United Nations Secretary-General's
Special Advocate for Inclusive Finance for Development

UNSGSA

Briefing on Cybersecurity

By the UNSGSA's Fintech Sub-Group on Cybersecurity

What is cybersecurity?

- Technology-enabled innovation in financial services presents many opportunities for digital financial inclusion, but raises concerns about cybersecurity.
- The most serious cybersecurity risks—such as data breaches, credential theft, and credential reuse/abuse—can cause tangible harms.
- Although innovation and security don't always go hand-in-hand, fintech offers opportunities to address cyber risks and build cyber resilience, while also enhancing inclusion.
- Fintech can leverage data and new risk-modeling techniques to lower cybersecurity risks.
- Finally, fintech can help in improving the digital literacy and cyber hygiene of customers. An educated customer is much less likely to be the victim of a cyberattack.

What cybersecurity risks do customers face?

There are many cybersecurity risks from new fintech solutions and from the limited global approach to tackling financial cyber crime. In this respect, the fintech industry has a responsibility to improve the current security implementation, in order to guard and further expand the trust of customers in rich and poor countries. Rather than addressing all these issues, this briefing is focused on cybersecurity risks posed to mobile-money customers in developing economies.

Customers' cyber hygiene: Customers often have limited awareness of good cyber hygiene, such as changing their passwords regularly and not sharing them with their mobile money agent. Customers without basic cyber hygiene knowledge and practices expose themselves to constant risks.

Feature phones: In many developing economies, a majority customers use basic "feature phones," which lack the end-to-end security of smartphones. The resulting cyber risks can arise via the telecommunications provider, financial service provider, or the devices themselves. For example, it is easy and inexpensive to obtain fake mobile telecommunication base stations. This can allow hackers to capture customer data such as user names and passwords, or to send out counterfeit SMS messages asking for users' private data and credentials.

Data leaks from mobile phones: Valuable user data may "leak" from mobile phones used for DFS transactions, through:

- Malware loaded into repaired devices or stolen phones loaded with malware and resold as new

- Public Wi-Fi networks where data can easily be extracted
- "Free" phone charging stations may feed malware into a mobile phone
- Intercepting customer information transmitted using near-field communications

Signaling System 7: Mobile networks contain systemic design flaws thanks to the 1970s-era Signaling System 7 (SS7), which is still the current "DNA" of all telecommunications and mobile networks globally. Unfortunately, it is easy for bad actors to gain access to SS7 and thus penetrate any mobile network being used to provide mobile money. In this way, hackers can intercept private data, steal customers' funds, and obtain customers' credentials. This results in losses to agents, users, and providers, and damages trust in mobile money.

Central data breaches: When customers are asked to change their credentials after a central data breach, they often do so hastily and without exercising best practices. There are centralization risks for customers storing their data in a handful of large-scale identity, verification, and financial services databases.

Why does cybersecurity matter for financial inclusion?

- DFS, especially through emerging fintech solutions, are essential to increase financial inclusion. To do so, they must build trust among unbanked and underbanked customers. Cyberattacks can undermine this trust.
- Unbanked and underbanked customers are more likely to be the victims of cyberattacks as they tend to have less financial and digital literacy. For example, they may use weaker security procedures, preferring convenience over security. PIN numbers are often shared in communities.
- The consequences can also be more significant for these customers too, as they typically are more sensitive to even small financial shocks.

How can cybersecurity solutions work?

Policymakers must establish frameworks to enable cyber-security and industry should adopt best practices, including:

- **Multifactor authentication** requires the presentation of at least two different types of authentication elements, not just a PIN. There are a host of experiments occurring in the public and private sectors looking at elements such as location, type of device, fingerprint, user behavior, iris scans, and facial recognition.
- **Tokenization** involves replacing sensitive financial data with an alias (or token). Sensitive data is stored in a highly secure location and tokens are created to match to the sensitive information.
  - When information needs to be shared, then only the token is sent instead of the sensitive information.
  - However, the first generation tokenization systems created their own cyber risks. They were attractive targets for hackers as they often stored all sensitive data in a single service center.
  - Tokens can now be created in real-time and delivered securely over the Internet, used for mobile device transactions, and securely shared between a wide variety of entities in the financial services ecosystem.

What can governments do to promote cybersecurity?

- **Funding for cybersecurity research.** Governments make grants and hold competitions to incentivize innovation and skill-building in the cybersecurity field. For example, the Indian government has a grant program for cybersecurity startups.
- **Risk-based approach to regulation.** Cybersecurity is a rapidly evolving field and creating rigid regulatory standards might quell innovation. Regulators should focus in on the type of data being collected and the type of service being provided. For example, the Singaporean government utilizes a risk-based approach when considering any updates to its financial services laws.
- Creation of public-private partnerships between regulators, DFS providers, and banks to monitor cyber threats as they arise. These may include:
  - Computer Emergency Response Teams. These have been established in a number of countries at national and regional levels to quickly collate, identify, and coordinate responses to cyberattacks.
  - Telecommunications regulators working with mobile networks to prevent intrusions, e.g. detecting fake mobile base stations that could cause financial harm.
  - Creating and/or strengthening rules for companies about conducting risk assessments and reporting network breaches to regulators.
  - Fraud forums enabling financial providers and telecommunications providers to regularly share best practices and threat intelligence.
  - Governments must work with universities and the private sector to develop and disseminate some of the cybersecurity best practices discussed above.

Annex: Resources

Programs

Selected jurisdictions with cybersecurity innovations

- European Union: EU Cybersecurity Strategy
- Nigeria: Regulatory Framework For The Use Of Unstructured Supplementary Service Data (USSD) For Financial Services In Nigeria
- Singapore: MAS Cybersecurity Advisory Panel
- USA: Federal Reserve Bank National Incident Response Team

Organizations involved in technical assistance and/or funding of relevant activities

- IBM
- IMF
- Hewlett Foundation
- National Science Foundation
- SWIFT
- World Bank

Selected Experts

- Joyce Hakmeh, Chatham House
- Jason Healey, Columbia University School of International and Public Affairs
- James Lewis, Center for Strategic International Studies
- Tim Maurer, Carnegie Endowment for International Peace
- Leon Perlman, DFS Observatory, Columbia University Business School
- Bruce Schneier, Harvard Belfer Center

Recommended Readings

Bank of International Settlements. 2017. *FSI Insights on policy implementation: Regulatory Approaches to Enhance Banks Cyber-Security Frameworks.* Basel, Switzerland: BIS.

Bank for International Settlements and International Organization of Securities Commissions. 2016. *Guidance on cyber resilience for financial market infrastructures.* Basel, Switzerland: BIS.

Butler, K; Perlman, L et al. 2017. *Security Aspects of Digital Financial Services (DFS).* Geneva, Switzerland: ITU.

European Central Bank. 2018. *TIBER-EU Framework – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.* Frankfurt am Main, Germany: ECB.

Financial Stability Board. 2017. *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices.* Basel, Switzerland: FSB.

World Bank. 2017. *Financial Sector's Cybersecurity: A Regulatory Digest.* Washington, DC: World Bank.

This note was drafted by Usman Ahmed of PayPal under the guidance of the office of the UNSGSA and with the support of the World Bank Group.