STANDARDS FOR RESPONSIBLE DIGITAL FINANCIAL SERVICES: CYBERSECURITY STANDARDS SECTION

19 May 2022

CERISE + SPTF
Draft Standards: Cybersecurity
(as of 19 May 2022)

Standards for Cybersecurity

1. Define board and management responsibilities related to data security, including how the board will ensure risk management related to digital innovation and activities.
2. Include cybersecurity costs in the budget every year.
3. Implement a cybersecurity system that has at minimum these features: physical security, daily (at minimum) data back-up, ongoing automated checks that flag any suspicious activity, and an always-operational data security system that detects attempts to hack into your files.
4. At least once every quarter, have a professional (either internal or external) try to hack your own data.
5. When setting up a data security system, take the following actions:
    - Increase awareness of management and the board.
    - Get an external audit of your data security.
    - Strengthen all gap areas.
    - Train the technical team on risk management.
6. Identify what is core to business function versus what is less important, and implement the strongest security measures for the fundamental functions.
7. Take the following actions to achieve acceptable cyber-resilience:
    - Develop threat scenarios for the kinds of incidents that relate to your organization's highest priority cyber risks.
    - Have a response plan for cyberattacks.
    - Build capacity to respond to those scenarios.
8. Any time you release a new digital product/service, assess data security for that product/service specifically, and implement new security measures as needed.
9. Monitor employees' use of computer systems and audit their activities.
10. Learn what cybersecurity measures any potential partner has in place, and work only with those with adequate cybersecurity systems.
11. If you work with a potential partner, assess cybersecurity risks that arise from the interconnection of your systems, and implement risk mitigation measures as needed.
12. Identify which person or team, either internal or external, is in charge of cybersecurity and, including who is in charge when the main person is out of the office.
13. Train customers on cybersecurity, on an ongoing basis.
14. Train employees on cybersecurity, on an ongoing basis., covering at minimum their own responsibilities, how to talk to customers about cybersecurity, and how to direct customers to the right person if customers raise an issue.
15. Train board members on cybersecurity, on an ongoing basis.
16. Report data on cybersecurity (e.g., hack attempts, measures taken, new risks identified) to the board at minimum quarterly.
17. Report data on security activities to management at minimum weekly.
18. Notify customers within 24 hours if you do get hacked.
19. If customers lose money because your systems got hacked, refund the customer.

20. Notify other FSPs in your market of any attempts hackers make on your data security, including sharing the specific methodology they used.
21. Participate in any initiatives in your country or region involving information sharing about cybersecurity threats.
22. If you do not have the resources to invest in cybersecurity, then do not offer digital financial services.

Guidance on cybersecurity: concepts, examples of real practice, and questions to address

Concepts

- We should have standards not just for cybersecurity, which helps reduce risk of cyber attaches, but also cyber-resilience, which allow FSPs to address problems when they are attacked and remain operational.
- In general, less access is more secure.
- There are several cybersecurity frameworks that say you must work on the physical security, the information systems themselves, and the vendors (interconnection with vendors and customers).
- Include in the contract with the vendor of your core banking system a requirement that they share with you their cybersecurity yearly assessment, to make sure the product has a secure development framework.
- Cybersecurity is a necessity but very expensive for each individual FSP. A solution could be to set up regional cybersecurity centers. FSPs would share resources.
- Some ideas for training customers on cybersecurity:
  - Send reminders via SMS at regular intervals
  - Provide specific examples of what the customer should not do, including if the network is down, do not leave the customer's cash, PIN or phone with an agent for them to complete the transaction when the network is restored.
- Note: Studies show that women are less likely to change the default PIN, more likely to use the same PIN as others in the community, and more likely to give their phones to agents.

Examples of real practice

- Conduct a self assessment using the Africa Cybersecurity Resource Centre (ACRC) self-assessment tool: https://start.cyber4africa.org/. This survey will ask a few questions and provide recommendations. Keep in mind that it is a self-assessment tool which only touches the surface of information security. It provides a very basic maturity level estimate and some basic recommendations.
- Consult *Carnegie Endowment for International Peace Cyber Resilience Capacity Building Toolkit*. Has specifics of roles related to board and management, including Chief Information Security Officer, and processes for protection of the FSP, protection of the consumer, workforce development, incidence response.
- Some mobile network operations have Internet management policies, which they update every six months.

Questions to address

- FSPs implementing these standards must also comply with cybersecurity regulation in their country. Ideally, the standards published by SPTF would be aligned with, or adapted to, the local regulatory context by the FSP. But, in some cases, the regulation is not good.
- Regarding cybersecurity measures, it is not easy to distinguish between what should be an obligation versus what would be optional.