DOI 10.62232/barp.8.2023.6774

Cyber Resilience Implications for the Financial System

D. Papuashvili

Georgian America University, Business School, 10 M. Aleksidze str., 0160, Tbilisi, Georgia.

Abstract

In August of 2008, cyber-attacks began to affect the Georgian public and private sectors. The cyber-attacks coincided with the Russian Invasion of Georgia, which is also known as the "Five-Day War". While most of the initial cyber-attacks that were directed against Georgia affected the public sector and media, including various government websites and Georgian news portals, a significant portion of the cyber-attacks affected the Georgian financial system.

The cyber-attacks that were directed at the financial system had the effect of bringing down online banking services. In addition, the National Bank of Georgia, which serves as the central bank of Georgia, had its website hacked. As a result of the hack, the official, reference exchange rate of the Georgian Lari to the U.S. Dollar was modified. Luckily, most consumers and other stakeholders were unable to see the unauthorized modification of the exchange rate due to the fact that most of the Georgian internet space was under a distributed denial-of-service attack at the time. If the exchange rate modification on the central bank's webpage would have been seen by a larger audience, when Internet services are generally readily available to the public, the implications and the impact to the financial system would likely have been much greater.

The events of August, 2008 and several other large-scale cyber risk-related incidents have shown that cyber resilience has become an increasingly vital part of financial stability. In addition, the growing use and adoption of electronic information systems in the face of digital transformation of the financial system has clearly brough cyber risk to the forefront of attention.

According to the U.S. National Institute of Standards and Technology (NIST), **cyber resilience** is defined *as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources* [1]. Financial institutions that make up the financial system, especially those institutions that are deemed as being systemically important to the safe and sound functioning of the economy, need to have relevant governance, management and control processes in order to ensure cyber resilience. Furthermore, cyber resilience also needs to include an aspect of stress testing in the wake of adverse or unexpected events. Without a robust stress testing framework, it will be difficult to gain assurance that an organization such as a commercial bank or a credit union will be able to cope with various cyber risk scenarios. It is therefore important to have a holistic approach towards cyber resilience and cyber risk, in general. This is especially true for the financial system, since it forms the backbone of most national economies.

The following paper presents the various aspects of cyber resilience, which need to be considered when analyzing cyber risk within the context of the financial system.

Cyber Risk as a Form of Financial Risk

Cyber risk is a form of operational risk. Operational risk is defined as the risk of loss arising from failed or inadequate processes, people, systems, external events[2]. Cyber risk is also clearly a form of information technology risk, which is itself a subset of operational risk.

While operational risk is mostly viewed as a form of non-financial risk, since in many cases, operational risk's impact on the organization is not as clearly defined in financial terms as those of credit, or market risk, there are several forms of operational risk that have clear and obvious financial implications. This includes the risk of fraud, which can lead to both direct and indirect financial loss, and cyber risk, which also can be linked to fraud and have various adverse financial consequences for financial institutions.

IT risk is the likelihood for an unplanned event involving a system failure or business disruption in information technology to negatively affect an organization's business objectives.[3] Information technology risk is a business risk. Therefore, if cyber risk is viewed as a subset of information technology risk, it is also clearly a form of business risk, with financial implications.

Cyber risk has become key to most business operations today, since information technology is often an enabler and a critical supporting process. Many companies, including financial

[1] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie, G. (February, 2020). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

[2] Basel Committee for Banking Supervision (BCBS).

[3] Westerman, G. & Hunter, R. (2007). IT Risk: Turning Business Threats into Competitive Advantage.

