DOI: 10.24234/wisdom.v25i1.970

CYBERSECURITY RISKS AND ITS REGULATIONS. THE PHILOSOPHY OF CYBERSECURITY AUDIT

Liana GRIGORYAN [1] Lilit MIRZOYAN [1,*]

1 Armenian State University of Economics, Yerevan, Armenia

* *Correspondence*
Lilit MIRZOYAN, Marx st., 18, 4 aprt. Artashat 0701, Armenia
E-mail:
lilit.mirzoyan.8888@gmail.com

Abstract: Since financial institutions are leading targets of cyber attacks, the article's main goal is to show that without dedicated action, the global financial system will only become more vulnerable as innovation, competition, and the pandemic further fuel the digital revolution. Also, the cost of cybercrime at financial institutions outpaces the cost of cybercrime in other industries. For example, according to a 2019 private study, the per-company cost of cybercrime is over $18 million for financial services companies, around 40% higher than the average cost for other sectors. If the entire system fails to address cybersecurity concerns adequately, this could lead to systemic risk – the risk that a cybersecurity incident would destabilize the financial system. The article considers the level of protection of confidential information in financial enterprises and the means of combating data leaks. In addition, the question of the need for an information technology audit, especially a cybersecurity audit, is raised.

Keywords: philosophy of cybersecurity, risk mitigation, cybersecurity audit, virtual bank, ransomware, security standards, information technology.

Introduction

Information systems change our lives a lot. The way we work, the way we play over many years. About 20 years ago, we had to go to the bank branch physically and get our services done. Then about 10 years ago, with e-Banking development, we could do some of the banking services in front of our computers. Now, we can see that almost everybody has a mobile phone in their hand. With this, then we have mobile banking. We could do everything using our mobile phone. Problem here is this, whether the money that I'm going to deposit in the virtual bank, will it be safe enough? Somebody need to check those information systems to make sure they function as they should. So the human touch is the one given by the IT auditor. The topic of cyber security threats is extremely relevant at the moment. Literally every day there are announcements of hacking attacks by hackers in the media. It is connected with continuous digitalization of business. Cyber threats follow users every step of the way, with just the click of a button and a cyber attack is now a reality (Karchija, 2014).

As businesses have become more reliant on technology, there have been increased attempts to disrupt financial institution operations; to steal, corrupt, or destroy data and intellectual property; or to divert funds have become more prevalent. As the Financial Stability Board points out, several recent events show the sizeable damaging effects such cyber incidents can have on the financial system. These include the attack on the Bangladesh Bank in 2016, which resulted in the theft of $81 million (Schwartz, 2016), the WannaCry ransomware attack in 2017, which infected more than 300 000 computer systems in 150 countries (Chappell & Neuman, 2017).

While all businesses face cyber risks, the stakes are particularly high in the financial services industry, given the critical role the financial system plays in the overall health of the global economy.

Okay, what is risk? Risk according to our understanding is a possibility of having a negative impact. So we take risk almost every moment of our life, like even if you go drive along the road, there's a risk about it.

You may be tempted to view cyber risk as a form of operational risk and work within the frameworks you have already established for evaluating such risks. Instead, we think it pays to put cyber risks into a special category, recognize they are becoming increasingly sophisticated, and realize that creative new solutions are needed to monitor and mitigate these risks. Cyber attacks have become more systematic, maliciously targeting financial firms and playing out over time for maximum effect. Detection can be difficult; an institution may believe it has backed up its good data, but those data may already have been compromised by malicious code that has infiltrated the institution's system. Data integrity will increasingly need to be a focus as firms develop plans for how they will recover from the inevitable attack. As financial institutions have adopted new technologies, sometimes through third-party suppliers, they are susceptible to risks that they may not have faced before. Those making the attacks are also adopting new technologies that more easily exploit gaps in financial firms' information technology, payment messaging and transaction authorization systems, and supply chains, which can widen the extent of the attack and make response or recovery more difficult. In such a landscape, weaknesses in financial firms' governance and communications structures – for example, not being clear about who has the decision rights to turn off a system, or what effect turning off one system will have on other systems – can exacerbate problems faced by a firm under attack (Mester, 2019).

Instead of being idiosyncratic and affecting only a few firms, as many operational risks are, cyber threats are more likely to be correlated across institutions because of the complex interconnections and dependencies among financial firms. This means that cyber threats are more likely to have wider spread, and potentially systemic, negative impacts than a typical operational problem that might arise from a failed system or process. Trading platforms, settlement and payments systems, and central securities depositories are all critical infrastructures on which financial firms depend, and if these systems go down, there are few substitutes. In addition, the advent of new technologies and the move to cloud computing create additional concentrated risk, as only a handful of third-parties provide these services.

