# CYBER SECURITY IN EMERGING FINANCIAL MARKETS

*May 2018, Hildah Nduati*

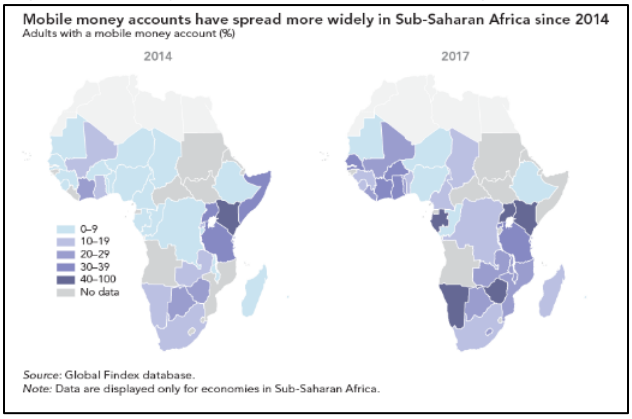
# DISCLAIMER

This work was funded in whole or in part by CGAP. Unlike CGAP's official publications, it has not been peer reviewed or edited by CGAP, and any conclusions or viewpoints expressed are those of the authors, and they may or may not reflect the views of CGAP staff.

Digital financial services (DFS) refers to a broad range of financial services such as payments, credit, savings, remittances and insurance accessed and delivered through digital devices such as computers and mobile phones. DFS offer tremendous promise in enabling financial inclusion by reducing the cost of delivery of formal financial services and thereby making them more affordable and accessible to low-income and remote segments of society. Five decades ago, it was still rare for companies and individuals in developing markets to conduct business using electronic communication channels. Indeed, before Safaricom's introduction of its mobile money service "M-PESA" in Kenya in 2007, it was unheard of for a financial transaction to be conducted over mobile phones. Today, however, millions of people perform transactions on the mobile phone daily and more and more companies rely on electronic communication channels to conduct business. Individuals are also increasingly reliant on mobile payment services to access a wide range of financial products including savings accounts, insurance policies, loans, investment products and bill payments, with the innovations in this area continuing to grow in leaps and bounds.

In Sub-Saharan Africa, mobile financial services have proliferated with non-financial innovators entering the scene to provide more convenient and customer-centered products and services. The region is considered as the global leader in the use of mobile money. In only three years, mobile money account ownership nearly doubled from 12 percent in 2014 to 21 percent in 2017. Kenya's population is still the forerunner with nearly three quarters using mobile money and making a total of 537 million transactions valued at US$ 16 billion during the first quarter of 2017.[1] Uganda and Zimbabwe are following the trend with about half their population using mobile money. In recent years, West Africa has been catching up significantly. In Burkina Faso, Côte d'Ivoire, and Senegal the share of adults owning a mobile money account has risen to about 33 percent—and to 39 percent in Ghana.[2] In both Gabon and Namibia, it has reached nearly 45 percent of the population. (See Figure 1)

*Figure 1: Spread of mobile money accounts across Sub-Saharan Africa between 2014 and 2017.*




Mobile payment services have had a particular impact on the poor by reducing the cost, effort and time while increasing transparency and reliability of money transfers. Across the continent, DFS systems have improved the physical security of people. Farmers, traders and other populations living in remote areas who used to carry cash over long distances, thus exposing them to the risk of theft, can now send and receive money from a mobile phone.

## DIGITZATION INTRODUCES HIGHER CYBER SECURITY CONCERNS

The uptake of DFS has, however, not been without its challenges. The use of mobile networks and the internet for the delivery of financial services has opened the door to new types of risks including denial of service attacks,

[1] Communications Authority of Kenya 2017 "Sector Statistics Report Q3 2017".
[2] Global Findex Database 2017.

unplanned system outages, fraudulent money transfers, identity theft and data breaches.[3] It is important to note that **risks are a product of threats and vulnerabilities**. Threat sources may be natural and environmental (e.g., fire, earthquake) or human (e.g., employees, contractors, customers, externals), while vulnerabilities are weaknesses in an organization's security procedures, design or implementation that make a compromise probable. Table 1 in the Annex summarizes how threats when coupled with certain vulnerabilities can lead to a risk materializing in the DFS environment. The impact that cyber risks can have on the sector is significant. In addition to the financial losses incurred by the industry and consumers, cyber incidents[4] and data breaches harm consumers' trust and confidence in the financial system or individual institutions. Cyber risk therefore is a financial consumer protection concern. Consumers who have been affected by a cyber incident or data breach often lack awareness of and access to customer support and redress mechanisms, particularly the lower income, less literate and remote populations. With the proliferation of cyber threats in the financial services sector and increasing acknowledgement of its potential to negatively affect financial sector stability, integrity, financial inclusion and consumer protection, policymakers are now showing growing interest in improving risk management practices and imposing liability on providers that fail to take reasonable precautions to address vulnerabilities in their environments