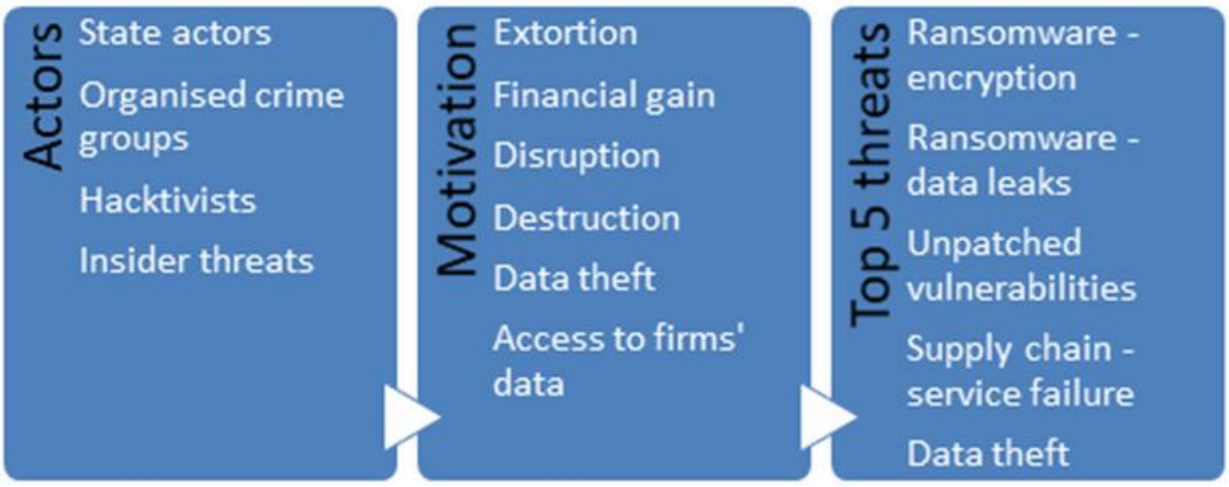
institutions, still have not adjusted their processes adequately to manage cyber risk. Research shows that IT risks arise not from technical or people-related issues at the lower level, but from a failure in governance and managerial (internal control) processes. As a result, cyber risk should be managed in such a manner, as to ensure the safe and sound functioning of a financial institution. IT risk can also have systemic risk implications.

Cyber risk is more likely to be realized with systemic consequences than other forms of operational risk. This makes cyber risk a unique form of operational risk, which can spread through the system at much greater speeds, affect multiple organizations at the same time and also lead to financial losses. The impact of cyber risk has also been studied less that both other forms of financial and operational risk. As a result, it is not fully clear what the exact financial impact might be when a hacker deliberately modifies the official currency exchange rate, or the interest rate of a key monetary policy instrument. Furthermore, if a financial institution's data integrity is compromised, it might be difficult to assess how a bank might be able to service its customers. Additionally, if access to client funds is impaired due to a cyber-attack at one commercial bank, this might also cause systemic risk implications, if customers lose trust in the viability of other financial institutions to provide basic financial services.

From a financial risk perspective, according to various estimates, cybercrime alone, excluding the risk associated with system disruptions and technological failure, is to cost the global economy around $10.5 trillion annually by the year 2025.[4] While this figure is a general estimate and includes different sectors of the economy, the financial system is a prime target of cybercrime crime and a significant portion of these financial losses is incurred by the financial system. Additionally, the average cost of a cyber-attack is approximately 2.4 million US Dollars. **It is also worth noting that cybercrime costs more to the financial sector than any other sector of the economy**. Furthermore, Cybercrime costs more to the financial sector than any other sector. The number of successful attacks has increased by approximately 3 times in the last several years. Figure 1 below depicts the cyber threat landscape for the financial market infrastructures in Europe. As can be clearly determined from the diagram, the motivation of the various threat sectors is clearly financial as evidenced by the threat of extortion, financial gain and financial data theft. In terms of the main threats that the European financial market infrastructure faces, top threats such as ransomware-encryption and data theft mostly have financial implications as an end-result, since hackers and other unauthorized parts usually either extort money from affected victim institutions, or execute cyber-attacks with the aim of financial gain.

[4] Morgan, S. (November 13, 2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Figure 1. Cyber threat landscape for financial market infrastructures in Europe



Note: Threats are arranged in descending order of estimated severity.

