IRSTI 81.93.29 https://doi.org/10.26577/JPCSIT.2023.v1.i1.06

L.M. Alimzhanova , Y.M. Spanova*

International Information Technology University, Almaty, Kazakhstan
*e-mail: yerkezhan.spanova@gmail.com

IDENTIFICATION OF CYBERSECURITY RISKS AND THREATS TO ENSURE THE INTEGRITY OF THE FINANCIAL SECTOR

Abstract. The article discusses possible threats and risks for the country's financial institutions associated with information leakage. Various measures are proposed to reduce and neutralize such risks and increase the awareness of employees in the basics of cybersecurity. The article also offers various tools, such as protective IT systems, to reduce these types of risks and threats. Since every year potential threats increase, it is necessary to ensure the security of financial institutions.

For the functioning of the company, these risks are the probability of the worst scenario, and the threat is everything that can negatively affect the scenario from the outside. These risks negatively impact the company's ability to operate properly and generate financial returns. In some cases, risks can even lead to the bankruptcy of the company. Therefore, identifying these risks allows companies to prepare their organizational structures for various types of threats and minimize the impact of adverse events. It is a standard procedure and a key element of business planning.

In addition, the article describes the most commonly used cyber-attacks; company security methods; conducted a financial analysis of cybersecurity in general.

Key words: cybersecurity, information security policy, protective IT systems, leakage of confidential information, software, threat neutralization, social engineering, financial risks.

1 Introduction

The functioning and development of each state are associated with many risks and are carried out in the context of growing crises. Their consequences destabilize many systems and pose global security threats. First of all, it concerns the economic system. And in a situation of continuous potentially destructive changes, each structure, organization, and company is constantly in contact with existing risks in the current environment.

At the moment, one of the most common risks is violating the confidentiality of information, namely the leakage of confidential data. It can occur for a number of reasons: hacking and penetration into the structure of the company by a third party, unauthorized downloading by an employee of illegitimate software (software) that contains a virus, industrial espionage, human factor, etc.

Every year, cybersecurity becomes an increasingly important factor in the security system for enterprises, companies, and firms of any size in almost all sectors of the economy. In 2020, amount of ransomware cases increased to 150%, and every 39 seconds, a new attack was being launched somewhere on the network. Moreover, in January 2021, there were more than 3 thousand cyber-attacks committed in Kazakhstan, which is 2.8 times more compared to January of the previous year. At the same time, a year earlier, the number of cyber-attacks has declined by 30.5%. Such data was published at different times by ranking.kz.

According to international expert data, financial, material, property, economic and other damages are increasing annually, and are associated with a rise in cyber-attacks. Currently, the global expert community predicts the amount of planetary damage is up to 8 trillion dollars [1].

Most often, data leakage affects the financial and banking sector and causes a dramatic increase in costs. Banks and financial organizations are the areas where both financial and monetary resources exist, and this is a reason why financial institutions are often the main targets of cyber-attacks at different levels. Cybercrime contains many ways to generate income through extortion, theft, and fraud. Parallely, such crimes are committed not only by hacktivists, but even by states that target the financial sector for political, ideological, and informational influence and influence. The authorities, being regulators of this sphere, constantly pay attention to this and intensify the development and implementation of new means of controlling cyber risks to counter the growing threats that weaken national security, the economy, etc.

The purpose of this article is to consider risks, ways to neutralize threats, and methods of protection in situations of information leakage.

The subject of this study is the risks associated with information leakage.

The object of this study is the financial sector.

Article objectives:

– describe reputational and operational risks;

– consider cyber-attacks in the financial industry;

– describe security practices at the corporate level

– conduct a financial analysis of cybersecurity in financial institutions

2 Financial risks

Traditionally, in the financial sector, the main risks are divided into several groups. Let's focus on the two main ones:

• reputational (image) risks;

• operational risks.

2.1 Reputational risk

Reputational risk management in financial institutions is one of the most valuable strategies for a financial institution. Reputation management is the basis of any company striving for efficient operation and long-term development. A solid reputation means high performance, increased demand for goods and services, a growing customer base, etc. At the same time, a negative reputation can repel potential customers and increase their outflow, which in a highly competitive environment can lead not only to a decrease in income, and profit loss but also to bankruptcy. Monitoring of customer feedback by many companies shows that there is a decrease in trust in financial institutions, which are increasingly ranked second to last in the reputation rating compared to other industries.

Concerning cybersecurity, it can be said that at present at the moment it is the main component of the company's reputation. And the most vulnerable now are payment portals, which are of great interest to criminals. This is a significant security risk for companies and their customers. The second most important risk is the compromise of login data. Many users and consumers use the same password for all of their platforms, so hacking one of them is a threat to everyone.

Since large corporations carefully protect their own and managed assets, the risks are significant both for their own and for third-party users (partners, suppliers, subsidiaries, etc.). For example, small businesses rarely have the same security protocols, but may store or access customer data. The simplest example of a data breach affecting reputation is the Target data breach in 2013. Sales plummeted after a third-party provider was hacked, exposing 40 million credit and debit cards worldwide. Subsequently, Target was forced to lay off thousands of corporate and retail employees and only recently managed to partially restore its reputation and regain some credibility.

