Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 16-19 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

THE ANALYSIS OF CYBERSECURITY PROBLEMS IN FINANCIAL SERVICES SECTOR

Oksana Kovalchuk, Sokhumi State University
Diana Popova, Georgian Technical University

ABSTRACT: The concentration of money, bank-centricity of the financial market, a vast range of online services, and a significant customer base make banks and other financial institutions an alluring target for cybercriminals, leading to a sophisticated form of fraud. This intellectualized form of fraud reduces trust in financial institutions, decreases resources in the economy, and negatively impacts the country's financial and economic security, along with its image as a trustworthy financial partner in integration processes. The international regulatory community recognizes the importance of finding solutions to combat cybercrime and safeguard the rights of consumers of financial services, and they prioritize these issues as critical scientific challenges.
The financial services sector is a prime target for cyber-attacks and is heavily regulated across the globe. Financial services organizations face a constant barrage of intrusion attempts and other attacks, and they often struggle to transition from a reactive to a proactive cybersecurity posture. Achieving this goal is complicated by the ever-increasing number of attack avenues that arise due to the use of new technologies as part of digital innovation initiatives. Along with this complexity, there is a growing need to comply with regulations regarding the use of financial and personal data.
Analyzing cyber threats and addressing issues related to financial organizations' activities is an extremely relevant topic. This article aims to examine the primary cyber problems faced by the financial sector while also providing recommendations for financial institutions to help mitigate these challenges.

KEYWORDS*: cybersecurity problems, financial sector, regulations, cyber threats*

1. OVERVIEW OF THE PROBLEM

Good progress in overall digitization of finance has been made over the recent years. Indeed, the World Bank reports that between 2014 and 2017 the number of adults using digital payments increased from 41 to 52% (11% increase) [1] and the share of adults with an account has grown from 62 to 69% (7% increase) [2]. This translates into half a billion new users connected to the digital financial infrastructure – as well as half a billion new targets for cyber attackers. Yet, just as cyber-attacks were not invented yesterday, so financial institutions are aware of potential risks. After all, cybersecurity risk is but one form of operational risk that 'needs to be part of general risk management procedures, of general crisis management, and general business continuity planning'. However, until recently, rules relating to cyber-resilience rarely took the form of dedicated cybersecurity instruments and instead were generally included into other regulations (e.g on data protection) – and, for this reason, often remained rudimentary. Over the past several years, the cybersecurity regulatory landscape has undergone substantial changes. New laws and regulatory instruments focusing exclusively on cyber resilience have been adopted in a number of jurisdictions, including Hong Kong, the USA and Singapore. Cybersecurity has also become the focus of international rules and recommendations adopted by numerous organisations, including the BCBS, CPMI, FSB, G7, IAIS, IMF, IOSCO, OECD and the World Bank Group. Nonetheless, the apparently high interest in possible international harmonization of cybersecurity regulatory regimes has not yet translated into hard international law.
Bank-centricity of the financial market, high concentration of money, variety of online services, and significant client base - all this makes banks and financial institutions attractive to cybercriminals and leads to the "intellectualization" of fraud. This reduces trust in financial institutions, reduces the number of resources in the economy, and negatively affects the financial and economic security of the country and its image as a reliable financial partner in integration processes. Solutions to the problems of combating cybercrime and protecting the rights of consumers of financial services are recognized by

international regulators and priority scientific problems at the world level by the expert community [3-4].

The financial services sector is a particularly important target for cyber-attacks and is heavily regulated by jurisdictions around the world. Faced with constant intrusion attempts and other attacks, financial services organizations often struggle to transition from a reactive to a proactive cybersecurity posture. Achieving this goal is complicated by the ever-increasing number of attack avenues as a result of the use of new technologies introduced as part of digital innovation initiatives. In addition to this complexity, there is the need to comply with a growing number of regulations regarding the use of financial and personal data.

Protecting highly sensitive data is a top priority for both business and compliance. But sacrificing network performance for security is unacceptable, as consumers and businesses, from online and mobile banking to high-frequency trading, increasingly need real-time access to every offer. At the same time, to remain competitive in a multi-player industry, organizations must control costs and optimize operational efficiency.

In addition to malware, most businesses have had to deal with the rapid shift to remote work in recent years. The changes took place in an extremely short period of time, so companies did not have enough time to ensure safe conditions for remote work. Many organizations still work remotely, and remote work remains one of the challenges for financial cybersecurity.

According to an IBM report, one of the top three causes of data breaches is human error, which accounted for 23% of breaches. Employee mistakes can take many forms — they can become victims of phishing, social engineering attacks, or other types of malware [5-7].

In recent years, losses from financial fraud have increased dramatically. This has negative consequences for clients of financial and economic agents, who become the main object of fraud and lose funds. Fraud also causes significant damage to banks, which is manifested in the loss of customers, the need to reimburse stolen funds, increased funds for the modernization of the cyber security service, and the strengthening of protective measures.

The most common are:

1) Fraud with bank cards, as the most simple, accessible, and mass payment method, which makes it possible to forge cards, devices that read information, and steal data from cards;

2) Internet fraud, where the Internet, which is a platform for bank customers through which online payments are made, is used by fraudsters as a tool to steal customers' personal financial data;

3) Social engineering, when a fraudster on behalf of the bank learns all his information from the client and steals funds from his account. In the arsenal of fraudsters, there are quite a few methods of fraud involving psychological tools, computer programs, various technical devices, databases with customer information, etc.

In general, the financial sphere faces a large scale of threats every day, therefore it is very important to analyze these threats, as well as to develop recommendations, first of all, for employees of the financial sphere.