In recent years, cybercriminals have been hijacking the digital transformation of financial institutions via island hopping. About 63% of financial institutions recorded a spike in destructive attacks by about 17% from 2021 (Duncan, 2022).

Institutions of all kinds, but especially central banks, must maintain cyberrisk awareness 24/7. Modern organizations use various digital devices (e.g., computers, tablets, smartphones, smart devices and Internet of Things [IoT] devices) to receive or provide digital services.

The number of IoT devices worldwide is projected to exceed 15 billion by 2025 and 25 billion by 2030. The digital world is far from perfect, and vulnerabilities appear and are discovered every day, even in devices and programs from reputable manufacturers and service providers. The complexity of the problem is obvious, and it does not have a simple solution (Vailshery, 2022).

The mass shift to remote working brought on by the COVID-19 pandemic in March 2020, exacerbated this complexity. Before COVID-19, organizations conducted business in their respective office buildings, where many hardware and software solutions were mostly protected from cybersecurity risk and attack prevention was

mostly effective. But throughout the COVID-19 pandemic, employees have been able to work from virtually anywhere. Because many organizations lack sufficient resources to equip their employees, they allow them to work on their own devices without enforcing an effective bring-your-own-device (BYOD) policy or putting effective mechanisms in place to manage risk.

Remote working has completely changed the security paradigm. Enterprises must be able to ensure the security of employees working beyond the organization's field of view on their own devices and using various cloud solutions such as Zoom's videoconferencing service (Stepanyan, 2022).

But what are the specific cybersecurity threats faced by financial enterprises in 2022, and what specific solutions can be deployed to mitigate the risk or eliminate the occurrence of cybercrimes?

Ransomware

Ransomware gangs consider financial enterprises as attractive targets because they can steal valuable information and sell online on the dark web. A ransomware attack involves locking out users from accessing their computers through malware encryption. Furthermore, since financial institutions deal with sensitive data, they may be forced to pay the ransom.

One of the largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks (Sanger et al., 2021).

The operator of the system, Colonial Pipeline, said in a vaguely worded statement late Friday that it had shut down its 5,500 miles of pipeline, which it says carries 45% of the East Coast's fuel supplies, in an effort to contain the breach. Earlier Friday, there were disruptions along the pipeline, but it was not clear at the time whether that was a direct result of the attack or of the company's moves to proactively halt it. Then Colonial Pipeline acknowledged that its corporate computer networks had been hit by a ransomware attack, in which criminal groups hold data hostage until the victim pays a ransom. The company said it had shut the pipeline itself, a precautionary act, apparently for fear that the hackers might have obtained information that would enable them to attack susceptible parts of the pipeline (Reuters, 2021).

Security experts advise financial enterprises against paying ransom since leaked data can be compromised and that the cost of ransom may be higher than the cost of data remediation.

Phishing

Phishing is a social engineering technique used by cybercriminals to trick users into providing their login details so the criminals can access an internal network. Email phishing is one of the most common threats faced by financial institutions.

Malware from email phishing attacks may be installed on user computers if the user opens infected attachments or links. It could also occur if victims load fake web pages designed to harvest their login details. According to Imperva Research Labs report (Terry, 2021), in the first half of 2021, the banking industry's phishing attacks rose by about 22%. Phishing attacks that target financial applications also increased by about 38% last year.

According to security experts, phishing attacks will further increase and urge financial enterprises to sensitize employees and customers to identify potential phishing threats in 2023.

Distributed Denial of Service (DDoS) Sttacks

DDoS attacks aren't going out of fashion, in fact, they're right on the runway. In the first six months of 2022, the number of DDoS attacks globally increased 203% compared to the first half of 2021. From cases of hacktivism to terabit attacks, the first half of 2022 saw 60% more DDoS events than in all of 2021 (Lazenby, 2022).

DDoS attacks on financial institutions have also been in the rise in 2022. 25% of all DDoS attacks in 2021 affected the financial industry, making it the most targeted sector (Lazenby, 2022). The goal of these types of attack is to overwhelm a bank's server using fake connection requests**.** The affected bank may be forced to

go offline with difficulties for recovery in a short-term perspective.

Since financial institutions have a diverse surface, including customer accounts, banking IT infrastructures, payment portals, etc., they become an attractive target by cybercriminals for DDos attacks. In the first six months of 2022, the number of DDoS attacks globally increased 203% compared to the first half of 2021. From cases of hacktivism to terabit attacks, the first half of 2022 saw 60% more DDoS events than in all of 2021 (Mahwah, 2022).

