors, and the governments they represent, or the Bill and Melinda Gates Foundation.

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW, Washington, DC 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

DISCLAIMER
The Financial Inclusion Global Initiative led in partnership by the World Bank Group (WBG), International Telecommunication Union (ITU), and the Committee on Payments and Market Infrastructures (CPMI), with the support of Bill & Melinda Gates Foundation (BMGF). The FIGI program funds national implementations in three countries (China, Egypt, and Mexico), supporting topical working groups to tackle 3 sets of outstanding challenges in closing the global financial inclusion gap, and hosting 3 annual symposia to gather the engaged public on topics relevant to the grant and share intermediary learnings from its efforts.

This work has been prepared for the Financial Inclusion Global Initiative by the Cybersecurity for FMI's Workstream of the FIGI Security, Infrastructure and Trust (SIT) Working Group The work is a product of the staff of the World Bank with external contributions prepared for the Financial Inclusion Global Initiative. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including The World Bank, its Board of Executive Directors, or the governments they represent, or the views of the Committee for Payments and Market Infrastructure, International Telecommunications Union, or the Bill & Melinda Gates Foundation.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Table of Contents

Abbreviations and Acronyms ii

Executive Summary 1

1. Introduction 3

2. Baseline Assessment 5

   2.1 Threats to Integrity 6

   2.2 Threats to Availability 9

   2.3 Threats to Confidentiality 12

   2.4 Baseline Assessment 13

3. Emerging Trends and the Future Threat Landscape 14

   3.1 Technological Factors 14

   3.2 Socioeconomic Factors 17

   3.3 Geopolitical Factors 18

4. Recommendations for Central Banks and Financial Authorities 20

   4.1 Strengthening Cyber Resilience of Financial Entities and the Financial Sector at Large 20

   4.2 Understanding and Strengthening the Financial-Sector Supply Chain 21

   4.3 Strengthening Cyber Resilience and Supervisory Capacity of Central Banks and Financial Authorities 21

   4.4 Strengthening Cyber Resilience of Government and Society at Large 22

   4.5 Actively Seeking Regional Cooperation 23

5. Conclusion 24

Appendix A **Definitions** 26

Appendix B **Case Studies** 28

References 31

Endnotes 37

Boxes

Box 1: List of Relevant International Guidance/Standards 21

Box 2: Role of National Cybersecurity Center and Computer Emergency Response Team 22

Abbreviations and Acronyms

CERT	computer emergency response team
DDoS	distributed denial of service
DoS	denial of service
FSI	financial-service institution
NCSC	national cybersecurity center
OCG	organized criminal group

Executive Summary

This paper provides an intelligence-led analysis of the current threat landscape for the financial-service sector across Africa, and an assessment of future trends.

African financial-service institutions currently face a significant threat from organized criminal groups and financially motivated nation-states conducting ***high-value thefts in heist-style*** operations. These operations build on previous successes against similar systems in the now-more-cyber-mature developed world and focus on exploiting generally inadequate cybersecurity controls to manipulate the integrity of payment-processing mechanisms and internal security controls. Malicious insiders have also shown the intent and capability to leverage privileged knowledge and system access and steal from their employers.

Ransomware also presents a prominent and growing threat, given its detrimental impact on the availability and confidentiality of critical systems and data. A growing number of organized criminal groups and individual hackers are showing both the intent and capability to direct this activity against African financial-service institutions; the majority of these attacks opportunistically take advantage of security issues and infrastructure vulnerabilities.

Furthermore, African financial-service institutions are also heavily affected by the ***large volume of low-sophistication scams***, thefts, and fraudulent activity directed against their customers. Scams harming victims abroad may also deter foreign investment, to the detriment of Africa's long-term economic potential. Such scams generally originate from domestic grassroots actors, likely compounded by socioeconomic factors such as unemployment and economic inequality.

Next to that, African financial-service institutions are currently experiencing ***high levels of espionage and data theft*** from nation-states, organized criminal groups, insiders, and individual hackers. Although these types of attack have fewer immediately tangible impacts than direct theft or extortion attempts, they can cause future issues, such as loss of competitive advantage or loss of customer trust. African financial-service institutions also face a small but growing risk of ***supply-chain compromise*** from the increasing use of third-party entities within the financial-services infrastructure, expanding the general attack surface.

Looking forward, the following emerging trends can be identified:

Large-scale rapid digitalization of financial products provides ***new avenues of opportunity for threat actors***. Greater levels of digitally enabled financial inclusion, coupled with customers who are unfamiliar with those products and services, open up new targets for scammers.

Digitalization also comes with an expanded supply chain, which will provide threat actors with new access vectors.

Short-term economic challenges will increase the ***attractiveness of cybercrime for the young and unemployed***. However, sporadic introduction and lax enforcement of cybersecurity regulations will not deter domestic cyber activity over the short to medium term. On top of that, increased security in the developed world will increase Africa's attractiveness to an array of threat actors.

Finally, it is to be expected that ***Africa's increasing geopolitical relevance*** will incite more targeting from nation-state threat actors.

The challenge of coping with the serious cyber threats facing Africa's financial sector—and, with it, society in general—is not borne by Africa's banks, payment service providers, and financial infrastructures alone; financial authorities (including central banks) and governments can help address these challenges by focusing on improving the cyber resilience of both individual financial entities and the financial sector as a collective, on strengthening the cyber resilience and supervisory capacity of central banks and financial authorities, and ultimately on bolstering the cyber resilience of African society at large. Central banks and financial authorities should also actively seek to cooperate with their peers in neighboring countries.

With regards to improving the cyber resilience of individual financial entities and the financial sector as a collective, it is recommended that authorities publish more specific ***operational guidelines and cyber resilience expectations*** to help financial entities and their relevant authorities to implement and assess the appropriate cyber resilience measures. Next to that, it is recommended that the responsible authorities invite systemically important financial entities to engage in ***threat-led penetration testing*** and team up in a ***cyber information and intelligence-sharing initiative***. The wheel does not need to be invented again; practical examples of these three recommendations have been published or implemented by other international authorities.[1]

The responsibility for being cyber resilient and having enough cyber capabilities does not lie with the private sector alone; central banks and other financial authorities also have to play their part. Therefore, ***central banks and other financial authorities must comply with their own guidelines and expectations***, especially as most central banks are also RTGS payment system operators and thus engage in activities covered by these guidelines and expectations. Furthermore, it will greatly contribute to the cyber capabilities and cyber resilience of the central bank if the senior managers of the supervision, oversight, payment systems, and information systems departments engage in ***structured internal dialogue***, to learn from each other and contribute to each other's policy and operational objectives.

Some of the cyber threats faced by Africa's financial sector can be addressed only by government action. On the preventive side, it is recommended that central banks call for—and contribute to—more focused government action to ***improve financial and digital literacy*** among its citizens and consider expanding the availability of basic cybersecurity studies to provide for a future career path for unemployed youth. Next to that, ***establishing a national cybersecurity center*** to assist the government and vital industry sectors with cyber advice and the services of a computer emergency response team will greatly contribute to a higher level of cyber resilience within a country's vital governmental and commercial sectors. Given their crucial institutional role in society, central banks could—and should—play a facilitating role in the establishment of such national cybersecurity centers. Unfortunately, cyber threats are here to stay, and cyberattacks will continue to happen. An efficient and credible judicial system is needed to prevent cybercrimes and—if they happen—to follow up with effective law-enforcement actions. Central banks and other financial authorities should urge governments to ***improve the cyber capabilities of the judicial system (police, prosecutor offices, courts)*** and should stand ready to make available specific financial or cyber expertise, if required.

Finally, cyber risks transcend geographic borders. Therefore, it is recommended that ***central banks and financial authorities reach out to their peers in neighboring countries*** to coordinate follow-up actions regarding the recommendations above and to establish and cooperate in joint initiatives, where appropriate.

1. Introduction

The ever-increasing digitalization of everyday life makes cybersecurity a prominent topic for entities in all industries, but particularly so for organizations of systemic importance, such as financial services, which have to secure systems processing billions of US dollars each day. The issue of cybersecurity has not gone unnoticed in the developed world. Countries have made significant moves toward improving broad cybersecurity standards, introducing robust and comprehensive legislation, educating the public on cybersecurity awareness, and increasingly subjecting critical national infrastructure entities to mandated intelligence-led penetration testing and intelligence sharing.

However, a number of factors, including economic constraints, political disagreements, civil unrest, inadequate infrastructure, and a general lack of awareness, have limited a similar progression of cybersecurity standards across much of the developing world, although this assessment varies significantly between states in this category. Although the continent's size and variety make it difficult to establish comprehensively the general state of cybersecurity across all of Africa, the following common issues make African cyberspace an attractive target for motivated threat actors:

- **Human factor:** While a problem worldwide, Africa suffers from a general lack of public cyber threat awareness and digital hygiene (Świątkowska 2020, 21). Researchers have cited difficulties in disseminating security materials, influenced by factors such as high levels of linguistic diversity and varying English language skills (Kabanda, Tanner, and Kent 2018, 270).
- **Lack of capacity:** Research in 2019 showed only 4 percent of information assurance specialists were located in Africa (Świątkowska 2020, 21). By 2020 there was also an estimated shortage of 100,000 cybersecurity professionals on the continent, further hampering organizations' ability to implement proper cybersecurity protocols and tooling (Kshetri 2019, 78).
- **Resources:** The majority of countries in the developing world rely on outdated, poorly secured, unlicensed, or unmanaged information security assets (Świątkowska 2020, 20). Numerous countries in Africa also have high rates of pirated software, compounding difficulties of checking software for malicious components: In 2017, investigations showed 90 percent and 89 percent of software in Libya and Zimbabwe, respectively, was pirated (Kshetri 2019, 78).

- **Economic constraints:** A 2017 study of African small and medium-sized enterprises indicated that about 95 percent of those polled were at or below the "security poverty line"—that is, they had few or no resources to invest in security or defensive solutions and were thus unable to plan for or manage cyberattacks effectively (Świątkowska 2020, 20). The cost and lack of immediate return on investment for security activities such as penetration testing or threat intelligence analysis leads many small and medium-sized enterprises to forgo these activities entirely (Kabanda, Tanner, and Kent 2018, 274).
- **Socioeconomic factors:** Varying levels of poverty, high unemployment, and a lack of opportunity push many Africans—particularly young people—to see cybercrime as a quick and lucrative source of income (Świątkowska 2020, 21).
- **Ineffective law enforcement:** As of 2016, 39 of the 54 African countries had no specific legal provisions for cybersecurity and cyber-enabled criminal activity. Furthermore, the lack of cybersecurity specialists means that many states suffer an inability to investigate cybersecurity incidents properly, and weak enforcement mechanisms for the laws that do exist make it harder to identify and arrest perpetrators, effectively making the continent a safe haven for malicious actors to operate with impunity (Świątkowska 2020, 22).

An analysis of historic cyber incidents against financial services confirms that as the developed world slowly but surely improves its cybersecurity posture, cyber threat actors are turning away from these hardening targets and pivoting toward what they perceive to be easier pickings in developing regions.

This paper aims to address this growing disparity between the developed and developing world by providing an intelligence-led analysis of the current threat landscape for financial services across Africa. The paper will then provide an assessment of future trends based on emerging patterns for African financial-service institutions (FSIs) (and for the respective financial authorities) and offer an assessment of the expected state of affairs on the continent. The ultimate aim of this research is to assist FSIs across Africa and in other developing regions to understand their own baseline threat models and to alter their cybersecurity strategies accordingly. As previously stated, Africa's size and diversity mean that this paper should be considered as a broad analysis of the state of cybersecurity in the wider African financial infrastructure; it does not provide in-depth threat assessments on a country-by-country basis.

2. Baseline Assessment

In general, African FSIs face three broad categories of cyber threat: threats to integrity through theft of funds, threats to availability through extortion and disruption, and threats to confidentiality through espionage and data theft.

- African FSIs currently face a significant threat from organized criminal groups (OCGs) and financially motivated nation-states conducting high-value thefts in heist-style operations. These operations build on previous successes against similar systems in the now-more-cyber-mature developed world and focus on exploiting generally inadequate cybersecurity controls to manipulate the integrity of payment-processing mechanisms and internal security controls. Malicious insiders have also shown the intent and capability to leverage privileged knowledge and system access and steal from their employers.
- Ransomware also presents a prominent and growing threat, given its detrimental impact on the availability and confidentiality of critical systems and data. A growing number of OCGs and individual hackers are showing both the intent and capability to direct this activity against African FSIs; the majority of these attacks opportunistically take advantage of security issues and infrastructure vulnerabilities.
- African FSIs are also heavily affected by the large volume of low-sophistication scams, thefts, and fraudulent activity directed against their customers. Scams that harm victims outside Africa may subsequently deter foreign investment, to the detriment of Africa's long-term economic potential. Such scams generally originate from domestic grassroots actors, likely compounded by socioeconomic factors such as unemployment and economic inequality.
- African FSIs are currently experiencing high levels of espionage and data theft from nation-states, OCGs, insiders, and individual hackers. Although these types of attack have fewer immediately tangible impacts than direct theft or extortion attempts, they can cause future issues, such as loss of competitive advantage or loss of customer trust.
- African FSIs currently face a small but growing risk of supply-chain compromise from the increasing use of third-party entities within the financial-services infrastructure, expanding the general attack surface.

2.1 THREATS TO INTEGRITY

African FSIs, including central and commercial banks, currently face a significant threat from financially motivated actors seeking to redirect funds into their own pockets by manipulating the integrity of internal systems and security controls. These threat actors use varying methodologies and techniques for this purpose, ranging from heists and the use of insiders to opportunistic malware deployment and scamming customers.

Direct theft of money is a clear issue for FSIs. Most obviously, loss of funds through theft reduces the institution's overall profit. However, cyber-enabled theft can also cause further damage through remediation costs, regulatory fines, and the need to expend time and resources investigating the incident. For example, the theft of $3.2 million from a South African bank forced the bank to spend over $58 million in investigation and mitigation efforts (Cimpanu 2020). Cyber incidents also cause reputational damage to victim organizations, which, although harder to quantify, can result in long-term loss of consumer trust and subsequent business. For example, the 2013 breach of US retailer Target, where threat actors accessed the financial information for 110 million customers, resulted in a 46 percent decrease in net earnings over the following quarter (CEA 2018, 7). As well as reputational damage among customers, cyber-enabled thefts can damage investor confidence in affected organizations. The average victim of cyber-enabled crime experiences a 15 percent drop in share value, and a lack of investor confidence is particularly damaging for emerging economies, which greatly benefit from external investment (CEA 2018, 14). Finally, cyber-enabled thefts at FSIs could cause long-term economic damage, as consumer trust in established FSIs and the use of digital services for financial services is reduced, stunting overall national and sociocultural growth.

