DOI: https://doi.org/10.62232/barp.9.2024.8568

Cyber Risk Crisis Simulation Exercises for the Financial System

Author: David Papuashvili

December, 2024

The financial system is critical for the effective functioning of the economy. Along with the many benefits that the financial system offers to consumers and the wider public, it also faces a multitude of challenges and risks. One such risk is cyber risk, which has been increasing over the past several decades due to the growing reliance of the financial sector on information technology. Cyber risk is a significant, emerging operational risk that requires considerable attention.

Since cyber risk is a systemic operational risk, which means that cyber risk can impact multiple organizations simultaneously, or within a short period of time, it makes considerable sense to conduct cyber exercises to test the readiness of financial system participants. Crisis simulation exercises offer a useful mechanism for assessing how effective the decision-making processes may be during times of crisis. In order to gain a maximum benefit from crisis simulation exercises, multiple organizations and entities can be involved in the implementation of crisis simulation exercises. These might include commercial banks, the Ministry of Finance, CERT, internet providers, and others.

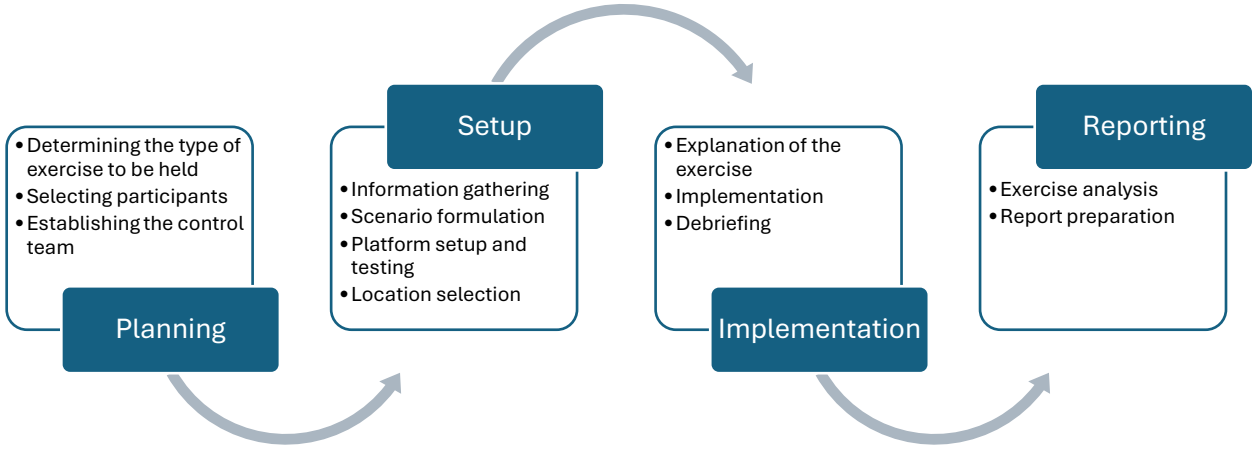
Crisis simulation exercises comprise of testing both intra and interorganizational decision-making and communication based on pre-determined risk scenarios. When conducting crisis simulation exercises specifically within the context of cyber risk, then the risk scenarios are likely to be based around various forms of cyber risk, including cyber-enabled fraud scenarios. It must also be noted that crisis simulation exercises are directly linked to communication and decision-making during times of crisis. The exercises themselves can

be held in different forms. The exercises offer a viable mechanism for testing both private and public sector entities' readiness should a materially significant cyber event occur.

Several key characteristics of cyber crisis simulation exercises must be pointed out. These exercises are not stress-tests per se. In most cases and scenarios, simulation exercises do not impact any of the information systems that the organization possesses, since the decision-making process is what is being tested. The exercises also do not represent an assessment or evaluation of the financial institutions that participate in these events. As a result, the participants are not penalized, or reprimanded in any way if it is assumed that the participants did not perform based on pre-determined perceptions or expectations. Furthermore, crisis simulation exercises should be conducted to enhance and aid the communication process during times of crisis. The exercises offer a good venue for determining organizational needs and what needs to improve based on current practices that may include the assessment of the effectiveness of procedures, regulations and supervisory mandates of financial supervisors.

