CGAP giz

On behalf of
Federal Ministry
for Economic Cooperation
and Development

CYBER SECURITY IN FINANCIAL SECTOR DEVELOPMENT

Challenges and potential solutions for financial inclusion

Silvia Baur-Yazbeck, Judith Frickenstein and David Medine

November 2019

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 Unlike CGAP's official publications, it has not been peer reviewed or edited by CGAP, and any conclusions or viewpoints expressed are those of the authors, and they may or may not reflect the views of CGAP staff.

Table of contents

1. Introduction

Digital financial services (DFS) hold great promise as a means to enable financial inclusion and thus help improve people's lives. However, cybercrime has become a key concern in developing and emerging countries' financial markets and is threatening to hinder global advances in building more inclusive financial sectors. Over recent years, financial markets in Sub-Saharan Africa, the East Asia and Pacific region, Latin America and South Asia have been affected by a rapid increase in the number of cyber incidents and data breaches – and particularly affected are those markets with higher volumes of DFS transactions.[1] While markets in Asia are recording the highest use rates of mobile banking and digital payment applications, they are also experiencing the highest volume of cyberattacks on financial institutions. In 2016, financial institutions in Bangladesh, Indonesia, Japan, the Philippines, Taiwan and Viet Nam were targeted in a series of attacks. In Sub-Saharan Africa and Latin America, cybercrime is also on the rise, with cyber-criminal communities in these two regions growing faster than anywhere else. One explanation for these trends may be the fact that DFS transactions are often carried out using insecure devices and over transmission lines that were not designed to protect the security of financial transactions, which leaves DFS systems and providers more vulnerable. Furthermore, with developed economies building up their defences against cyberattacks, cyber criminals seem to be shifting their attention to easier targets in emerging DFS markets and exploiting their vulnerabilities.[2]

Falling victim to a scam or experiencing system access errors can result in financial and psychological harm[3] and will most certainly affect a customer's confidence and trust in the financial service. A significant cause of customer dissatisfaction with DFS provider services is unplanned system outages. Research on the attitudes and behaviours of low-income mobile money users shows that inability to transact due to network or service downtime was rated as one of the greatest annoyances and resulted in irresponsible behaviours that put the users at risk of being defrauded.[4] The negative experiences prove to deter DFS consumers from using mobile money services more frequently and significantly decreased the level of trust in providers and the financial system altogether.[5] Poor people are particularly vulnerable to fraud and system access errors that can result from a cyber incident. They are often less aware and educated about social engineering attacks,[6] they are more likely to use devices and channels that are not designed to offer the security needed for a financial transaction (e.g., USSD technology[7]) and, most importantly, they can least afford to lose money. Another problem is that in developing countries customers are often liable for losses associated with a cyber incident, or they bear the burden of proving that they were the victim. In 2016 the International Telecommunication Union (ITU) and CGAP surveyed 5,220 mobile money users from Ghana, the Philippines and Tanzania. Fraudulent or scam SMSs had been received by 83% of the Philippine respondents, 56% of the Ghanaian respondents and 27% of the Tanzanian respondents. In both the Philippines and Tanzania, 17% of the mobile money users interviewed reported having lost money to a fraud or a scam, while 12% of the Ghanaian respondents made the same admission.[8] Because trust and confidence in financial service providers (FSPs) and payment systems are key ingredients for sustained financial inclusion, cyber incidents and their associated losses can hinder efforts to expand access to financial services. Furthermore, these kinds of incidents and customers' negative

[1] SWIFT Institute, *Working Paper No. 2016-004: Forces Shaping the Cyberthreat Landscape for Financial Institutions*, 2017; Symantec and the African Union Commission, *Cyber Crime & Cyber Security: Trends in Africa*, November 2016; IBM, *IBM X-Force Threat Intelligence Index 2018*; and Serianu, *Africa Cyber Security Report 2017. Demystifying Africa's Cyber Security Poverty Line*, Digital4Africa, 2017.

[2] SWIFT Institute*, Working Paper No. 2016-004: Forces Shaping the Cyberthreat Landscape for Financial Institutions*, 2017.

[3] Psychological harm may involve feelings of fear, shame and low self-confidence. For those who have fallen victim to a scam, such feelings may also be due to the reputational harm, bullying and ridicule that may result.

[4] McKee, K. et al., *Focus Note: Doing Digital Finance Right*, CGAP, 2015.

[5] Ibid.

[6] See Box 1 for a description of social engineering attacks.

[7] Unstructured supplementary service data (USSD) is currently the simplest communications technology available for delivering mobile financial services to low-income customers. To use USSD, a customer simply dials a number that starts with an asterisk (*) and ends with a hashtag (#). For a useful overview of USSD, see Hanouch, M., *What is USSD & Why Does it Matter for Mobile Financial Services?,* CGAP, 2015.

[8] ITU, *ITU-T Focus Group Digital Financial Services: Commonly identified Consumer Protection themes for Digital Financial Services*, ITU, 2016.

experiences can spread quickly by word of mouth and may potentially end up splashed across the media. In the wake of such damage, it takes a lot of time and effort to rebuild reputations and people's trust.