## A SURVEY HIGHLIGHTS FOUR CYBER RISKS THAT DFS PROVIDERS IN AFRICA FEAR MOST

In 2017, CGAP conducted a survey of key informants from eleven DFS providers across five countries in Sub-Saharan Africa (including Kenya, Tanzania, Zambia, Uganda, and Ghana) to get a better understanding of how they perceive cyber risks, what threats they are most concerned about and what practices and processes they have in place for managing cyber risks.

*Figure 2: The four most commonly experienced cyber threats in the DFS sector.*


The research found that DFS providers are most concerned about four types of cyber risks: fraud arising from insider and third-party threats, data breaches, phone takeover identity theft, and system downtimes (see Figure 2). These risks have an impact on information systems' Confidentiality, Integrity and Availability—the so-called 'CIA' of information security. The purpose of information confidentiality is to ensure that only those individuals who have the authority to view a piece of information may do so. Unauthorized individuals should not be able to view information that they are not entitled to access. Information integrity is concerned with generation and modification of data. Only authorized individuals should be able to create, change or delete information. Finally, information availability is concerned with ensuring that data, or the system itself is available for use when an authorized user wants to use it.

**Fraud arising from insider and third-party threats**. While providers in the survey highlighted the threat of external attacks as a key concern, the risk that was on most providers' radar was insider attacks arising from a combination of various vulnerabilities in provider environments. The primary vulnerability mentioned was inadequate logical controls, such as lack of user account creation procedures, administrators with excessive access rights, and failure to conduct reviews of current system user access rights, which have led to inappropriate access being granted. Lack

[3] Breaches are incidents that results in the disclosure (not just potential exposure) of data to an unauthorized party.
[4] Incidents are security events that compromise the integrity, confidentiality or availability of an information asset.

of reviews of user access rights was noted to have resulted in retained active access to information systems by employees who had left the organization. Incidents of misuse of these access rights to perpetrate fraud has been observed by most of the providers. In fact, one of the leading mobile network operators in Kenya highlighted in their 2017 annual report that they had fired 52 staff members who were caught engaging in fraudulent activities. While employees remain an organization's most important resource, we observed that providers are now taking a keen interest in how staff access and utilize information assets to achieve corporate objectives, with some providers automating their user access management processes, introducing multi-factor authentication and single sign-on in their systems. We also noted increased audit logging and monitoring of user activities, where anomalies are automatically flagged for review by senior management or independent parties.

*Third parties*. DFS providers are increasingly relying on third parties, including contractors, vendors, partners and suppliers, in the provision of services to their customers. One of the providers interviewed shared that a third-party contractor had misused their existing access rights to fraudulently gain access to confidential subscriber information, the contents of which were sold to interested parties. We found that providers have implemented safeguards to address third party threats such as due diligence reviews of third parties with access to organization systems, implementation of third party access security policies, and stricter logical access controls. One provider noted that third parties were only granted limited access to test systems with no direct access to the operational systems. The third parties thoroughly tested work instructions in the test environment and only after validation, authorized staff members of the DFS provider implemented them on the operational systems.

Data breaches. Data breaches have become an almost daily news item globally and in Africa. A data breach is one of the indicators that an organization's security efforts have failed. While all three elements of CIA are important, for systems that collect and hold a vast amount of confidential, sensitive data, such as customer personal identifying information (PII) and financial transactions, information confidentiality and integrity are the most critical. Through the use of social engineering, phishing and malware, external attackers repetitively attempt to access, disclose or use critical information that can be readily monetized. This information may include credit card numbers, customer personal identification numbers (PINs), login credentials and intellectual property.

Weaknesses in patch management within a DFS provider's environments, coupled with issues such as old legacy systems and lack of system monitoring make these systems particularly susceptible to hacking attacks. In data breach incidents attackers are frequently after personally identifiable information in order to use it or sell it on the black market for identity fraud purposes. For example, in 2017, it was reported that customers of a DFS provider in Kenya were signed up illegally for loan products. From our discussions with key informants, we learned that this was the result of a data breach, where customer details have been acquired and later used to fraudulently swap SIM cards and apply for loans on these customers' behalves. The fraudsters had accessed sensitive information such as the type of account that the customer had, the last transaction done by the customer and other details that are typically used for customer verification.