Figure 1 below describes the four-step crisis simulation process. The four high-level phases include planning, setup, implementation and reporting. During the initial, planning phase the financial system participants such as commercial banks, microfinance institutions, credit unions, financial regulatory authorities or other entities determine the type of an exercise that needs to be held. Participants and control team members that will be running the exercises are usually established at this stage. The setup phase consists of information gathering, scenario drafting and determination, the setup of the information technology platform that will be used to run the exercise and the selection of the location where the crisis simulation exercise will be run. Phase three includes the implementation of the exercise which comprises of explaining the exercise to the participants, implementation and overview. The final phase of the testing process consists of reporting where the results of the exercise are analyzed and a final report on the exercise is prepared.

Figure 1. The process of crisis simulation exercises

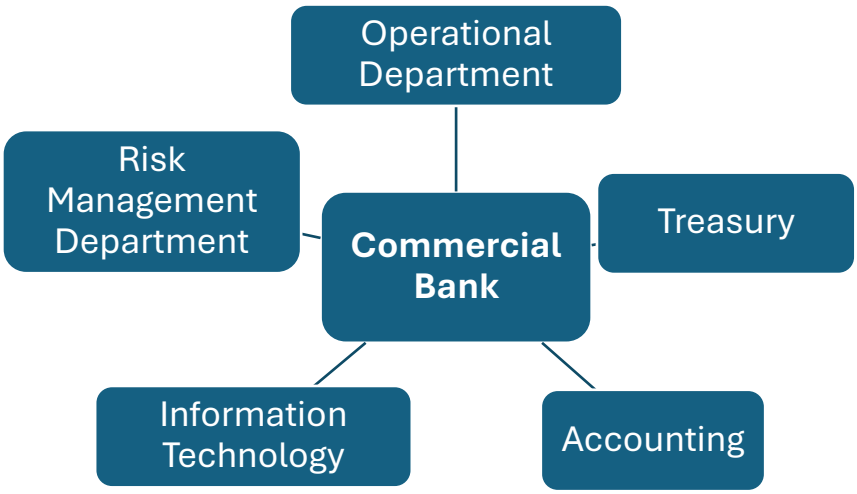


When it comes to the implementation of the cyber risk crisis simulation exercises, the format is usually electronic and e-mail is one of the most common method via which the crisis simulation exercises are conducted. All communication between the participants must be logged via the e-mail (electronic mail) server so that the communication streams and the subsequent decision-making process can be analyzed after the exercise has been conducted. Again, as mentioned earlier, organizational information systems such as core-banking systems, ATMs, or other electronic banking systems such as payment systems must not be impacted by the crisis simulation exercise.

The type and form of the crisis simulation exercise depends on the content and context of the exercise itself. The exercise can be run either individually within the financial institution, or with multiple different financial institutions and other entities that are linked to the financial sector. In multilateral crisis simulation exercises, both the financial sector as well as participants from other sectors of the economy may be involved in the exercise. For example, the central bank (or financial regulatory authority), commercial banks as well as information technology and telecommunications service providers may be involved in the crisis simulation exercises. It is important to note that the participants must be pre-determined before the actual implementation of the exercise.