Box 1. Understanding the symptoms and causes of cybercrime

A cyber or internet fraud targeted at consumers may comprise SMS, emails or telephone calls requesting these customers to send money or to share sensitive personal information (e.g., their personal identification number or PIN) that can then be used for account takeover or identity theft, or it may show up as unauthorised transactions being made from their accounts. A cyber incident can also result in system downtime, making it impossible for customers to access their funds.

In most cases, fraudsters exploit vulnerabilities in the DFS system (which includes DFS providers, payment and settlement systems, point-of-sale networks, regulators and customers) to access, disclose or use critical information that can be readily monetised. The most common cybercrime-related threats include data breaches,[9] customer identity theft,[10] fraudulent money transfers and unplanned system downtime.

Interviews with providers from across Africa identified four types of cyberattack that frequently affect DFS:[11]

1. In a **social engineering attack**, a fraudster manipulates a customer or a provider's employee, getting them to share confidential information or provide access to internal systems and databases. Fraudsters telephone, text message (SMS) or email their targets (a process also known as phishing) to access personally identifiable information, such as credit card numbers, PINs and account login credentials. These can then be used to steal the target's identity, take over their accounts and access customer funds.
2. **Insiders** intent on causing harm are the most common and greatest concern of DFS providers.
3. **Malware, ransomware and denial of service attacks**[12] prevent provider staff, customers and/or third-party systems from accessing a DFS platform and its services. They may also be used to initiate and camouflage a data breach. In a ransomware attack, criminals demand the payment of a ransom in order to return access to devices or encrypted data.
4. **Scams**: The most common DFS scams are advance fee scams and transfer reversal requests. In an advance fee scam, a customer is tricked into sending funds to participate in a fake lottery or to receive a fake reward or gift. In a reversal request, a customer is requested to refund an apparently incorrect deposit that has been transferred into her account.

Based on this understanding, cyber and data security should aim to achieve two goals:

1. **Protect data**, especially sensitive data and personally identifiable information,[13] from unauthorised access.
2. **Protect financial systems** from attacks by cyber criminals, which can result in system downtime and reduced, inefficient or erroneous processes.

Governments in emerging markets have started implementing cyber security strategies with the aim of setting standards for risk management and providing clarity regarding liabilities. However, cyber security management and monitoring require new expertise and resources that are often not available in developing countries due to the lack of: personnel with sufficient background and experience; training centres; providers of cyber assessment and penetration analysis; and financial resources. Research shows that financial sector regulators and providers are finding it increasingly difficult to keep up with cyber criminals, and they frequently have limited resources and in-house expertise. While cyber security support services exist or are emerging in some regions, they seldom include

[9] Breaches are incidents that result in the actual disclosure (not just the potential exposure) of data to an unauthorised party. Attackers frequently seek to obtain personally identifiable information (PII) that they can use or sell on the black market for identity fraud purposes.

[10] A common type of identity theft in the DFS context is SIM swaps. For this, 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, which enables access to temporary PINs or security codes sent via SMS for customer verification.

[11] In 2017, CGAP interviewed 11 DFS providers from Ghana, Kenya, Tanzania, Uganda and Zambia to better understand their perceptions and their practices for mitigating cyber threats. See Baur-Yazbeck, S., *4 Cyber Attacks that Threaten Financial Inclusion*, CGAP, 2018; and Nduati, H., *Cyber Security in Emerging Financial Markets*, CGAP, 2018.

[12] A denial of service (DOS) attack typically functions by overwhelming or flooding a targeted server or system with multiple requests until normal traffic is unable to be processed, resulting in the denial of service to other users. While a DOS attack is launched from a single computer, a distributed DOS (DDOS) attack is launched from many distributed sources.

[13] Personally identifiable information (PII) can include credit card numbers, customer PINs, and login credentials.

provision of the specialized, and affordable, advice and services required by the (digital) financial sector serving low-income populations.

International convening and standard-setting bodies like the G7, the G20 Finance Ministers and Central Bank Governors, and the Committee on Payments and Market Infrastructures (CPMI) at the Bank for International Settlements (BIS) have recognised the risk of cybercrime in the financial sector and the need for a global response to it.[14] In a 2016 joint guidance note,[15] the BIS and the Board of the International Organization of Securities Commissions (IOSCO) emphasised the need for financial market systems, as well as their participants and other connected actors, to enhance their cyber resilience. As a result of this increased attention, cyber risk is now largely acknowledged as “a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide”.[16]

This paper assesses the relevance of data and cyber security for the development of inclusive financial systems in developing countries. Section 2 outlines the challenges that financial institutions and their customers, regulators and supervisors face in managing cyber risks and addressing cyberattacks. Section 3 then offers examples from around the world of governments, industry initiatives and public-private partnerships that are taking steps towards addressing resource and capacity gaps in the sector. Based on this analysis and on lessons drawn from existing examples, section 3.4 set outs a proposal for a regional approach with the potential to effectively provide the support services that are currently missing. The paper concludes with suggestions for further research and experimentation aimed at identifying effective approaches for improving the sector’s resilience to and preparedness for cyber incidents.