Practice shows that after the disclosure of information about a hack, stock prices fall by at least five percent. However, stocks can recover their value if the company immediately reports violations/hacks/leaks openly within a few days, thereby not only stabilizing the situation but also increasing its reputation in the field of security and overall reputation brand. In addition, such mechanisms of interaction with customers increase their level of loyalty.

2.2 Operational risk

Operational risk is defined as the possibility of losses as a result of the failure of internal processes/systems/external events, etc. This also includes the human factor. The following types of operational risks are distinguished:

• fiduciary violations;

• aggressive sales;

• privacy violations;

• failure of IT systems;

• litigation;

• misuse of confidential information, etc.

The organization controls operational risks by assessing real and potential threats, developing methods for improving security, and strengthening risk management, including external and internal factors. External factors may include natural disasters, political factors, destabilization of the financial system, and external interference (including offenses, cybercrime, fraud, etc.). Internal factors include technical failures of existing systems, inefficient maintenance of equipment and servers, and unregulated technical and organizational processes.

One of the most common threats in today's digital world is the possibility of using DDOS attacks. This is a common method of interrupting business operations, which is an intense attack on the target firm's server. For example, several years ago in Kazakhstan, the servers of several banks were subjected to DDoS attacks. According to Interfax, from September 26 to September 29, 2017, hackers used a botnet from devices located in more than 50 countries [2].

In addition to such threats, there are other types of them. The most common are identity and card fraud, phishing emails, skimming, and card fraud. The latter is the main type of fraud associated with the use of debit cards. In cases of such fraud, criminals gain access to confidential information, and customer credentials, and use online payments for personal gain, causing enormous damage to the financial structure, consumers of financial services, the client, etc.

3 Cyber-attacks in the financial industry

The following are the most common types of attacks used against financial services companies that can leak sensitive data.

Attacks on web applications. Many organizations rely on web applications for their business operations, with Google Suite being one of the most popular. These applications make it easier for employees to share files and collaborate. However, these services are vulnerable to attacks due to their ease of access and dependency on user actions. These types of attacks can lead to unverified redirects or links that trick users into clicking.

Botnets: Botbets are essentially automated programs designed to perform tasks on the Internet. Many businesses in the financial sector frequently use bots. They are often used to improve customer service. However, there are good bots and there are bad bots. A malicious bot can be programmed to directly or indirectly attack an institution—for example, it can be used to send spam emails or crack passwords using brute force.

Ransomware. Ransomware is a type of malware that, after infecting a system, can encrypt your files or even your operating system (OS). This effectively blocks access to important documents or the device itself. This is called ransomware because often the perpetrator behind the attack does not decrypt the system until the ransom is paid. This has become one of the most common types of attacks on financial companies and one of the most dangerous.

Phishing. Phishing attacks are almost as common as ransomware attacks. These attacks use social engineering to trick employees into taking action that allows the malware to be installed on your network.

4 Protection against cyberattacks at the corporate level

4.1. Training employees to detect phishing emails.

Today, phishing is a major social attack on businesses, accounting for over 75 percent of security breaches. Because no cybersecurity solution can 100% block these types of attacks, existing phishing education needs to be implemented or reinforced. This is important for understanding this process and ensuring individual protection against phishing attacks, as the elimination of their consequences is a lengthy, costly process and can compromise the entire infrastructure network. Therefore, the organization in terms of protection must work as a single team, acting according to the established regulations. In addition, a system of regular notification of attacks should be established (for example, the same mass mailing, informing through available sources, etc.).

While structured annual or semi-annual cybersecurity pieces of training are recommended, companies should develop on-the-fly phishing awareness training programs where link use includes immediate feedback. Such products include, for example, the KASAP (Kaspersky Automated Security Awareness Platform) programs, according to which you can receive training, and testing, as well as assistance from the system administrator, who can distribute legitimate phishing messages that increase cyber literacy.

4.2. Integration and update of information security policy.

IT security policy is critical to the success of any organization and is the foundation of all, shaping the ability of organizations to effectively respond to security incidents. Information security is based on the developed documented regulations, which are observed by all members of the company/organization. In this issue, for financial institutions, the importance of such procedures as the password policy of systems and users, the regulations of mail and corporate tools, and the information security policy itself are updated. Information security policies must be updated according to the approved standard.

4.3. Constant notification of employees about new attacks.

Cybersecurity statistics from past pandemic years show a huge increase in hacked data from sources that are increasingly found in the workplace (mobile and IoT devices). In addition, COVID-19 has expanded the opportunities for cyberattacks through the active use of forms of remote work. In this regard, it is necessary to increase the awareness of employees about new types of attacks (through the same mass mailing, regular notifications, posts in corporate networks, etc.).

