Developing Country Central Banks of the Future as Cybersecurity Champions, Coordinators and Cheerleaders

By David Medine and Silvia Baur-Yazbeck, Consultative Group to Assist the Poor

Paper: Central Bank of the Future: A project organized by the University of Michigan Center on Finance, Law & Policy and the Gerald R. Ford School of Public Policy

Topic: Cybersecurity

Abstract:

Financial sectors are prime target for cyber criminals, both individuals and state actors, and no government entity has a greater interest in protecting the functioning of financial institutions than a country's central bank. Furthermore, when exercising its supervisory and enforcement powers, central banks have a unique insight into whether appropriate steps have been taken by regulated financial institutions, and sometimes even unregulated entities, to be more resilient against cyber attacks. Because central banks are repositories of highly sensitive information concerning their country's financial system, they also have a strong interest in defending against misappropriation of their own data.

Financial markets in developing and emerging countries are becoming increasingly attractive targets for cyber criminals as more developed countries strengthen their cyber defenses. The proliferation of digital financial services and increasing interconnectedness of financial systems and markets is exacerbating the threat that cyber attacks pose to financial sectors in developing countries as well as globally. Building strong cyber resilience is crucial for the stability of financial markets as well as for financial inclusion. Cyber attacks could chill financial inclusion efforts because, if successful, they could deter customers from adopting new financial products and services.

In most developing countries, there is no government agency that has been assigned or has assumed the responsibility for protecting the financial sector from cyber threats. Governments are setting up computer security incident response teams and similar structures, with a few already up and running, but two things are lacking: (1) national coordination and (2) technical capacity. Coordination has been a challenge because governmental authority over the financial sector is often divided between multiple agencies including both bank and non-bank financial institution regulators. Entities such as money transmitters, mobile money operators, microfinance institutions, fintechs, and others have their own regulators or fall through the cracks. There may have been reasonable rationales for this as the safety and soundness considerations for banks may

not apply to other financial entities. However, given the growing interconnectedness of financial and non-financial systems and providers, cyber attacks pose a threat to the financial sector as a whole. Therefore, there is a growing need for one entity to have a national perspective on the threat that is posed and the steps taken to combat it. This policy paper suggests that due to central banks' unique institutional advantages, the central bank of the future could fill this oversight and coordination role, even if its regulatory scope is not expanded.

Background

Cybercrime has become a key concern of financial sector regulators in developing and emerging countries as it is threatening to hinder their advances in building more stable and 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 high volumes of digital financial transactions. 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 digital financial 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 digital financial services (DFS) systems and providers more vulnerable. Furthermore, with developed economies building up their defenses against cyberattacks, cyber criminals seem to be shifting their attention to easier targets in emerging markets and exploiting their vulnerabilities.

Financial services providers (FSPs) and their customers, as well as financial sector regulators and supervisors, face challenges in adjusting their behaviors, 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 prioritize 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 often lack access to specialized and affordable cybersecurity 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 cybersecurity resources is also manifested in local labor markets, where specialized 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. Representatives from both the public and private sectors would welcome more public-private dialogue and collaboration to address cybersecurity risks effectively and comprehensively, for example with joint efforts on consumer education.

Cybersecurity Is a Priority Responsibility for Financial Sector Regulators

The security and reliability of financial sector infrastructure and institutions is a cornerstone of formal financial systems' value proposition to its customers. As a result, historically a key role central banks have played is to ensure the stability and integrity of banks. Countries' economic systems could collapse if this is not maintained. Likewise, central banks can also serve an important role in adopting consumer protection requirements and promoting and enabling financial inclusion. Cybersecurity goes beyond central banks' core expertise which in the past has been focused on safety and soundness and prudential regulation. In the digital age, central banks cannot afford not to step up to the challenge of effectively regulating and supervising on cybersecurity. Otherwise, the entities they oversee could suffer massive losses and bring the financial system down with them. As central banks develop cyber expertise, it positions them to serve more broadly as their country's cyber threat coordinator.

From the consumer's perspective, falling victim to a scam or experiencing system access errors can result in financial and psychological harm and will most certainly affect a customer's confidence and trust in the financial service. A significant cause of customer dissatisfaction with DFS is unplanned system outages. Research on the attitudes and behaviors 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 behaviors that put the users at risk of being defrauded. 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. 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, they are more likely to use devices and channels that are not designed to offer the security needed for a financial transaction (e.g., Unstructured Supplementary Service Data (USSD) technology) and, most importantly, they can least afford to lose money. A related 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. 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 and use of financial services. Furthermore, these kinds of incidents and customers' negative 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.

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

Governments in emerging markets have started implementing cybersecurity strategies with the aim of setting standards for risk management and providing clarity regarding liabilities. However, cybersecurity 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 centers; 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 cybersecurity support services exist or are emerging in some regions, they seldom include provision of the specialized, and affordable, advice and services required by the digital financial sector serving low-income populations.

Role that Central Banks of the Future Can Play

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 recognized the risk of cybercrime in the financial sector and the need for a global response to it.[1] In a 2016 joint guidance note,[2] the BIS and the Board of the International Organization of Securities Commissions (IOSCO) emphasized 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".[3]

Many countries have national support structures in the form of computer emergency response teams (CERTs) or national computer security incident response teams (CSIRTs) that assist when an IT or data system has been attacked.[4] For instance, Ghana's National Information Technology Authority supports government agencies needing IT assistance, hosts and provides security for the national data center, and shares threat information. Israel's government has established a Cyber and Finance Continuity Center to provide cybersecurity support services to the financial sector by proactively identifying threats and promoting protection and preparedness.

[1] 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.
[2] BIS and IOSCO, *Guidance on cyber resilience for financial market infrastructures*, BIS and IOSCO, 2016.
[3] IOSCO, *Annual Report 2017*, IOSCO, 2017.
[4] 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 formalized team or an ad hoc team.

Aside from identifying what needs to be done, there is also the question of technical cybersecurity capacity. National 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 specialize 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 centers,[5] industry-wide and regional threat information sharing, policy advisory services, financial-sector-specific advisory services, and educational programs for businesses and individuals.

While central banks are not likely to have the necessary level of technical expertise, they can be the key actor in a country trying to acquire it. As discussed further below, particularly in the case of small- and medium size economies, the central bank of the future could work with central banks of neighboring countries to help form regional cybersecurity resource centers.

Central Banks of the Future Could Promote Centers for Regional Cooperation and Collaboration on Cybersecurity

Two key challenges arise when working to make cybersecurity support services available in developing countries. First, these countries have a limited number of cybersecurity 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 cybersecurity resource center. Therefore, an effective solution to the cybersecurity resource gap may be the creation of regional cybersecurity resource centers that can harness a region's available expertise and create a critical mass by serving the demands of multiple countries. These regional centers can be specialized 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 centers 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 centers is the possibility of linking them with cybersecurity resource centers 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 cybersecurity center 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 cybersecurity resource centers.

At present, there are only a handful of initiatives that support stakeholders across multiple countries and facilitate dialogue and exchange across borders. Examples of global cybersecurity efforts include the Global Cybersecurity Capacity Centre at the University of Oxford in the UK, which focuses on the development and provision of cybersecurity capacity building programs. It also offers training and support to governments and companies in developing countries. The World Economic Forum's Global Centre for Cybersecurity also operates at a global scale. Its goal is to promote cooperation on cybersecurity challenges by facilitating collaboration, information

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

exchange and the development of common standards among governments, businesses, experts and law enforcement agencies.

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 criticize 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.[6] Inclusive multi-country efforts that provide affordable and specialized services for the digital financial services sector are urgently needed to effectively support the growing DFS sector in developing countries.

Central banks as champions of regional cybersecurity resource centers have the regulatory advantage of being able, in many cases, to mandate their use. This creates an immediate customer base for the centers, which increase the time frame in which they can become self-supporting. It also creates a nationwide standard of care which will put pressure on all financial firms to follow, even if not mandated by the central bank.

In addition, central banks typically are members of regional or other networks of central banks. Such networks could serve as a forum for establishing or promoting the establishment of regional centers, and possibly even housing such centers. In some cases, it will be necessary to obtain startup grants to cover organizational and capital expenses associate with getting regional centers off the ground. Central banks could join forces with the private and philanthropic sectors to provide the necessary funding.

Central Banks of the Future Could Promote Threat Sharing

As new cyber threats appear, it is critical that attacked entities share those threats with others in their sector, country, region and beyond. Banks and other financial institutions around the world that are normally fierce competitors, often join forces to share cyber threats because they well understand the risk that such threats pose to their sector, customers and reputation.

Central banks, in their role as national cyber coordinators, can mandate (where authorized to do so) or strongly encourage and incentivize all financial service providers in their jurisdiction to participate in threat sharing systems.

There are good examples of threat sharing communities that facilitate exchange of threat information among public sector private sector players, including 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 **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 organized bank-related financial crime, violent crime and cybercrime.

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

- The **Thailand Banking Sector CERT** (TB-CERT), set up by the Thai Bankers' Association and the Thai Government, 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 United States' Financial Services Information Sharing and Analysis Center** (FS-ISAC) is a global organization that supports the financial services sector through threat intelligence sharing, cyber exercises, training and education. The FS-ISAC threat sharing network has been expanding globally with regional hubs in Asia and Europe.

Central Banks of the Future Could Promote Security Standards

Protecting against cyber attacks involves more than firewalls and antivirus software. It entails educating staff to avoid social engineering, including phishing attacks, care with use of thumb drives, and locking computer center doors. The central bank of the future could be the country's central repository for standards, guidance and tips for how to protect data, as well as consumer and business education. It could also emphasize to financial institutions the sometimes underappreciated insider threat posed by employees by ensuring that cameras, audit mechanisms, background checks and related precautions are taken.

Central Banks of the Future Could Promote Development of New Technologies

Central Banks are uniquely positioned to promote innovation in cybersecurity technology solutions for the financial sector. As a related example, Israel has implemented a National Fintech-Cyber Innovation Lab. The Lab is led by the Israeli Ministry of Finance, Financial CERT and Cyber Directorate with the objective of promoting innovation in the fintech and cyber industries and stimulating foreign investment. It enables Israeli startups to develop, test and demonstrate cybersecurity technologies for the financial sector, offering them a testing ground with simulated financial systems, processes and data. The initiative is supported by national stakeholders in the financial and regulatory ecosystem, government agencies and academia.

Technological applications, including the use of machine learning and artificial intelligence, can help in environments where capacity, skills and resources are scarce. Globally, there is an urgent need for easy-to-use and open source applications that help the financial sector with incident preparation, detection, response and recovery. Technology can also support the sharing and translation of threat information, and remote provision of technical advice and training. Central Banks of the Future can team up with the private sector and other agencies to organize hackathons and innovation platforms for the development of new technologies.

Central Banks Would Not Have to Do It All Themselves – Just Lead the Effort

Many promising cybersecurity initiatives are building on public-private partnerships. Central Banks of the Future would not need to implement cybersecurity resource centers and similar initiatives by themselves, but could lead by facilitating cross-sectoral and public-private collaboration to effectively combat cybercrime and mitigate cyber risks in the financial sector. In most countries, some form of public-private dialogue is already happening, particularly in the financial and telecommunications sectors.

Examples that demonstrate the value of public-private collaboration in fighting cybercrime, include: Luxembourg's Cyber Competence Center – a centralized and shared resource center that supports the public and private sectors, as well as individuals, in effectively managing cybersecurity; 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.

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 defenses and ability to respond and recover from potential attacks.

Protecting the financial sector and securing global advances in financial inclusion not only depends on financial service providers 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.

The central bank of the future can play the important role of being the champion, coordinator, and cheerleader for its country's efforts to address the ever-growing threat posed by cyber attacks.