2. The current state of cyber security in developing countries’ financial markets

FSPs and their customers, as well as financial sector regulators and supervisors, face challenges in adjusting their behaviours, processes and policies to appropriately address the growing risk of cybercrime and technological failures. To better understand the prevalence and causes of these challenges, in 2018 CGAP conducted a survey of FSPs, DFS providers, financial systems operators, policymakers and data security experts from sub-Saharan Africa. The research showed that policymakers are aware of the issue. They are working to develop regulatory frameworks and build their own in-house capacity so that they can not only effectively guide and supervise the sector but also protect their own data and systems. FSPs tend to become more sensitive to the risk of cybercrime only after they have themselves been targeted. Smaller FSPs tend not to prioritise cyber risks over other risks as the likelihood of an attack is still considered small. Broadly speaking, mobile money operators are more prepared and better equipped to handle cyber risks, especially those operators that are run by international mobile network operators (MNOs), which already adhere to the international security standards set by the telecommunications sector.

The good news is that there is a growing interest among providers and policymakers to mitigate the sector’s exposure to cyber risks. However, these groups lack access to specialised and affordable cyber security support services, and they struggle to source information on cyber threats and good practices that is timely and accessible for people without an IT degree. The lack of cyber security resources is also manifested in local labour markets, where specialised and experienced IT and data security professionals are in high demand and are expensive to hire. The global talent gap in this area is even more pronounced in developing countries, especially in Africa.[17] Representatives from both the public and private sectors would welcome more public-private dialogue and collaboration to address cyber security risks effectively and comprehensively, for example with joint efforts on consumer education.

[14] In 2015 the G7 established the Cyber Expert Group with the aim of identifying cyber risks for the financial sector and developing recommendations for areas of action.
[15] BIS and IOSCO, *Guidance on cyber resilience for financial market infrastructures*, BIS and IOSCO, 2016.
[16] IOSCO, *Annual Report 2017*, IOSCO, 2017.
[17] Serianu 2017 (see full reference above).

2.1. The industry is ill prepared

The financial services industry, in developed as well as developing and emerging economies, has recognised the growing risks of cybercrime. In recent years, the industry has developed standards and guidance for FSPs to help them better protect their networks and their customers. The introduction of multi-factor authentication and chip cards has significantly reduced the theft of consumer credentials, and new tools like machine learning and artificial intelligence are enhancing the industry's fraud detection and resolution processes. More and more FSPs are investing in cyber defences and resilience.

While cyber defences and good online practices are being adopted in developed countries and by large multinational FSPs, medium-sized and smaller FSPs, and particularly those operating in developing countries, remain underprepared. A review of over 700 organisations from across Africa found that the banking sector lost USD 1.05 trillion as a result of cyberattacks in 2017. The review reported that 75% of organisations were not employing security testing techniques, 60% of organisations were not keeping up to date with cyber security trends and attacks, and 75% of the vulnerabilities identified within organisations involved missing patches and software package updates. Indeed, the review states that "Africa's savings and credit cooperative organizations, financial cooperatives and microfinance institutions are the most vulnerable due to weak system safeguards and protections".[18]

Box 2. Cyber risk exposure of Ghana's DFS market

In 2016 Ghana's high rates of credit card fraud, phishing and ransomware attacks placed it in the top ten of African countries affected by fraud and cybercrime attacks.[19] Studies estimate that Ghana lost a total of USD 50 million to cybercrime in 2016.[20] The sector that has been most impacted is banking. Of the attempted frauds affecting Ghana's banking sector in 2017, cybercrime-related fraud cases had the highest overall value (USD 25.8 million), with around one per cent of these cases resulting in an actual loss.[21] Recent years have seen a rise in cyber incidents in the banking sector, involving unauthorised access to FSPs' banking systems by external parties, email fraud, and crime perpetrated through internet banking and other localised payment and mobile banking platforms.[22]

In 2018 Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH and CGAP partnered with the Bank of Ghana to conduct a diagnostic of consumer protection in Ghana's DFS market. The research found that 14% of the 101 interviewees had fallen victim to a scam, including reversal requests (50%) and fraudulent phone calls and SMS (29%). People on lower incomes were more likely to have experienced a scam (19%). Two thirds of the victims (64%) did not take any action after experiencing the fraud; only 14% reported it to the provider's customer care centre and 7% to an agent. Of the individuals who reported the scam to the provider, 57% indicated that no action was taken. In the other cases, providers explained what had happened and the limited liability of the provider (i.e., that they wouldn't recompense). A few offered guidance how to protect themselves from falling victim to a scam.