4.4 Use of various types of protective IT systems.

According to statistics, in 2021 the number of cyber-attacks increased by 6.5% compared to 2020 [3]. Criminals are increasingly using social engineering, exploiting security flaws and vulnerabilities in software, as well as using deliberately malicious software. To ensure the security of the system, it is necessary to use such protection tools as antiviruses, DLP systems, "traps" programs, various kinds of SIEM, etc.

5 Financial analysis of cybersecurity in financial institutions

To ensure the protection of the entire infrastructure, various types of IT systems are used. These systems should cover 100% corporate servers, and laptops, and protect and monitor in real-time. The priority of each company is to protect corporate laptops first, since, according to research, 90% of data leaks occur due to human error, and not external actions of hackers. To prevent the leakage of confidential data, special technologies are used, namely DLP systems. They can analyze and foresee the data flow. Also, with the help of such systems, you can block connections, view histories, and also identify incompetent employees, including those who exceed their authority. So in 2021, a large company prevented a data leak to a competing company when employees using a portable device tried to send data to competitors.

The next no less important protection tool is various types of antiviruses, which are installed both on servers and employees' devices. At a minimum, they can block the launch of illegitimate software, remotely update the policies of the device itself, and monitor user actions. Antiviruses can block up to 80% of cyber-attacks on a company. The most important advantage is the constant automatic updating.

Honeypot are also successfully used to protect infrastructure. They are a decoy that helps to block the attacker's actions. Such traps are often referred to as honeypots. The biggest strength of this system is that cybersecurity staff may not know that a cyberattack has occurred and a hacker has penetrated the company's internal network. However, due to pre-set traps that can simulate a network, a server, or another system, he will not be able to continue his actions. Although they do not cover the infrastructure 100%, they are considered very effective.

SIEM systems, like antiviruses, and DLP systems can provide real-time event analysis, but they are more used to ensure the integrity of servers. They conduct an examination more deeply, so you can find out where the cyber-attack was made.

Table 1 below shows the prices for the above-described IT products.

Table 1 – Prices for IT products

Antivirus	From 10 000 tenge, 1 device
DLP system	From 60 000 tenge, 100 devices
Honeypot	From 20 000 tenge, 1 device
SIEM system	From 20 000 000 tenge
Note: compiled by the author from open sources	

6 Conclusion

Shortly, due to the increase in the frequency of cyber-attacks, the neutralization of threats and risks in the financial sector within the framework of cyber security comes to the fore and involves the creation of system security at all levels of both performers and management. It also requires constant monitoring of risks, which involves increasing the level of computer literacy of employees and staff through various cybersecurity training courses and annual audit checks, and compliance with controls by the current year's standard for effective information management.

The emergence of new technologies and spyware requires constant software updates and additional financial and technical resources.

References

1. Zhandybaev Kairat, How the cybersecurity of Kazakhstan is developing, https://strategy2050.kz/ru/news/kak-razvivaetsya-kiberbezopasnost-kazakhstana/;

2. http://lib.itsec.ru/newstext.php?news_id=119080.

3. Akhmedov R. T., Saidaev A. M. Globalization of cyber threats in the modern world // ECONOMICS. – 2022. – T. 12. – No. 3-1. – S. 257-265.

4. https://www.reviewtrackers.com/blog/bank-reputation-risk-management.

5. Shukla A., Kukreja M. A Study of Risk Management in Finance Sector //Available at SSRN 2576131. – 2014.

6. Zinovieva E. S. et al. Strategic management of financial risks and methods of their assessment // Innovative economy: prospects for development and improvement. – 2019. – no. 2 (36). – S. 226-233.

7. Kazantseva S.Yu., Mezentseva Yu.R., Gaidarova L.V., Kleimenova K.A. Financial risks of business entities and their impact on the investment attractiveness of the enterprise // Bulletin of the Eurasian Science. – 2018 No. 5. – URL: https://esj.today/PDF/23ECVN518.pdf.

8. Mouton F., Leenen L., Venter H. S. Social engineering attack examples, templates and scenarios //Computers & Security. – 2016. – T. 59. – C. 186-209.

9. QuickBooks Canada Team, Train Your Employees to Recognize Phishing Emails, https://quickbooks.intuit.com/ca/resources/running-a-business/train-employees-recognize-phishing-emails.

10. Mohammed D. Cybersecurity compliance in the financial sector //The Journal of Internet Banking and Commerce. – 1970. – T. 20. – №. 1. – C. 1-11.

11. Lukyanenko A. V., Kuzmicheva I. A. Management of financial risks of an enterprise // International Journal of Applied and Fundamental Research. –2015. –no. 8-1. -P. 129-131.

12.Kapital.kz, The number of cyber-attacks in Kazakhstan has almost tripled, https://kapital.kz/tehnology/93798/kolichestvo-kiberatak-v-kazakhstane-uvelichilos-pochti-v-3-raza.html.

13. Rene' M Stulz, "Risk Management and & Derivatives, 2003. RS Raghavan, Risk Management in Banks -ICAI publication, Feb 2013.

14. Verma S B, Risk management -Deep & Deep publications.