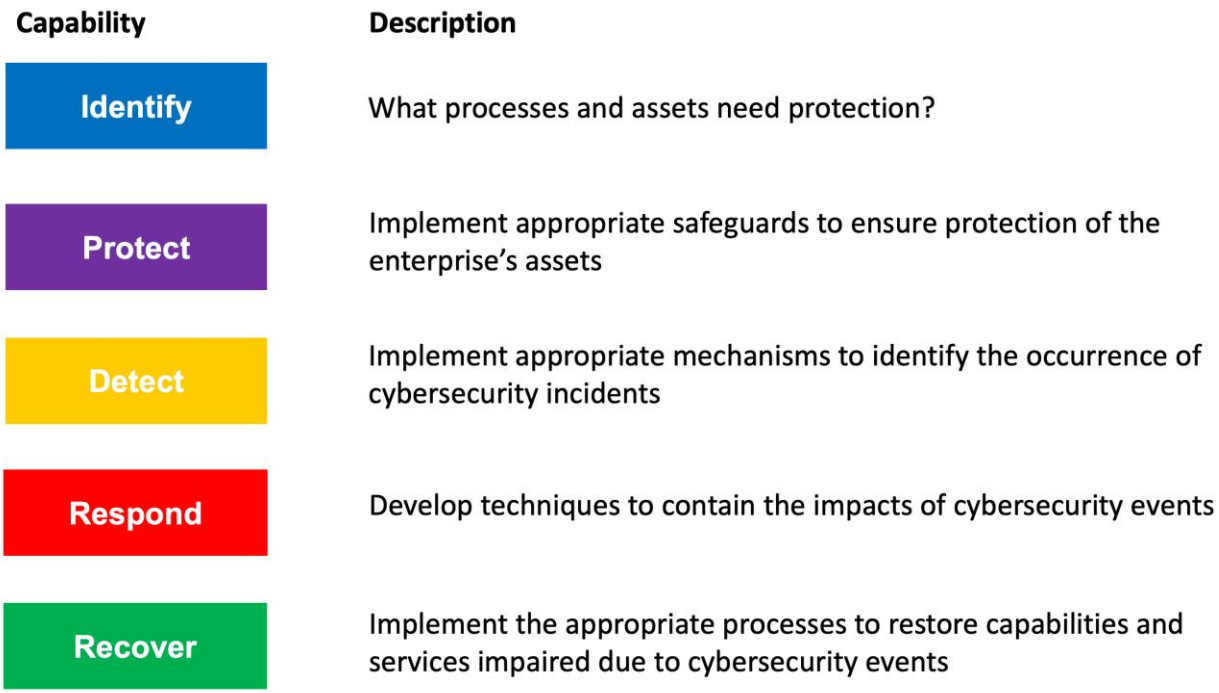
Source: European Central Bank

Cyber Resilience

Executive and senior management of financial institutions need to be responsible for setting the tone at the top for cyber resilience processes. If the organization's employees perceive that there is a lack of interest and initiative from the part of executive management, it will be very difficult and challenging to implement an effective cyber resilience framework within the organization. The executive management of a financial institution is the one that is responsible for establishing the cyber resilience framework and making sure that cyber risk is effectively managed. The executive management is also responsible for setting the relevant risk tolerance for cyber risk.

The cyber resilience framework should be based on a widely accepted standard or framework that can be independently verified and assessed by relevant entities, such as external audit. For example, the cyber resilience framework can be based on the NIST framework, as advocated by the Basel Committee for Banking Supervision (BCBS) and include the five main functions of asset identification, protection, detection and incident response. Figure 2 describes the cybersecurity framework as prescribed by the U.S. National Institution of Standards and Technology.