The 2018 analysis found that customers are more likely to be informed about DFS fraud and scams by their family and friends than by their DFS providers. Overall, customers show little confidence that their providers will help them to resolve incidents of fraud, including cybercrime. Most providers have implemented basic controls and fraud management systems that prevent and help detect cyber fraud. Any actual and suspected fraudulent activities they identify are then reported to the Bank of Ghana on a monthly basis. However, a review of DFS providers' internal policies and processes concluded that only a few of these providers had documented how cases of fraud should be investigated and in which cases customers would be refunded (e.g., where fraud is found to be perpetrated by staff or is the result of inappropriate information security processes). The study also found gaps in providers' policies and procedures to control employee access to customer data and accounts through access controls and, segregation of duties.

[18] Idem.
[19] Symantec and the African Union Commission 2016 (see full reference above).
[20] Serianu 2016 (see full reference above).
[21] Bank of Ghana, *State of Banking Sector Fraud*, 2017.
[22] Arku, J., *Ghana loses Gh¢30.1 million to bank fraud*, Graphic Online, 6 September 2018.

Another study highlights the increase in attacks on mobile banking systems. In Africa, cybercrime in mobile transactions in 2017 cost the sector USD 140 million, which includes losses from SIM swaps,[23] social-engineering[24] and insider fraud (see also Box 2).[25] The vulnerabilities are present on both the provider's and the user's side. Mobile money users frequently fall victim to social engineering attacks due to insufficient awareness and higher levels of credulity. Also, many mobile money applications lack basic security controls such as data encryption, making it easy for criminals to intercept transactions or eavesdrop (see also Box 3). CGAP identified that a consumer's financial information can be intercepted at many stages of a mobile money transaction, meaning there are at least five possible types of attack:[26] (i) eavesdropping by external hackers; (ii) eavesdropping via fake network base stations; (iii) exploitation of roaming technology;[27] (iv) insider eavesdropping; and (v) other threats from malefactors operating inside MNOs and DFS providers.

Other DFS systems have vulnerabilities too. Point-of-sale (POS) devices, for example, which enable digital payments and other types of transactions, have been compromised by malware.[28] Due to the decentralised nature of POS systems, which are located in manifold individual retail outlets, attacks are hard to detect and remedy. In developing countries in particular, POS devices and systems are found to be insufficiently well monitored and protected.

Box 3. Mobile malware

Mobile banking fraud is on the rise and, with customers increasingly using mobile banking applications and mobile payment systems, it will soon become more prevalent than traditional credit card fraud and POS attacks.[29] Between 2016 and 2018 the number of mobile malware attacks nearly tripled. In 2018 at least 9.9 billion users were affected by mobile malware and increasingly by mobile banking malware.[30] Mobile malware is more prevalent in the developing world: the top ten countries by share of users attacked by mobile malware are primarily low and lower-middle income countries, including Bangladesh, Nigeria, India, Indonesia, Pakistan, Tanzania, Kenya and the Philippines.[31] The percentage of mobile devices that were infected with malware are consistently higher in developing countries.[32] Whilst Russia and most countries in Central Asia have the highest reported numbers of mobile malware infections, it is markets in South and East Asia that are seeing the most rapid growth in mobile banking malware.[33] The trend is also true for mobile banking applications. A comprehensive review of 46 Android mobile money applications from 28 developing countries uncovered pervasive vulnerabilities that would allow an attacker to impersonate legitimate users, modify transactions and steal financial records.[34] The majority of these apps failed to provide the protections needed for financial transactions.

Small and medium-sized financial institutions, particularly those in emerging markets, can serve as easy entry points for criminals to access the global financial system. In several cases, criminals have exploited the connections between financial institutions by breaching small banks in order to rob large ones or by taking advantage of less equipped and protected institutions in developing markets in order to gain entry to global banking systems. Frameworks are therefore needed that look beyond individual institutions and take an ecosystem approach to risk assessment and management. So far, there is very little guidance available for assessing vulnerabilities, risks and threats across the (digital) financial services ecosystem. Such assessments could help the industry and policymakers alike to invest their limited resources and capacity where risks are highest and to focus support towards the

[23] See footnote 4 for a description of SIM swaps.
[24] See Box 1 for a description of social engineering attacks.
[25] Idem.
[26] Makin, P., *Cybersecurity for Mobile Financial Services: A Growing Problem*, CGAP, 2018.
[27] When customers use roaming services, they connect to their home network via another MNO's network. Exploiting the links between MNOs that facilitate roaming, an external attacker can impersonate an MNO or DFS provider by sending and intercepting text messages, pushing USSD sessions to customers or listening to voice calls.
[28] IBM 2018 (see full reference above).
[29] McAfee*, McAfee Labs Threats Report: April 2017*, 2017.
[30] Chebyshev, V., *Mobile malware evolution 2018*, Kaspersky Labs, 2019.
[31] Ibid.
[32] McAfee*, McAfee Labs Threats Report: August 2018*, 2018.
[33] Ibid.
[34] Reaves et al., *Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications*, *ACM Transactions on Privacy and Security (TOPS)*, DOI, 2017.

weaker links that pose a threat to the stability and robustness of the overall financial services ecosystem.