Phone takeover identity theft. Identity theft usually occurs when a subscriber's Mobile Station International Subscriber Directory Number (MSISDN) is transferred from its current SIM card to a different SIM card without the subscriber's knowledge or consent. In this way, the attacker fraudulently acquires full control of the customer's mobile number. The fraudster may obtain the PIN via social engineering or through breaches of the provider's information system (through an insider or external attack). In an attempt to curb identity theft, most of the providers interviewed have started to use a more elaborate, manual customer verification process. Others are exploring voice biometrics and fingerprint technology to address this concern.

*Social engineering attacks.* One of the most frequently used strategies for perpetrating phone takeover identity theft are social engineering attacks, in which a fraudster convinces an authorized individual to provide confidential

information or access to internal systems and databases. Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) realizing that they are being manipulated. It is made possible due to lack of information security awareness by employees and customers. A variety of social engineering schemes have been observed by the DFS providers surveyed. The most common social engineering attacks that target customers aim for performing a SIM swap. In this scenario, the attacker social engineers a customer into sharing their PIN, security questions and any other details that would be requested by mobile network operators for transferring an existing mobile number to a new SIM card. The fraudster then uses this information to request a SIM swap from the mobile carrier, who deactivates the customer's SIM card and links the phone number to the fraudster's SIM card. As a result, the fraudster gains access to the customer's mobile money account (i.e., account takeover) and can transfer the funds to a mobile money account from which they can withdraw. Newly banked financial consumers are more likely to fall victim to this type of schemes because of their limited previous experience with social engineering and cyber fraud. Social engineering is also targeted at provider employees and seek to gain access to customer details such as their ID number, last number called and PIN, which they then use to perform a SIM swap and mobile money account reset. Social engineering on employees is also used when an attacker plans to breach a provider's systems. DFS providers from all five countries had experienced cases where an employee was social engineered into sharing their user login details which allowed the fraudster to access the providers' key information systems. Sixty percent of the respondents stated that careless or unaware employees are one of the vulnerabilities that have contributed most to their organization's cyber risk exposure.

System downtime. A significant factor that causes customer dissatisfaction with provider services are unplanned system outages. In a study conducted by CGAP in 2015, inability to transact due to network or service downtime was rated as one of the greatest risk areas for DFS consumers, eroding or significantly decreasing the level of trust of consumers and potential consumers.[5] In another study by UNCDF's Mobile Money for the Poor (MM4P) in Uganda in 2015, non-users in urban areas cited an unstable network as the number one barrier to start using mobile money. Likewise, failures in provider change management processes during system upgrades or patches that led to system outages appeared as a common theme in our study. In one of the providers, a mistake made during an approved change process led to a system outage that lasted for more than seven hours, greatly inconveniencing millions of customers. The issue was exacerbated by the failure of the provider's disaster recovery planning as the system was unable to dynamically or manually switch over to the disaster recovery site. At another provider in Kenya, a system outage in 2017[6] left customers without access to their savings and loans products for five days. In this instance, once the system outage was resolved, there were reports of inconsistencies in customer account balances. In fact, system outages have at times acted as a cover up for fraudulent activities during the outage. Denial of service attacks brought about by external threat sources are another leading cause of system outages. To address this type of incidents, providers are placing increased focus on proper change management processes and disaster recovery planning.

## WHAT DOES THIS MEAN FOR THE INDUSTRY AND HOW CAN CYBER RISKS BE EFFECTIVELY ADDRESSED?

First of all, it is important to understand that the relevant question is not how the cybersecurity problem can be solved, but rather how it can be made manageable. Cybersecurity management, a subset of information security, refers to the protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems. It refers to an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are reasonably protected from and/or defended against damage, unauthorized use or modification, or exploitation. It is important

[5] McKee et al. 2015 "Doing Digital Finance Right", CGAP.
[6] Business Daily Africa 2017 "M-Shwari downtime persists for fifth day"

for DFS providers to bear in mind that there are four options for managing risk: risk avoidance, risk mitigation, risk transfer, and risk acceptance.

