Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Understanding and analyzing the cyber risk in financial services

Ibrokhim SAIDOV[1]

Tashkent State University of Law

ARTICLE INFO

Article history:
Received July 2023
Received in revised form
15 July 2023
Accepted 25 July 2023
Available online
15 August 2023

Keywords:
cyber-crime,
hacking,
banking,
financial services.

ABSTRACT

This paper will closely look through all possible reasons for cybercrime, discuss those who commit the crime, bring some current actions which are being taken against online frauds, and propose some possible preventative regulations which may help to decrease the number of cybercrimes.

2181-1415/© 2023 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol4-iss6/S-pp322-328

Moliyaviy xizmatlarda kiberxavfni tushunish va tahlil qilish

Kalit so‘zlar:
kiberjinoyat,
xakerlik,
bank,
moliyaviy xizmatlar.

ANNOTATSIYA

Ushbu maqolada kiberjinoyatning barcha mumkin bo‘lgan sabablari batafsil ko‘rib chiqiladi, jinoyat sodir etgan shaxslar muhokama qilinadi, onlayn firibgarliklarga qarshi ko‘rilayotgan ba’zi joriy choralar ko‘riladi va jinoyatlar sonini kamaytirishga yordam beradigan ba’zi mumkin bo‘lgan profilaktik qoidalar taklif etiladi.

Понимание и анализ кибер-риска в финансовых услугах

Ключевые слова:
киберпреступность,
взлом,
банковское дело,
финансовые услуги.

АННОТАЦИЯ

В данной статье подробно рассмотрены все возможные причины киберпреступлений, обсуждены лица, совершающие преступление, приведены некоторые текущие меры, принимаемые против онлайн-мошенничества, и предложены возможные превентивные правила, которые могут помочь уменьшить количество киберпреступлений.

[1] Lecturer, Business Law Department, Tashkent State University of Law. E-mail: ibrohim.saidov.1991@gmail.com

INTRODUCTION

Digitalization has brought innumerable opportunities not only for individuals but also the companies, organizations, and other institutions. Today, the positive influence of the virtual world, the Internet, and the digital world can be seen in almost all spheres. Thanks to digitalization, people can do tasks in a few minutes, or even a few seconds which took days to months in the past. It has also brought plenty of reductions in the costs of organizations and companies. They are operating much more efficiently, in the shortest time possible earning the most profit possible. Due to the Internet, individuals can now do many things not leaving their homes ranging from shopping to banking. Moreover, connecting with other people and keeping in touch with others has now become much easier. People can not only send messages and letters to one another easily but they also video chat, etc.

However, digitalization has also brought some drawbacks, which are becoming a global problem today. Even though people benefit from the advantages of the digital world, they are also becoming the victims of online fraud. Besides, large companies and organizations have been the victims of several cyber-attacks. That is why, today almost all international institutions are looking at this problem seriously, as they are losing several billions of dollars, and this is affecting the economies of several countries negatively. The global economy has also been affected by these cybercrimes. Besides, since the cyber-attacks have gone international, they have created problems in the political affairs of the countries. There are, of course, several reasons why these online frauds are happening, and the organizations. The political instability between countries, financial motives, and other factors can be the incentives for cyber attackers to commit their crimes.

The problem has become one of the most urgent issues in the world, and organizations and companies are trying to find out why these are happening, who are committing the crime, how they can be solved, and what preventative actions should be taken in order to prevent possible frauds. This paper will closely look through all the possible reasons of the cybercrime, discuss those who commit the crime, bring some current actions which are being taken against online frauds, and propose some possible preventative regulations which may help to decrease the number of cybercrimes.

WHY CYBER-CRIME IS DANGEROUS FOR THE ECONOMY?

The world has been changing in an extremely high speed and the technological advancement can be seen in almost all spheres, including banking. These changes not only brought positive progress but also created some problems for the government and society. Today individuals enjoy using technology in buying and selling process, online banking, communication, etc. While using these services people have to depend on different third-party applications and products such as virtual wallets and cloud services. However, this dependence on technology has also brought several problems that have become crucial to be illuminated and solved. According to Richard Home, third-party systems have become weapons of attack on businesses, banks, and even individuals as they are interconnected. Today cybercrime is not a local problem in a specific country, but it has become a global issue. According to a recent PwC survey cited in “The cyber threat to banking”, 93 percent of large organizations report cyber-attacks on their system. Another fact by a BIS paper given in the article is that today the UK’s annual expenditure on cyber security has become £700 million. Another statistic about cybercrime cited in (cybercrime: the growing threat to global banking) is that in 2015 alone, Asian companies lost $81 billion due to cybercrime.

WHO ARE HACKING?