2.1.1 Cyber-Enabled Heist-Style Attacks

Current evidence suggests that there is a significant threat from heist-style attacks. This type of attack typically involves threat actors compromising bank networks and gaining privileged access to interbank payment systems such as SWIFT (Society for Worldwide Interbank Financial Telecommunication). Threat actors can then use this privileged position to issue fraudulent transaction requests and obtain large amounts of money. A notorious incident of this type is the North Korea–linked theft of $81 million from the Bangladesh Central Bank in 2018, after attackers compromised the bank's internal network and exploited the bank's access point to the SWIFT network to make several fraudulent transactions (BBC News 2021). These attacks are now less common in the developed world due to a number of factors, including improved cybersecurity, more robust operational controls, and increased network segregation. Although the likes of SWIFT and other providers have worked on global programs to protect their payment network, domestic solutions and fintechs are less mature and may be more susceptible to attack. Improved law-enforcement capability and capacity to target individual cyber threat actors and take down infrastructure used for malicious purposes also likely plays a part in deterring threat actors. Furthermore, the success of easier methods—such as deploying ransomware, engaging in email-based scams, or targeting less well-secured industries, such as retail or insurance, for payment manipulation—makes the labor- and resource-intensive heist-style operations less popular across the board. Attacks in the developed world are also increasingly leading toward international law-enforcement action. Similar developments are unlikely to come to fruition in developing nations due to the lack of the security tools and expertise needed to collect the forensic data required to identify and trace the perpetrators.

Instead, threat actors are now consistently recycling these techniques against FSIs in Africa and other parts of the developing world, capitalizing on the generally lower cybersecurity standards and other issues encountered in these regions. For example, in May 2018, researchers revealed a financially motivated nation-state group engaging in a long-term espionage operation against the financial sector; the intrusions touched a number of African FSIs. The operation's likely objective was large-scale data reconnaissance to identify potential targets for future compromise (Sherstobitoff 2018). In 2019, the same group targeted banks in five African countries to compromise internal banking infrastructure and redirect funds (Lederer 2019; The Chronicle 2019). Other types of threat actors also target African FSIs: In May 2016, an OCG targeted South Africa's Standard Bank, compromised internal banking systems, customer databases, and operational safeguards, and managed to use forged cards to withdraw over $19 million from ATMs across Japan (Carnegie Endowment for International Peace 2021). More than 260 suspects were eventually arrested, highlighting the extensive infrastructure available to these more sophisticated threat actors. In January 2018, an OCG stole at least K Sh 29 million (approximately $261,000) from the National Bank of Kenya, and anecdotal reporting suggested the actual sum was about K Sh 340 million (approximately $3 million) (PC Tech Magazine 2018). The bank cited a compromise of its internal network. Additionally, from 2017 to 2019, several FSIs in West Africa were targeted by cyberattacks aimed at compromising internal networks

and making fraudulent transactions (Symantec Threat Hunter Team 2019). These examples highlight an already substantial volume of sophisticated attacks successfully stealing funds from African FSIs.

Evidence also indicates that African FSIs are routinely targeted by opportunistic threat actors who typically use automated tools to probe the infrastructure of numerous organizations in the hope of finding vulnerabilities or system misconfigurations that could provide network access. For example, in September 2019, a human intelligence source reported that the TA505 OCG was actively targeting large South African FSIs with phishing campaigns, aiming to obtain employee credentials and establish a foothold on banks' networks.[2] TA505 has a history of conducting direct theft operations, suggesting that this was the objective in this scenario. Additionally, in January 2020, the South African Banking Risk Information Centre warned about a significant number of attacks on African banks from a Russia-based OCG. The OCG was reportedly attempting to compromise vulnerable FSIs and deploy a variety of malware on compromised systems, with the objective of bypassing internal security controls and redirecting funds (Githahu 2020).

These examples demonstrate that African FSIs face a significant threat from threat actors such as financially motivated nation-states and OCGs that seek to compromise the integrity of their systems and steal significant amounts of money. Not only do the threat actors cause financial damage to the banks by directly removing funds, but the banks targeted in this way have to expend resources by reimbursing customers, investigating and remediating network breaches, and expanding cybersecurity capabilities, while banks in certain regions may also face regulatory fines. Harder to measure but still significant nonetheless are the long-term effects of cyberattacks, such as reputational damage, loss of customer trust, and loss of potential business.

2.1.2 Insiders

Historic examples also indicate there is a significant threat that current or former employees will act against their employer to steal funds, either directly from the FSI itself or from its customers. It is also important to note that the majority of insider attacks go unreported, and the number of incidents is likely higher than reported. For example, in January 2019, an employee at a South African bank attempted to transfer approximately R 100 million (approximately $6.6 million) from a customer's account into accounts controlled by accomplices. The employee used privileged system access to approve replica cards, which would be used to withdraw the funds from ATMs (Hlungwani 2019).

The insider threat intent is usually driven by money, ideology, coercion, or ego (MICE). The vast majority of insider incidents in financial services are driven by financial motives: A study in 2006 found that 81 percent of malicious insider incidents were motivated by money (Liang and Biros 2015, 162). In many cases, these thefts can reach the equivalent of millions of US dollars, representing a significant source of financial damage to the FSI itself. Clearly demonstrating this point, in June 2020 employees at a South African bank stole a master key used to decrypt bank operations, access and modify banking systems, and generate keys for customer cards. The employees used the key to access customer accounts, make fraudulent transactions, and steal over $3.2 million (Cimpanu 2020). The incident cost the bank over $58 million in remediation, as well as harder-to-measure reputational damage and loss of customer trust and loyalty. The incident also demonstrates how insiders can leverage their privileged system knowledge and access to manipulate internal systems without immediate detection. While difficult to calculate exactly, it can be assumed that incidents like this, where customer funds are directly affected, will damage the affected FSI's reputation and cause long-term loss of customer trust, loyalty, and future business.

Coercion can also be a motive for insider incidents, which, as OCGs drive recruitment efforts to elicit insider support, will likely become more common. There are several cases of insiders cooperating with external threat actors to steal funds from their employers. In May 2020, Gambian authorities arrested 12 suspects linked to an attack on The Gambia's Trust Bank. Evidence suggests that the suspects worked with insiders in attempts to make fraudulent transactions (The Point 2020). Co-opting insiders is also an established OCG tactic: The Kenyan group SilentCards consistently uses the services of current bank employees to transfer and withdraw significant sums of money from ATMs, resulting in the theft of approximately $174 million from Kenyan banks since 2019 (Niba 2019).

It is likely that insiders in these cases lack the skill, knowledge, or infrastructure to compromise their employer's network effectively and "cash out" their operations; working with an external actor can bypass these issues. In several cases, the insider provides the external actor with knowledge of or access to internal systems, and the external threat actor steals the funds and provides the insider with a cut of the profits. These cases can be very hard both to detect and to prove intent. While ego-based attacks are less common, ideology will likely become a growing motive for individual hackers and insiders, particularly those aligned with environmental, religious, or social-justice issues. The above examples demonstrate the significant threat posed to African FSIs

by financially motivated insiders in terms of theft and integrity of funds.

2.1.3 Theft from Customers

The body of evidence suggests that there is a significant level of low-sophistication, high-volume, cyber-enabled activity focused on stealing money directly from financial-services customers across Africa. Such activity is growing in volume across Africa: In 2020, the Ghanaian central bank reported a 584.1 percent year-on-year increase in card fraud affecting Ghanaian customers (Ghanaian Times 2020). This type of activity usually involves obtaining customer card details or personal information via a range of methods, including online scams, business email compromise, impersonating legitimate banking applications, or compromising point-of-sale systems and e-commerce sites.

In many cases, this activity takes the form of confidence trickery: hackers target vulnerable people and pose as friends, relatives, or trusted businesses and convince the victim to make a fraudulent payment or disclose confidential personal or financial information. The scammers then use this information to steal funds from the victim's bank account. For example, the World Bank has previously warned of advance-fee fraud schemes originating from Côte d'Ivoire, Nigeria, and Sierra Leone in which actors impersonate the World Bank to obtain victims' banking details and personal information for fraudulent purposes or to direct victims to send payments to attacker-controlled accounts (WBG 2021b). Additionally, 19 percent of African mobile payments made in the first half of 2021 were made without users' consent, showing this to be a highly targeted area for scams and fraud (Agosto 2021).

Scammers also exploit consumers' lack of familiarity with new products or technologies. For example, in 2020 several hundred thousand victims were defrauded out of $588 million through a pyramid scheme bitcoin scam (Chelin 2021). In April 2021, the founders of South African cryptocurrency exchange Africrypt staged a hack and stole $3.6 billion from investors (Ryan 2021).

Another popular scam format is business email compromise, the process of impersonating an entity to trick a company or individual into transferring funds to an attacker-controlled account. A significant amount of grassroots business email compromise activity originates in Africa, particularly in Nigeria, and affects both African and foreign victims. In 2019, police arrested 77 Nigerians, including a local entrepreneur, for engaging in an online financial-fraud scheme worth almost $11 million (Iwenwanne 2021). In November 2020, Nigerian authorities arrested three OCG members who were engaging in phishing, malware campaigns, and business email compromise scams against almost 500,000 victims located in Japan, Nigeria itself, Singapore, the United Kingdom, and the United States (Scroxton 2020). In October 2021, a joint United States-South Africa operation arrested members of the Nigeria-based Black Axe OCG, which had stolen over $6.85 million from victims via romance and business email compromise scams (Hyman 2021). The involvement of US authorities indicates that a number of victims were likely based abroad.

African banking customers are also targeted by hackers who develop malicious applications mimicking official banking applications. For example, research found that malicious mobile banking applications designed to capture personal and financial data made up 17.6 percent of all fraud attempts in the first half of 2021 in Angola (Agosto 2021). Additionally, in October 2021 the Nigerian Communications Commission alerted the public of a malicious app mimicking popular Android mobile banking applications to spread the Flubot malware. The app, when installed, harvests users' online banking credentials and gains access to SMS messages to intercept two-factor authentication codes to approve the fraudulent log-in (Sahara Reporters 2021).

There have also been examples of threat actors compromising both physical point-of-sale systems and e-commerce payment portals to obtain customer card data. Research conducted in March 2021 shows that the FIN7 OCG conducted attacks on point-of-sale systems in South Africa, aiming to steal customer card data (Seals 2021). The details were then used to make counterfeit cards, which the group used to commit fraud or sold to other cybercriminals. Additionally, in September 2019, Garmin South Africa warned customers that their financial information was at risk after a card-skimming script was found on its e-commerce site. Customers who shopped on the site had their home addresses, phone numbers, email addresses, and full payment card and billing address data stolen (Karabus 2019).

Overall, threat actors use a range of techniques to obtain customers' personal and financial information for use in fraud, clearly establishing this activity as a lucrative source of income. Superficially, this cyber-enabled malicious activity directed at banking customers does not directly affect the integrity of FSIs' networks or funds. However, this activity does have an indirect impact, in that it removes money from the legitimate economy; the aggregate impact of low-value but high-volume thefts can, in turn, cause or exacerbate economic issues on a regional or national scale. Furthermore, if the bank is assessed to

be negligent in preventing the attack, it could face significant reimbursement or even compensation costs.

Additionally, thefts from customers can damage consumer trust in formal banking services if victims believe FSIs failed to secure their money or protect customers from scams. For example, in October 2021, the Central Bank of Nigeria warned that scammers were using Twitter to defraud customers by falsely claiming to disburse 50 billion eNaira, Nigeria's new digital currency, launched on October 25, 2021 (Adegboyega 2021). The campaign likely aimed to obtain Nigerians' banking details for use in further fraudulent activity. This example shows how low-level scammers quickly capitalize on technological developments in the banking sector for their own personal gain.

The evidence also shows a high concentration of Africa-based scamming and other fraudulent activity targeting victims across the world. Scams and fraud affecting foreign victims can damage African FSIs and national economies by compounding the image of Africa as an unsafe business environment. For example, in July 2021 a Nigerian citizen was sentenced for defrauding a US retirement fund out of $1 million by conspiring with an insider to create unauthorized bank accounts, change legitimate bank deposit information, and reroute payments to controlled accounts (Nwezeh 2021). As a result of this activity, some businesses now automatically categorize online transactions originating from Africa as risky and either require the purchaser to enter more information or block the transaction entirely (Kshetri 2019, 78). By contributing to this image, globally targeted scams could deter future foreign investment in the continent or harm the establishment of business relationships with African companies, damaging economies' growth potential and contributing to long-term economic stagnation.

2.1.4 Third-Party Risk

African FSIs also currently face a smaller—but nonetheless significant—risk from the growing involvement of third parties in Africa's financial infrastructure. While growth is inconsistent across the continent, in general African FSIs are steadily increasing their use of fintechs (third-party firms providing technology for financial services). For example, Nigeria's central bank recently partnered with Bitt Inc. to launch the digital currency eNaira (Francis and Emejo 2021). Fintechs are also increasingly focusing on Africa's growing mobile money market (Chironga, de Grandis, and Zouaoui 2017).

However, the inclusion of third parties in Africa's financial infrastructure opens up a significant level of risk. Threat actors consistently perceive new financial technologies as immature and therefore more susceptible to compromise. As such, they elicit significant interest from both malicious actors and security researchers. More detailed analysis and testing of the security of these technologies is needed before they become commercially available.

For example, in October 2020 hackers compromised Pegasus Technologies, a fintech service used by numerous mobile network operators, including MTN and Airtel, for mobile money payments, as well as providing financial services for a mobile banking platform. Pegasus Technologies was not overseen or regulated at the time. The attackers stole about $1 million from Uganda's digital payments system, and 20 million people were affected by the subsequent service shutdown (Kasemiire and Ajuna 2020). The threat actors were able to access all transactions between banks and mobile money providers by exploiting Pegasus Technologies' central position in the financial infrastructure, highlighting the threat posed by integrating third parties into financial-services architecture. But it has since become a regulated entity and received a license from the Bank of Uganda to operate as a payment service operator (Matooke Republic 2021).