Bank Drops

Bank Drops are fake bank accounts opened by cyber criminals to store their stolen funds**.** Criminals create bank drops to confuse authorities from knowing their location. Cyber gangs collect bank customers' details to create so called "full" accounts. They collect information including date of birth, address, full names, credit score, driver's license details, and social security details.

In addition, the stolen data may be sold on the dark web for about $15 to $60 for each record. Aside from generic "fullz" data (an information package that contains a person's address, real name and other personal information), business fullz data of bank customers are sold for higher prices - about $35 to $60.

Supply Chain Attacks

Supply chain attacks are carried out to breach a bank's third-party vendor in its chain that is compromised. Usually, vendors take cybersecurity less seriously than their clients, and since they store sensitive clients' data, cybercriminals can exploit their vulnerability to attack the financial enterprises.

Supply chain attacks have risen in 2022 and are further expected to increase. Thus, the financial enterprises are advised to implement zero trust cybersecurity measures to deter supply chain attackers.

To mitigate cybersecurity risk of financial institutions, the latter shall employ the following strategies:

- *Multi-factor authentication.* By implementing a multi-factor authentication policy, financial enterprises can make it more challenging for cyber criminals to compromise their customers' sensitive and privileged data (Shacklett, 2021).
- *Two-factor authentication (2FA).* For financial enterprises, 2FA is most commonly accomplished when a bank sends a temporary code to the customer's cell phone, which is needed to log into their account. In this scenario, the hacker would need to have access to both the computer or account credentials and the cell phone. Several financial enterprises don't use 2FA for account login. The reason most often cited is that their customers find 2FA inconvenient (Bowcut, 2022).
- *Attack surface management.* ASM consists of four core processes: Asset discovery, classification and prioritization, remediation, and monitoring. Financial enterprises can embrace attack surface management solutions to reduce the risk of data breach by ensuring that data leaks are detected internally or from a compromised vendor before it becomes available for the cybercriminal (Michael, 2021).
- *Third part risk management.* Common types of third party risks include: cybersecurity, operational, legal, regulatory, and compliance, reputational, financial, and strategic risks. Implementing third-party risk management solutions will help in preventing supply chain attacks. It can help financial enterprises to identify any security vulnerability from third-party services (Tunggal, 2022).
- *The use of an up-to-date firewall solutions.* A secure firewall is a key defense against cyber attacks. Financial enterprises should ensure that their firewall protection program is updated regularly to help detect any attempt of malware injection (Mazzanti, 2019).
- *Employee training and customer sensitization.* Financial institutions should continuously train employees about cybersecurity best practices, including how they can identify potential threats and mitigate data breaches. They should also educate customers on the need to avoid divulging personal financial details to anyone without reaching out to their banks.

But what is risk mitigation? Risk mitigation means reduce the risk using controls. So let's think about an example. The current example

that we're going to think about is, you keep your confidential information in your server and it's connected to internet. So anybody can access to the information in the server. So in that case, it's really high risk because not only your employees or your customers can access the information but also somebody would like steal the data, or maybe hackers will be able to access your data. So risk is 100% because there is no control whatsoever. Now, how can we reduce the risk? We want to reduce risk to 80%. To do that, we have come up with some controls. I would like to have a control having just authentication, just username and password. So that at least a controlled access to the server, 80%. I would like to reduce further. Is it possible to reduce further? That means we have to come up with more controls to reduce the risk, right?

Now we decided to add the firewall. So adding a firewall would reduce the risks for example up to 60%. Still not happy. So we would like to reduce further. So now I want to reduce the risk to 50%. To do so we have to add more controls. Now what we are going to do now is to encrypt the data. What we are going to keep in the server so that only who can do the decoding, the data would be able to find the information in the server. So still 50% but I went to reduce further to 40%. So we need to have more controls. To do so then we are going to add the bio-metric devices as an additional way of authentication. So it's 40%. Now another question is we come up with all the controls in the world and then can we decide in one point of time that our risk is 0%. That means we eliminate the risk. Is it possible? I don't think so. So that means that it's not possible to eliminate the risk. That's very important remember that. We can reduce the risk using controls. But now you can see that we started from 100% total exposure and then 80, 60, 50 and 40.

Now the next question is this, which level are we going to stop and who make that decision? Answer is that decision is made by the senior management, because if something goes wrong within the organization, they have to have ultimate responsibility. So the decision is made to stop with the 60, 40 or 50 by the senior management. Why? This stops at where because as you can see that, more and more controls means cost is higher and higher. So they would try to balance between cost and the benefit and the cost and the risk. Then they would balance between these two and said stop. In this case, for example 60%. We put only username and password and the firewall and they think that is alright. But now still there is a 60% of risk right? Now management's not happy. Because if something goes wrong it's going to be ultimately their responsibility. So do they have any other choices? Yes. The next choice we have is to transfer the remaining risk to third-party for example, buying insurance.