Figure 2. NIST Cybersecurity Framework



Source: Bablix

A key aspect of cyber resilience is incident response and recovery, in addition to business continuity management. A financial institution, such as a central bank, plays a vital role in the stable functioning of the financial system. As a result, financial institutions should have a well-functioning incident response mechanism for various operational risk (including cyber risk) events. In the event of a cyber-attack on a systemically important organization, which is often considered as a significant part of a country's critical infrastructure, the organization should be able to recover effectively and rapidly from such events. These include large-scale operational events that can have significant and adverse effects on the financial system as a whole.

Building the Foundation: An Effective IT Governance Process

IT risk management is built on three core principles. Without these three core principles, having an effective information technology risk management and consequently, an effective cyber resilience process becomes considerably more challenging. These three principles include:

1. Well-structured Foundation of IT assets.
2. Well-designed and executed risk governance process. This must include an enterprise-wide view of all risks, making sure that executives can prioritize risk appropriately, while enabling lower-level managers to independently manage most risks in their areas.

3. Risk-aware culture in which everyone has appropriate knowledge of risk and in which open, nonthreatening discussions of risk are the norm.

An effective cyber and IT risk management framework needs to include a specific set of objectives and a relevant strategy, the aim of which is to implement the objectives that have been established by management. The various management bodies/persons of the financial institution should have respective responsibilities, the main points of which are presented below.

An effective information technology risk management and cyber resilience framework should classify information technology risk losses by loss event type. Executive management of the organization should therefore take the lead in establishing a strong risk management culture, develop a management culture, and supporting processes, to understand the nature and scope of the information technology risk inherent in the institution's strategies and activities, and develop comprehensive, dynamic oversight and control environments that are fully integrated into or coordinated with the overall framework for managing all risks across the whole organization.

It is also important to note that the organization should implement a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices for all of the employees of the organization. Executive management should also approve and periodically review policies comprehensively and appropriately documenting the IT risk management framework. A risk appetite and tolerance statement for IT and other operational risk areas that identifies the nature, type and levels of information technology risk that the organization is willing to assume need to be developed.

Furthermore, the executive management needs to oversee and supervise senior management in order to ensure that the policies, processes and systems are implemented effectively at all levels of the organization, including the operational level. Last, but not least, the executive management should also ensure that the institution's IT risk management framework, including the cyber resilience framework is subject to effective independent review by audit or other appropriately trained parties.

Senior management should, subsequently translate the IT risk management framework established by executive management into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage information technology risk in line within the institution's risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit's activity.

Other key areas that the senior management is responsible for is to ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to

resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee. In addition, senior management should maintain an effective issue-resolution processes. This process should generally cover and include a reporting process to track and, when necessary, escalate issues in order to make sure that issues are addressed and resolved.

There should also be a mechanism that is set up to implement a process to regularly monitor information technology risk and material exposures to losses. Again, in this respect, senior management should make sure that an appropriate level of information technology risk training is available at all levels throughout the organization. This process should also cover cyber resilience processes and the training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended. Senior management should implement business resiliency and continuity plans as a result, and both plans should be in place to ensure an ability to operate on an ongoing basis and limit losses in the event of a cyber-event or other forms of severe business disruption.

Cyber resilience using the 4A framework for Information Technology Risk Management

Managers, including the executives of a central bank, should take a comprehensive approach towards to cyber resilience and IT risk management, in general. The approach should be based on addressing availability, access, accuracy and agility risks of the bank. **The 4A framework is a bottom-up risk management approach, which assumes that availability (risk) is at the bottom of a four-step pyramid, without which access, accuracy and agility risk cannot be mitigated.** Likewise, accuracy and agility risk depend on availability and access risk, while agility risk depends on availability, access and accuracy risk, which precede it. Figure 1 shows the 4A approach towards IT risk management, involving the 4-step pyramid.