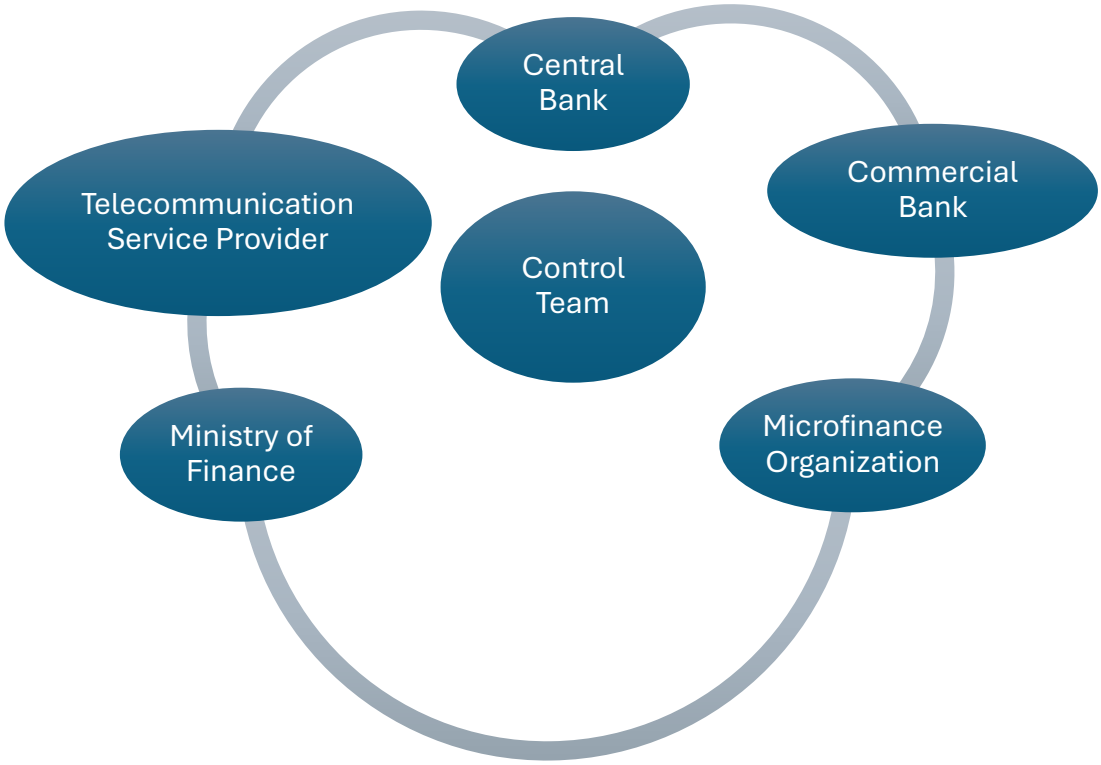
Figure 2 below provides an example of an individual crisis simulation exercise that is run within the organization such as a commercial bank. During the exercise, the commercial bank tests a specific cyber risk scenario such as a distributed denial of service attack, ransomware, phishing, or cyber-enabled fraud and the associated decision-making process between the different structural units such as the operational department, treasury, accounting, information technology and risk management departments.

Figure 2. Example of an Individual Crisis Simulation Exercise



Crisis simulation exercises can also be used to test communication and coordination among the various entities throughout the financial system. Figure 3 provides an overview of an example multilateral crisis simulation exercise where entities outside of the financial system are also involved. For example, besides the central bank and a commercial bank, the crisis simulation exercise may involve those organizations that provide critical services such as the Internet or banking-related software to the financial system. These organizations may include any relevant entity within the telecommunications sector and/or the information technology sector.

Figure 3. Example of a Multilateral Crisis Simulation Exercise



When a specific event happens, financial institutions must communicate with different entities and stakeholders internally and externally. Some of the exercises that can be carried out by regulators and regulated entities, such as central banks, financial regulatory authorities and banks, should mimic this process. This includes communication both within the various structural units internally, as well as with customers/consumers, other regulatory bodies and government organizations. The process of communicating with customers and media, as well as potentially other stakeholders can be tested within the context of the crisis simulation exercises as would be carried out normally under organizations' business continuity plans.

To summarize, crisis simulation exercises offer a viable and effective option for testing the decision-making process of key stakeholders within the financial system. These exercises should mimic reality, but should typically not be identical to historical events that have happened in the past. This includes the development of realistic and plausible scenarios that

may happen in the future, around which the decision-making process will be tested. Relevant people with the necessary experience should be involved in the conduct of the simulation exercises. Organizations that carry out crisis simulation exercises can also incorporate a wide spectrum of scenarios that may not have necessarily happened in the past. Last, but not least, in order for these exercises to be beneficial, the participants of these exercises must act based on existing organizational policies and rules.

References:

1. Systemic Cyber Risk Reduction. (n.d.). Retrieved from https://www.cisa.gov/resources-tools/programs/systemic-cyber-risk-reduction.
2. Lee, Y. C. Crisis Simulation Exercises. Retrieved from https://www.itu.int/en/ITUT/extcoop/figisymposium/2019/Documents/Presentations/Yejin_C_Lee_Presentation.pdf
3. Curry, J., & Drage, N. (2020). The Handbook of Cyber Wargames: Wargaming in the 21st Century. The History of Wargaming Project.
4. Papuashvili, D. (2021). Crisis Simulation Exercises (CSEs) - National Bank of Georgia. International Telecommunications Union. Retrieved from https://figi.itu.int/wp-content/uploads/2021/06/6_David-Papuashvili_NBG.CSEs_.DP_.pdf