Outsourcing IT and cybersecurity capabilities, while helpful in temporarily solving Africa's capacity and resource problems, also represents a risk. Recent history shows evidence of sophisticated threat actors targeting IT service providers and managed service providers to gain access to multiple institutions via one convenient access point. The United States' Cybersecurity and Infrastructure Security Agency warned managed service providers of heightened malicious activity in 2021 (Office of the Director of National Intelligence 2021). A learning point from this example is that third-party service providers must be held to the same—if not higher—security standards than the FSIs for which they provide services.

2.2 THREATS TO AVAILABILITY

Loss of system or data availability is a significant issue for all organizations, but particularly so for FSIs whose business operations typically require system availability 24 hours a day, seven days a week, or carry out a high frequency of financial activity, such as payments, transactions, or trades. Loss of connectivity can render customers and clients unable to carry out transactions, which in turn can harm the wider economy as well as individuals. For example, a denial-of-service (DoS) attack on the UK bank HSBC in 2016 left customers unable to access online banking services for several hours; the attack was timed to coincide with payday (Osborne 2016). As with

direct theft, cyber-enabled disruption may also force victims to expend resources investigating and remediating the issue and, in some countries, could result in regulatory fines. Disruption to services for long periods of time will also likely reduce customer trust in FSIs and growing dependence on digital services, which, as previously stated, could hinder future economic growth if disillusioned consumers reject digitalization. Unreliable connectivity or availability could also deter future investment from or establishment of business relationships with foreign partners.

Available evidence, provided throughout the report, suggests the African financial sector faces a high and growing threat from malicious actors compromising the availability of critical systems and functions, such as through ransomware or DoS extortion. The reliance on third parties or market infrastructures should also be noted for availability concerns. For example, in 2020 the New Zealand stock exchange was targeted with a simplistic but effective distributed denial-of-service (DDoS) attack, rendering its services unavailable for approximately two days (BBC News 2020). (DDoS attacks use multiple sources, such as large botnets, networks of hijacked devices, to conduct the attack.) This example demonstrates how even unsophisticated attacks can cause significant disruption for FSIs.

2.2.1 Ransomware

Ransomware is currently one of the most prominent and potentially damaging threats for the majority of organizations. Ransomware involves threat actors compromising a target, usually via ingress mechanisms such as spearphishing, vulnerability exploitation, or, in some cases, supply-chain compromise, and moving laterally within internal networks to obtain a position of privilege. The threat actors then deploy the final ransomware payload, a piece of malware that encrypts the victim's systems and data and demands that the victim pay a ransom to regain access.

Trends from other regions show ransomware operators now typically focus on "big game hunting," the practice of targeting singular high-revenue organizations, rather than many smaller entities, to obtain a large ransom payout, although recent law-enforcement action may deter groups from targeting critical infrastructure or systemically important entities in the developed world. Ransomware groups also consistently steal and threaten to leak confidential data as extra leverage on the victim and employ such additional tactics as conducting simultaneous DDoS attacks or harassing senior executives.

Financial services are therefore attractive targets for ransomware operators, although there are few cases of ransomware attacks against FSIs in the developed world in recent years due to factors such as more secure networks (in comparison to other industries) and the increasing threat of law-enforcement action. In October 2021, a multicountry operation seized infrastructure belonging to the operators of REvil ransomware after the strain compromised a large number of prominent targets in the United States and Europe (Menn and Bing 2021).

Ransomware can cause serious problems for targeted companies. Losing access to critical systems disrupts business operations and causes financial and reputational damage. Companies have to expend time and resources investigating and remediating the attack, while being the victim of a ransomware attack or having data leaked and stolen can significantly reduce customer trust and loyalty, causing long-term losses.

Ransomware groups have been less reluctant to target FSIs in Africa and other developing regions, likely capitalizing on the perception of lower security standards and a lack of law-enforcement capability to investigate cyber incidents and target OCG personnel and infrastructure. There are a significant number of historic ransomware incidents against African FSIs: For example, in February 2021, the operators of REvil ransomware compromised the Union Bank of Nigeria, disrupted system availability, and stole and leaked confidential customer and business data (Hack Notice 2021). The operators of Egregor ransomware targeted the South African/Botswanan Norsad Finance in July 2021 and compromised Zimbabwe's Steward Bank in November 2020.[3] In September 2020, the Calix ransomware strain infected the Development Bank of Seychelles, a branch of the Seychelles Central Bank (Sweny 2020).

A high volume of ransomware activity is a trend seen across the majority of the developing world, not just in Africa. For example, in October 2021, an unknown ransomware group compromised the network of Papua New Guinea's Department of Finance, disrupting access to its payment systems and subsequently preventing the country from accessing domestic funds and foreign aid reserves for several days. Anecdotal evidence suggests that the threat actors gained access via software and infrastructure vulnerabilities in the government's network. A commentator blamed the poor security on a lack of resources to invest in cybersecurity and other issues, such as COVID-19, taking priority over cybersecurity and infrastructure resilience (Tarabay 2021). Overall, it is clear that ransomware operators see FSIs in the developing world as soft and lucrative targets.

Ransomware incidents can also affect financial services indirectly even when targeted at other industries. For example, in July 2021 ransomware disrupted operations at Transnet, South Africa's state-owned enterprise for rail, port, and pipeline infrastructure. The incident took most systems offline, forcing employees to record vessel movements manually and causing significant logistical backlogs (Reva 2021). Additionally, in July 2019 an unknown OCG deployed ransomware against the large South African energy supplier City Power. The incident was timed to occur when many South Africans received monthly paychecks to pay for electricity for the next month. The ransomware encrypted City Power's entire network, including databases and application servers, and temporarily kept many customers from purchasing electricity packages (BBC News 2019). The incident affected City Power customers and revealed how cybersecurity vulnerabilities in other industries can harm FSIs: A loss of power for an FSI could render it unable to process transactions, conduct trading, or engage in other business-critical operations. Although not directly targeting the financial sector, these incidents demonstrate how ransomware targeting other industries can have a knock-on effect for the availability and operational capacity of FSIs.

2.2.2 Denial of Service

In addition to ransomware, some threat actors use DoS attacks to take down targets' public-facing assets and cause significant disruption. DoS attacks work by flooding targets (usually servers) with high volumes of incoming traffic to overload systems and prevent legitimate requests from getting through.

The motivation for using such attacks varies. Some threat actors use the threat of disruption to extort payments. There is significant evidence to suggest that this activity is a growing threat to African FSIs, although the effects of DDoS attacks are usually limited and less severe than other extortion methods, such as ransomware. For example, in October 2019, the South African Banking Risk and Information Centre reported a series of DDoS attacks against multiple African banks' public-facing assets. The attacks were accompanied by a ransom note demanding payment to stop the attacks. The attacks were timed to coincide with payday to cause maximum disruption. While the effects of this campaign were limited, it demonstrates how less sophisticated threat actors seek to disrupt FSIs' availability for financial gain. These attacks coincided with a ransomware attack against the City of Johannesburg's network, which shut down all electronic services, including bill-payment mechanisms, and coincided with month-end processes for supplier and customer payments (Paton 2019).

Other threat actors, such as hacktivists, use DoS attacks to disrupt targets' operations or publicly embarrass the victim. A lack of motivation and specific intent means hacktivists are unlikely to target FSIs directly with DDoS attacks but could harm the industry as part of broader campaigns. In October 2020, for example, a hacktivist group protesting police brutality targeted the website of the Central Bank of Nigeria with DDoS attacks (Vermeulen 2019). The incident was part of a wider campaign against the Nigerian government, demonstrating how FSIs can be caught up in wider politically or ideologically motivated campaigns (Olufemi 2020). In June 2020, ideologically motivated hacktivists defaced the website of Sudan's Ministry of Endowment and Religious Affairs with political slogans, also allegedly targeting the Ministry of Finance (Sudan News Agency 2020).

Some threat actors also conduct DDoS attacks without overt ideological or financial motivation, likely testing their skill level and ability to take down an organization or to boost their reputation among the cybercriminal community. In July 2021, Angola's largest state-owned bank suffered a disruptive attack against several servers, leaving services at branches in its commercial banking network temporarily limited (Lusa/Ver Angola 2021). No demands were made, and no responsibility was claimed.

Financial services may also be indirectly affected by availability attacks against other critical national infrastructure providers. In November 2017, unknown threat actors temporarily took down the services of Algeria's state telecommunications operator, Algerie Telecom, with a series of DDoS attacks (Paganini 2017). Additionally, in October 2016 an individual hacker for hire was contracted by a rival firm to use a botnet to conduct DDoS attacks against a Liberian telecommunications company. The incident left half the country unable to access the internet (Casciani 2019). Currently the global leader in mobile money usage, Africa is unusually reliant on mobile infrastructure and internet access to conduct financial activity; disrupting mobile network provision through DDoS attacks therefore has an indirect impact on customers' ability to make and receive payments, thus having an aggregate negative impact on the wider financial industry.

Motivations aside, DDoS attacks are usually low impact and short-lived and limited to public-facing assets. However, the growing use of botnets harnessing millions of Internet of Things devices or insecure smartphones for DDoS attacks can result in prolonged outages and significant disruption for vulnerable targets.

2.2.3 Other Factors

The availability of financial services and their critical systems can also be affected by other factors. For example, in November 2018 Mozambique's banking system (including ATMs and card machines) went offline for several days after the Portuguese fintech provider BizFirst cut off its services when Mozambique refused to pay a disputed bill (Verdade 2018). This example highlights issues with relying on third parties to provide core aspects of critical national infrastructure.

Political issues can also affect the availability of infrastructure underpinning financial services. In July 2020, Somalia suffered an almost complete internet blackout after the parliament removed the president in a vote of no confidence. The blackout was likely intended to impede coverage of the incident but affected a large number of businesses and Somalia's mobile money services (Netblocks 2020). This example shows how political and civil unrest can disrupt FSIs' availability, particularly as FSIs become more reliant on digitalization and the internet for the provision of services.

2.3 THREATS TO CONFIDENTIALITY

A less tangible but nonetheless prominent threat to financial services in Africa is cyber-enabled activity that affects the confidentiality of data. Theft of data, such as business strategy plans or high-level financial intelligence, can lead to a future loss of competitive advantage—for example, with information regarding upcoming contracts or partnerships with third parties. Theft of data such as technical intellectual property or trade secrets relating to fintech solutions can also significantly harm FSIs' future competitiveness. Additionally, theft or exposure of customer information can cause direct reputational damage, incite regulatory measures, trigger remediation and recovery costs, or push customers toward rival entities.

2.3.1 Espionage

Various threat actors are currently targeting African organizations, including FSIs, for espionage and data-collection purposes. As demonstrated when African Union staff members discovered that a nation-state threat actor was using compromised security cameras installed in their headquarters for espionage purposes, the majority of this espionage activity is targeted at governmental and regional political bodies. With a developing economy, a wealth of natural resources, growing political clout in international bodies, and opportunities for economic growth, Africa is an attractive target for expansionist nation-states (CSIS 2021). This activity highlights the already extensive extracontinental nation-state interest in obtaining political intelligence from African organizations.

However, available evidence indicates that FSIs in Africa are also valuable espionage targets. Vendor research in 2017 revealed a nation-state group targeting a number of Africa-based FSIs since at least 2011 and perhaps even 2007. The custom malware used by the group had sophisticated system fingerprinting, discovery, and exfiltration capabilities, indicating that the group was conducting long-term espionage of its targets (Johnson 2017). Additionally, in February 2021 a sophisticated threat actor compromised Angola's Ministry of Finance, accessed emails and shared folders, and stole confidential data (Massala 2021).

Financial services, especially large international banks and payment processors, likely provide nation-states threat actors with a high-level overview of African states' transaction flows and business and political relationships both within Africa and with extracontinental nations. Nation-states can provide this information to domestic companies, who can then use the intelligence to gain an advantage over competitors when negotiating with African companies for contracts or partnerships. It is also plausible that other threat actor types, such as state-aligned OCGs or independent hackers, also target financial intelligence to provide to interested nation-states.

2.3.2 Data Theft/Exposure

Threat actors are also targeting African FSIs to obtain customer information, including personally identifiable information and personal financial information. For example, in December 2020 a credit analyst at a South African bank stole and sold the personal information of 200,000 customers to an unknown third party (Carnegie Endowment for International Peace 2021). In July 2021, an unidentified threat actor compromised a South African financial-services provider and stole databases containing policyholder information, including bank account numbers and card details (Vermeulen 2021). This information can be used for a range of purposes, such as conducting identity theft, opening fraudulent bank accounts or cards, or applying for fraudulent loans, or can be sold on underground marketplaces to other cybercriminals. As previously stated, data theft or exposure can have serious reputational and financial consequences for affected organizations, particularly for entities like FSIs that hold highly valuable data, such as financial data and bank card details.

Data can also be exposed through misconfigurations in software or inadequate security provisions. In August 2020, Experian South Africa suffered a data breach,

resulting in the exposure of personal information belonging to 24 million South Africans and almost 800,000 business entities (Times Live 2020). Accidental data breaches can damage customer trust in a brand or institution and could result in significant fines, depending on national regulations.

2.4 BASELINE ASSESSMENT

To summarize, it is clear that African FSIs, including central banks and finance ministries, face a wide range of threats. In a broad sense, these threats harm integrity through the theft of funds, availability through the disruption of service, and confidentiality through the theft of or exposure of data. These threats are compounded by structural issues affecting the African cyberspace, including comparatively poorer security than found in the developed world, a lack of awareness about cybersecurity and cyber-enabled scams, and a lack of appropriate legislation and law-enforcement capability to deal with cyber-enabled theft on this level.

Building on the current baseline established by this threat assessment, the next section of this paper will establish several emerging trends and extrapolate on their likely impact on the African financial sector's future cyber threat landscape.

3. Emerging Trends and the Future Threat Landscape

This section will build on previous analysis and the current state of financial services in Africa to identify the key emerging trends for the industry and region. This section will then assess the likely impact of these trends on the African financial sector's future cyber threat landscape.

- Large-scale rapid digitalization of financial products represents new avenues of opportunity for threat actors.
- Greater levels of digitally enabled financial inclusion, coupled with unfamiliar products and services, open up new targets for scammers.
- Expanding the supply chain provides threat actors with new access vectors.
- Short-term economic challenges will increase the attractiveness of cybercrime for the young and unemployed.
- Sporadic introduction and lax enforcement of cybersecurity regulations will not deter domestic cyber activity over the short to medium term.
- Increased security in the developed world will increase Africa's attractiveness to an array of threat actors.
- Africa's increasing geopolitical strength and importance will incite more targeting from nation-state threat actors.