2.2. *Policymakers' capacity constraints inhibit understanding and effective regulation and supervision of cyber security*

Cyber criminals are not just targeting consumers and providers; central banks and financial sector agencies can also be the target of attacks. Regulators and supervisors collect and handle confidential and sensitive information about the sector that can be of interest to criminals or may be enough of an asset for criminals to hold them hostage. One example is Bangladesh's central bank, which fell victim to a cyber heist in 2016 (see Box 4).

In addition, regulators and supervisors are becoming aware of the need to develop regulatory frameworks, industry guidance and supervisory processes to ensure that the financial sector is implementing the necessary processes and systems to prevent, detect and effectively manage cyberattacks.

Box 4. The Bangladesh Bank cyber heist[35]

In 2016, hackers obtained the credentials of an employee at Bangladesh Bank, the country's central bank, and installed six types of malware on its IT system. Once they had performed a series of test runs, logging into the bank's system several times, they installed additional monitoring software and deleted files from databases. The hackers then used the access they had gained to the SWIFT system to send payment requests to Bangladesh Bank's account at the Federal Reserve Bank of New York (NY Fed). Because these payment requests from Bangladesh Bank were unusual – the names of the correspondent banks were missing in all the messages – the transfers were not automatically executed. In addition, the sums were unusually high, and most payments were made to individual accounts rather than to institutions. After the first 35 messages were rejected due to incorrect formatting, the hackers simply corrected the formatting and resent them. This time, five payment requests totalling USD 81 million were executed, with the funds being paid into accounts in the Philippines. The money was then transferred to accounts at the Manila-based Rizal Commercial Banking Corporation, after which it disappeared into the Philippine casino system, which is exempt from the country's anti-money laundering regulations.[36]

The hack was successful because the perpetrators managed to erase the fraudulent transcriptions from Bangladesh Bank's records. They also sabotaged communications between Bangladesh Bank and the NY Fed, so the latter's queries and warnings did not reach the Bank. Most banks take special precautions for computers with access to SWIFT. They create multiple firewalls[37] to isolate the system from other bank networks and have the machines in a separate, locked room. Bangladesh Bank's investment in cyber defences was lower than that of other central banks. According to news reports, they used unsophisticated routers and had no firewalls. In addition, the NY Fed's transaction monitoring system was not able to detect the anomalies in real time as it analyses payments only after they are made.[38]

Hackers who tried to steal nearly USD 2 million from India's City Union Bank in 2018 used tactics similar to those employed in the unsolved Bangladesh Bank cyber heist case.[39] Other banks in Ecuador, Russia and Viet Nam have also fallen prey to similar attacks, with individual banks' weaknesses again being exploited to make SWIFT transfers and steal millions. SWIFT claims that its system was not compromised on these occasions. However, with financial security experts pointing out that the SWIFT system is only as secure as its weakest link, SWIFT now requires its users to regularly report on their respective security infrastructure.[40]

[35] This description of a widely-reported event is primarily based on news articles and not official sources. Therefore, it contains information that has not been corroborated. Our intention here is merely to describe how a cyberattack on a financial institution could happen.

[36] Gopalakrishnan, R. and Mogato, M., *Bangladesh Bank official's computer was hacked to carry out $81 million heist*, Reuters, 19 May 2016.

[37] A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

[38] Das, K.N. and Spicer, J., *How the New York Fed fumbled over the Bangladesh Bank cyber-heist*, Reuters, 21 July 2016.

[39] Varadhan, S., *India bank hack 'similar' to $81 million Bangladesh central bank heist*, Reuters, 19 February 2018.

[40] Paulus, S., *Hacker greifen erneut Zahlungsverkehrsystem von Swift an*, DerTreasurer, 19 February 2018.

Regulators, whose aim is to ensure the stability of the financial sector, are being called upon to develop appropriate regulatory frameworks to respond to the challenges that financial institutions and their customers face and to strengthen cyber resilience. At present, law enforcement agencies in developing and emerging countries are struggling to keep up with changes in technology, a situation that is allowing a cybercrime-based economy to flourish. Software that enables encrypted communication and virtual private networks (VPN)[41], on the one hand, can protect activists and dissidents from oppressive regimes but, on the other, has allowed cyber criminals to hide from law enforcement. Encryption makes it more challenging for law enforcement agencies to identify malicious web traffic and track the communications of criminal groups. At the same time, criminals have developed skills and tools to thwart investigators. Law enforcement agencies have long struggled with a lack of resources (i.e., funding, skills, equipment and training) to combat cybercrime, but that is only one of the challenges they face. It is even more difficult to pursue transnational criminals.

In many developing countries, legislation addressing cybercrime is inadequate, punishments are insufficient, and the legal expertise required to prosecute cybercrimes is in short supply. There are also significant procedural hurdles, including issues of jurisdiction, challenges in maintaining standards of evidence, and the difficulty of explaining complex digital crimes to juries. Criminals are frequently left to operate with impunity for several reasons; for example, absence of adequate evidence-sharing and extradition treaties between countries and lack of capacity to investigate cybercrimes, identify or locate offenders, or take culprits into custody.[42]

3. Approaches for addressing the cyber security resource gap

Public and private sector initiatives, including national and international efforts, are now emerging that seek to address the urgent need for information, technical advice, training and incident response. The markets in developed, emerging and developing countries feature a number of good practice examples, where providers and/or public sector agencies have teamed up to share information and provide support to the financial sector. Some of these efforts are led by the public sector, but most are private sector led or comprise public-private partnerships.