The first method is **risk avoidance**, where the business activity is not allowed to take place. If this had been followed during the advent of mobile money services, then mobile money would not have spread as successfully, if at all, due to the risk of the unknown for most providers. **Risk mitigation** is the second fundamental way of risk management and includes both technical and procedural approaches, many of which have been explained in the previous paragraphs. The final two methods of risk management address those risks that cannot be avoided nor mitigated. These risks are either transferred or accepted. Providers in emerging markets are now beginning to embrace **risk transfer** through cyber insurance or through outsourcing of various elements of the value chain, such as the management of data centers. Finally, **risk acceptance** has been observed amongst providers with legacy (i.e., old) operating systems that may not be good candidates for patching and upgrades. Coupled with limited budgets, insufficient understanding of the risks and basic mitigation practices as well as limited access to human resources with relevant skills, this has led to providers accepting some of the identified risks and continuing operations with some form of compensating controls.

In the survey, ninety percent of the DFS providers surveyed said that data protection and privacy was a priority for them and a functional area in which they planned to invest more. Eighty percent of the providers have implemented safeguards to mitigate the likelihood of unauthorized access, including data mapping and classification initiatives, as well as technical measures to identify unauthorized access attempts, such as data encryption, data tokenization, audit logging and monitoring. However, overall there is acknowledgement that more safeguards and measures need to be introduced to mitigate the threats and be better prepared to react and respond to cyber incidents.

## WHAT IS THE ROLE OF POLICY TO PROMOTE CYBER SECURITY IN THE DFS SECTOR?

In the near future, regulators will need to nurture a more collaborative approach to keep themselves abreast with the increasingly volatile cyber risk universe given the fast-changing technology and innovations in the DFS sector.

Policy makers in Sub-Saharan Africa recognize the privacy and confidentiality risks that arise from the vast amounts of information held in custody by various organizations. Increasingly, data protection regulations are being developed that require institutions to institute controls to reduce the likelihood of unauthorized release or theft of customers' personal information. In Africa there are twenty-three countries that have put in place legislation to secure the protection of data and privacy and seven countries with draft legislations that are yet to be passed into law.[7]

For example, in 2017, the Central Bank of Kenya released a *Guidance Note on Cyber Risk*[8] as a response to the increasing occurrence of cyber-attacks in the financial sector. This guidance note applies to any financial institution that operates under the Kenya Banking Act (Cap. 488) and outlines minimum requirements that institutions shall build upon in the development and implementation of internal strategies, policies, procedures and related activities aimed at mitigating cyber risk. One of the requirements is the hiring of skilled resources who manage and provide assurance on providers' cyber security programs. Over the past year, there has been an increase in appointments of Chief Information Security Officers (CISOs) in Kenya's financial institutions and a continued up-skilling of internal audit teams to include information system auditors who can assess and propose measures for cyber risk

[7] The twenty-three countries include Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Mali, Gabon, Gambia, Ghana, Ivory Coast, Lesotho, Madagascar, Malawi, Mali, Morocco, Niger, Nigeria, Senegal, Seychelles, South Africa, Swaziland, Tunisia and Zimbabwe. See UNCTAD 2018 "Data Protection and Privacy Legislation Worldwide" and "Cybercrime Legislation Worldwide".
[8] Central Bank of Kenya 2017 "Guidance Note on Cybersecurity".

management. According to the global association of information systems governance, security, audit and assurance professionals (ISACA), as of mid-2018 there were 5,700 certified cybersecurity professionals in Sub-Saharan Africa.[9] These numbers represent only 4 percent of ISACA certified information assurance experts globally.[10]

The Bank of Ghana took a different approach and issued in 2017 a directive for all financial institutions and payment systems operators to obtain international security certifications, such as the ISO 27001 and the PCI DSS, in a bid to promote the integrity of the financial and payment systems.[11]

Given the global and cross-sectoral nature of cyber threats, policy makers will need to collaborate across sectors by sharing information, harmonizing their regulatory requirements and supervising jointly to stay abreast of quickly evolving cyber risks. At the same time, policy makers can benefit from a more collaborative relationship with the industry. For example, the Central Bank of Kenya, worked very closely with Safaricom as they launched their mobile money services in 2007 and benefited from the opportunity to learn together and from each other.

One element that has not been considered much in regulatory frameworks is the principle of data minimization, which requires organizations to collect only the data that is required for providing a specific service, data collected for one purpose cannot be repurposed, and data has to be deleted once the service or transaction was completed. This requirement reduces the amount of information stored and thus reduces the data that could be compromised.