There are several theories about the criminals that commit cybercrime. The ones that are most common are known as “hackers”; however, the types of criminals are not only them. Richard Home divides the malicious actors into three main categories: Hacktivists, Organized criminals, and Nation State. Hacktivists are mostly motivated to cause disruption and embarrassment to the targets and their favored techniques include SQL and DoS. Another main type is organized criminals who mostly aim at gaining financial resources. They are getting more and more sophisticated day by day, and they mainly use integrated attacks both technical and social engineering. The third type mentioned in the article is Nation State who is considered to be most targeted. They may not be highly complex and they use phishing as their tool.

The criminals may belong to any group and they mainly focus on the weakest points. Besides, the employees play a major role in electronic crimes aware or unaware. According to statistics given by the PwC cited in Richard Home’s article, a little more than two-fifth of the economic crimes are committed by the insiders that are employees within the organization. The hackers utilize different types of techniques and tools to commit their electronic crimes ranging from malware to social engineering that is sending voice or electronic mails to obtain the victims’ data. In addition, they never seem to stop getting sophisticated. The more the technology is developing, the more complex the attackers are getting. William A. Carter reports that attackers, especially, nation states having bigger budgets, protection from law enforcement, and access to top talents in cybercrime are causing more sophisticated threats.

There are various reasons why cybercrimes are committed. Financial gain is considered to be one of the most common incentives for hackers. Another cause of cybercrime is suggested to be political issues by Alexander Jones. He mentions that owing to the dispute over the territory in the South China Sea, Asian countries and companies have become vulnerable to cyber-attacks. This idea is restated by Richard Home that because of the political instability between Ukraine and Russia, the firms and organizations were attacked several times by Russian and Ukrainian cyber groups. There is another case given by Richard Home that a hacktivist from the group al-Qassam Cyber hacked the US banks in response to the video posted on Youtube.com miniaturizing the founder of Islam. This list goes on with many more examples. Moreover, what is letting electronic criminals commit such crimes is that the companies, mostly from Asia, have less sophisticated cyber security, or none at all. According to Alexander Jones, only after the incidence when 80 million JPMorgan Chase accounts were hacked, the firm doubled its expense on cyber security to 500 million USD.

Due to the cyber-attacks, not only the individuals and firms, but also the banks are suffering. The clients of the banks are mostly targeted by the cyber criminals, as they see them as the weakest point of the banks. Banks, too, have been the victims of the e-criminals, owing to several factors. One of the examples given by Alexander Jones is Bangladesh Bank from which 101 million USD was transferred to different bank accounts and that became a whole global case. According to William A. Carter, the five largest banks are located in Asia, and the continent shows the highest levels of mobile banking and transactions in the world. However, unlike Europe and the United States, they do not invest in cyber defense significantly, and their defense system still remains less sophisticated.

As mentioned above global digitization has brought efficiency to what most companies and organizations do and it helps them save plenty of time. However, according to the article "Understanding Systematic Cyber Risk", the interconnectedness among the 50 billion technological devices has also brought some issues. Those problems have negative consequences as well, which can be divided into two categories: primary and secondary influences. The former might include the loss of financial resources, embarrassment, etc. However, the latter involves the loss of reputation, as a result losing reputation in the local and global market. The company may see huge declines in share prices. Richard Home states "If publicized, network security breaches can affect share prices, cause irreparable reputational damage, and impact on the stability of the wider financial market". Besides, the staff and management do definitely experience psychological difficulties. Eventually, the customers will lose their trust and loyalty towards the company and the banks, which are the most important things for the firms to operate successfully.

The issues arisen from highly interconnectedness seem to be inevitable, that is why, the solutions to the problems should be proposed, or most effectively, they should be prevented before they happen. Even if they happen to take place, organizations and companies should be ready to find the criminals more easily, unlike the case which took place in Bangladesh Central Bank. The criminals have used such tricky ways that they still have not been found.

CURRENT SOLUTIONS

A number of steps have been taken against cybercrime. Companies and organizations have not only developed their defense systems on the networks, but they have also been providing individuals with information and new defensive tools to protect themselves from possible online fraud. Such tools are chip cards and multi-step authentications. However, the attackers have not ceased further development, they have become more complex and more sophisticated. In the past, military systems, and government networks were the main targets of cyber criminals, but at present, they mainly focus on the financial sectors. Willam A Carter brought several examples in his article. First, the banks are being robbed by nation-states. Second, currently, criminals have access to nation state capabilities. Furthermore, there are open-source malware libraries that provide advanced capabilities to cyber-criminals.

Another action against the online fraud is the law enforcement. Nevertheless, this action has also been criticized as it is having difficulties in keeping up with the new technologies. According to William A. Carter, those include anonymization tools such as VPN and Tor which hide the cybercriminals and their locations. Another factor that makes hackers unreachable is the rise of virtual wallets and cryptocurrencies. Using them, the criminals become highly anonymous and difficult to investigate legally. Moreover, law enforcement does not have enough funding, skills, and tools. For instance, Brazil's legislation is criticized in that its punishments are inadequate, funding to prosecute cybercrime is low, etc.

PREVENTATIVE ACTIONS

Even though the organizations and companies have been trying keep up with the cybercriminals both technologically and legally, a key point is taken into account very little that is human factor. Overall, it is the individuals who click the link, not the computers. Even the computers of the largest organizations and the firms are controlled

by people, open an e-mail containing malware, the hackers will then be able to have an access to the system. This is the reason why individuals should be paid attention and explained all the possible ways that they may become the victims of online fraud. Most online frauds occur because of the lack of awareness of cyber risks. It is mainly thought that personnel of the organization are mainly responsible people, however, there were some cases when the CEOs of large companies were tricked by the hackers. That is why, the employees of the organizations should be informed about any possible threats.

Another possible preventative action is that informing the customers about the possible cyber risks, as they are becoming the main targets of cybercriminals. According to Kaspersky Lab 'For criminals targeting bank's customers is often cheaper and easier than targeting the banks themselves. Most banks see their customers as the weakest link in their IT security.

The jurisdictions with specific regulatory requirements against cybercrime are initially suggested to document cyber-security programs and policies, which follow the typical pattern of CPMI framework involving governance, identification, protection, detection, response, and recovery. According to this article, cyber-event reporting is also a usual way of regulation, where all the banks in a specific area, or all the international banks are expected to be connected and whichever experiences an online fraud, all the others are alarmed and informed instantly, which is thought to prevent cybercrime to some degree.

Even though cyber-threat intelligence-sharing programs may not be one of the explicit regulations, it is highly encouraged to be used by banks. Juan Carlos Crisanto and Jermy Prenio bring Hong Kong as the only region, which includes such system.

RECOMMENDATIONS

The importance of proposing solutions has been understood by the whole world, and all the organizations and companies are trying to solve the issues, give recommendations and take preventative actions. The reason why it should be taken seriously is that day by day the threats of the digitalized world have been increasing although digitization has brought several advantages. Several recommendations are proposed in order to avoid online frauds. Initially, raising is the key point in being safe online. If both customers and staff members as well as the management are aware of the possible cyber threats, there is high possibility that the criminals can hack into their systems.

Other key points are leveraging trusted resources and building an economic framework are important to protect banks against cyber-attacks. Additionally, connecting and cooperating with the international organizations such as the United Nations, INTERPOL is supposed to be one way of protection against the online frauds Besides, the problem of cyber-crime is an international one and the reason is that currently, the financial organizations are interconnected which enables the hackers to identify the systems of the chain of the banks more easily. The availability of more sophisticated strategic policies to protect the banks is extremely important. For example, European and International Bank Federations should be responsible for controlling online frauds which may arise in the financial sector and if possible, they should identify and propose regulations. As cybercrime has become international, the international organizations and the companies are required to be equipped with state-of-the-art technology and systems. Nevertheless, there are many actions to be accomplished in this sphere. The banks, which operate in different jurisdictions, need alignment of regulatory

expectations to avoid any conflicts and threats. In order to combat the online threats, firms and organizations need coordinated strategic policies, as the capacity of law enforcement is considered to be limited.

Another suggestion is that information about past cyber-attack should be widely available as other organizations should be aware and have a chance to protect themselves. Financial organizations should have an access to a special platform which shares information about the recent cyber-attacks, and the platform should be internationally accessible in order to prevent cross-border cyber-attacks. For instance, the member banks of BBA Collaboration system have an access to the centers of the cyber information through which they can get the necessary data both quickly and safely. The compulsory requirements are needed for the banks to be able to report cyber-events. If the banks have clear accountability for cyber-risk issues such as Chief Information Security Officer, it would may it much easier to monitor the situation. However, the last point is not popular among companies and organizations as the number of professionals in the Information Systems field is considered to be low.

Juan Carlos Crisanto and Jermy Prenio state that the national governments should be responsible for further defense structure against cybercrimes, as it is not only about international companies and organizations but is also about the security of the individuals living in the country.

Finally, organizations and companies as well as banks should increase hygiene education of cyber-risks in order to avoid future threats and risks. As mentioned above, firms and organizations have been developing their technology and virtual system, however, the human factor should also be taken into consideration. The priority has mostly been on the technology not on individuals. For example, social engineers mostly target the employees of banks to gain access to their systems. They may send infected e-mails. That is the reason why individuals should be the main priority while defending against cyber-attacks. According to By Juan Carlos Crisanto and Jermy Prenio, ‘raising cyber-security awareness among bank staff is an important component of a bank’s initiative to protect itself from cyber-risk’.

Several meetings and conferences about the possible cyber-attacks may also be very helpful in order to raise the awareness of the staff members and the management. A number of cases can be brought as examples so that the employees of banks and other institutions could witness the consequences of those cyber-crimes. Overall, Juan Carlos Crisanto and Jermy Prenio mention that cyber-security awareness should be promoted as much as possible and this plays a major role in any regulatory framework. These actions will not definitely end all the online frauds, but they help to decrease the number to some extent. Moreover, individuals should take some responsibilities to decline the number, as most of the crimes happen through human factors.

In conclusion, the digital world has not only brought benefits, but it has also brought some issues which have become global these days. Many companies have had their money stolen, and many banks have suffered from the cyber-attacks. Moreover, individuals have let the cyber criminals have an access to their different accounts and do things with their identities. As most of the international companies and organizations suffer from the current cyberattacks, they have come to conclusion that the cybercrime should be taken seriously and several actions against it should be taken. Thorough investigation of the criminals, different types reasons of cybercrimes, possible negative consequences of online frauds, current actions against them and future preventative actions have been mentioned and discussed in the current paper.

REFERENCES:

1. H. Richard, 'BBA, 'The Cyber Threat to Banking: A Global Industry Challenge' (2014) https://www.bba.org.uk/wpcontent/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf [acceded 05 May 2021]

2. A Carter, 'Forces shaping the cyber-threat landscape for financial institutions' (2017) Swift Institute Working Paper https://www.swiftinstitute.org/wpcontent/uploads/2017/10/SIWP-2016-004-Cyber-Threat-Landscape-Carter-Final.pdf [acceded 05 May 2021]

3. A Jones, 'Cybercrime: The Growing Threat to Global Banking' (2016) https://internationalbanker.com/banking/cybercrime-growing-threat-global-banking/ [acceded 05 May 2021]

4. World Economic Forum, 'Understanding Systemic Cyber Risk' (2016) White Paper http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf [acceded 05 May 2021]

5. Kaspersky Lab. "New Technologies, New Cyberthreats: Analyzing the State of IT Security in Financial Sector." 2017. https://go.kaspersky.com/rs/802-IJN240/images/Financial_Survey_Report_eng_final.pdf?aliId=372190581 [acceded 05 May 2021]

6. J C Crisanto and J Prenio, 'regulatory approaches to enhance banks' cyber-security frameworks' (2017) https://www.bis.org/fsi/publ/insights2.pdf [acceded 05 May 2021]

7. B. ROBERT '5 strategies for addressing cybercrime' (2017) https://gcn.com/articles/2017/01/11/strategies-addressing-cybercrime.aspx [acceded 05 May 2021]

8. Y.Fedotov 'Taking action where we can to stop cybercrime' (2018) https://www.unodc.org/unodc/en/frontpage/2018/May/taking-action-where-we-can-to-stop-cybercrime.html [acceded 05 May 2021]

9. Qizi A. S. A. RAQOBAT HUQUQI: USTUN MAVQE TUSHUNCHASI VA UNI TARTIBGA SOLISHNING AHAMIYATI //Ta'lim fidoyilari. – 2022. – T. 14. – №. 1. – C. 19-27.

10. Kalandarov, Aminjon. "HOW A TYPICAL CROWDFUNDING ROUND WORKS." World Bulletin of Management and Law 18 (2023): 135-138.

11. Kalandarov, A. "LEGAL REGULATION OF VENTURE INVESTMENTS IN THE REPUBLIC OF UZBEKISTAN." Herald pedagogiki. Nauka i Praktyka 2.1 (2022).

12. Saidov, Ibrokhim. "THE PHENOMENON OF SEPARATION OF OWNERSHIP AND CONTROL IN CORPORATE LAW." The American Journal of Political Science Law and Criminology 5.01 (2023): 1-9.

13. Anvarovich, Saidov Ibrokhim. "Corporate social responsibility under the UK Corporate Governance system." Eurasian Research Bulletin 21 (2023): 120-125.

14. Saidov, Ibrokhim. "The notice and action procedures in the eu and its role in internet-related disputes." The American Journal of Political Science Law and Criminology 4.08 (2022): 40-47.

15. Saidov, Ibrokhim. "NATURE OF ELECTRONIC COMMUNICATION EFFECTIVENESS OF THE INCORPORATION OF TERMS AND THE VALIDITY OF ELECTRONIC SIGNATURES IN THE LIGHT OF UK AND EU LAW." The American Journal of Political Science Law and Criminology 4.08 (2022): 90-98.

16. Askarov J. DIGITAL MEDICINE AND LAW //International Journal Of Law And Criminology. – 2023. – T. 3. – №. 01. – C. 11-15.

17. Askarov J. T., Ishbulatov R. F. FOREIGN LEGISLATION IN THE FIELD OF E-COMMERCE //Herald pedagogiki. Nauka i Praktyka. – 2022. – T. 2. – №. 1.