3.1 TECHNOLOGICAL FACTORS

A diverse array of factors will affect the future development of African financial services. For example, rapid improvements in the efficiency, utility, and availability of technology in support of financial services and products across the continent will almost certainly help to engage Africa's significant unbanked population and promote formal financial inclusion across the continent. Additionally, the expansion of private-sector involvement within Africa's financial infrastructure will likely drive technological innovation and be able to respond to consumer demands and needs. However, despite its benefits, technology will bring with it a number of increased risks.

3.1.1 Large-Scale Rapid Digitalization of Financial Products Represents New Avenues of Opportunity for Threat Actors

One of the biggest trends set to affect African financial services over the near and medium term is large-scale rapid digitalization of financial products and services (Świątkowska 2020). Broadly speaking, digitalization refers to the adoption of technology-based solutions to combine with or replace the physical components of an existing business model, such as using a smartphone application to transfer money, rather than writing a check or paying in cash.

Generally, digitalization is already a well-established trend for African financial services. Key areas include Africa's already substantial mobile money network (digital payments usually sent via SMS). The continent is already the global leader in mobile money: 562 million mobile money accounts were registered in Africa as of 2021, representing a 12 percent year-on-year increase (AfricaNenda 2021; Chironga, de Grandis, and Zouaoui 2017). Likely exacerbated by COVID-19, Africans' use of digital platforms for shopping and e-commerce has seen similar growth: e-commerce revenue increased 53 percent from 2020 to 2021. As with other aspects of African digitalization, mobile phones and smartphones are the primary technologies for conducting e-commerce transactions (Varrella 2021). The shift toward digitalization is also being compounded on a state level, as numerous African governments have already introduced digital currencies like Nigeria's eNaira (Further Africa 2021).

Digitalization is highly likely to accelerate in the future, given high latent demand for digitalized services, large areas of the continent that still lack access to physical financial infrastructure, and the expected expansion of internet services to more than one billion Africans by 2022 (Kshetri 2019, 77; Świątkowska 2020, 18). The need to reduce face-to-face contact during the COVID-19 pandemic has undoubtedly accelerated this trend across both the developed and developing world. For example, the Seychelles' technological integration strategy aims to eliminate the use of physical cash and to digitize the financial system entirely by 2023 (Seychelles News Agency 2021).

Despite advantages in service provision, innovation, and efficiency, digitalization also brings increased risk. As more and more parts of Africa's financial architecture move online or embrace digital components, the industry's attack surface also expands. Ultimately, digital products and services are likely to contain some form of exploitable vulnerabilities, security issues, or misconfigurations, opening the door for exploitation by malicious threat actors and carrying a heightened risk of harm to the entire financial system (WBG 2021a, 2–3). To this point, the rapid demand-driven pace of digitalization threatens to result in "hollow diffusion," where the provision of digitalized services outpaces the establishment and implementation of technical controls and legal frameworks for cybersecurity (Świątkowska 2020, 19).

This trend toward exploiting digital financial products is already occurring in Africa and is likely to expand. For example, in the first half of 2021, 19 percent of all mobile payments in Africa were made without the user's consent, highlighting the vulnerability of this technology (Agosto 2021). Nigeria's central bank was forced to warn its customers after hackers attempted to steal banking details by offering free eNaira just days after the digital currency was officially launched (Adegboyega 2021). Additionally, the near-instantaneous payments facilitated by digital products such as mobile money and smartphone-based banking can allow threat actors to move stolen funds out of compromised accounts quickly, making it harder for FSIs to stop, intercept, or recover fraudulent payments.

The expansion of digital services such as mobile money without an accompanying expansion and implementation of adequate security and operational controls is highly likely to result in the increased exploitation of these services by opportunistic cybercriminals and individual hackers to steal funds and data from consumers and FSIs in the near future.

A further threat accompanying African digitalization is the continent's overwhelming reliance on mobile technology and smartphone-based products to conduct financial activity, such as e-commerce, transactions, and online banking. As African internet usage grows, this established preference indicates that a vast number of new internet users will predominantly use mobile devices and smartphones as their primary method of accessing the internet. While figures vary, mobile operators estimate that the number of unique mobile users just in Sub-Saharan Africa will increase to over 600 million (or half its population) by 2025 (GSMA 2019, 2). While undoubtedly beneficial for internet users, an increasing number of mobile devices brings the increased risk that threat actors will compromise unsecured or out-of-date devices for malicious purposes, such as for use in botnets for large-scale DDoS attacks or to install malware to steal information such as log-in credentials or personal data. Mobile malware has indeed become more commonplace in developed nations, and this trend is highly likely to cross over as the developing world becomes more connected (Kaspersky 2021). It is probable that this trend will have a more significant impact in the African region, given its reliance on mobile payments and generally lower cyber maturity.

3.1.2 Greater Levels of Digitally Enabled Financial Inclusion, Coupled with Unfamiliar Products and Services, Open Up New Targets for Scammers

Another core trend likely to accelerate across Africa (albeit with varying speed and distribution across the continent) is the use of digital financial products to expand the provision of formal financial services to Africa's significant unbanked population. As of 2020, only 20 percent of adults in developing regions saved through formal

FSIs (Pazarbasioglu et al. 2020, v–vii). The level of financial inclusion across Africa varies from region to region. In West Africa, for example, low numbers of ATMs and bank branches disproportionately affect the rural population: As of 2018, only 22 percent of adults held accounts with formal FSIs, while in Central Africa, only 19 percent of adults had a formal bank account (Cooper et al. 2018, 15–21).

Despite these regional differences, a common factor behind low levels of formal financial inclusion is a lack of sufficient physical infrastructure to support formal participation, a trend particularly pronounced in rural areas. Digitalization, and its ability to transcend the need for physical infrastructure, is therefore a key facilitator of greater financial inclusion.

Financial inclusion has significant benefits on both a micro and macro scale, such as reducing poverty, improving social mobility, and providing economic opportunities for individuals while bolstering participation in and stimulating economic growth. However, bringing large numbers of previously unbanked people into the formal financial sector via digital services is not without risk. These new joiners may lack the knowledge and technical skill to use digital services and handle sensitive data and information correctly, and they will likely be targeted by scammers, hackers, and individual cybercriminals looking to exploit this naivety for their own financial gain (WBG 2021a, 3).

Africa already has a significant level of grassroots scamming activity, as discussed in the first half of this report. It is highly likely that this class of threat actor will seek to exploit the increased numbers of unsophisticated users entering the digital financial-services space through a range of methods, such as social engineering, to obtain log-in credentials or financial information or to trick users into transferring funds into attacker-controlled accounts. It is also possible scammers will exploit for their own gain the dearth of consumer knowledge about new products. Indeed, the introduction of microcredit services in Kenya and Tanzania has already produced a large number of borrowers who are unable to repay loans due to irresponsible lending practices and a lack of effective oversight and regulation for this emerging sector (WBG 2021a, 1). Novelties such as cryptocurrency present similar threats, as unsuspecting users may be tempted to invest funds without understanding the level of risk associated with this activity. The Africrypt case, where a professed cryptocurrency firm allegedly scammed customers out of approximately $3.6 billion, is one example of this risk (Ryan 2021).

In short, mass financial inclusion provides threat actors with the opportunity to exploit consumer naivety in using new digital products and services.

3.1.3 Expanding the Supply Chain Provides Threat Actors with New Access Vectors

Current evidence also indicates that the integration of third-party products and services into financial-services infrastructure will increase in the near future. These third parties include fintechs, mobile network operators, and software providers, among others, and their inclusion en masse will greatly expand the supply chain for African FSIs. As previously mentioned in this report, African entities are already making use of fintechs in financial products, such as Nigeria's use of a private-sector third party to support the rollout and provision of its digital currency eNaira (Kshetri 2019, 78). Fintechs are also rapidly entering into the mobile money market, identifying a sector with high latent demand and opportunity for growth (Chironga, de Grandis, and Zouaoui 2017; Lukonga 2018, 11).

The state of affairs in the developed world shows that an expansive supply chain, while important for obtaining specialized components and services, is a significant risk: Threat actors increasingly compromise large well-secured entities not directly but by infiltrating the network of trusted suppliers and exploiting connections to client infrastructure. Two of the most prominent examples of this risk are the SolarWinds compromise, where nation-state threat actors compromised a software supplier to gain access to clients' networks for espionage purposes, and the Kaseya ransomware attack, where ransomware operators compromised a an IT solutions developer for the purposes of deploying ransomware across client systems (Jibilian and Canales 2021; Osborne 2021). Introducing third parties into the supply chain brings further issues for FSIs, such as a lack of transparency or loss of insight into internal processes (Lukonga 2018, 20–21).

These examples demonstrate that expanding the supply chain brings with it an increased risk to African financial services. It is likely that supply-chain expansion without implementation of necessary security and operational controls, such as network segmentation and limiting supplier access to the client environment, will result in a greater number of threat actors looking to exploit these supplier-client relationships for their own gain. In addition, it is logical to assume that new products and solutions introduced by third parties will contain vulnerabilities or security misconfigurations that are exploitable by malicious actors, representing another avenue by which threat actors can gain access to financial services' networks.

3.2 SOCIOECONOMIC FACTORS

Along with technological improvements, socioeconomic factors will influence the future threat landscape for African FSIs. For example, ongoing economic challenges and higher-than-average poverty levels across the continent may influence the uptake and attractiveness of grassroots cybercrime for individual Africans, while economic constraints at the national and government levels may affect states' abilities to devise, implement, and effectively enforce much-needed legislation and regulations to tackle cybersecurity challenges.

3.2.1 Short-Term Economic Challenges Will Increase the Attractiveness of Cybercrime for the Young and Unemployed

Poverty continues to be a significant issue for African economies. About 36 percent of Africa's population (or 490 million people) live in extreme poverty as of 2021 (Human 2021). As with most of the issues covered in this report, the level and impact of poverty varies significantly across the continent.

Following global patterns, the COVID-19 pandemic cast the continent into its worst economic recession for half a century, and there is significant uncertainty about the level of recovery expected over the next few years. Only a third of emerging economies are expected to recover to their prepandemic per-capita income levels by 2022 (African Development Bank Group 2021, 20; Brooks 2021). Current evidence suggests that the pandemic has exacerbated poverty issues across the continent but harmed those with lower levels of education, fewer assets, and working in informal employment the most; women and young people were particularly affected (African Development Bank Group 2021, 20–21). Generally low levels of vaccine provision across Africa and, indeed, most of the developing world—while developed states begin to roll out booster programs—will further delay the continent's recovery from the pandemic (Selassie and Hakobyan 2021).

Along with the lingering effects of the pandemic, other issues are likely to exacerbate economic uncertainty and individual poverty across the continent, such as general political and civil unrest, a lack of employment opportunities, high levels of corruption, and a lack of social mobility. Global climate change will also hurt African economies, causing long-term effects, such as mass population displacement or the disruption of traditional industries, such as farming (Reuters 2021).

As shown by current evidence, economic instability and a lack of employment opportunities—particularly among young people—are key factors driving Africans to participate in cyber-enabled crime (Świątkowska 2020, 21). Over the short to medium term, it is therefore highly likely that these aforementioned economic challenges will drive the attractiveness and subsequent growth of Africa's "cybercrime sector." Additionally, these current and future economic challenges will likely constrain the ability of governments and businesses alike to establish and implement effective cybersecurity capabilities across the board, further increasing the attractiveness of cybercrime. Following trends seen in the developed world, which has seen an increase in the volume and affordability of commodity tools such as exploit kits and rentable botnets, cybercrime will likely become more profitable and accessible to less technically skilled individuals and groups (Koegler 2017).

3.2.2 Sporadic Introduction and Lax Enforcement of Cybersecurity Regulations Will Not Deter Grassroots Cyber Activity over the Short to Medium Term

Current cybersecurity regulations differ extensively from state to state. Many states have yet to adopt specific cybersecurity strategies and continue to lack capabilities to conduct national risk analyses and information exchanges, hindering efforts to create a functioning and united cybersecurity ecosystem across Africa (Świątkowska 2020, 22). For example, as of 2016 only 15 of the 54 African countries had specific legal provisions in place for categorizing or dealing with cybersecurity issues; indicating a slight improvement, by 2021 that number had risen to 29 (Saeed and Osakwe 2021). Many states are enacting specific policies, such as South Africa's 2021 Cybercrimes and Cybersecurity Act compelling communications service providers and FSIs to report cybersecurity incidents, or Ghana's 2020 Cybersecurity Act establishing a national authority and providing protection for critical national infrastructure (Baker McKenzie 2021). Some states are also benefitting from external aid, such as Nigeria's participation in the United Kingdom's £22 million cyber capacity-building initiative for developing regions (This Day 2021).

States that have comprehensive legal, regulatory, and institutional frameworks and laws to detect and investigate cybercrime, such as Nigeria, have a higher level of arrests and successful prosecutions. For example, in November 2020 Nigerian authorities arrested three OCG members who were engaging in phishing, malware campaigns, and business email compromise scams against almost 500,000 victims located in Japan, Nigeria itself, Singapore, the United Kingdom and the United States

(Scroxton 2020). These examples clearly demonstrate the necessity of establishing similar frameworks across Africa.

However, there are still significant gaps in Africa's general regulatory framework and law-enforcement capacity regarding cybersecurity. As of 2021, only 10 African countries have a comprehensive national cybersecurity strategy fully addressing issues pertaining to critical national infrastructure. Africa is also home to just 19 of the 131 computer incident and emergency response teams across the globe, indicating a lack of general cybersecurity maturity. Although there are of course exceptions, African states are generally lacking in collaborative capabilities: only 19 African countries are signatories to multilateral cybersecurity agreements, and only 10 are part of bilateral agreements. Furthermore, only six states have adequate capacity-development incentives in place to address issues such as the digital divide and building institutional knowledge regarding cybersecurity (Saeed and Osakwe 2021).

This {-lack of?-} regional and international cooperation and regulatory streamlining, combined with porous international borders and a lack of centralized state control over remoter territories, challenges effective investigation and arrest of cybercriminal actors (Kshetri 2019, 78). The dearth of effective legislation and forensic investigative capacity and capability also hampers efforts to identify and investigate properly varying types of cybercrime, making successful prosecutions even more difficult. Ultimately, this lack of punishment creates a safe haven for cybercriminals to operate with almost-guaranteed impunity. It should also be considered that a history of political corruption and authoritarianism in some African states may cause public pushback against attempts to enact laws that could be considered detrimental to individual privacy and personal security (Świątkowska 2020, 19–21).