[9] This includes 3,795 holding a Certified Information Systems Auditor (CISA) designation, 945 Certified Information Security Managers (CISM), 646 professionals with a Certified in Risk and Information Systems Control (CRISC) designation, and 324 with other recognized certifications. Note that the highest concentration of cyber security professionals is in Africa's biggest DFS market, Kenya. ISACA registered 586 CISA, 134 CISM, and 42 CRISC professionals in Kenya.

[10] Globally, there were 84,484 CISA, 32,233 CISM, 19,163 CRISC, and 5749 CGEIT and CSXP professionals. See ISACA 2018 "ISACA Certifications by Region".

[11] ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an information security management system. The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

ANNEX

**Examples of Vulnerabilities and Weaknesses that can cause Cyber Security Risks**

| THREAT | | VULNERABILITY |
|---|---|---|
| Malicious insiders | *Coupled with* | Weaknesses in user access rights management e.g.<br>• Inappropriate user authorization policies, processes and procedures<br>• Failure to review user access rights |
| Malicious insiders | *Coupled with* | Lack of logging and monitoring e.g.<br>• Logs do not exist<br>• Logs do not capture key fields / key transactions<br>• Logs are not reviewed<br>• Logs are manual and review is too tedious |
| External attacker | *Coupled with* | Lack of awareness or care by customers and staff<br>• Lack of awareness by customers to not share sensitive information and be alert of scams<br>• Lack of awareness by staff on keeping information secure, e.g. sharing of passwords<br>• Customers or staff vulnerable to phishing or smishing due to lack of awareness |
| External attacker (may use internal resources to infiltrate) | *Coupled with* | • Software vendors do not have the signatures for this malware<br>• Lack of systems monitoring<br>• Shortage of cyber security skills<br>• Background checks not carried out on employees |
| External attacker | *Coupled with* | • Lack of vulnerability and patch management<br>• Lack of system monitoring |
| External attacker | *Coupled with* | • Lack of vulnerability and patch management<br>• Systems not scanned for malware<br>• Lack of system monitoring<br>• Unpatched operating systems, applications, network devices<br>• Lack of cybersecurity awareness and training of staff<br>• Lack of cybersecurity experts e.g. CISO in the organization<br>• Poor security practices, such as employees able to insert thumb dives/ USB sticks into systems in the network; or BYOD introducing insecure devices |
| Malicious insiders/ External attackers | *Coupled with* | Weaknesses in user access rights management<br>• Inappropriate user authorization policies, processes and procedures<br>• Failure to review user access rights |
| Malicious insiders/ External attackers | *Coupled with* | Failure to securely store personal customer data<br>• Visibility of sensitive data (sensitive data stored in plain text)<br>• Customer PII are stored in plain text in the DFS information systems, such as customer PINs, e-Value balances, ID Numbers, collection of data that is not required e.g. credit/ debit cards. |

**Glossary**

| | |
|---|---|
| Application | Any software that is designed to perform a specific function either for a user or another application. |
| Backup | The act of storing data from one system to another system or electronic medium (tape, CD, etc.). Backups can be full, incremental or differential. |
| Database | A collection of data that is organized so that its contents can easily be accessed, managed and updated. |
| Network | A group of computers and associated devices that are connected to share resources. A local-area network (LAN) refers to connected computers and devices geographically close together. A wide-area network (WAN) refers generally to a network of devices that are connected by telecommunications lines. |
| Operating System | Provides the software platform on which all other software programs and applications can run. |
| Patch management | Patch: A piece of software designed to fix problems with or update a computer program or its supporting data<br>Patch Management: An area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system. |
| Recovery | The act of applying stored data to a system in order to allow it to resume normal operations. |

**Acronyms**

| | |
|---|---|
| MSISDN | Mobile Station International Subscriber Directory Number (MSISDN) is a number used to identify a mobile phone number internationally. |
| SIM | A subscriber identity module or subscriber identification module (SIM) is an integrated circuit that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices |
| PIN | Personal Identification Number |
| SMSC | Short Message Service Center (SMSC). This is a network element in the mobile telephone network whose purpose is to store, forward, convert and deliver Short Message Service (SMS) messages. |
| BIA | Business Impact Analysis |
| BCP | Business Continuity Plan |
| DRP | Disaster Recovery Plan |
| GSM | Global System for Mobile Communications |
| ISACA | Global association that advocates for professionals involved in information security, assurance, risk management and governance |
| IMEI | International Mobile Equipment Identity |