3.1. A few governments invest in building public cyber security support structures for the financial sector

In developing markets, the cyber security efforts led by governments or public agencies often do not target the private sector as customers. Due to limited capacity and resources, national cyber security initiatives tend to focus on serving public agencies and critical infrastructure - the most important assets for market stability and integrity. Yet, even for serving their own agencies and market infrastructure, capacity and resources are often insufficient to effectively train and educate public agency staff, recruit technical experts and provide the support that regulators and supervisors need.

Common national support structures are computer emergency response teams (CERTs) or national computer security incident response teams (CSIRTs) that assist when an IT or data system has been attacked.[43] In Africa, more and more governments are setting up such structures, with a few already

[41] A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security and management of the private network.

[42] SWIFT Institute, 2016 (see full reference above).

[43] While the terms CSIRT and CERT are often used synonymously, they are technically distinct. CERTs usually work with the internet community to facilitate its response to computer security events and to raise awareness and provide guidance on improving computer system security. A CERT's work usually involves providing 24-hour technical assistance to respond to computer security incidents and system vulnerabilities. CSIRTs are usually the teams responsible for receiving, reviewing and responding to computer security incident reports and activities. Their services are usually performed for a defined party, which can vary from a corporation to a paying client. A CSIRT may be a formalised team or an ad hoc team.

up and running. However, the CERTs and CSIRTs often lack capacity and struggle to keep up with the rapid changes occurring in the cyber threat landscape, which, in turn, impacts on the advice and support they can provide to industry. Only a handful of countries have CERTs that specialise in responding to financial sector threats and incidents. It is usually the case that the range of services provided by these teams is very limited, services are not available 24/7 and seldom include an emergency response line. Important service gaps include security operations centres,[44] industry-wide and regional threat information sharing, policy advisory services, financial-sector-specific advisory services, and educational programs for businesses and individuals.

Good practice examples include the following:

- **Ghana's National Information Technology Authority** (NITA) has set up a team that supports government agencies with IT services and support, including data and IT security services. In addition, the NITA hosts the national data centre and manages its operations and security. They facilitate threat information sharing across Ghana's agencies and critical infrastructure and collaborate with the cyber security unit of the National Police.
- In **Israel**, the Ministry of Finance and the Cyber Directorate in the Prime Minister's Office jointly established in 2017 a **Cyber and Finance Continuity Center**. This Center is part of the country's Financial CERT and offers specialised cyber security support services to the financial sector, including training, situation analyses, a platform for threat information sharing and cooperation, and incident response. The Center is responsible for strengthening the financial sector's resilience against attacks, which it achieves by proactively identifying threats and promoting protection, advancing preparedness, and collaborating with financial institutions worldwide.

3.2. *Financial sector providers and associations are leading collaborative efforts to enhance their cyber resilience*

In most developed countries, and several emerging and developing countries, private sector players are teaming up to share threat information and jointly combat financial fraud and cybercrime. In many cases banking associations have taken the lead in formalising exchange of cyber threats. Sometimes, only a few actors will agree to collaborate and set up a partnership, with other parties then joining over time. Partnerships come in different forms and they are not always limited to financial sector actors; they have also included firms from the IT, telecommunications and intelligence sectors. More recently, there has also been a sharp increase in the number of cyber security and financial security companies (so called 'FinSec' companies), often of a smaller size, that see a niche market in providing cyber security products and services to FSPs and fintech companies. Another development is the increase in cyber insurance products, especially among large multinational insurance companies.

Good practice examples include the following:

- **The German Competence Centre against Cyber Crime e.V.** (G4C) was set up by three commercial banks in 2013 to collaborate on identifying and eliminating security risks at an early stage. The G4C has expanded its partnership to other members, including German credit bureaux, KfW Development Bank, banking consultancy firms and IT security firms. It also cooperates with Germany's Federal Criminal Police Office and Federal Office for Information Security. G4C's approach consists of addressing the challenges posed by the high degree of networking in business processes and the consequent dependence on functioning IT systems. It builds highly specialised teams that work together on an interdisciplinary basis with the overall objective of exchanging knowledge and experiences and sharing threat information to improve participants' cyber resilience.
- **Suricate Solutions in Senegal** has established a cyber security support centre for microfinance institutions that offers a range of services and solutions, including technical advisory services, systems monitoring and incident response, technical audits and assessments, and training. Suricate Solutions was set up in 2015 to support the financial inclusion sector in West Africa. With

[44] A security operations centre (SOC) monitors and analyses activities in a computer system to detect anomalies and protect the system from cyberattacks.

its headquarters in Senegal and one service point in Côte d'Ivoire, Suricate Solutions provides basic cyber security services to microfinance institutions in these two countries. In Senegal, Suricate Solutions partners with a local university, offering on-the-job training to IT students. While the local teams are equipped to detect suspicious activity and handle basic incidents, more difficult cases are escalated to a partner firm in Luxembourg with relevant capacities. The company's vision is to expand across the continent, serving clients throughout Africa.