Figure 1. 4A IT Risk Management Model

Source: Westerman & Hunter

Availability risk consists of all potential scenarios that pose a risk to the organization's information systems and associated processes that are linked to systems and processes becoming unavailable or inaccessible. Availability risk is closely linked to an organization's business continuity management processes. It must be mentioned that availability risk increases when a financial institution such as a bank uses many different information systems that are not standardized. Examples of risk in this category include:

- Lack of recovery policies/instructions for the recovery of critical data (i.e. core-banking system).
- Damage/disruption to information systems (i.e. applications) due to cybercrime.
- Poorly understood processes and information systems (applications/programs)
- Old, outdated technology that often breaks down (i.e. the use of legacy systems)

Access risk comes from insufficient or inadequate access controls to an organization's information systems. Access risk can arise from insufficient internal controls. This can include such topics as network segmentation that is not implemented properly or unreliable network services, among others. Examples of risk in this category include:

- An inadequate information security policy
- Use of weak passwords, several employees using the same username and password.
- No encryption for sensitive data that can lead to a data compromise
- Lack of internal controls within applications/programs
- Lack of standardization and applications that need to be standardized (many programs with different rules and access rights)
- Databases that are not segregated (sensitive information is stored together with non-sensitive information)

Accuracy risk is the risk that is associated with the storage, use and processing of data and information that might be stored in an organization's information systems. A major contributor to accuracy risk is a lack of a single data exchange standard for information systems, the result of which can lead to the manual transfer and conversion of data that is stored in different systems. Accuracy risk also increases with the complexity of information systems that are being used by a financial institution. Examples of risk in this category include:

- Programs/Applications thta do not meet business requirements
- Bad, or poor communication between the business side of a bank and the information technology side (or structural units).
- Poorly understood processes associated with the accuracy of information and/or reporting.
- Lack of automation

- Information is mostly entered by hand in various information systems.
- Considerable errors in reports.

Agility risk can be caused by inflexible processes and systems that are difficult to either merge or separate. Poor project management practices as well as bad communication and coordination between an organization's business units and information technology employees/structural units can lead to increased agility risk. Examples of risk in this category include:

- It is difficult to make modifications/changes to existing information systems.
- Badly, or poorly implemented projects (lack of effectiveness).
- Poor IT-business relations.

All products and processes of a bank/financial institution are supported by information technology (IT). Information technology consists of different layers that need to be addressed by management, specifically: 1) infrastructure; 2) applications; and 3) data. These layers determine the IT risks that need to be controlled by adequate control measures. The different layers are described in the diagram below.

Complexity of IT systems

As a rule of thumb, the greater the complexity of an organization's information systems, the more likely it is that problems may happen. This also applies to cyber risk. Cyber resilience may be challenged, when a financial institution has highly complex information systems that are difficult to manage and operate. The complexity of information systems is determined by the number of information systems used by an institution and the level/degree of sophistication of interrelated applications and infrastructure components. When assessing information systems complexity, risk managers should closely look at the level of diversity in financial products, physical locations and outsourcing service providers of the financial institution.

In most cases, an organization's list of information systems, infrastructure (network) and application architecture documentation can provide the basic information required to assess the complexity of the IT systems environment.

Vulnerability of IT systems to internal and external threats

Vulnerability, measures the level of exposure that the information (IT) systems have to threats, both internal and external to the organization. Overall, IT systems that can be exploited maliciously for personal interests (financial or non-financial) will be subject to more threats. IT Systems that allow access to cash or other monetary reward are usually targeted (for example, pawn shop/lombard loan systems, ATM, online banking and other systems).

If a threat is able to effectively exploit a vulnerability, the institution has the risk that its IT systems will be compromised/hacked. An institution's fraud and security incident history (both internal and external), and IT risk register are useful in assessing the IT system's vulnerability.

Maturity of Information Systems

Financial organizations with information systems (including technologies) that have a proven track record of functioning well with minimum system failures and disruptions over time, may experience fewer problems than those with IT systems that are new. In the case of new systems, there might be problems or issues, that are not as well understood.

Risk managers should also take into consideration that more mature IT systems may be legacy systems, which are difficult to update since there may be few people who can support the system, or who understand the system.

An institution's IT strategy and the age of key systems can be useful in assessing the maturity of its IT systems.