These ongoing issues indicate that, despite a general upward trend toward implementing regulatory frameworks and legislation, over the short to medium term, African FSIs' ability to deter or respond effectively to cyber threats will continue to be hampered by sporadic and patchwork legislation at the governmental and regional level.

Additionally, establishing legal and regulatory frameworks for dealing with malicious cyber activity is not enough; evidence from the developed world indicates that African states must simultaneously establish the capacity and capability to investigate cyber activity; actively identify, arrest, and prosecute individual participants; and disrupt criminal assets and infrastructure. One example of this is the recent US-led action against members of the REvil ransomware group. A joint public- and private-sector investigation enabled authorities to identify individuals behind the attacks, resulting in the eventual seizure of criminal infrastructure and the arrest of several REvil operators in November 2021 (Krebs 2021). Failure to develop effective forensic investigative capability and law-enforcement capacity will ensure that Africa remains a safe haven for cybercriminal activity.

3.3 GEOPOLITICAL FACTORS

Finally, geopolitical factors, such as security improvements in the developed world, and Africa's growing importance on the global stage will also affect the future threat landscape for African FSIs.

3.3.1 Increased Security in the Developed World Will Increase Africa's Attractiveness to an Array of Threat Actors

The developed world is currently trending toward broad improvement of its cybersecurity standards. While issues undoubtedly remain across many industries, financial services in particular are now subject to stringent security and regulatory requirements. Operational controls are being designed to protect the confidentiality, integrity, and availability of entities' systems and data.

FSIs in the developed world generally have sufficient liquid assets to invest heavily in cybersecurity and are thus likely to be initial adopters of new technologies and security standards. For example, several states have already claimed to have developed supercomputers with quantum supremacy—that is, quantum computers that complete tasks quicker than classic machines (Nield 2021). One of the security benefits of quantum computing is the use of quantum key distribution for encrypting information and assets, exploiting quantum mechanical properties to ensure that an external force is unable to read or copy encoded data. While predictions vary, quantum key distribution and other functions of quantum computing are likely to be commercially available to most industries by 2030 (Fowler 2021). It is highly likely that financial services across the developed world, as an industry with the resources to invest heavily in cybersecurity, will be among the first to adopt these new technologies for security purposes.

However, the ongoing economic challenges previously outlined in this paper are likely to hamper adoption of this technology on a similar timeframe and scale across the developing world. Therefore, the already significant disparity in security between the developed and developing world will widen in the future. Threat actors lacking the

capability to compromise these now theoretically impenetrable entities in the developed world will likely pivot toward targeting financial services elsewhere, taking advantage of the security disparity. In the future, African financial services will therefore face a heightened threat from sophisticated, highly skilled, and well-resourced threat actors looking to steal funds and data or conduct extortion attacks.

These threat actors may also attempt to compromise African FSIs to use them as conduits for accessing well-secured entities in the developed world. Comparatively poor security in the developing world, therefore, represents a significant weakness in the global financial system and may deter global interaction with the developing world, ultimately to the economic, geopolitical, and sociocultural detriment of these regions (Świątkowska 2020, 23–24).

3.3.2 Africa's Increasing Geopolitical Clout and Importance Will Incite More Targeting from Nation-State Threat Actors

Africa is already an important global player, and it has significant potential to increase this importance over the near and long term. For example, Africa is an abundant source of energy, currently a major exporter of oil and gas (Ford 2021). Africa also has the potential to produce colossal amounts of renewable power, such as solar energy, as global demand grows.

Africa is also rich in natural resources such as minerals and rare earth metals. For example, African countries such as the Democratic Republic of Congo, Ghana, Mali, Namibia, and Zimbabwe all contain large amounts of lithium, a key component in batteries for electric vehicles (BGS 2021). As climates change and dwindling supplies of fossil fuels heighten the importance of cleaner sources of energy, Africa's resources will be even more hotly contested.

In addition to providing energy and raw materials in response to continental and global needs, Africa will become even more important to the global economy. Africa is currently home to the world's largest free trade area, making it an important target for states and corporations alike (WB 2021). The short-term effects of COVID-19 have undoubtedly hampered Africa's economic growth, as previously explained, and recovery is likely to be slow and sporadic across the continent. Looking more over the long term, Africa has a high potential for economic growth. Currently underdeveloped sectors such as technology and financial services will therefore become key targets for external parties in the future (Yade 2021).

Factors such as climate change, potential post-pandemic economic recession, and continued geopolitical power struggles mean Africa's importance on the global stage will only increase in the future. It is highly likely that nation-state threat actors will increasingly target African entities. While governments and political bodies are likely to be primary targets, financial services will also be important sources of information for this type of threat actor. For example, FSIs can provide states with financial intelligence, monetary policy, business relationships, or financial flows across the continent. This information can then be passed on to domestic companies and used to bolster their competitiveness when dealing with African businesses. Targeting the financial industry can also assist in broader espionage efforts against African governments, businesses, and individuals. It is possible that other threat actors, such as corporations, hacker-for-hire groups, and OCGs, will capitalize on Africa's immense economic potential and also seek to steal financial intelligence and business-sensitive data from FSIs. Overall, as Africa's global importance grows, the targeting of its financial-services sector by a diverse range of threat actors will simultaneously increase.

4. Recommendations for Central Banks and Financial Authorities

Based on the analysis of the current threat landscape for Africa's financial sector and the subsequent emerging trends, it is clear that a strategic approach is needed to address the challenges ahead. While following normal supervisory practice, such an approach would entail focusing on individual financial entities and aiming to improve their cyber resilience by applying stricter rules and enforcing compliance. However, the analysis in this paper indicates that such an approach would likely be insufficient. The challenge of coping with the serious cyber threats faced by Africa's financial sector—and, with it, society in general—is not borne by Africa's banks, payment service providers, and financial infrastructures alone; financial authorities, including central banks and governments too, must step up their cyber capabilities and improve their own cyber resilience by pursuing the following four-track approach:

4.1 STRENGTHENING CYBER RESILIENCE OF FINANCIAL ENTITIES AND THE FINANCIAL SECTOR AT LARGE

The improvement of the cyber resilience of financial entities and the financial sector at large can be achieved only by focusing on both individual financial entities and the financial sector as a collective.

It is the responsibility of supervisors and overseers to ensure that appropriate regulations on operational and cyber risk are in place. While this is often the case, what is lacking in many instances is a more practical understanding by both the supervised/overseen entities and the supervisor/overseer on how these regulations are to be implemented in practice.

Therefore, several authorities have come up with more specific—but technology-neutral—operational guidelines and cyber resilience expectations to provide a common understanding to financial entities and their relevant authorities regarding how to implement and assess the appropriate cyber resilience measures.

It is recommended that authorities *publish such operational guidelines and cyber resilience expectations*, if not available already, taking into account guidelines and expectations already published by relevant international authorities, including the World Bank.[4]

Compliance with regulations alone is not enough to ensure cyber resilience. Testing—and for systemically important entities, *threat-led penetration testing*—is a critical tool for assessing the cyber resilience of supervised and overseen entities. Threat-led penetration testing is a concept already applied in several countries in Europe and Asia,

BOX 1

LIST OF RELEVANT INTERNATIONAL GUIDANCE/STANDARDS

- Financial Stability Board's Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices
- Financial Stability Institute's Cyber Resilience Practices
- CPMI-IOSCO guidance on cyber resilience for financial market infrastructures
- European Central Bank's Financial Stability Review: Financial stability vulnerabilities stemming from cyber risks within financial market infrastructures
- National Institute of Standards and Technology Cybersecurity Framework
- ISO/IEC 27000, 27001, 27002, 27031, 27032, 27701
- COBIT 5
- Information Security Forum's Standard of Good Practice for Information Security
- Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool

and the frameworks could also be applied by authorities in other countries.[5] It is recommended that the responsible authorities invite systemically important financial entities to engage in threat-led penetration tests.

The chain is as strong as its weakest link. One way to improve the cyber resilience of the financial sector as a whole is for the financial entities (in most cases the systemically important banks, payment service providers, fintechs, and financial market infrastructures) to cooperate in a *cyber information and intelligence-sharing initiative*. Within such an initiative, financial entities could work together closely by exchanging the threats they have identified, attacks they have endured, and the possible mitigation measures they have taken. By doing so, they would help themselves and their peers increase their situational awareness, prepare for the threats and imminent attacks they face, and take the appropriate cyber resilience measures. Blueprints for how to set up information and intelligence-sharing initiatives as a financial-sector community are freely available, as are more commercial alternatives.[6]

4.2 UNDERSTANDING AND STRENGTHENING THE FINANCIAL-SECTOR SUPPLY CHAIN

The financial sector is a networked industry in which many financial entities are mutually dependent on each other. However, many of these financial entities also depend on the same third-party service providers, such as cloud service operators, security vendors, or hardware providers. As previously mentioned in this report, an extensive supply chain brings with it both benefits and risks—specifically, the risk of large-scale, opportunistic, supply-chain compromise operations allowing threat actors, through the compromise of a single third party, to disturb the supply chain or even access multiple victims. As a result, third-party entities that are used by numerous financial entities can themselves become systemically important.

It is therefore recommended that the financial authorities and central banks conduct *sector mapping to establish a clearer understanding of which third-party service providers are of systemic importance to their financial sector* and ensure that the relevant providers also comply with the applicable cyber regulations, operational guidelines, and cyber resilience expectations.[7]

4.3 STRENGTHENING CYBER RESILIENCE AND SUPERVISORY CAPACITY OF CENTRAL BANKS AND FINANCIAL AUTHORITIES

The responsibility for being cyber resilient and having sufficient cyber capabilities lies not only with the private sector but also with central banks and other financial authorities.

First, *central banks and other financial authorities must comply with their own cyber guidelines and expectations*. Just like commercial financial entities, central banks and financial authorities perform critical functions that are supported by critical assets (including data) and systems. Therefore, most cyber guidelines and expectations are also relevant for these entities, especially as

most central banks also act as operators of critical financial infrastructures.

Second, there is often a lack of communication and alignment of policy and action among departments responsible for the institutional and organizational functions of a central bank. Senior managers engaging in *structured internal dialogue* will greatly contribute to the cyber capabilities and cyber resilience of the central bank, allowing decision-makers to learn from each other and to contribute to the other's policy and operational objectives (for example, by sharing specific expertise).[8] This recommendation is especially significant for departments responsible for supervision and oversight, for payment systems, and for the bank's own information systems.

Third, if financial authorities other than the central bank have supervisory responsibilities in a jurisdiction, a proper structural cyber dialogue with the same objectives as described above should be established.

4.4 STRENGTHENING CYBER RESILIENCE OF GOVERNMENT AND SOCIETY AT LARGE

This paper has clearly established that some of the challenges threatening Africa's financial sector can be addressed only by governmental action.

First, the *establishment of a national cybersecurity center* (NCSC),[9] to assist the government with cyber advice and to provide government and vital industry sectors with computer emergency response team (CERT)[10] services, will greatly contribute to a higher level of cyber resilience within a country's vital governmental and commercial sectors. Given their crucial institutional role in society, central banks could play a facilitating role in the establishment of such NCSCs.

An NCSC could also be earmarked by means of regulation as the so-called competent authority to which market participants from vital industry sectors have to report their significant cyber incidents, allowing the NCSC to perform its governmental advisory function and national CERT role even better. Furthermore, by also stimulating nonfinancial sectors to set up *cyber information and threat intelligence-sharing initiatives* (see paragraph 4.1), NCSCs could position themselves as linchpins between those initiatives and actively feed those initiatives with cyber information and intelligence while simultaneously receiving new information and intelligence.

Ultimately, while the financial sector and its authorities focus on improving cyber resilience (that is, improving the capability to cope with cyberattacks), preventing cyber incidents from happening in the first place should be the focus of government. It is recommended that central banks call for—and contribute to—more focused action by governments on *improving financial and digital literacy* among its citizens and *expanding the availability of basic cybersecurity studies* to provide a future career path for unemployed youth.

Unfortunately, cyber threats are here to stay, and cyberattacks will continue to happen. Banks, financial market infrastructures, payment service providers, and especially ordinary citizens will continue to be targeted by adversaries trying to steal their money, data, or intellectual property. An efficient and credible judicial system is therefore needed to deter these crimes and—if they happen—to follow up with effective law-enforcement actions. Central banks and other financial authorities should urge governments *to improve the cyber capabilities of the judicial system (that is, police, prosecutor offices, courts, and so on)* and should stand ready to make available specific financial or cyber expertise if required.

BOX 2

ROLE OF NATIONAL CYBERSECURITY CENTER AND COMPUTER EMERGENCY RESPONSE TEAM

National Cybersecurity Center

The NCSC responds to cybersecurity incidents across organizations in the country and uses industry and academic expertise to build the country's cybersecurity capability. The NCSC also works to secure public and private-sector networks and prepares publicly available practical guidance to promote knowledge sharing.

Computer Emergency Response Team

Also known as the incident response team (IRT) or the computer security incident response team (CSIRT), the CERT comprises appropriately skilled and trusted members of the organization that handle incidents during their life cycle.

4.5 ACTIVELY SEEKING REGIONAL COOPERATION

Financial entities are often active internationally. In addition, cyber risks do not stop at geographic borders. Therefore, it is recommended that central banks and financial authorities reach out to their peers in countries in their region to *coordinate follow-up actions* regarding the recommendations above and to *establish and cooperate in joint initiatives* where appropriate. As the European Commission and the European Central Bank do at the level of the European Union, the institutions of the African cooperation and/or economic and monetary integration initiatives could play a facilitating role in this.

5. Conclusion

The evidence presented in this report demonstrates that African financial services are already a significant target for a wide range of threat actors. High-value thefts conducted by OCGs and financially motivated nation-states represent the most significant current threat to financial integrity across the continent, while ransomware is an already prominent but growing concern for organizations across all industries. Both African FSIs and their customers face an almost-constant barrage of scamming and social-engineering activity from a largely homegrown class of opportunistic threat actors looking to exploit security loopholes and individual naivety. Additionally, state-level espionage and prolific data theft threaten the confidentiality of financial systems and their data and threaten to cause long-term reputational damage and potential mistrust of digital technologies within the global system.