- The **South African Banking Risk Information Centre** (SABRIC) is a non-profit company that was set up by South Africa's four major banks to coordinate interbank activities aimed at addressing organised bank-related financial crime, violent crime and cybercrime. SABRIC is housed within the South African Banking Association, from where it serves all its 20+ members from the banking and payments sector. A key aspect of SABRIC's work is to facilitate collaboration and the exchange of information among its private sector members and South Africa's regulatory and supervisory bodies. SABRIC also leads public awareness and education programmes that seek to educate the public on how to protect themselves.
- The **Thailand Banking Sector CERT** (TB-CERT) was set up in late 2017 by the Thai Bankers' Association and the Thai Government. It focuses on sharing threat information and best practices among its members, provides training and capacity building, and facilitates dialogue between the industry and its regulator. The public sector – primarily the Bank of Thailand and the Thai Electronic Transactions Development Agency – has supported the establishment and operations of the TB-CERT.
- **The United States' Financial Services Information Sharing and Analysis Center** (FS-ISAC) was set up in 1999 by a consortium of US-based FSPs in response to a Presidential Decision Directive that mandated the public and private sectors to share information about physical and cyber security threats and vulnerabilities via information sharing and analysis centres (ISACs). In recent years, the FS-ISAC has developed into a global organisation that supports the financial services sector through threat intelligence sharing, cyber exercises, training and education. They also share threat information with government agencies and other critical infrastructure ISACs and collaborate with international and regional financial sector councils. The FS-ISAC has over 7,000 members from 50 countries across Africa, Asia, Europe, North America, Oceania and South America.

3.3. *Promising cyber security initiatives are building on public-private partnerships*

Cross-sectoral and public-private collaboration is increasingly seen as a necessity for combating cybercrime and effectively mitigating risks. In most countries, some form of public-private dialogue is already happening, particularly in the financial and telecommunications sectors.

Good practice examples include the following:

- **Israel's National Fintech-Cyber Innovation Lab** is led by the country's Ministry of Finance, Financial CERT and Cyber Directorate with the objective of promoting innovation in the fintech and cyber industries and stimulating foreign investment. The Innovation Lab enables Israeli startups to develop, test and demonstrate cyber security technologies for the financial sector. It offers startups a testing ground with simulated financial systems, processes and data. The initiative is supported by the country's Cyber and Finance Continuity Center (see section 3.1), national stakeholders in the financial and regulatory ecosystem, government agencies and academia.
- **Luxembourg's Cyber Competence Center** is a centralised and shared resource centre that supports the public and private sectors, as well as individuals, on effectively managing cyber security. Created in 2015, the Center is a public-private partnership that receives two-thirds of its funding from government and the remainder from its commercial operations. Its services include the Computer Incident Response Center, awareness raising and information sharing, the security level ranking of internet service providers, malware information sharing, information leakage analyses, training and tools for IT security, and the management of a community of practice.

- **Nigeria's Electronic Fraud Forum** is a public-private dialogue platform for exchanging information and sharing knowledge on fraud issues among key stakeholders, which include representatives from banks, mobile payment operators, payment systems operators, national security and intelligence authorities and the Central Bank of Nigeria. The Forum meets every two months to facilitate collaboration on mitigating and tackling fraud as well as restoring public confidence in card usage and electronic payments.

3.4. Multi-country approaches can help overcome the resource gap through economies of scale and scope

Two key challenges arise when working to make cyber security support services available in developing countries. First, these countries have a limited number of cyber security experts, particularly experts that understand cyber threats in the DFS context. Second, there is a likelihood that the economies of some developing countries may not generate enough in-country demand to fully support the business of an affordable cyber security resource centre. Therefore, an effective solution to the cyber security resource gap may be the creation of regional cyber security resource centres that can harness a region's available expertise and create a critical mass by serving the demands of multiple countries. These regional centres can be specialised for financial services sectors and their related sectors, can serve both the public and the private sectors, and can act as an impartial platform for public-private collaboration and exchange, including the sharing of threat information. Due to their multi-country set-up, regional centres will be able to facilitate cross-border exchange, operate early warning systems, and share regional trends, threats and good practices with other regions and global platforms. Another advantage of the regional centres is the possibility of linking them with cyber security resource centres in more developed economies, which can provide backup support, expertise and tools that may not be available at the regional level. For example, a regional cyber security centre in West Africa could escalate severe incidents to a cyber support hub in Europe. Indeed, a number of actors in Europe and Africa are already working to design and develop such regional cyber security resource centres.[45]

At present, there are only a handful of initiatives that support stakeholders across multiple countries and facilitate dialogue and exchange across borders. One such example is the FS-ISAC threat sharing network, which has been expanding globally and establishing regional hubs in Asia and Europe. Most of the multi-country initiatives tend to be global efforts with sector-generic services; their specialization is usually in the type of services provided. Small and medium-sized financial services providers and governments with limited resources and capacity criticise that these initiatives are difficult to access. They would prefer a one-stop shop where they can access specialized services and exchange information with peers from their region.[46] Inclusive multi-country efforts that provide affordable and specialised services for the (digital) financial services sector are urgently needed to effectively support the growing DFS sector in developing countries.