Stress Testing and Cyber Resilience

Stress testing is a vital part of cyber resilience. The two main aspects of resilience are to ensure a financial institution's profitability through business continuity and incident response planning. The organizations' business continuity process needs to include the identification of critical business processes, risk assessment, regular testing of business continuity tests and monitoring.

This will allow financial organizations to identify how quickly and effectively they can react to any given scenario that might develop. An important note to point out is that financial institutions should not rely solely on historical events and losses. A prime example of this was the 2008 Russian Invasion of Georgia. The country had not experienced extensive cyber-attacks, such as those that were seen in August of 2008, prior to those events. It was therefore more difficult to prepare for such an event. As a result, financial institutions need to be forward-looking when they develop their scenarios. Just because an event has not happened in this past, does not guarantee that it will not happen in the future.

This is what cyber risk stress tests should cover. The main precept behind such stress tests is to identify the critical organizational systems, people and locations needed to continue to serve customers on a continuous basis and how to protect and recover the assets.

When conducting cyber risk stress tests for the purposes of cyber resilience, financial institutions must make sure that there is sufficient backing for the process from executive management. As already mentioned above, cyber resilience is a top down process. If there is no commitment from the management of the organization in order to show that cyber resilience is an aspect that the organization pays considerable attention to, there is only a small chance that such processes can succeed. It is consequently vital to ensure backing of both executive and senior management. There should also be sufficient time for testing and validation of the stress test framework.

When conducting stress testing for the purposes of cyber resilience, it is important to identify the goals and objectives of the stress tests that are being conducted. The financial institution must also identify the key people and functions that are critical to the business, in order to prioritize the order in which the processes will be recovered during incident response. This process is generally referred to as incident response. The organization needs to emphasize that all key employees/staff are involved in the stress testing process. These will likely be individuals who perform or supervise the critical operations, as identified during the business impact analysis.

It is worth noting that in some cases, external parties, such as outsourcing service providers, such as technology service providers or organizations that are responsible for incident response, may also be involved in the stress testing process. This can help to identify any potential vulnerabilities or deficiencies that might come from the outside. As a result, the testing process should be comprehensive and involve any, and all relevant people.

When it comes to the development of individual scenarios, an organization can come up with scenarios that are relevant, but slightly beyond the scope and nature of what has happened in the past. In order to make cyber resilience stress testing effective, it is therefore important to cover adverse, but relevant scenarios, that might affect a financial institution. Such a scenario might deal with ransomware that has happened in the financial system, but has not directly affected the financial institution that is conducting the stress test. Other scenarios might include distributed denial-of-service attacks that attempt to bring down an organization's online banking presence, or a phishing attack that has compromised the integrity of an organization's general ledger.

Last, but not least, an effective form of stress testing can include crisis simulation exercises. These can comprise an important aspect of preparedness. While not testing the business continuity processes of an organization directly, crisis simulation exercises can test how well a financial institution may respond to a specific event. The simulation exercises never usually mimic reality fully, but they do allow the participants to rehearse beforehand what an actual event may lead to. Therefore, crisis simulation exercises are a good mechanism to test incident response. They would also allow key decision-makers such as executive management to practice their decision-making skills.

References

1. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie, G. (February, 2020). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
2. Westerman, G. & Hunter, R. (2007). IT Risk: Turning Business Threats into Competitive Advantage.
3. Lee, Y. C. Crisis Simulation Exercises. Retrieved from https://www.itu.int/en/ITUT/extcoop/figisymposium/2019/Documents/Presentations/Yejin_C_Lee_Presenta tion.pdf
4. Papuashvili, D. (June 15, 2021). Crisis Simulation Exercises (CSEs) National Bank of Georgia. Retrieved from https://figi.itu.int/wp-content/uploads/2021/06/6_David-Papuashvili_NBG.CSEs_.DP_.pdf
5. Curry, J., & Drage, N. (2020). The Handbook of Cyber Wargames: Wargaming the 21st Century. The History of Wargaming Project.