Now the question is to ask is this, we reduced up to 60% and then transfer to the third-party. Why can't we just transfer it without doing any controls whatsoever? But problem here is this, if you do it without any controls, then the insurance agent will come and do their own risk assessment to the organization, then the insurance premium that you have to pay would be extremely high. So organizations always reduce the risk using controls to a level they feel comfortable. In other words, to a level that management feel most comfortable. Then if they are still worrying about the remaining risk, then we buy the insurance and transfer it to the third-party. Now, we reduce the risk using controls. We transfer the remaining risk to third party. Do you have any other options? Yes. The last option I would say is to avoid the risk. Let me explain with an example. We are bank and we would like to go for e-banking and it seems that e-banking is high risk to organization. We are worrying about the data lost, may be hacking to your customers information. So you decided, we'll continue with our traditional banking but no e-banking whatsoever. So that is avoid the risk. What is the difference between eliminate the risk and avoid the risk? Eliminate the risk means we still go for e-banking and we come up with many controls and decide, we don't have risks at all. That's eliminating. If we don't do e-banking, but we do traditional banking only, it is about avoiding the risk. At the same time this is the last option. Why? Because if we don't do e-banking, there are some customers within the organization. You have some customers who'd like to have services from your bank but they like e-banking? So since you don't provide debt service to those customers, they would like to go to other banks. As a result of that, you might lose some customers. So we can say that risk mitigation is about reducing use controls to a level acceptable to the manage-

ment, transferring the risk to a third party and avoiding the risk, not just eliminating it.

During the assessment of cybersecurity risks, it is necessary to pay attention to the following questions:

- *How closely is business related to information technology?* For example, if we are dealing with the bank, any attack or information system will directly affect the services provided, as well as customers satisfaction. We cannot say the same about agricultural business.
- *What information systems and resources are used and how vital are they?* To answer these questions, it is necessary to understand the extent and scale of damage the organization will suffer if the confidentiality, availability and integrity of information resources are violated. For example, a breach of confidentiality will lead to the leakage of internal information, which will ultimately lead to the loss of customers and loss of competitive positions.

Thankfully, there are ways in which people and groups at both ends of the scale can reduce their level of susceptibility to attacks, with virtual private networks (VPNs) and antivirus software programs among the most commonly used.

But one of the main problems disrupting cybersecurity compliance in the financial system is the sheer volume of different security standards and the significant overlaps between them - an expected problem for the most heavily regulated of all industries. This can be resolved by only focusing on regulations that are mandatory for financial organizations.

Each of the following cybersecurity regulations supports customer data security and data breach resilience (Kost, 2023).

The European General Data Protection Regulation (EU-GDPR) is a security framework by the European Union designed to protect its citizens from personal data compromise. The EU mandates GDPR compliance for financial services collecting or processing personal data from EU residents, regardless of the physical location of the business (Van Remoortel, 2016). Any organization must comply with the GDPR if it processes the data from EU citizens, meaning residents of the following countries: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

The United Kingdom General Data Protection Regulation (UK-GDPR). Brexit has removed the United Kingdom from any affiliations with European policies, including the European GDPR. However the UK-GDPR still retains EU-GDPR laws, they've just been slightly modified to accommodate certain areas of domestic law in the United Kingdom. Another difference is that the UK-GDPR is solely focused on the protection of the personal data of UK residents.

ISO/IEC 27001 is an internationally recognized standard for reducing security risks and protecting information systems. ISO/IEC 27001 is comprised of a set of security policies and processes that offer organizations across any industry guidance on how to improve their security posture. Because ISO/IEC is an internationally recognized standard for cyber attack resilience, financial entities wishing to demonstrate their exemplary cybersecurity practices to stakeholders should pursue ISO 27001 certification. Financial service providers not wishing to pursue the effort of ISO 27001 certification, could still improve their cybersecurity by just complying with the list of domains and controls of the framework. Certification is only recommended if an organization wishes to publicly display proof of ISO/IEC 27001 compliance. The other benefit of adopting this framework is that it could assist with GDPR compliance when coupled with an Information Security Management System (ISMS).

The Bank Secrecy Act (BSA), also known as the Currency and Foreign Transactions Reporting Act, aims to prevent financial institutions from laundering money, either willfully or through force during a cyberattack. The BSA is the primary anti-money laundering law in the United States. The BSA forces financial institutions to work alongside the U.S Government in the fight against financial crime. BSA compliance is regulated by the Office of the Comptroller of the Currency (OCC) through regular audits. Banks are expected to verify the legitimacy of all currency transactions. Compliance with the BSA is mandatory for financial institutions accepting money from customers including: national banks, federal branches, agencies of foreign banks, federal saving associations.