Building on this evidence and a number of technological, socioeconomic, and geopolitical factors, this report also postulates the most likely threat landscape for African FSIs in the near future. Well-established trends, such as the large-scale and rapid digitalization of financial products and the expansion of the software and hardware supply chain for FSIs, open up new opportunities for cyber-enabled compromise, while efforts to improve formal financial participation across the continent provide Africa's already prolific scammers and hackers with fresh, naive, and digitally unsophisticated targets.

Long-standing economic challenges faced by the continent, compounded by the slow and sporadic recovery from the effects of the COVID-19 pandemic, are likely to exacerbate the existing trend of young, technically skilled, and unemployed (or precariously employed) Africans turning to cybercrime as a quick and lucrative source of income. Technical developments, such as the commodification of hacking tools, accelerate this trend. Conversely, while many African states are pushing to enact robust and effective cybersecurity legislation, significant gaps remain. These gaps, coupled with a general lack of capability and capacity to investigate cybercrimes effectively and arrest and successfully prosecute those involved, will not deter this projected uptake of cybercrime across the continent.

On a global scale, developments in cybersecurity and technologies will exacerbate the already significant security divide between FSIs (and, indeed, most entities) in the developed and developing world. This trend will push threat actors to target entities that are now comparatively less secure in developing regions in greater numbers and volume. Finally, as developments such as climate change, energy insecurity, and geopolitical

power struggles heighten Africa's importance on the global stage, espionage activity from nation-states and other motivated threat actors against such relevant targets as governments, big business, and financial services will similarly increase.

The challenge of coping with the serious cyber threats that Africa's financial sector is facing—and, with it, society in general—is not borne by Africa's banks, payment service providers, and financial infrastructures alone. Financial authorities (including central banks) and governments can help address these challenges by focusing on improving the cyber resilience of both individual financial entities and the financial sector as a collective; on strengthening the cyber resilience and supervisory capacity of central banks and financial authorities; and ultimately on bolstering the cyber resilience of African society at large. Central banks and financial authorities should also actively seek to cooperate with their peers in neighboring countries.

APPENDIX A

Definitions

The intelligence-led model uses historical precedent, trend examples, and prior examples to establish the level of threat of a particular entity. Cyber threat intelligence typically divides threat actors into the following categories, based on their intent and capability:

- **Nation-states:** Established groups working for or on behalf of an incumbent government. Typically, these threat actors are highly sophisticated and well resourced and are capable of compromising even hardened targets. Their motivations typically align with their state's broader strategic objectives, such as conducting espionage against targets, obtaining data, or, for some states, stealing money.
- **Organized cybercriminal groups:** Loose affiliations of individual cybercriminals who pool expertise, tooling, and resources to compromise their victims. OCGs range in capability: Some rival nation-state actors in terms of skill and sophistication, and in some geographies, OCG infrastructure, personnel, and targeting rationale may overlap closely with that of nation-state actors. OCGs are typically financially motivated and seek financial gain in a variety of ways, including manipulating financial networks, stealing and selling data, or using disruptive tactics to extort payments from victims.
- **Hackers:** Individuals unaffiliated with OCGs. Hackers are motivated by a range of factors, including financial gain, notoriety, and general curiosity. Their skillset varies widely. Less skilled hackers are restricted to exploiting system misconfigurations, while more sophisticated individuals have proven capable of compromising well-secured networks to steal data, conduct disruption, or sell access to other cybercriminals. These highly capable hackers tend to be absorbed by collective entities such as nation-states or OCGs.
- **Hacktivists: I**ndividual or loosely affiliated threat actors driven primarily by ideological motivations. Hacktivist attacks focus on disrupting or embarrassing their targets—for example, through DoS attacks, data breaches, website defacement, and social media campaigning. Like hackers, individual hacktivists vary in skill and capability.
- **Malicious insiders:** Former or current employees or staff members who act against their employers. Insiders are driven by a number of motivations, including financial gain or to take revenge on an employer. Although some insiders, such as IT staff, have high levels of technical skill, even unskilled employees can cause serious damage through privileged knowledge of, and access to, systems.
- **Corporations:** Companies, corporations, or enterprises that adopt cyber techniques to obtain a competitive business advantage. Activities usually involve espionage and theft of sensitive data, such as technical intel-

lectual property, trade secrets, or business intelligence, but some corporations may also seek to disrupt the activities of industry competitors for their own gain.

- **Hackers for hire:** Either groups or individuals with moderate to high technical skill who rent out hacking services to third parties. Hacker-for-hire activity usually involves espionage against designated targets. The contractual nature of their activities means that victims are located in a wide range of geographies and industries, depending on the objectives and motivations of their "employer."

Threat intelligence also divides types of attack into the following groups, based on their likely impact on the victim:

- Confidentiality attacks focus on stealing or exposing secret, confidential, or otherwise private information, ranging from customer data to technical intellectual property.
- Integrity attacks focus on manipulating target assets for various purposes, such as adapting security controls to facilitate lateral movement within networks or altering the contents of financial messaging systems to divert legitimate payments or create fraudulent ones.
- Availability attacks disrupt the continuation of systems underpinning key services, such as websites or payment portals, via methods such as DoS attacks, ransomware, or destructive malware.

APPENDIX B

Case Studies

This table details the case studies collected and analyzed for this report. The nature of the report means that these studies are skewed toward more recent events. This should not be taken to mean that malicious cyber activity did not occur in Africa before these dates.

Date	Example
2021	In October 2021, a joint United States-South Africa operation arrested members of Nigeria-based Black Axe OCG, which had stolen over $6.85 million from victims via romance and business email compromise scams (Hyman 2021). The involvement of US authorities indicates that a number of victims were likely based abroad.
2021	In October 2021, the Nigerian Communications Commission alerted the public of a malicious app mimicking popular Android mobile banking applications to spread the Flubot malware. When installed, the app harvests users' online banking credentials and gains access to SMS messages to intercept two-factor authentication codes to approve a fraudulent log-in (Sahara Reporters 2021).
2021	In October 2021, the Central Bank of Nigeria warned that scammers were using Twitter to defraud customers by falsely claiming to disburse 50 billion eNaira, Nigeria's new digital currency, launched on October 25, 2021 (Adegboyega 2021). The campaign likely aimed to obtain Nigerians' banking details for use in further fraudulent activity. This example shows how low-level scammers quickly capitalize on technological developments in the banking sector for their own personal gain.
2021	In August 2021, authorities arrested 39 Nigerians for using lost or stolen SIM cards to empty bank accounts. The group's operating model involved purchasing SIM packs in bulk and reactivating old phone numbers to obtain bank account details (Isamotu 2021).
2021	In July 2021, the Egregor ransomware operators targeted the South African investment and private credit firm Norsad Finance.[11]
2021	In July 2021, ransomware disrupted operations at Transnet, South Africa's state-owned enterprise for rail, port, and pipeline infrastructure. The incident took most systems offline, forcing employees to record vessel movements manually and causing significant logistical backlogs. Although not directly targeting the financial sector, the incident shows ransomware groups' clear intent to capitalize on inadequate security and target critical infrastructure entities in Africa (Reva 2021).
2021	In July 2021, a Nigerian citizen was sentenced for defrauding a US retirement fund out of $1 million by conspiring with an insider to create unauthorized bank accounts, change legitimate bank deposit information, and reroute payments to controlled accounts (Nwezeh 2021).

Date	Example
2021	In July 2021, Angola's largest state-owned bank suffered a disruptive attack against several servers, leaving services at branches in its commercial banking network temporarily limited (Lusa/Ver Angola 2021).
2021	In July 2021, an unidentified threat actor compromised a South African financial services provider and stole databases containing policyholder information, including bank account numbers and card details (Vermeulen 2021).
2021	In April 2021, the founders of South African cryptocurrency exchange Africrypt staged a hack and stole $3.6 billion from investors (Ryan 2021).
2021	Research in March 2021 shows OCG FIN7 conducted attacks on point-of-sale systems in South Africa, aiming to steal customer card data (Seals 2021). The details were then used to make counterfeit cards, which the group used to commit fraud or sold to other cybercriminals.
2021	In February 2021, the operators of REvil ransomware compromised the Union Bank of Nigeria, disrupted system availability, and stole and leaked confidential customer and business data (Hack Notice 2021).
2021	In February 2021, unknown threat actors compromised Angola's Ministry of Finance, accessed emails and shared folders, and stole confidential data (Massala 2021).
2020	In December 2020, a credit analyst at a South African bank stole and sold the personal information of 200,000 customers to an unknown third party (Carnegie Endowment for International Peace 2021).
2020	In December 2020, African Union staff discovered that nation-state threat actors had compromised the security camera system installed in their headquarters for espionage purposes (CSIS 2021).
2020	In November 2020, the Egregor ransomware operators targeted Zimbabwe's Steward Bank, causing several days of system disruption.[12]
2020	In November 2020, Nigerian authorities arrested three OCG members engaging in phishing, malware campaigns, and business email compromise scams against almost 500,000 victims located in Japan, Nigeria itself, Singapore, the United Kingdom, and the United States (Scroxton 2020).
2020	In October 2020, hackers compromised Pegasus Technologies, a fintech service used by numerous mobile network operators such as MTN and Airtel for mobile money payments, as well as providing financial services for a mobile banking platform. The attackers stole about $1 million from Uganda's digital payments system, and 20 million people were affected by the subsequent service shutdown (Kasemiire and Ajuna 2020).
2020	In October 2020, a hacktivist group protesting police brutality targeted the website of the Central Bank of Nigeria with DDoS attacks (Vermeulen 2019). The incident was part of a wider campaign against the Nigerian government, demonstrating how FSIs can be caught up in wider politically or ideologically motivated campaigns (Olufemi 2020).
2020	In September 2020, the Calix ransomware strain infected the Development Bank of Seychelles, a branch of the Seychelles Central Bank (Sweny 2020).
2020	In August 2020, the New Zealand stock exchange was taken offline for approximately two days following several DDoS attacks (BBC News 2020).
2020	In August 2020, Experian South Africa suffered a data breach, resulting in the exposure of personal information belonging to 24 million South Africans and almost 800,000 business entities (Times Live 2020).
2020	In July 2020, Somalia suffered an almost complete internet blackout after the parliament removed the president in a vote of no confidence. The blackout was likely intended to impede coverage of the incident but affected a large number of businesses and Somalia's mobile money services (Netblocks 2020).
2020	In June 2020, employees at a South African bank stole a master key used to decrypt bank operations, access and modify banking systems, and generate keys for customer cards. The employees used the key to access customer accounts, make fraudulent transactions, and steal over $3.2 million (Cimpanu 2020). The incident cost the bank over $58 million in remediation, as well as harder-to-measure reputational damage and loss of customer trust and loyalty. The incident also demonstrates how insiders can leverage their privileged system knowledge and access to manipulate internal systems without immediate detection.
2020	In June 2020, ideological hacktivists targeted the website of Sudan's Ministry of Endowment and Religious Affairs with political slogans. They also allegedly targeted the Ministry of Finance (Sudan News Agency 2020).
2020	In May 2020, Gambian authorities arrested 12 suspects linked to an attack on The Gambia's Trust Bank. Evidence suggests that the suspects worked with insiders in attempts to make fraudulent transactions (The Point 2020).
2020	In January 2020, the South African Banking Risk Information Centre warned about a significant number of attacks on African banks from a Russia-based OCG. The OCG was reportedly attempting to compromise vulnerable FSIs and deploy a variety of malware on compromised systems, with the objective of bypassing internal security controls and redirecting funds (Githahu 2020).
2020	A fraud report from the Ghana central bank reported a 584.1 percent year-on-year increase in card fraud affecting its customers from 2019 to 2020 (Ghanaian Times 2020).

Date	Example
2020	Several hundred thousand victims were defrauded out of a total of $588 million through a pyramid scheme bitcoin scam in 2020 (Chelin 2021).
2019	In October 2019, the South African Banking Risk and Information Centre reported a series of DDoS attacks against multiple African banks' public-facing assets. The attacks were accompanied by a ransom note demanding payment to stop the attacks. The attacks were timed to coincide with payday to cause maximum disruption. While the effects of this campaign were limited, it demonstrated how less sophisticated threat actors seek to disrupt FSIs' availability for financial gain. These attacks coincided with a ransomware attack against the City of Johannesburg's network, which shut down all electronic services, including bill-payment mechanisms, and coincided with month-end processes for supplier and customer payments (Paton 2019).
2019	In September 2019, Garmin South Africa warned customers that their financial information was at risk after a card-skimming script was found on their e-commerce site. Customers who shopped on the site had their home addresses, phone numbers, email addresses, and full payment card and billing address data stolen (Karabus 2019).
2019	In September 2019, a human intelligence source reported that the TA505 OCG was actively targeting large South African FSIs with phishing campaigns, aiming to obtain employee credentials and establish a foothold on banks' networks.[13] TA505 has a history of conducting direct theft operations, suggesting that this was the objective in this scenario.
2019	In July 2019, an unknown OCG deployed ransomware against the large South African energy supplier City Power. The incident was timed to coincide with when many South Africans received monthly paychecks to pay for electricity for the next month. The ransomware encrypted City Power's entire network, including databases and application servers, and temporarily kept many customers from purchasing electricity packages (BBC News 2019). In addition to harming City Power customers, this incident shows how cybersecurity vulnerabilities in other industries can affect FSIs: A loss of power for an FSI could render it unable to process transactions, conduct trading, or engage in other business-critical operations.
2019	In January 2019, an employee at a South African bank attempted to transfer approximately R 100 million (approximately $6.6 million) from a customer's account into accounts controlled by accomplices. The employee used privileged system access to approve replica cards, which would be used to withdraw the funds from ATMs (Hlungwani 2019).
2019	Active since 2019, a Kenyan group named SilentCards has stolen approximately $174 million from Kenyan banks. The group purchases legitimate dormant accounts and co-opts the services of current bank employees to transfer and withdraw significant sums of money from ATMs (Niba 2019).
2019	In 2019, police arrested 77 Nigerians, including a local entrepreneur, for engaging in an online financial-fraud scheme worth almost $11 million (Iwenwanne 2021).
2017–19	Several FSIs in West Africa were targeted by cyberattacks aimed at compromising internal networks and making fraudulent transactions (Symantec Threat Hunter Team 2019).
2018	In November 2018, Mozambique's banking system (including ATMs and card machines) was offline for several days after Portuguese fintech provider BizFirst cut off its services when Mozambique refused to pay a disputed bill (Verdade 2018).
2018	In May 2018, researchers revealed that a financially motivated nation-state group was engaging in a long-term espionage operation against the financial sector. The intrusions affected a number of African FSIs. The operation's likely objective was large-scale data reconnaissance to identify potential targets for future compromise (Sherstobitoff 2018). In 2019, the same group targeted banks in five African countries to compromise internal banking infrastructure and redirect funds (Lederer 2019; The Chronicle 2019). This example shows significant nation-state interest in capitalizing on Africa's generally weaker cybersecurity posture for financial gain.
2018	In January 2018, an OCG stole at least K Sh 29 million (approximately $261,000) from the National Bank of Kenya, with anecdotal reporting suggesting that the actual sum was about K Sh 340 million (approximately $3 million) (PC Tech Magazine 2018). The bank cited a compromise of its internal network.
2007–17	Vendor research in 2017 revealed that a nation-state group had been targeting a number of Africa-based FSIs since at least 2011 and perhaps even 2007. The custom malware used by the group had sophisticated system fingerprinting, discovery, and exfiltration capabilities, indicating that the group was conducting long-term espionage operations against its targets (Johnson 2017).
2017	In November 2017, unknown threat actors temporarily took down the services of Algeria's state telecommunications operator, Algerie Telecom, with a series of DDoS attacks (Paganini 2017).
2016	In May 2016, an OCG targeted South Africa's Standard Bank, compromised internal banking systems, customer databases, and operational safeguards and managed to use forged cards to withdraw over $19 million from ATMs across Japan (Carnegie Endowment for International Peace 2021). More than 260 suspects were eventually arrested, highlighting the extensive infrastructure available to these more sophisticated threat actors.
2016	In October 2016, an individual hacker for hire was contracted by a rival firm to use a botnet to conduct DDoS attacks against a Liberian telecommunications company. The incident left half the country unable to access the internet (Casciani 2019). It was not directed at FSIs, but the level of reliance on mobile infrastructure and the internet to conduct daily banking activities indicates how infrastructure and connection disruption can significantly affect the wider financial industry across Africa.

