The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 11 Pages: 48-51
SJIF IMPACT FACTOR (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523

Publisher: The USA Journals

Journal Website: https://theamericanjournals.com/index.php/tajpslc

Research Article

SUBJECTIVE SIGNS OF CYBER CRIME

Submission Date: November 20, 2023, Accepted Date: November 25, 2023,
Published Date: November 30, 2023 |
Crossref doi: https://doi.org/10.37547/tajpslc/Volume05Issue11-09

Durbek Rustamjon Ogli Dusmatov
Senior Assistant Prosecutor, Yashnabad District Prosecutor's Office, Uzbekistan

ABSTRACT

In this article, small and medium-sized enterprises (SMEs) are very easy victims of cybercrime, they primarily related the growth of cybercrime to SMEs, not large enterprises. Such enterprises, because of their small budget, lack of qualified personnel and gaps in the knowledge of employees, cannot provide high-quality information security to the required level, and they should approach subjectively this.

KEYWORDS

Cyber-attacks, cyber-crimes, small and medium enterprises (SMEs), social networks

INTRODUCTION

The seriousness of cyber-attacks, the fear of their increasing number, and the increasing number of unsolved crimes are based not only on the financial damage affecting the country's GDP and the world GDP but also on the damage caused to individual companies and structures. As individuals. Cybercrimes cause real economic damage to organizations and structures, which can take months and years to recover[1]. According to Cisco survey respondents, more than half (53%) of all attacks resulted in financial losses of more than $500,000, including but not limited to loss of revenue, customers, opportunities, and out-of-pocket expenses. Among respondents analyzed by Cisco, losses from attacks are shown [2].

The criminalization of cybercrime in the criminal legislation of foreign countries covers not only actions that directly violate information security (combined taking into account the identity of the common object of the attack), but also other socially dangerous attacks related to the use of information. and telecommunications networks (crimes in which the information sector is a voluntary object). Currently, the vector of "distribution" of such norms in the criminal laws of foreign countries is aimed at:

1. Introduction of liability for theft in the field of computer technology under special criminal law.
2. Designation of the sign of the use of information technology as a sign of the crime of theft.
3. Recognizing computer data as the subject of a criminal attack or criminalizing the use of computer technology as one of the methods, means, or qualifications for committing various types of crimes.
4. Matching types of cybercrimes.

Today, there are Articles 539, 541, the third part of Article 542, and Article 545 of the Criminal Procedural Code of the Republic of Uzbekistan (consisting of 17 chapters, including Article 96), which in some sense refers to cybercriminal activity. related to, according to:

Some types of IT crimes can be seen in:

- distribution of virus software;
- stealing users' confidential information;
- stealing other people's intellectual activity products;
- hacking other people's accounts on social networks;
- spreading false information, defamation;
- inciting inter-ethnic conflict or inter-religious enmity.
- illegal operations with bank plastic cards (card details);
- Internet fraud in the stock market;
- financial pyramids on the Internet;
- crimes related to mobile communication;
- other crimes in the field of electronic commerce.

Taking into account the above examples, some recommendations can be made for Internet users to prevent illegal offenses that may be committed against them:

- access to the Internet, use devices with special software designed to combat malicious activity, and update them on time;

- use an operating system with security updates installed, and current versions of other software;

- when using sites, pay attention to their appearance, and web address: maybe you have entered a fake copy of it;

- personal data that uses only secure protocols

enter websites (usually the browser will show a block icon on a green background next to the address of such a site);

- do not use the same logins and passwords on different sites;

- do not use very light or easily guessed passwords (date of birth, phone numbers, etc.).

One of the most serious limitations of national computer crime legislation is that it does not effectively combat the global phenomenon of cybercrime. The Committee of Ministers of the Council of Europe adopted the European Convention, designed to create an international framework for combating cybercrime, in November 2001 [3].

The Convention covers a wide range of issues, including crimes such as illegal access to computer systems and interception of data, tampering with data, interfering with system operation, illegal use of devices, forgery and computer fraud, and child pornography. Violations of copyright and related

The American Journal of Political Science Law and Criminology
(ISSN – 2693-0803)
VOLUME 05 ISSUE 11 Pages: 48-51
SJIF Impact Factor (2020: 5. 453) (2021: 5. 952) (2022: 6. 215) (2023: 7. 304)
OCLC – 1176274523
Publisher: The USA Journals

rights. Cybercrime can only be effectively countered by joining forces. Therefore, in 2018, the First International Congress on Cyber Security was held in Moscow on June 5-6. It was attended by 681 organizations from more than 50 countries, including Interpol, the World Economic Forum, SWIFT, ICANN, and representatives of more than 45 Russian and foreign government agencies and ministries. The latest threats in the digital world and the main directions of global cyber security development were discussed on the agenda.

Congress reached several important conclusions:

1 The losses to the global economy and Russia from cybercrime are unprecedented and continue to grow.

2 Cybersecurity is 2-5 years behind technological developments.

3 There is a critical shortage of skilled cyber security professionals.

4 Cybercriminals operate with impunity.

5 Effective international cooperation is necessary to successfully combat cybercrime [4].

Thus, the high social danger of cybercrime is explained by its transnational and organized nature, so today no country can actively counter this threat independently, and therefore the need to activate international cooperation is urgent. Effectively fighting cybercrime requires a collective effort. For this purpose, it is necessary to carry out constant explanatory work among the population. It takes a long and, most importantly, continuous education process to make people understand the need to take precautions. In order to effectively fight cybercrime, which has increased dramatically in recent years, it is necessary for government agencies and commercial companies to consider information security as one of the main components of their activities. Issues of responsibility, compliance with Russian legislation in the field of information security, and raising the level of citizens' security culture should be the top priorities.

CONCLUSION

In conclusion, it should be said that small and medium-sized enterprises (SMEs) are very easy victims of cybercrime, the growth of cybercrime is primarily related to SMEs, not large enterprises. Due to their small budget, lack of qualified personnel and gaps in the knowledge of employees, such enterprises cannot provide high-quality information security as needed. Also, internet banking is still one of the leaders in the list of cybercrimes; banking institutions, regardless of time and technological progress, are an attractive target for quick wealth acquisition; criminals make their fortunes through cyber blackmail, extortion and bank extortion. Hackers use weaknesses in the software of popular servers, primarily social networks, various government services and institutions. Social networks are particularly attractive to criminal activity due to their popularity among large numbers of people and the unwarranted trust they have in terms of security. Accessing such networks allows you to obtain a large amount of confidential information for your use, among which you can find information for further online fraud, blackmail and resale of information to interested parties.

REFERENCES

1. Морозов Н.А. Борьба с компьютерной преступностью в Японии // Общество и право. – 2014. – № 2 (48). – 141 с.
2. О преступлениях в сфере компьютерной информации: федер. Закон от13.06.1996 №63-ФЗ (ред. От 23.04.2019) – URL:

http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/#dst101786: 18 ICC: About the Congress. – URL: https://icc.moscow/about/ (дата обращения 21.05.2019)

3. Kaspersky: Киберпреступность и закон. – URL: https://securelist.ru/kiberprestupnost-i-zakon-obzor-polo/1315/#7 (дата обращения 21.05.2019)
4. Official Annual Cybercrime Report 2019 report from Cybersecurity Ventures sponsored by Herjavec Group. – URL: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (дата обращения: 9.05.2019).