The Gramm–Leach–Bliley Act (GLBA) requires financial institutions to protect customer data and honestly disclose all data-sharing practices with customers. Under this U.S law, financial entities must establish security controls to protect customer information from any events threatening data integrity and safety. This includes strict financial information access controls to mitigate the chances of unauthorized access and compromise. The financial entities that must comply with GLBA include those that: sell financial products., sell or offer financial services, offer financial loans, any financial or investment advice, sell insurance.

Payment Card Industry (PCI) Data Security Standards (DSS) - PCI DSS for short - is a set of standards for reducing credit card fraud and protecting the personal details of credit cardholders. The security controls of this regulation are designed to secure the three primary stages of the cardholder data lifecycle: processing, storage, transfer. Every organization that processes customer credit card information must comply with PCI DSS, including merchants and payment solution providers.

PCI DSS is an internationally recognized standard that applies to all entities globally that process credit card data. Merchants are expected to complete Self Assessment Questionnaires (SAQs) to validate compliance. There are varying degrees of compliance processes depending on the size of the merchant. For example, enterprise merchants processing millions of transactions require annual onsite audits conducted by a Qualified Security Assessor. An upcoming PCI compliance audit may be cause for concern for many organizations, who are left scrambling to ensure their cybersecurity practices are up to scratch (Chipeta, 2022).

The Payment Services Directive (PSD 2) is a directive by the European Union supporting competition in the banking sector. PSD-2 is part of the Payment Card Industry Data Security Standard (PCI DSS) for financial data security. To ensure banking activities in the EU proliferate security, the PSD 2 also includes regulations for protecting online payments, enhancing customer data security, and strong customer authentication (eg, multi-factor authentication). All banks and financial institutions in the European Union must comply with the PSD 2 directives. All countries in the European Union are impacted by PSD 2.

The Federal Financial Institutions Examination Council (FFIEC) is an interagency body that aims to prescribe uniform principles of best practices for financial institutions. The FFIEC is governed by five financial regulators. The FFIEC outlines its cybersecurity guidelines in its Information technology examination handbook series consisting of the following 10 handbooks: audit, business continuity, development and acquisition, information security, management, architecture, infrastructure and operations, outsourcing technology services, retail payment systems, supervision of technology service providers, wholesale payment systems.

Such laws have raised the bar for organizations and encouraged them to make protecting personal data and privacy a top priority. Any disclosure of data can lead to financial penalties and reputational damage, which are directly tied to the loss of digital trust.

However to ensure that you're getting the protection you deserve, it's important to do some research and check out some reviews, to ensure that your weapon of choice is giving you adequate protection – particularly if you've paid a lot of money for it.

In these circumstances the only way to know that your organization can meet the challenge of cybersecurity risk is to perform a cybersecurity audit. Such an audit measures every aspect of your cybersecurity program – including those parts of the program found to be lacking. The latter helps the organization find solutions against cyber threats, cyber crimes and cyber attacks that have become increasingly aggressive in the cyber landscape.

Cybersecurity audits are extremely significant in validating that the required cybersecurity controls are in place and are functioning to detect vulnerabilities of insufficient and obsolete controls or non-existent security. To keep up with the sophistication of increasing threats and attacks, cybersecurity guidelines and standards ought to be more comprehensive while the diverse cybersecurity standards to be more compliant and aligned (Sabillon et al., 2018).

More broadly, one could say that a cybersecurity audit is an opportunity to review your IT systems, find weaknesses, and implement remediation measures to make your cybersecurity stronger. The purpose of cybersecurity audit is to act as a "checklist" confirming what the policy

says is actually implemented and there is a control mechanism to enforce it (*Cybersecurity audits*, 2022).

Cybersecurity audit is an information security audit and assurance program that provides the management with an assessment of the effectiveness of cybersecurity processes and activities that identify, protect, detect, respond and recover. Cybersecurity audits focus on cybersecurity frameworks, standards, guidelines and procedures, as well as implementation control. Part of auditing is to ensure that organizations have implemented controls. Organizations must always monitor cybersecurity practices, policies and plans. This is where audits play an important role. Once a cybersecurity plan has been created, the organization should make an audit to test the effectiveness and efficiency of the controls and protocols especially in protecting against cyberattacks and providing board and management with the guarantees of such protection (Tan & Libby, 1997).