Existing multi-country efforts include the following:

- **The Global Cyber Security Capacity Centre** at the University of Oxford in the UK is a research centre for cyber security capacity building. The Capacity Centre operates globally, and its offerings include the provision of training and support to governments and enterprises in developing countries. The Capacity Centre's capacity-building programmes and its Cybersecurity Capacity Maturity Model for Nations (a framework for assessing the maturity of a country's cybersecurity capacity) span sectors and do not involve financial-sector-specific guidance.
- **The World Economic Forum's Global Centre for Cybersecurity** is a global platform that was launched in 2018 to support collaboration between Forum members on successfully countering organised digital crime. The goal of the Global Centre is to promote cooperation on cyber security challenges by facilitating collaboration, information exchange and the development of common

[45] CGAP is currently working on a concept and business plan for regional cyber security resource centres for forthcoming publications.

[46] Feedback from CGAP interviews with providers, regulators and supervisors from across Africa.

standards among governments, businesses, experts and law enforcement agencies. Similar to the University of Oxford’s Capacity Centre, the platform does not yet offer specialised services for financial sector actors.

3.5. Development partners can support the sector to become more cyber resilient

Development partners and donors have an important role to play in supporting developing and emerging markets to address the cyber security resource gap. Specific approaches for supporting the sector include the following:

1. Raising partners’ and clients’ awareness and building data security and protection into programme design.
2. Supporting public and private partners to implement good cyber security hygiene and train their staff on this subject. This work may involve developing curricula and training trainers, which donors can support financially and by facilitating North–South exchange and collaboration.
3. Supporting regulators and supervisors to build their capacity to regulate, supervise, enforce and advise the industry and consumers on good cyber security hygiene and appropriate responses to cyber incidents. Plus, raising awareness of the need to develop corporate cyber security strategies and involve both board and management in the leading of these strategies.
4. Supporting the public and private sectors on their provision of consumer education and consumer recourse. Lower-income populations in particular, are less aware of the risks associated with using digital devices and services and feel less empowered to seek help from providers or policymakers. Although CGAP research shows that poor people care about their privacy and data security, their need for funds can pressure them into accepting less-protective products.[47] Donors and development partners can support public education programmes and can advise policymakers and industry actors on building appropriate and effective customer recourse and support mechanisms.

For example, GIZ is working with its public and private financial sector development partners on building up and integrating strong cyber security controls across the entire risk management structure. In India and Pakistan, GIZ is involved in the development of a Health Risk Management App,[48] which provides users with: an electronic wallet for making payments for health services in hospitals and pharmacies; digital health training courses for better risk management; and, online consultations and prescriptions. Because a large amount of sensitive data is collected via and used by the app, user data security and privacy are crucial. Simulated cyberattacks are carried out that seek to hack the app and, in so doing, identify any security gaps, which can then be addressed. Further work to protect app users’ personal data includes the regular analysis of the app’s IT infrastructure, work to identify weak points and the adaptation of the app to meet EU General Data Protection Regulation (GDPR) standards.

[47] CGAP, Data Privacy and Protection, CGAP, 2019.

[48] The app was created as part of the work of the strategic alliance between GIZ and Allianz SE. See also https://www.developpp.de.

4. Conclusion

Banking services are moving to digital at an ever-faster rate and, in developing economies, are increasingly being used by low-income and low-literacy users. However, concurrent with this progress, sector actors are facing a growing risk from cyber criminals seeking to attack their systems and consumers. If the sector is to continue building and maintaining consumers' trust and confidence in financial systems, it needs to build its defences and ability to respond and recover from potential attacks.

Protecting the financial sector and securing global advances in financial inclusion not only depends on FSPs improving the security of their own systems, but also requires a system-wide approach to security. Governments and providers need to collaborate within their jurisdictions as well as with peers around the world to exchange intelligence and support each other in fighting cyber criminals. Actors with more capacity will need to provide their weaker peers with support, because doing so will provide benefits in terms of reciprocity and will help safeguard these actors' own systems and the public's confidence in the sector.

In addition, debates on cyber and data security in the financial sector must be accompanied by and embedded in discussions on data protection and the responsible use of personal data. Data protection policies and regulations cannot be successful unless the information systems and the data they contain are secured against unauthorised access and misuse. Regulatory frameworks need to require the financial sector to implement adequate information and data security standards that ensure the reliable provision of the sector's products and services, safe processing of data by its systems and responsible use of personal data.

Given that the development community is promoting financial inclusion through digital and remote financial service solutions, it also has a responsibility to support the sector to manage cyber risks. As impartial actors, international organisations and development partners can facilitate public-private dialogue, support effective policy reform processes and help build support structures that enable the sector to keep up with the rapidly evolving risk landscape.