References

Adegboyega, Ayodeji. 2021. "eNaira: CBN Warns Nigerians of Fraud, Denies Disbursing 50 Billion." *Premium Times,* October 27, 2021, accessed November 2021. https://www.premiumtimesng.com/news/top-news/492085-enaira-cbn-warns-nigerians-of-fraud-denies-disbursing-50-billion.html.

African Development Bank Group. 2021. *African Economic Outlook: From Debt Resolution to Growth: The Road Ahead for Africa*. African Development Bank Group, accessed October 2021. https://www.afdb.org/en/documents/african-economic-outlook-2021.

AfricaNenda. 2021. *The State of Instant Payments in Africa: Progress and Prospects*. AfricaNenda, October 2021, accessed November 2021. https://www.africanenda.org/uploads/files/211005_AfricaNenda-Instant-Payments-in-Africa-Report_vF-1.pdf.

Agosto, Pedro. 2021. "Angola a Top Target for Global Cyber Crooks." *CAJ News Africa*, July 26, 2021, accessed October 2021. https://www.cajnewsafrica.com/2021/07/26/angola-a-top-target-for-global-cyber-crooks/.

Baker McKenzie. 2021. "Africa: Implementation of Cybersecurity and Data Protection Law Urgent across Continent." Baker McKenzie, June 7, 2021, accessed October 2021. https://www.bakermckenzie.com/en/insight/publications/2021/06/africa-cybersecurity-data-protection-law.

BBC News. 2019. "Ransomware Hits Johannesburg Electricity Supply." *BBC News*, July 26, 2019, accessed October 2021. https://www.bbc.co.uk/news/technology-49125853.

BBC News. 2020. "New Zealand Stock Exchange Halted by Cyber-Attack." *BBC News*, August 26, 2020, accessed November 2021. https://www.bbc.com/news/53918580.

BBC News. 2021. "The Lazarus Heist: How North Korea Almost Pulled Off a Billion-Dollar Hack." *BBC News*, June 21, 2021, accessed October 2021. https://www.bbc.com/news/stories-57520169.

BCBS (Basel Committee on Banking Supervision). 2021. *Principles for Operational Resilience*. Bank for International Settlements, March 2021. https://www.bis.org/bcbs/publ/d516.pdf.

BGS (British Geological Survey). 2021. "Lithium Resources and Their Potential to Support Battery Supply Chains in Africa." British Geological Survey, July 14, 2021, accessed November 2021. https://www.bgs.ac.uk/news/lithium-resources-and-their-potential-

to-support-battery-supply-chains-in-africa/.

Brooks, Acadia. 2021. "World Bank 'Growth in the Time of Crisis' Forum to Begin." *Foreign Brief*, October 11, 2021, accessed October 2021. https://www.foreignbrief.com/daily-news/world-bank-growth-in-the-time-of-crisis-forum-to-begin/.

Carnegie Endowment for International Peace. 2021. "Timeline of Cyber Incidents Involving Financial Institutions." Carnegie Endowment for International Peace, 2021 (updated 2021), accessed October and November 2021. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Casciani, Dominic. 2019. "Briton Who Knocked Liberia Offline with Cyber Attack Jailed." *BBC News*, January 11, 2019, accessed October 2021. https://www.bbc.com/news/uk-46840461.

CEA (Council of Economic Advisers). 2018. *The Cost of Malicious Cyber Activity to the U.S. Economy*. Council of Economic Advisers, February 2018, accessed July 2020. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, p. 14.

Chelin, Richard. 2021. "Africa—New Playground for Crypto Scams and Money Laundering." *All Africa*, August 9, 2021, accessed October 2021. https://allafrica.com/stories/202108100118.html.

Chironga, Mutsa, Hilary de Grandis, and Yassir Zouaoui. 2017. "Mobile Financial Services in Africa: Winning the Battle for the Customer." McKinsey & Company, September 1, 2017, accessed October 2021. https://www.mckinsey.com/industries/financial-services/our-insights/mobile-financial-services-in-africa-winning-the-battle-for-the-customer.

The Chronicle. 2019. "UN Investigating North Korean Cyber Attacks in Gambia, 16 Other Countries." *The Chronicle*, August 14, 2019, accessed October 2021. https://www.chronicle.gm/un-investigating-north-korean-cyber-attacks-in-gambia-16-other-countries/.

Cimpanu, Catalin. 2020. "South African Bank to Replace 12M Cards after Employee Stole Master Key." *ZDNet*, June 15, 2020, accessed November 2021. https://www.zdnet.com/article/south-african-bank-to-replace-12m-cards-after-employees-stole-master-key/.

Cooper, Barry, Christine Hougaard, Laura Munoz Perez, Christiaan Loots, Rose Tuyeni Peter, Matthew Ferreira, and Matthew Dunn. 2018. *Payment Systems in Sub-Saharan Africa: Note 2: Case Studies of National and Regional Payment Systems Market Development*. Centre for Financial Regulation and Inclusion, December 2018, accessed October 2021. https://cenfri.org/wp-content/uploads/2018/12/Payment-systems-in-SSA-Note-2.pdf.

CREST. 2021. "An Introduction to CBEST." CREST, 2021, accessed December 2021. https://www.crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf.

CSIS (Center for Strategic and International Studies). 2021. *Significant Cyber Incidents since 2006*. Center for Strategic and International Studies (updated 2021), accessed October 2021. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

ECB (European Central Bank). 2021. "Cyber Information and Intelligence Sharing Initiative (CIISI-EU)." European Central Bank, 2021, accessed December 2021. https://figi.itu.int/wp-content/uploads/2021/06/5_Constantinos_Fiona_ECB.pdf.

Feltman, Jeffrey. 2020. *China's Expanding Influence at the United Nations—and How the United States Should React*. Brookings Institution, September 2020, accessed November 2021. https://www.brookings.edu/wp-content/uploads/2020/09/FP_20200914_china_united_nations_feltman.pdf.

Ford, Neil. 2021. "Africa Walks Development Tightrope as Calls for Oil and Gas Restraint Grow." *African Business*, October 31, 2021, accessed November 2021. https://african.business/2021/10/energy-resources/africa-walks-development-tightrope-as-calls-for-oil-and-gas-restraint-grow/.

Fowler, Gary. 2021. "When Will Quantum Computers Impact Our Day-to-Day?" *Forbes*, April 28, 2021, accessed November 2021. https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/04/28/when-will-quantum-computers-impact-our-day-to-day/.

Francis, Ndubuisi, and James Emejo. 2021. "Nigeria: Digital Currency Gains Traction as CBN Appoints Technical Partner." *All Africa,* August 31, 2021, accessed November 2021. https://allafrica.com/stories/202108310106.html.

Further Africa. 2021. "Angola: e-Kwanza Currency Yields over US$6M." *Further Africa*, January 14, 2021, accessed October 2021. https://furtherafrica.com/2021/01/14/angola-e-kwanza-currency-yields-over-us6m/.

Ghanaian Times. 2020. "Bankers Association Calls for Increased ATM Fraud Education." *Ghanaian Times*, 2020, accessed October 2021. https://www.ghanaiantimes.com.gh/bankers-association-calls-for-increased-atm-fraud-education/.

Githahu, Mwangi. 2020. "SA Banks Ready in Case of Cyber Attack by Russian Hackers." *IOL,* January 16, 2020, accessed October 2021. https://www.iol.co.za/capeargus/news/sa-banks-ready-in-case-of-cyber-attack-by-russian-hackers-40677478.

GSMA. 2019. *The Mobile Economy: Sub-Saharan Africa 2019*. GSMA, 2019, accessed November 2021. https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=45121567&file=2794-160719-ME-SSA.pdf.

Hack Notice. 2021. "Union Bank of Nigeria." Hack Notice, February 27, 2021, accessed October 2021. https://app.hacknotice.com/#/hack/6039759f3d050599d8af9597.

Hlungwani, Victor. 2019. "Bank Worker Stole R1M from Client!" *Daily Sun*, January 31, 2019, accessed November 2021. https://www.dailysun.co.za/News/National/bank-worker-stole-r1m-from-client-20190131.

Hoffmann, Christiane, and Christoph Schult. 2021. "I Have Eliminated 'the West' from My Vocabulary." *Spiegel International*, September 23, 2021, accessed September 2021. https://www.spiegel.de/international/germany/interview-with-merkel-s-former-foreign-policy-adviser-i-have-eliminated-the-west-from-my-vocabulary-a-e3ab1e9d-998f-4d56-9b17-ab950cef5334.

Human, Jurie Hendrik. 2021. "African Countries Continue to Have the Highest Poverty Rates in the World." Development Aid, February 25, 2021, accessed November 2021. https://www.developmentaid.org/#!/news-stream/post/84943/highest-poverty-rates-in-africa.

Hyman, Aron. 2021. "Nigerian Mafia Leaders Arrested after Hawks Swoop in Cape Town." *Times Live*, October 19, 2021, accessed October 2021. https://www.timeslive.co.za/news/south-africa/2021-10-19-nigerian-mafia-leaders-arrested-as-sa-and-us-forces-swoop-in-cape-town/.

Isamotu, Idowu. 2021. "How We Emptied Many Nigerians' Bank Accounts, Stole Millions of Naira—Suspect." *Daily Trust*, August 17, 2021, accessed October 2021. https://www.dailytrust.com.ng/how-we-emptied-many-nigerians-bank-accounts-stole-millions-of-naira-suspect.

Iwenwanne, Valentine. 2021. "More than Email Scams: The Evolution of Nigeria's Cyber-Crime Threat." *N World*, July 21, 2021, accessed November 2021. https://www.thenationalnews.com/world/africa/2021/07/22/more-than-email-scams-the-evolution-of-nigerias-cyber-crime-threat/.

Jibilian, Isabella, and Katie Canales. 2021. "The US Is Readying Sanctions against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal." *Business Insider*, April 15, 2021, accessed November 2021. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T.

Johnson, A. L. 2017. "Longhorn: Tools Used by Cyberespionage Group Linked to Vault 7," Broadcom, April 10, 2017, accessed October 2021. https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7.

Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018. "Exploring SME Cybersecurity Practices in Developing Countries." *Journal of Organizational Computing and Electronic Commerce* 28, no. 3: 269–82, accessed October 2021. https://www.researchgate.net/profile/Salah-Kabanda-2/publication/326385562_Exploring_SME_cybersecurity_practices_in_developing_countries/links/5cd56c2ea6fdccc9dd9d5ae4/Exploring-SME-cybersecurity-practices-in-developing-countries.pdf.

Karabus, Jude. 2019. "Charmin'. Garmin Admits Customers' Full Credit Card Data Nicked from South African Web Store." *The Register*, September 13, 2019, accessed October 2021. https://www.theregister.com/2019/09/13/garmin_breach_notification/.

Kasemiire, Christine, and David Vosh Ajuna. 2020. "Hackers Steal Billions in Mobile Money Heist." *The Monitor*, October 6, 2020, accessed October 2021. https://www.monitor.co.ug/uganda/news/national/hackers-steal-billions-in-mobile-money-heist-2458494.

Kaspersky. 2021. "Types of Mobile Malware." Kaspersky, 2021, accessed November 2021. https://www.kaspersky.co.uk/resource-center/threats/mobile.

Koegler, Scott. 2017. "Cybercrime Has Become a Commodity." *Security Intelligence*, May 23, 2017, accessed November 2021. https://securityintelligence.com/cybercrime-has-become-a-commodity/.

Krebs, Brian. 2021. "REvil Ransom Arrest, $6M Seizure, and $10M Reward." *Krebs on Security*, November 8, 2021, accessed November 2021. https://krebsonsecurity.com/2021/11/revil-ransom-arrest-6m-seizure-and-10m-reward/.

Kshetri, Nir. 2019. "Cybercrime and Cybersecurity in Africa." *Journal of Global Information Technology Management* 22, no. 2: 77–81, accessed October 2021. https://www.tandfonline.com/doi/pdf/10.1080/1097198X.2019.1603527.

Lederer, Edith M. 2019. "UN Probing 35 North Korean Cyberattacks in 17 Countries." *AP News*, August 13, 2019, accessed October 2021. https://apnews.com/ece1c6b122224bd9ac5e4cbd0c1e1d80.

Liang, Nan, and David Biros. 2015. "Identifying Common Characteristics of Malicious Insiders." Paper prepared for the Annual ADFSL Conference on Digital Forensics, Security and Law, May 21, 2015, accessed October 2021. https://core.ac.uk/download/pdf/217154843.pdf.