Here are some signs that you need a cybersecurity audit (*Cybersecurity audits*, 2022):

- you are experiencing unexplained hardware or software problems,
- firewall protections are incomplete or disorganized,
- you don't have a clear cybersecurity policy,
- you lack existing benchmarks for cybersecurity performance,
- it's unclear who is in charge of various aspects of cybersecurity,
- you lack an incident management and business continuity plan,
- your personnel have low levels of cybersecurity awareness,
- you've made recent changes to your network, including hardware or software,
- businesses similar to yours have recently experienced cyberattacks.

The only way to know for certain how effective your network security measures are is to conduct an audit, which will help you identify any risks to your cybersecurity.

When conducting a cybersecurity audit IT auditors typically address the following (*What is a cybersecurity audit and why is it important?*, 2022):

1. Data security.
2. Operational security.
3. Network security.
4. System security.
5. Physical security.

However, success is not guaranteed solely on implementing cybersecurity, doing effective cybersecurity audit or using a newer technology. This is because many of the risks and challenges are present at organizational level.

A proactive cybersecurity program can play a crucial role in fostering digital trust. There are a number of strategies that support digital trust that an enterprise can implement as part of its cybersecurity program: adopt best practices and standards, strengthen security policies, monitor human behavior, invest in cybersecurity and so on.

Armenia and its financial system can be an ideal example in this regard. Armenia's information security is threatened by cyber attacks by foreign countries, international terrorist organizations, criminal groups and individuals. To adequately counter modern information wars, it is necessary to increase the level of public awareness and media literacy. The implementation of the latter is hindered by problems such as the imperfection of the comprehensive state policy regulating the information and cyber security sphere, the lack of legislation ensuring the protection of vital information infrastructures, the insufficient level of institutional capacity of computer emergency response structures, and the lack of cyber security coordination structures.

The coordinator of the technical (cyber security) component of information security in Armenia is the National Security Service. In addition, there is a separate approach related to the financial sector, which to some extent provides for the transition to the information security standards of the financial system (The Central Bank of the RA, 2013). However, Armenia is still far from being an informationally secure country in all spheres, including financial ones. Currently Armenia has no data retention legislation. All of this is evidenced by the national cyber security index (NCSI, 2023b), a global index that measures countries' preparedness to prevent cyber threats and manage cyber incidents. In this context, the top three are Greece (96.10), Belgium (94.81) and Lithuania (93.51), while Armenia is 90th in the list of 161 countries (NCSI, 2023a).

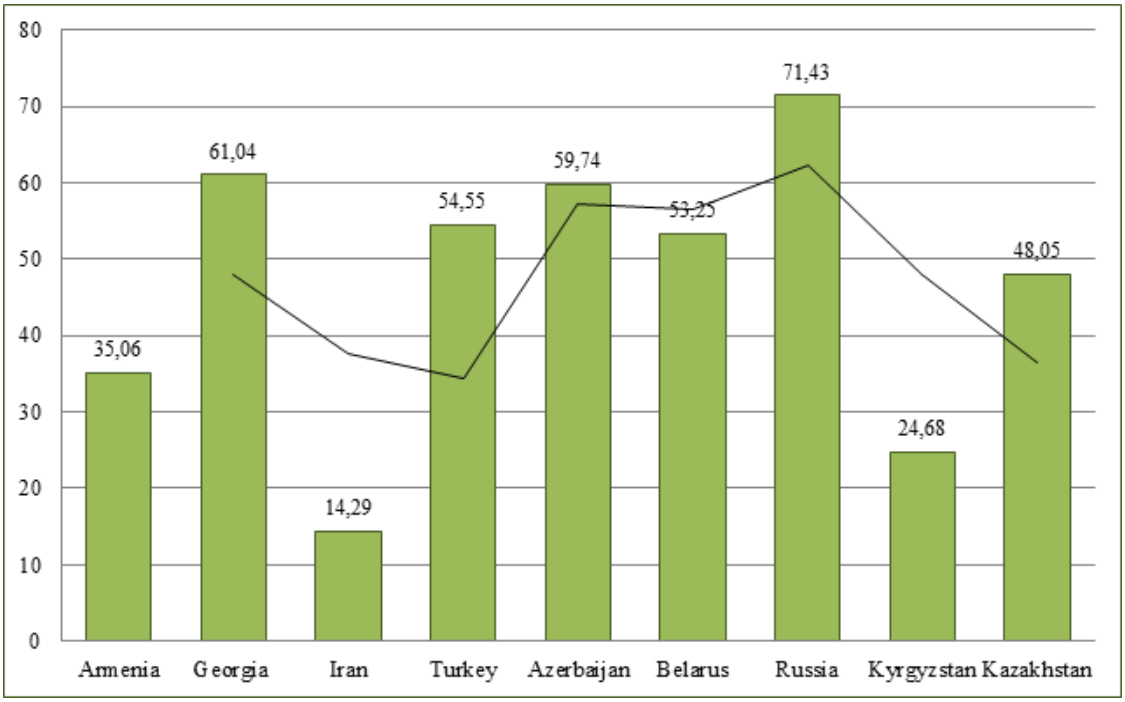

Figure 1. NCSI of Armenia, Neighboring States and EAEU Member States (NCSI, 2023a).

Unfortunately, Armenia is not behind only Kyrgyzstan and Iran in its ability to counter cyberattacks among neighboring countries and EAEU member states, indicating that cyber security issues need a systemic solution in all areas.

For the realization of the latter, first of all, after studying the experience of leading countries in the field of cyber security, to develop state policies and strategies for information, technological and cyber security and subject them to continuous monitoring. It is necessary to develop the financial system with higher security positions compared to other sectors, as well as the normative-legal framework of relations between other vital information infrastructures and the state, which will be possible especially through the localized implementation of many international standards.

Conclusion

The philosophy of cybersecurity is infinite. Cybersecurity is a journey rather than a destination. It has a beginning, but there is no end. The point at which an organization decides to protect its assets from cyber threats is the beginning, and because technologies, processes, and people are everchanging, the journey is endless.

Unfortunately, not all financial organizations have their own cybersecurity team. The concept that security is everyone's responsibility can be the first step toward an optimal mitigation strategy for organizations that lack the resources or budget for dedicated cyber teams.

The financial system of Armenia and the sectors directly connected with it, despite the efforts of the Central Bank, still remain attractive to cyber attacks. Taking these considerations into account the authors emphasize that fintech organizations should use cybersecurity frameworks and best practices to have a more stable security system.

All the considerations presented in the article allow the US, Canada and EU member states to have a financial system that is as secure as possible against cyber attacks, which cannot be said about Armenia. No matter how much we argue that countries at different levels of development cannot be considered at the same level, the progressive growth of financial fraud and cyber attacks in Armenia demonstrates that it is necessary to start by applying strict policies that are not limited to passwords and regulatory policies.

Financial regulatory authorities must adopt an

up-to-date and leading-edge cybersecurity philosophy. They should also be proactive in ensuring that minimum cyber hygiene exists at any organization that provides financial services. Cybersecurity strategies in the financial sector should also go towards increasing cooperation between banks and other financial organizations. Sharing information on attacks and organizing attack simulations are great exercises and though, they may not stop all cyberattacks – they can make a big difference in guarding against an attack and reducing detection and response times.

References

Bowcut, S. (2022, November 10). Cybersecurity in the financial services industry. *Cybersecurity guide*. Retrieved January 31, 2023 from https://cybersecurity-guide.org/industries/financial/

Chappell, B., & Neuman, S. (2017, December 19). U.S. says North Korea 'Directly responsible' for WannaCry Ransomware attack. *The Two-Way*. Retrieved January 27, 2023, from https://www.npr.org/sections/thetwo-way/2017/12-/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack

Chipeta, C. (2022, November 28). How to prepare for a PCI DSS audit in 7 steps. *UpGuard.* Retrieved January 29, 2023, from https://www.upguard.com/blog/-how-to-prepare-for-a-pci-dss-audit

Cybersecurity audits: Best practices + checklist (2022, April 26). *Reciprocity*. Retrieved February 1, 2023, from https://reciprocity.com/resource-center/best-practices-cybersecurity-audits/

Duncan, C. (2022, September 8). 5 Biggest threats to cyber security in the banking industry in 2022. *Deskalerts*. Retrieved February 1, 2023, from https://www.alert-software.com/blog/cybersecurity-in-banking#:~:text=What%20is%20cyber%20security%20in,legal%20action%20by%20aggrieved%20customers

Karchija, A. A. (2014). *Kiberbezopasnost' i intellektual'naja sobstvennost'. Chast' 1* (Cybersecurity and intellectual property, Part 1, in Russian). *Voprosy kiberbezopasnosti* ("Cybersecurity issues", in Russian), *1*(2), 61-66.

Kost, E. (2023, January 10). Top 13 Cybersecurity Regulations for Financial Services. *UpGuard.* Retrieved February 1, 2023, from https://www.upguard.com/-blog/cybersecurity-regulations-financial-industry#toc-10

Lazenby, S. (2022, October 6). DDoS attacks in the financial industry: How to protect your infrastructure and payments. *Inetco.* Retrieved January 29, 2023, from https://www.inetco.com/blog/ddos-attacks-in-the-financial-industry/#:~:text=In%20the%20first%20six%20months,than%20in%20all%20of%202021

Mahwah, N. J. (2022, August 17). Radware H1 2022 report: Malicious DDoS attacks climb 203%. *Radware*. Retrieved January 30, 2023, from https://www.radware.com/newsevents/pressreleases/2022/radware-h1-2022-report-malicious-ddos-attacks-climb/

Mazzanti, C. (2019, June 12). Keep your business secure with an up-to-date firewall. *Emazzanti technologies*. Retrieved January 25, 2023, from https://www.emazzanti.net/keep-business-secure-date-firewall/

Mester, J. L. (2019). Cybersecurity and financial stability. *Speech, Financial Stability Conference – Financial Stability: Risks, Resilience, and Policy - Federal Reserve Bank of Cleveland and the Office of Financial Research.* Retrieved January 31, 2023, from https://www.clevelandfed.org/newsroom-and-events/speeches/sp-20191121-cybersecurity-and-financial-stability#cf-fn-4

Michael, C. (2021, October). What is attack surface management and why is it necessary? *TechTarget security.* Retrieved January 30, 2023, from https://www.-techtarget.com/searchsecurity/tip/What-is-attack-surface-management-and-why-is-it-necessary

NCSI (2023a). The national cyber security index: Country ranking. In *NCSI*. Retrieved February 1, 2023, from https://ncsi.ega.ee/ncsi-index/?order=rank

NCSI (2023b). The national cyber security index: The methodology of calculation. In

NCSI. Retrieved February 1, 2023, from https://ncsi.ega.ee/methodology/-#:~:text=The%20National%20Cyber%20Security%20Index,national%20cyber%20security%20capacity%20building

Reuters. (2021, May 8). Colonial Pipeline halts all pipeline operations after cybersecurity attack. *Reuters*. Retrieved January 25, 2023, from https://www.reuters.-com/article/usa-products-colonial-pipeline-idAFL1N2MV01W

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2018, April 2). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *2017 International Conference on Information Systems and Computer Science, 2017 November 23-25* (pp. 253-259). https:-//doi.org/10.1109/INCISCOS.2017.20

Sanger, D. E., Clifford, K., & Perlroth, N. (2021, May 8). Cyberattack forces a shutdown of a top U.S. pipeline. *The New York Times*. Retrieved January 25, 2023, from https://www.nytimes.com/2021/-05/08/us/politics/cyberattack-colonial-pipeline.html

Schwartz, M. J. (2016, March 10). Bangladesh bank hackers steal $100 million. *Data Breach Today*. Retrieved January 20, 2023, from https://www.databreachtoday.com/bangladesh-bank-hackers-steal-100-million-a-8958

Shacklett, M. E. (2021, November). What is multifactor authentication and how does it work? *TechTarget security*. Retrieved February 1, 2023, from https:-//www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Stepanyan, K. (2022, October 5). Addressing the complexities of cybersecurity at fintech enterprises. *Isaca Journal, Vol. 5*. Retrieved February 1, 2023, from https://-www.isaca.org/resources/isaca-journal/issues/2022/volume-5/addressing-the-complexities-of-cybersecurity-at-fintech-enterprises

Tan, H. T., & Libby, R. (1997). Tacit managerial versus technical knowledge as determinants of audit expertise in the field. *Journal of Accounting Research, 35*(1), 97-113. https://doi.org/10.2307/24914-69

Terry, R. (2021, August 19). Financial services: Web application attacks grow by 38% in first half of 2021. *Imperva*. Retrieved January 31, 2023, from https://www.-imperva.com/blog/financial-services-web-application-attacks-grow-by-38-in-first-half-of-2021/

The Central Bank of the RA (2013). *"Teghekatvakan anvtangut'yan apahovman nvazaguyn pahanjneri sahmanman veraberyal kargy" hastatelu masin HH KB 173-N voroshum* ("Procedure on the definition of minimum information security requirements", in Armenian). Retrieved January 31, 2023 from https:-//www.arlis.am/documentview.aspx?docid=84836

Tunggal, A. T. (2022, November 24). What is third-party risk management? TPRM clearly explained. *UpGuard*. Retrieved January 28, 2023, from https://www.-upguard.com/blog/third-party-risk-management

Vailshery, L. S. (2022, November 22). Number of internet of things (IoT) connected devices worldwide from 2019 to 2030. *Statista*. Retrieved January 29, 2023, from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Van Remoortel, F. (2016, November). Financial institutions and the general data protection regulation. *Financier Worldwide*. Retrieved January 29, 2023, from https://www.financierworldwide.com/financial-institutions-and-the-general-data-protection-regulation#.Y9uyWHZB-xaS

What is a cybersecurity audit and why is it important? (2022, August 11). *Easydmarc*. Retrieved February 1, 2023, from https://easydmarc.com/blog/what-is-a-cybersecurity-audit-and-why-is-it-important/