2. REASONS FOR INCREASING CYBER THREATS

The daily activities of financial institutions are closely related to the use of modern computer technologies and are completely dependent on the reliable and uninterrupted operation of electronic computing systems. World experience shows the unconditional vulnerability of any company given the fact that cybercrimes have no national borders, so hackers have the opportunity to equally threaten information systems anywhere in the world.

Cyber threat - existing and potentially possible phenomena and factors that pose a danger to the interests of people, society, and the state due to violations of the availability, completeness, integrity, reliability, and authenticity of the regime of access to information that circulates in critical objects of the national information infrastructure.

The fundamental causes of cyber threats are:

- lack of necessary legislation and uniform safety standards;
– insufficient funding from the financial organizations themselves;

- lack of corporate culture in the field of cyber security within the financial institution.

3. THE MAIN PROBLEMS OF CYBER SECURITY IN THE FIELS OF FINANCIAL SERCISES

We analyzed and highlighted the main cybersecurity issues in the financial services industry. In this section, we will look at the most basic problems and those that tend to increase:

1) Tracking

The attack surface is constantly growing, complicating the process of protecting against threats. The proliferation of Internet of Things (IoT) devices, the adoption of multi-cloud solutions for business services, and the use of mobile devices by customers and employees lead to a rapid increase in the number of attack vectors. As a result, financial services companies are being forced to deploy more and more specialized defenses to close the gaps created by the growing number of such attack avenues. The resulting security silos negatively impact traceability, increasing operational inefficiencies and increasing risk.

2) Operational efficiency

The lack of integration between different security elements and the fragmentation of the architecture increase operational inefficiencies. In the absence of integration, many work processes must be managed manually. In addition to delaying threat detection, prevention, and response, architectural storage creates redundancy, increases operational costs, and creates potential gaps in an organization's cybersecurity system.

3) Flexibility

As financial services organizations increasingly use cloud-based applications and infrastructure, the security architecture must be flexible enough to ensure the high speed, security, and interoperability of public, private, and hybrid cloud services while simultaneously protecting traditional on-premises services.

4) Compliance reporting

Financial services are one of the most demanding industries in the world, and all financial data, personal and corporate, is stored online—from the campus to the data center, the edge, and the cloud. Organizations must demonstrate compliance with several norms and standards. They should not involve employees performing strategic tasks to manually prepare audit reports.

5) Cost reduction

Financial organizations are constantly under pressure to limit and reduce the costs of maintaining their IT environment. In connection with the limitation of budgets for cyber security, it is necessary to use a strategic approach to the distribution of financial and human resources. Given the fact that money and staff time is limited, a strategy that limits the margin of risk and trade-offs is required.

These problems are exacerbated by the lack of personnel in the field of cyber security, which leads to the complexity and cost of the process of finding certain specialists, and also calls into question the possibility of finding them.

4. CONCLUTIONS AND RECOMMENDATIONS

Given the recent trends, financial institutions are obliged to invest significantly in the modernization of the cyber protection system by purchasing or creating modern fraud detection and prevention systems, which in the end may also prove to be ineffective. Therefore, to fight against cyber-attacks, the financial sector must take a consistent and systematic approach.

1) First, a clear regulation of the actions of personnel regarding access to data is necessary, which will allow avoid the facts of their access to the personal information of clients and, accordingly, its theft.

   Financial cyber security will reduce the chances of becoming a victim of phishing. To reduce the chances of infection, institutions should ensure that employees are informed about the basic rules of Internet security. It is important that employees know how to recognize phishing or

social engineering attempts. In addition, it is a good idea to provide staff with advice on safe remote work. Using even these measures will help organizations avoid financial and reputational losses.

2) Second, implement strategies that include fraud awareness training, public outreach through mass media and the Internet, fraud risk assessment, and continuous monitoring.

3) Thirdly, to improve the software and information support of the automated banking system, taking into account intelligent processing algorithms, which will allow identifying the fraudster and the victim at the stage of fraud, to prevent the implementation of such an operation, and to identify the criminal.
Criminals breach the financial cyber security of companies due to the lack of reliable IT solutions. Although financial institutions remain profitable targets for cybercriminals, there are a sufficient number of modern solutions and tools that allow timely detection of suspicious processes on the network and immediate response to incidents.

4) Another common mistake is that organizations overestimate their own cybersecurity. Even though a company may use quality solutions, not regularly updating the operating system and all software can compromise the security of the entire network.

In order to build strong enough defenses, companies need to take a balanced approach that combines employee training and the use of powerful security technology solutions.
While employee training is an important aspect of improving an organization's financial cybersecurity, the primary protection against threats is provided by the security solutions implemented in the corporate network and compliance with international standards.

5. RESOURCES:

1. Trend Report "Financial Cyber Threats Q1 2017". Electronic resource: http://www.level3.com//media/files/infographics/en_infg_financialserv_topnetworksecuritythreats_regionalbanks.pdf
2. IT threat evolution Q3 2017. Statistics. Electronic resource: https://securelist.com/it-threat-evolution-q3-2017-statistics/83131/
3. Ryan C. Hybrid Risk: The truth behind first party fraud / Chris Ryan // The official site of the company "Experian". – 2015. – Electronic resource: http://www.experian.com/blogs/insights/2015/10/hybrid-risk-the-truth-behind-first-party-fraud/.
4. Third Party Fraud // Open Risk Manual. – 2017. – Electronic resource: https://www.openriskmanual.org/wiki/Third_Party_Fraud
5. IBM Annual reports 2019-2022. – Electronic resource: https://www.ibm.com/annualreport
6. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, AndriyFesenko, Security methods against modern cyber-attack vectors in countries of Europe, Scientific and practical cyber security journal, 2019
7. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, AndriyFesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019