Lukonga, Inutu. 2018. "Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions." IMF Working Paper WP/18/201, September 11, 2018, accessed October 2021. https://www.imf.org/en/Publications/WP/Issues/2018/09/11/FinTech-Inclusive-Growth-and-Cyber-Risks-Focus-on-the-MENAP-and-CCA-Regions-46190.

Lusa/Ver Angola. 2021. "BPC Suffers Cyber Attack." *Ver Angola*, July 20, 2021, accessed October 2021. https://www.verangola.net/va/en/072021/BankingInsurance/26365/BPC-suffers-cyber-attack.htm.

Massala, Guilherme. 2021. "Angolan Finance Ministry Suffers Cyber Attack." *Menos Fias*, February 23, 2021, accessed October 2021. https://www.menosfios.com/en/angola-finance-ministry-suffers-cyber-attack/. {-OK? PAGE NOT FOUND AT URL-}

Matooke Republic. 2021. "Pegasus Technologies Becomes the First Indigenous Ugandan Fintech to Get BoU License for Mobile Payments." *Matooke Republic*, October 18, 2021. https://www.matookerepublic.com/2021/10/18/pegasus-technologies-becomes-the-first-indigenous-ugandan-fintech-to-get-bou-license-for-mobile-payments/.

Menn, Joseph, and Christopher Bing. 2021. "Governments Turn Tables on Ransomware Gang REvil by Pushing It Offline." *Reuters*, October 21, 2021, accessed October 2021. https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.

Netblocks. 2020. "Somalia Internet Blackout after Parliament Votes to Remove Prime Minister." *Netblocks*, July 26, 2020, accessed October 2021. https://netblocks.org/reports/somalia-internet-blackout-after-parliament-votes-to-remove-prime-minister-DA3lx6BW.

Niba, William. 2019. "Focus on Africa: Kenya: Home-Grown Hackers Have Looted Millions from Banks." *RFI*, May 3, 2019, accessed October 2021. http://en.rfi.fr/africa/20190502-focus-africa-kenya-cyber-crime-buster-trace-home-grown-hackers-looting-millions-bank.

Nield, David. 2021. "Record-Breaking Chinese Supercomputer Marks New Quantum Supremacy Milestone." *Science Alert*, July 14, 2021, accessed November 2021. https://www.sciencealert.com/china-s-latest-56-qubit-computer-marks-another-quantum-milestone.

Nwezeh, Kingsley. 2021. "Nigerian Sentenced to Eight Years Imprisonment in U.S. for $975,863 Fraud." *All Africa*, July 19, 2021, accessed October 2021. https://allafrica.com/stories/202107300104.html.

Office of the Director of National Intelligence. 2021. *Annual Threat Assessment of the US Intelligence Community*. Office of the Director of National Intelligence, April 9, 2021, accessed November 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.

Olewe, Dickens. 2021. "Why African Countries Back China on Human Rights." *BBC News*, May 2, 2021, accessed October 2021. https://www.bbc.com/news/world-africa-56717986.

Olufemi, Alfred. 2020. "#EndSARS: Anonymous Attacks CBN Website." *Premium Times*, October 16, 2020, accessed October 2021. https://www.premiumtimesng.com/news/headlines/421284-updated-endsars-anonymous-attacks-cbn-website.html.

Osborne, Charlie. 2021. "Updated Kaseya Ransomware Attack FAQ: What We Know Now." *ZDNet*, July 23, 2021, accessed November 2021. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.

Osborne, Hilary. 2016. "HSBC Suffers Online Banking Cyber-Attack." *The Guardian*, January 29, 2016, accessed October 2021. https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack.

Paganini, Pierluigi. 2017. "A Massive Cyber Attack Hit the Algerian State Telecom Operator Algerie Telecom." *Security Affairs*, November 21, 2017, accessed October 2021. https://securityaffairs.co/wordpress/65822/hacking/algerie-telecom-cyberattack.html.

Paton, Carol. 2019. "City of Joburg, Banks under Cyber Attack." *Times Live*, October 25, 2019, accessed October 2021. https://www.timeslive.co.za/news/south-africa/2019-10-25-city-of-joburg-banks-under-cyber-attack/.

Pazarbasioglu, Ceyla, Alfonso Garcia Mora, Mahesh Uttamchandani, Harish Natarajan, Erik Feyen, and Mathew Saal. 2020. *Digital Financial Services*. World Bank Group, April 2020, accessed October 2021. https://pubdocs.worldbank.org/en/230281588169110691/Digital-Financial-Services.pdf.

PC Tech Magazine. 2018. "National Bank of Kenya Suffered a Breach—Admits Ksh 29 Million Was Stolen." *PC Tech Magazine*, January 22, 2018, accessed October 2021. https://pctechmag.com/2018/01/national-bank-of-kenya-suffered-a-breach-admits-ksh-29-million-was-stolen/.

The Point. 2020. "Beware of Cyber-Criminals!" *The Point*, May 8, 2020, accessed October 2021. https://thepoint.gm/africa/gambia/editorial/beware-of-cyber-criminals.

Reuters. 2021. "Climate Change to Displace Tens of Millions of East Africans by 2050—World Bank." *Reuters*, October 27, 2021, accessed October 2021. https://www.reuters.com/business/cop/climate-change-displace-tens-millions-east-africans-by-2050-world-bank-2021-10-27/.

Reva, Denys. 2021. "Cyber Attacks Expose the Vulnerability of South Africa's Ports." *ISS Today*, July 29, 2021, accessed October 2021. https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

Ryan, Ciaran. 2021. "Africrypt 'Hack' of Nearly R54Bn Dwarfs Mirror Trading." *Moneyweb*, June 23, 2021, accessed October 2021. https://www.moneyweb.co.za/moneyweb-crypto/africrypt-hack-of-nearly-r54bn-dwarfs-mirror-trading/.

Saeed, Mustapha, and Sone Osakwe. 2021. "Are African Countries Doing Enough to Ensure Cybersecurity and Internet Safety?" *MyITU*, September 1, 2021, accessed October 2021. https://www.itu.int/en/myitu/News/2021/09/01/06/54/Are-African-countries-doing-enough-to-ensure-cybersecurity-and-Internet-safety.

Sahara Reporters. 2021. "New Virus Impersonating Mobile Banking Apps to Steal Money—Agency Warns Nigerians." *Sahara Reporters*, October 22, 2021, accessed October 2021. http://saharareporters.com/2021/10/22/new-virus-impersonating-mobile-banking-apps-steal-money-%E2%80%93-agency-warns-nigerians.

Scroxton, Alex. 2020. "Three Cyber Criminals Arrested in Nigerian BEC Investigation." *Computer Weekly*, November 25, 2020, accessed October 2021. https://www.computerweekly.com/news/252492711/Three-cyber-criminals-arrested-in-Nigerian-BEC-investigation.

Seals, Tara. 2021. "FIN8 Resurfaces with Revamped Backdoor Malware." *Threat Post*, March 11, 2021, accessed November 2021. www.threatpost.com/fin8-resurfaces-backdoor-malware/164684.

Selassie, Abebe Aemro, and Shushanik Hakobyan. 2021. "Six Charts Show the Challenges Faced by Sub-Saharan Africa." *IMF News*, April 15, 2021, accessed November 2021. https://www.imf.org/en/News/Articles/2021/04/12/na041521-six-charts-show-the-challenges-faced-by-sub-saharan-africa.

Seychelles News Agency. 2021. "Seychelles: Cashless Economy—Seychelles' Financial System to Be Entirely Digital by 2023." *All Africa*, September 2, 2021, accessed October 2021. https://allafrica.com/stories/202109030270.html.

Sherstobitoff, Ryan. 2018. "Analyzing Operation GhostSecret: Attack Seeks to Steal Data Worldwide." *McAfee Blog*, April 24, 2018, accessed October 2021. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/.

Sudan News Agency. 2020. "Sudan: Endowments Website Hacked." *All Africa*, June 18, 2020, accessed October 2021. https://allafrica.com/stories/202006190145.html.

Sweny, Gillian. 2020. "Calix Ransomware Attack Hits Development Bank of Seychelles." *AgileBlue Blog*, September 17, 2020, accessed November 2021. https://agileblue.com/calix-ransomware-attack-hits-development-bank-of-seychelles/.

Świątkowska, Joanna. 2020. *Tackling Cybercrime to Unleash Developing Countries' Digital Potential*. Background Paper 33. Pathways for Prosperity Commission, January 2020, accessed October 2020. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf.

Symantec Threat Hunter Team. 2019. "West African Financial Institutions Hit by Wave of Attacks." *Threat Intelligence Blog*, January 17, 2019, accessed November 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/african-financial-attacks.

Tarabay, Jamie. 2021. "Ransomware Hackers Freeze Millions in Papua New Guinea." *Bloomberg*, October 27, 2021, accessed October 2021. https://www.bloomberg.com/news/articles/2021-10-27/papua-new-guinea-s-finance-department-hit-with-ransomware-attack.

This Day. 2021. "Nigeria to Benefit from UK's £22M Cyber Capacity Building Fund." *All Africa*, May 20, 2021, accessed October 2021. https://allafrica.com/stories/202105200105.html.

Times Live. 2020. "Massive Data Attack Exposes Personal Info of 24 Million South Africans." *Times Live*, August 19, 2020, accessed October 2021. https://www.timeslive.co.za/news/south-africa/2020-08-19-massive-data-attack-exposes-personal-info-of-24-million-south-africans/.

Varrella, Simona. 2021. "E-Commerce in Africa—Statistics & Facts." Statista, September 28, 2021, accessed November 2021. https://www.statista.com/topics/7288/e-commerce-in-africa/#topicHeader__wrapper.

Verdade. 2018. "Mozambique: Central Bank Governor Blames Cyber-Attack for Banking Crisis." *All Africa*, November 21, 2018, accessed November 2021. https://allafrica.com/stories/201811210152.html.

Vermeulen, Jan. 2019. "How Much Money DDoS Attackers Demanded from South African Banks." MyBroadband, October 29, 2019, accessed October 2021. https://mybroadband.co.za/news/security/324929-how-much-money-ddos-attackers-demanded-from-south-african-banks.html.

Vermeulen, Jan. 2021. "Bank Account Details Stolen in Major Insurance Hack in South Africa." MyBroadband, July 16, 2021, accessed November 2021. https://mybroadband.co.za/news/security/405878-bank-account-details-stolen-in-major-insurance-hack-in-south-africa.html.

WB (World Bank). 2021. "The World Bank in Africa." World Bank, updated 2021, accessed November 2021. https://www.worldbank.org/en/region/afr/overview.

WBG (World Bank Group). 2021a. *Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches*. Policy Research Paper. World Bank Group, April 2021, accessed October 2021. https://documents1.worldbank.org/curated/en/515771621921739154/pdf/Consumer-Risks-in-FinTech-New-Manifestations-of-Consumer-Risks-and-Emerging-Regulatory-Approaches-Policy-Research-Paper.pdf.

WBG (World Bank Group). 2021b. "Scams and Fraudulent Investment Schemes That Misuse Our Name." World Bank, last updated August 25, 2021, accessed November 2021. https://www.worldbank.org/en/about/legal/scams.

Yade, Rama. 2021. "Africa Is America's Greatest Geopolitical Opportunity. Does the US Know It?" *Africa Source Blog*, May 25, 2021, accessed November 2021. https://www.atlanticcouncil.org/blogs/africasource/africa-is-americas-greatest-geopolitical-opportunity-does-the-us-know-it/.

Endnotes

1. Threat-led penetration testing is also advocated for by the G-7. A good practical example is TIBER-EU, the threat-led penetration testing framework developed by the European Central Bank and currently applied in 11 EU countries. The TIBER-EU framework is jurisdiction and sector agnostic and free to be used. Next to that, reference is made to the CIISI-EU initiative, which has been developed under the aegis of the Euro Cyber Resilience Board and the European Central Bank. The CIISI-EU blueprint is sector and jurisdiction agnostic, free to be used, and currently being implemented in several countries and regions.
2. Closed source.
3. Results obtained from DarkTracer ransomware tracking platform, https://platform.darktracer.com:4430/ (October 2021).
4. In November 2019, under the aegis of the Financial Inclusion Global Initiative, the World Bank published Cyber Resilience for Financial Market Infrastructures, which spells out in concrete, practical terms the expectations for the oversight of cyber resilience developed by the European Central Bank. Next to that, one could be referred to the Principles for Operational Resilience published by the Basel Committee on Banking Supervision (BCBS 2021).
5. Threat-led penetration testing is also advocated for by the G-7. A good practical example is TIBER-EU, the threat-led penetration testing framework developed by the European Central Bank and currently applied in 11 EU countries. The TIBER-EU framework is jurisdiction and sector agnostic and free to be used.
6. Reference is made to the CIISI-EU initiative, which has been developed under the aegis of the Euro Cyber Resilience Board and the European Central Bank. The CIISI-EU blueprint is sector and jurisdiction agnostic, free to be used, and currently being implemented in several countries and regions.
7. September 2020, as part of its Digital Finance Package, the European Commission issued a proposal for an EU regulation on digital resilience for the financial sector, the Digital Operational Resilience Act. While in the final stages of negotiations with European Parliament and EU member states (status February 2022), the legal proposal aims—among other things—to establish an EU-wide oversight regime for "critical ICT third party service providers."
8. This does not need imply that institutional roles and responsibilities are being blurred, nor that it needs to be done in a fully formalized setting. Already agreeing to meet regularly at the senior management level and starting the dialogue will probably make a great difference.
9. The role of an NCSC is ultimately to support organizations in protecting against, identifying, and responding to cyber threats. More acutely, an NCSC distills cybersecurity knowledge into practical guidance for organizations and individuals, responds to cybersecurity incidents to reduce the potential impact, uses industry and academic expertise to bolster national cybersecurity capabilities, and reduces general risk by securing public- and private-sector networks. For more information, see https://www.ncsc.gov.uk/information/about-the-ncsc.
10. The role of a national CERT is to coordinate the management of national cybersecurity incidents; support critical national infrastructure entities in managing cybersecurity incidents; promote cybersecurity situational awareness across industry, academia, and the public sector; and act as a single international point of contact for coordination and collaboration with other national CERTs. For more information, see https://www.gov.uk/government/news/uk-launches-first-national-cert. CERTs can also be established at the sectoral level.
11. Results obtained from DarkTracer ransomware tracking platform, https://platform.darktracer.com:4430/ (October 2021).
12. Results obtained from DarkTracer ransomware tracking platform, https://platform.darktracer.com:4430/ (October 2021).
13. Closed source.

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP