Cybersecurity:

A governance framework for mobile money providers

GSMA Mobile Money

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at www.gsma.com

Follow the GSMA on Twitter: @GSMA

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

Web: www.gsma.com/mobilemoney

Twitter: @gsmamobilemoney

Email: mobilemoney@gsma.com

Author: Juliet Maina, Advocacy and Regulatory Manager, Mobile Money

Editor: Killian Clifford, Director of Policy and Advocacy, Mobile Money

GSMA contributors: Mariana Lopez, Senior Advocacy Manager, Mobile Money
Policy and Security teams within the GSMA

THE MOBILE MONEY PROGRAMME IS SUPPORTED BY THE BILL & MELINDA GATES FOUNDATION, THE MASTERCARD FOUNDATION, AND OMIDYAR NETWORK

Contents


ange
e ici

Introduction

Cybercrime has become one of the greatest challenges of the digital age. The ubiquity of technology has intensified the risk of cyberattacks, and the rise of innovative and disruptive technologies in the digital economy has heightened the need for trust and stability. All over the world, policymakers, regulators and industry players are grappling with how to curb this emerging risk of cybercrime.

Cybersecurity is a vital issue for mobile money providers, who must maintain trust and confidence in their services to drive adoption and use, and continue to innovate in new directions. With 1.7 billion people in the world still unbanked,[1] it is critical that mobile money remains a reliable path to financial access and that services continue to expand and innovate. The mobile industry has worked to strike this balance, educating consumers about cyber risks while developing new features that build trust in its services. Each new iteration of technology has introduced new features, such as encryption and user identification validation, which have made mobile services increasingly secure and minimised the potential for fraud, identity theft and other possible threats.[2]

However, increasingly the risks go beyond the technology and devices, and this calls for innovative ways in addressing cybercrime. This report presents a holistic framework that mobile money providers can use to improve security and provide safeguards against cybercrime. The framework has three dimensions — People, Process and Technology — and provides guidance for mobile money providers to ensure the security of their operations and their customers.

1. Global Findex (2017). Chapter 2: The Unbanked.
2. GSMA (2017). Safety, privacy and security across the mobile ecosystem.

Cybersecurity in Mobile Money

Cybersecurity is a broad and multifaceted issue that is interpreted differently across different sectors. For the mobile industry, 'cybersecurity' generally refers to the protection of network-related systems and devices and the software and data they contain. This includes technical infrastructure, procedures and workflows, physical assets, national security, and the confidentiality, integrity and availability (CIA triad) of information.[3] For the purposes of this report, cybersecurity is defined as a collection of practices that support the secure operations and activities of mobile money providers and the integrity of their customers. These fall under three key dimensions: people, process and technology.

The global financial cost of cybercrime for mobile money providers is difficult to estimate because it is unevenly distributed among countries and data on cybercrime remains sparse because of underreporting. The Center for Strategic and International Studies (CSIS) report, *Economic Impact of Cybercrime – No Slowing Down,* estimates that the cost of cybercrime in 2018 worldwide was USD 600 billion.[4] These costs can be both direct and indirect (see Figure 1), with direct costs representing the immediate impacts of a cyberattack, and indirect costs the broader, more long-term impacts.

In Kenya, one of the world's largest mobile money markets, the estimated cost of cybercrime in 2018 was reported to be $295 million, $88.5 million of which were direct costs and $206.5 million indirect costs.[5] This demonstrates that, invariably, indirect costs are more expensive for mobile money providers than direct costs. Cyberattacks that harm a mobile money provider's reputation and lead to customer dissatisfaction and loss of trust may not only affect their mobile money business, but also put a dent in their core mobile business.

Figure 1

The direct and indirect costs of cybercrime for mobile money providers

Direct Costs

- Financial loss;
- Corruption, loss or destruction of data;
- Unauthorized access to confidential information;
- Compromised systems and applications, and
- Opportunity costs, including disruption in service delivery.

Indirect costs

- Reputational damage and liability risk for the company and its brand;
- Loss of consumer trust;
- Financial cost of further securing networks post-security breach;
- Regulatory fines and penalties for non-compliance;
- Loss of intellectual property;
- Weakened market competitiveness; and
- Online fraud and financial crimes resulting from stolen personal data.

3. GSMA (2019). Mobile Policy Handbook.
4. Center for Strategic and International Studies (2018). Economic Impact of Cybercrime – No Slowing Down.
5. Serianu (2018). Kenya Cybersecurity Report 2018.

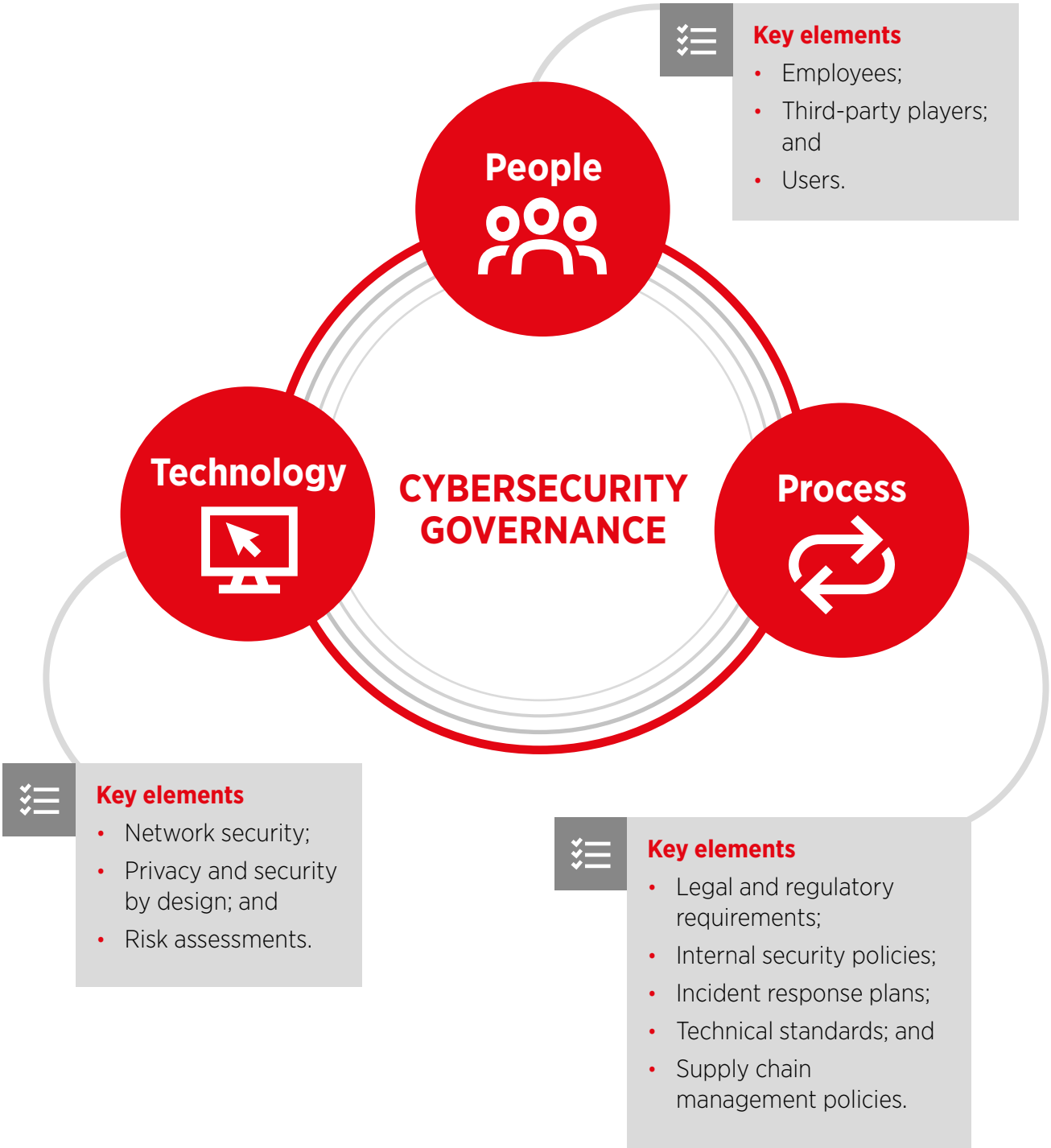
A cybersecurity governance framework for mobile money providers

Mobile money services are delivered within a large and complex ecosystem, which multiplies the risk of cyberattacks for mobile money providers and users. Addressing these risks is not just a technical problem, however, and technological solutions alone are not a sufficient response to the myriad threats and challenges in the current cyber environment.[6] A more effective response involves an approach that covers the mobile money provider's entire workforce, as well as its end users. A holistic framework that covers people, process and technology is therefore necessary to understand and address the growing concern of cybercrime in mobile money services. Figure 2 summarises the key elements of each of these dimensions, which are analysed in more detail in the following sections.

6. GSMA (2017). Safety, privacy and security across the mobile ecosystem.

Figure 2

A cybersecurity governance framework for mobile money providers



PEOPLE

The human resource component of a mobile money provider plays a key role in cybersecurity and is often considered the weakest link, as individuals are the first line of defence against cyber threats. However, the biggest investments in cybersecurity tend to be in technology solutions rather than in the people involved. This dimension of the framework includes three main elements: a mobile money provider's employees, third party players in the ecosystem, and the end users of mobile money services. Employees and third-party players can be the cause of successful cyberattacks due to a lack of awareness and/or inability to deal with threats, or by colluding with external attackers to exploit the system for unfair gain. Meanwhile, users can be victims of attacks that take advantage of their trust and/or lack of awareness to convince them to share confidential or personal information that is subsequently used to commit fraud.

Employees

Whether by accident or intent, representatives of mobile money providers are often the cause of most successful cyberattacks.[7] There are two main employee-related risks: a lack of skills and capacity to adequately identify and prevent cyber breaches, and collusion to commit fraud. The Accenture State of Cyber Resilience Index 2018 identified accidental publication of confidential information by employees and insider attacks as having the greatest impact, second only to hacker attacks.[8]

To embed cybersecurity in the fabric of the organisation and guard against insider threats, mobile money providers must bring together their human resources, learning and development, and legal and technical teams to work closely with the technology and business units. Training employees on all aspects of the mobile money system and various points of access is critical to ensure they are aware of potential threats and their responsibilities in the event of an attack.[9] For employees, a top-down approach is vital, with clear involvement and support from the board and senior management. Training and awareness exercises throughout the organisation are critical to mitigate the human-related risks of cybercrime. In some jurisdictions cyber-risk regulations include a provision for regular board and senior-level management training.[10]

This helps to ensure that an organisation's leadership team receives enough support to understand the importance of cyber risks and to encourage the allocation of resources for capacity building across the organisation. Additionally, organisational policies will need to reflect these changes and include access controls, regular training and awareness exercises, as well as accountability for any breaches that occur. This is covered in more detail under Processes.

In addition to building awareness of cyber risk across the workforce, mobile money providers must also build the skills and capacity of the cybersecurity staff responsible for monitoring systems and responses in the event of an attack. The ISACA State of Cybersecurity 2019 Survey revealed that 58 per cent of organisations have unfilled security positions and 32 per cent reported that it takes at least six months to fill these open jobs. One reason for the cybersecurity skills gap is a lack of technical security expertise; another is a lack of business insights.[11] Ultimately, building the cybersecurity skills of technical staff will also serve to create a strong culture of security throughout the entire organisation and provide the strongest defence against cyberattacks.

Third-party players

Mobile money agents and financial technology providers (fintechs) are integral to the provision of mobile money services, but do not form part of the mobile money provider workforce. To ensure the security of these services, third-party players should ideally be held to the same security standards as the mobile money provider. Training and awareness-raising, as well as skill building for cybersecurity experts, should be considered. This can be effected through the use of contractual agreements which serve to define the roles and responsibilities of other players and to share liability (where applicable). To secure the entire customer journey, mobile money providers may also impose minimum security standards and requirements that third party players must meet to provide the service.

7. Accenture (2019). The Cost of Cybercrime.
8 Accenture (2018). State of Cyber resilience.
9. In a 2018 survey, it was found that 90 per cent of organisations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%) and the increasing complexity of information technology (35%). See: CA Technologies (2018). Insider Threat Report.

Users

Users represent a cybersecurity risk for mobile money providers since most cyberattacks target individuals rather than technology infrastructure. However, the security systems and policies of the mobile money provider cannot safeguard the user from targeted attacks. These types of attacks, commonly known as "social engineering" (see Box 1), take advantage of consumer trust and lack of awareness of cyber threats.

Consumers therefore need to be able to recognise illicit behaviour and protect their personal data. To mitigate this risk, mobile money providers should continue to invest in education and awareness campaigns that provide users with clear and sufficient information on how to protect their personal information and their mobile money accounts from attacks, such as SIM swaps.[12]

BOX 1: What is social engineering?

Social engineering fraud uses manipulation to influence a person to divulge personal details or passwords. Once this information has been accessed, criminals can then record it and use it to commit other fraud-related crimes, such as identity theft and bank fraud. Scammers that engage with their intended victims typically build rapport and confidence, at times by leveraging publicly available information.

Examples of social engineering:

- Phishing – A method used to infect computers or mobile devices to access valuable personal details. Phishing fraudsters generally use communications such as email to tempt people to access what appear to be authentic websites or services in order to extract personal details;
- SMShing or "SMS phishing" – The use of phone text messages to deliver "bait", which then induces people to divulge their personal information; and
- Vishing – When fraudsters persuade victims to provide personal details or transfer money over the phone by impersonating a genuine service, such as a bank.

Source: GSMA (2017). Safety, privacy and security across the mobile ecosystem.

Recommendations to mitigate People related risks

- Educate consumers on safe behaviours to build their confidence when using mobile money services;
- Involve the board and senior-level management to drive cybersecurity from the top and embed a culture of cybersecurity in the organisation;
- Invest in training and awareness exercises for all other employees (including board and senior level management) on cyber threats and how to mitigate these;
- Invest in regular trainings for internal cybersecurity staff to develop their skills to address the current skills gap;
- Ensure that training programs include the roles and responsibilities of employees, as well as clear accountability mechanisms if these are not satisfied;
- Collaborate with other industry players to develop mechanisms to deal with insider threats;
- Ensure a strict level of vetting for all employees and third party players that the mobile money provider engages with; and
- Conduct agent training on acceptable practices and the mobile money provider's terms and conditions for dealing with end users.

10. The Central Bank of Kenya issued raft Cybersecurity Guidelines for payment service providers which, among other things, mandates training and awareness exercises for board level members of the organisation. See: Central Bank of Kenya (2019). Guidelines on Cybersecurity for Payment Service Providers.
11. See ISACA (2019). State of Cybersecurity 2019 Survey.
12. SIM swap is where, through social engineering, attackers gather enough information on a target, such as ID details and PIN numbers, to create a false identity. Using this information, the attackers contact the mobile money service provider and request a SIM card replacement and begin transacting using the victim's phone number. With the rise of internet and mobile banking, attackers can easily access bank accounts and transfer money to parallel malicious accounts they have created. The attacker can also empty mobile money and bank accounts. See Serianu (2018). Kenya Cybersecurity Report 2018.

PROCESS

While a growing mobile money ecosystem has been fostering innovation and supporting access to financial services, the entrance of new players has created new vulnerabilities. It is therefore important to have policies that cover an organisation's main internal business processes and also takes the entire supply chain of service delivery into account. Cybersecurity comprises several processes that outline an organisation's security system and, typically, the technical security policies and written descriptions of these policies. In some instances, these policies form part of an organisation's legal and regulatory requirements, and are therefore critical for regulatory compliance. Organisational processes for cybersecurity should be available to managers, employees and contractors who manage the operational units such as those contained in the GSMA Mobile Money Certification scheme.[13] Adopting specific policies for employees, contractors and managers may limit the risks of data breach.

Legal and regulatory requirements

As the impact of cybercrime is felt around the world, governments are developing or reviewing existing laws that govern cybersecurity. At a national level, the adoption of appropriate legislation on the misuse of technology for criminal or other purposes, and activities intended to damage the integrity of critical national infrastructure, are vital. Legislation should also support the coordinated action of government authorities, the private sector and citizens necessary to prevent, prepare for, respond to and recover from cybercrime incidents.[14]

While several countries have yet to adopt national cybercrime or cybersecurity legislation, some regulators are developing sector-specific regulations for mobile money providers, such as mandatory internal and external audits and compulsory reporting of data breaches for payment service providers. In countries where these are in place, such as Kenya and Nigeria, there are provisions to create internal processes for cybersecurity governance.[15] There is an increasing appreciation that the platform on which information is processed and transmitted should be managed in a way that ensures the confidentiality, integrity and availability of information as well as the avoidance of financial loss and reputation risk, amongst others.[16] Failure to adhere to these would lead to non-compliance and regulatory fines and liabilities. Where there are no legal or regulatory requirements, mobile money providers will need to independently develop and adopt sufficient organisational policies.

Internal security policies

Mobile money providers typically have a range of internal security policies in place. These are vital as they describe a company's security controls and activities. The policies tend to cover three broad areas — physical security, personnel management, and hardware and software — and while they do not specify a technological solution, they do provide specific intentions and conditions to protect assets.[17] The development of security policies should therefore be a multi-disciplinary activity, with input from IT and legal teams, as well as board-level participation. Security policies should be informative, regulative and advisory to address all security gaps within an organisation.

Incident response plans

In addition to policies governing security controls and activities, mobile money providers should also develop strategies to mitigate risks in the event of an attack. Incident response plans are necessary to ensure timely and effective action when products or systems are compromised by a cyberattack. A clear incident response plan also makes an organisation more resilient. Clear processes and defined roles and responsibilities enable an attack to be discovered quickly, contain any incurred damages and restore the integrity of networks and systems.[18] Incident response plans should be accompanied by incident response teams with representatives from all key areas of the business, including board level. This will help ensure that the impacts of a cyberattack are addressed effectively across the mobile money provider.

13. The GSMA Mobile Money Certification defines and promotes excellence in the provision of mobile money services which is measured against global industry best practice. The Certification enhances consumer trust, accelerates commercial partnerships, and sets a public bar to which all providers can aspire. Principle five of the scheme covers security as it pertains to mobile money services. See GSMA (2018) GSMA Mobile Money Certification.
14. ITU (2015). Understanding cybercrime: Phenomena, challenges and legal response.
15. The Central Bank of Nigeria hereby issued Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs), which represent the minimum requirements to be put in place by all DMBs and PSPs in their respective cybersecurity programmes. See Central Bank of Nigeria (2018). Risk-Based Cybersecurity Framework And Guidelines For Deposit Money Banks And Payment Service Providers.
16. Ibid.
17. Infosec Institute. An Introduction to Cybersecurity Policy.
18. UK Department for Digital, Culture Media & Sport (2018). Secure by Design – Improving the Cybersecurity of Consumer Internet of Things Report.

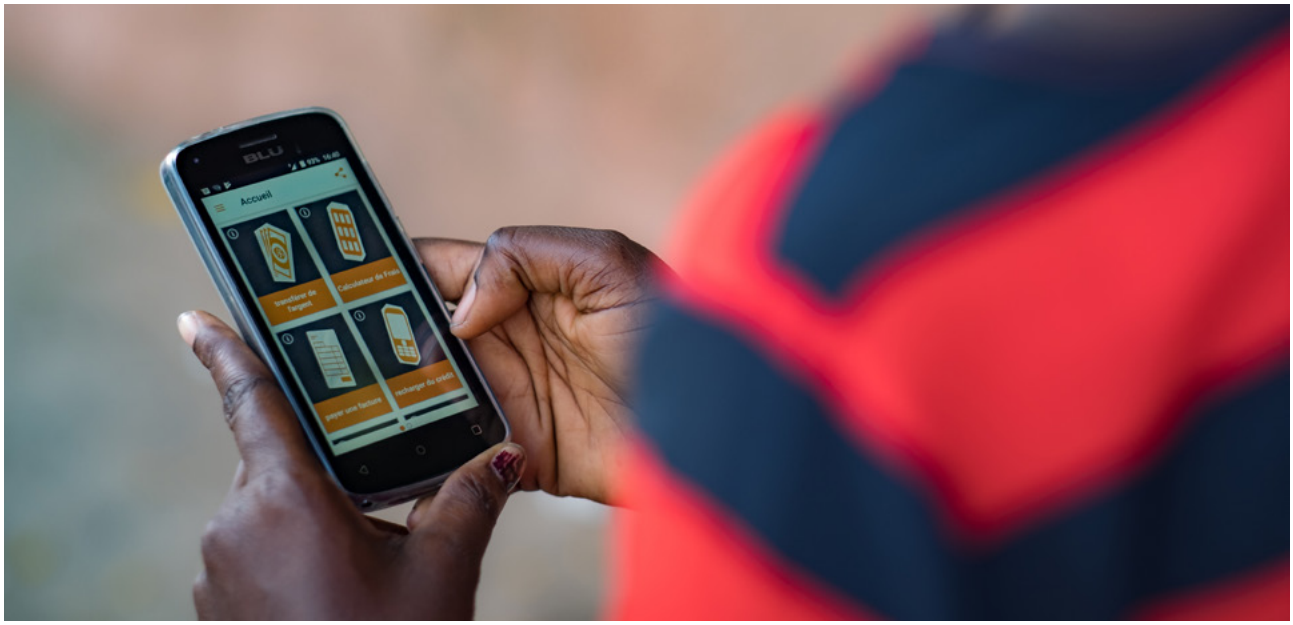
> **"Extended supply chain threats are also challenging organizations' broader business ecosystem. Cyber-attackers have slowly shifted their attack patterns to exploit third- and fourth-party supply chain partner environments to gain entry to target systems—including industries with mature cybersecurity standards, frameworks, and regulations."**
>
> *Accenture (2019). The Cost of Cybercrime.*

Industry standards

Due to the ever-changing landscape of cybersecurity, industry standards remain extremely fragmented. The lack of uniform global standards also prevents collaboration and limits the efforts of organisations to share security expertise and solutions.[19] Gaps and fragmentation in standards and protocols need to be addressed, as standards are an important requirement in providing a framework for the safe and secure provision of services. For mobile money providers with global operations, this fragmentation can lead to significant variation in their systems and security requirements, and hamper efforts to become interoperable and scale their operations. Mobile money providers should therefore adopt industry-wide accepted standards on cybersecurity, which include NIST and ISO frameworks. Ultimately, this will unify the approach to cybersecurity across all their operations.[20]

Supply chain management

As noted earlier, the evolution of mobile money services typically leads to more actors and stakeholders entering the ecosystem. Fintechs, aggregators, banks and other players are increasingly participating in the offering of a broad range of mobile money-enabled financial services. Today, supply chains for the provision of services are more dynamic, flexible and interdependent.[21] However, they are also becoming more complex as players are covered by different schemes and legal and regulatory frameworks. Mobile money providers should therefore ensure they have visibility over the entire supply chain, as this will enable them to assess the level of risk at every point of the chain, and to implement adequate measures to guarantee the safe delivery of their services. Mobile money providers can also ensure their partners and third parties apply the required level of security by passing on the obligation contractually and/or requiring them to meet certain security industry standards.



19. ENISA (2019). Industry 4.0 – Cybersecurity Challenges and Recommendations.
20. NIST is a voluntary framework that consists of standards, guidelines and best practices to manage cybersecurity-related risk. The cybersecurity framework's prioritised, flexible and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. See: NIST Cybersecurity Framework. ISO/IEC 27000 "provides an overview of information security management systems" (and hence the ISO27k standards), and "defines related terms". See: ISO/IEC 27000:2018.

Accountability mechanisms

For an organisation's processes to be effective, clear mechanisms for accountability should be in place.[22] Ultimately, the key to successful cybersecurity governance is the ability to demonstrate this compliance and measure the effectiveness of the mechanisms that have been put in place. Accountability is key to ensuring that employees and third-party providers are aware of their roles and responsibilities and adhere to them.

Such measures can range from the appointment of a Chief Information Security Officer (CISO) to the adoption of risk assessment procedures, and are typically aimed at embedding a culture of good security practices throughout the organisation. Accountability measures therefore bring all aspects of cybersecurity governance together. For simplicity, these are often organised into seven functional categories[23] (Figure 3).

Figure 3

22. The General Data Protection Regulations (GDPR) presents Accountability as a key principle of data protection, which can be applied here. The regulation requires that organisations demonstrate compliance, which can be done through a number of mechanisms and requirements.
23. GSMA (2019). Smart Data Privacy Laws.

Recommendations to mitigate Process related risks

- Ensure compliance with existing and applicable legal and regulatory requirements on cybersecurity;
- Develop and enforce an information security policy and appoint a main point of contact for all cybersecurity-related incidents in the organisation;
- Develop additional policies that govern various areas of the security policy, such as access control policies, social media policies and a bring-your-own device policy;[24]
- Provide for disaster recovery and business continuity plans in the event of a cyberattack;
- Adopt internationally accepted security standards to facilitate the harmonisation of security approaches across borders, including NIST and ISO;
- Integrate regular audits/assessments of systems into policies to ensure technological vulnerabilities are identified and effectively addressed;
- Establish incident response plans and teams that will guide employees on how to contain cyberattacks;
- Ensure that the security standards of the mobile money provider extend to other players in the supply chain via contractual agreements; and
- Participate in industry forums and specialist groups to stay abreast of new developments and to share best practices that help to harmonise security approaches across borders.

24. CSO Online (2018). 9 policies and procedures you need to know if you're starting a new security program.

TECHNOLOGY

IT asset management is a major part of cybersecurity. The technology dimension covers the inventory and control of hardware and software assets that support the operations and activities of mobile money services. As cyberattacks become increasingly sophisticated, mobile money providers must continually improve their security mechanisms. However, given the complexity of the ecosystem, there is no one-size-fits-all approach.

According to the internationally accepted NIST security framework, the key elements of technology systems in cybersecurity should consider the ability to identify, prevent, detect, respond and recover from threats.[25] Additionally, mobile money providers should apply principles of security by design and privacy by design to products, services, protocols, communications and processes, and conduct regular assessments of their systems to identify gaps.

Network and device security

The safe and secure use of mobile services depends on the security of the network infrastructure. Protecting mobile networks is highly complex because they are accessible to a wide range of users via a variety of devices and connection protocols. Mobile networks also interconnect with many other communications networks (e.g. fixed, mobile, internet providers, private enterprise) to offer anywhere-anytime functionality. For mobile network operators, safeguarding the integrity of communications across the network entails securing critical assets (hardware, software and data) and preventing unauthorised access to any of the nodes in the networks. Moreover, since the end user of a mobile device is one of the primary access points to the network, protecting the integrity of mobile devices is as critically important as safeguarding the network itself.[26] Figure 4 highlights some of the key technical preventive and detective controls that mobile money providers can implement to protect networks and devices.[27] While the controls themselves typically fall under processes, they require technical solutions to bring them to life.

Figure 4

Preventive and detective controls to protect mobile networks and devices

Preventive controls

- Control access rights to protect customer information;
- Separate responsibilities to reduce error or fraud on high-risk procedures (e.g. e-money reconciliation); and
- Introduce transaction limits to reduce risks associated with AML/CFT.

Detective controls

- Monitor and analyse suspicious activities;
- Monitor activity on system access;
- Create robust customer recourse and escalation procedures;
- Monitor agent transaction activity;
- Send SMS alerts to customers to provide information on transactions and account changes; and
- Introduce management reviews of high-value transactions.

25. NIST Cybersecurity Framework.
26. GSMA (2017). Safety, privacy and security across the mobile ecosystem.
27. GSMA (2012). Managing the risk of fraud in mobile money.

Privacy and security by design

The implementation of cybersecurity should include the principles of privacy by design and security by design, which require organisations to identify and mitigate risks throughout the lifecycle of a product, service or process.[28] Privacy and security by design requires that key principles of data protection are inculcated into the organisation's systems and product development process to create a culture of data protection and security. Additionally, it serves to place the responsibility of safeguarding devices on the mobile money provider rather than on users.[29] These can also make the security mechanisms behind mobile money services more transparent and reduce user uncertainty about the security measures that are in place. These principles can also help to measure and improve the effectiveness of existing and new products.

Risk assessments

Regular vulnerability assessments, whether conducted internally or externally, are critical to ensuring the security of operating systems, products and services. These continuous checks can be carried out in the form of audits or penetration testing exercises. Some organisations carry out "red team vs. blue team" activities in which an external entity (the red team) is hired to test the effectiveness of an organisation's security systems (blue teams).[30] The objective of the exercise is to test the preparedness of the organisation's security systems and its ability to detect and respond to an attack. This and "bug bounty" programs have become popular among organisations seeking to address emerging cyber threats in innovative ways and ensure they are prepared.[31] Certain cybersecurity regulations also require that organisations regularly assess their systems to mitigate risks as effectively as possible.[32]

Recommendations to mitigate Technology related risks

- Ensure the principles of security by design and privacy by design are built into technology solutions, products and services across the entire supply chain;
- Adopt tools and technologies that enable the organisation to identify, protect, detect, respond and recover, in accordance with the NIST framework;
- Conduct regular risk and vulnerability assessments on security systems to ensure gaps are identified and addressed quickly; and
- Implement preventive and detective measures to protect the integrity of mobile devices and mobile networks.

28. Secure Controls Framework: Security and Privacy by Design (S/P) Principles.
29. UK Department for Digital, Culture Media & Sport: Secure by Design: Improving the cyber security of consumer Internet of Things report.
30. EC Council (15 June 2019). Red Team vs Blue Team.
31. A bug bounty program, also called a vulnerability rewards program (VRP), is a crowdsourcing initiative that rewards individuals for discovering and reporting software bugs. Bug bounty programs are often initiated to supplement internal code audits and penetration tests as part of an organisation's vulnerability management strategy. See: Rouse and Haughn. (2017). bug bounty program. TechTarget.
32. A risk based approach to cybersecurity as prescribed by cybersecurity guidelines in Kenya and Nigeria require that regular assessments are carried out to identify all cybersecurity vulnerabilities, threats, likelihood of successful exploit, potential impact (reputational, financial, and regulatory) to information assets; and the associated risks. See Central Bank of Nigeria (2018). Risk-Based Cybersecurity Framework And Guidelines For Deposit Money Banks And Payment Service Providers; Central Bank of Kenya (2019). Guidelines on Cybersecurity for Payment Service Providers.

Conclusion

The ever-changing digital landscape offers major opportunities for the mobile money industry to expand the value proposition and reach of their services. However, the potential risks of cyberattacks underscore the need for mobile money providers to ensure their operations are cyber-resilient and able to safeguard consumer trust. The integration and application of the holistic People, Process and Technology framework can help mobile money providers better understand the risks associated with cyberattacks and to continue to embed the best security practices into the fabric of their operations.

The GSMA remains committed to providing support to our key stakeholders in addressing this growing risk. We will continue to conduct research to develop practical approaches to cybersecurity governance mechanisms for the mobile money industry, including specific recommendations for mobile money providers and other stakeholders to improve the overall security landscape of mobile money services. As such, we invite all interested parties to join forces and work with us to offer best-in-class security safeguards in the protection of network-related systems as well as the confidentiality, integrity and availability of information within mobile money providers.

To download the report please visit the GSMA website at
www.gsma.com

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601