International Journal of
Business Diplomacy and Economy

ISSN: 2833-7468
Volume 2 | No 7 | Jul -2023

Cybersecurity Issues in Uzbekistan

[1] Abdullaeva D. K., [2] Narzullaeva D.K

[1] Associate Professor, Candidate of Economic Sciences, Tashkent State University of Economics
[2] senior teachers, Tashkent branch of the Russian Economic University named after G.V. Plekhanov

Abstract: Cybersecurity has become increasingly important recently as governments, corporations, and people collect, process, and store vast amounts of confidential information and transmit that data across networks. Cybersecurity focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access. This is especially urgent when working remotely. The article considers that in recent times, cases of cyber hacks have increased the demand for cybersecurity products.

Key words: digitalization, cyber security, cyber hacks, information technology.

In Uzbekistan, there was no specific law on cyber security until 15 April 2022. General issues of cybersecurity, such as security in telecoms and the internet, were mentioned in several laws already in force. At the time of publication, Law of the Republic of Uzbekistan of 15 April 2022 No. RK-764 on Cybersecurity has not yet consolidated the provisions on cybersecurity of several sector-specific laws.

The Law on Cybersecurity mostly regulates the State Security Service of the Republic of Uzbekistan's ('DXX') powers without further developing particular mechanisms of exercising such powers and duties. It directly states that either such mechanisms are regulated 'in accordance with legislation', or 'developed by the Regulatory authority'. It should be also noted that the Law on Cybersecurity introduced substantial notions and consolidated the bare minimum of cybersecurity legislation which was scattered among several sector-specific laws, as well as presidential and government by-laws. [1]

In Uzbekistan, the state is successfully coping with its role of creating the necessary conditions for the development of the digital economy, as evidenced by the results achieved and the ambitious goals set for the near future.

The year 2022 was a successful one for the economy of Uzbekistan and turned out to be decisive in achieving one of the main goals of the ongoing reforms - strengthening macroeconomic stability and maintaining high economic growth rates.

The main role in the digital economy should be played by private business with a strong entrepreneurial and innovative approach and the state should create conditions for private initiative.

The presidential decree of “Digital Uzbekistan-2030” Strategy was approved, which provides for the implementation of over 280 projects for digital transformation of regions and sectors in the next two years. [2]

To double the share of digital services in Uzbekistan’s GDP was highlighted as an emergency task in coming two years.

It is planned to attract about $2.5 billion investment for the development of digital infrastructure in the next two years. [4]

As a result, households of Uzbekistan will have access to the Internet with a speed of at least 10 Mbit/s in each settlement. Because the main thing while developing information communication technologies (ICT) in the country, affordable high-speed Internet should keep pace with the interest of businesses to introduce digital technologies into various production processes to increase labor productivity.

Cybersecurity focuses on protecting computers, networks, programs, and data from unauthorized and/or unintended access.

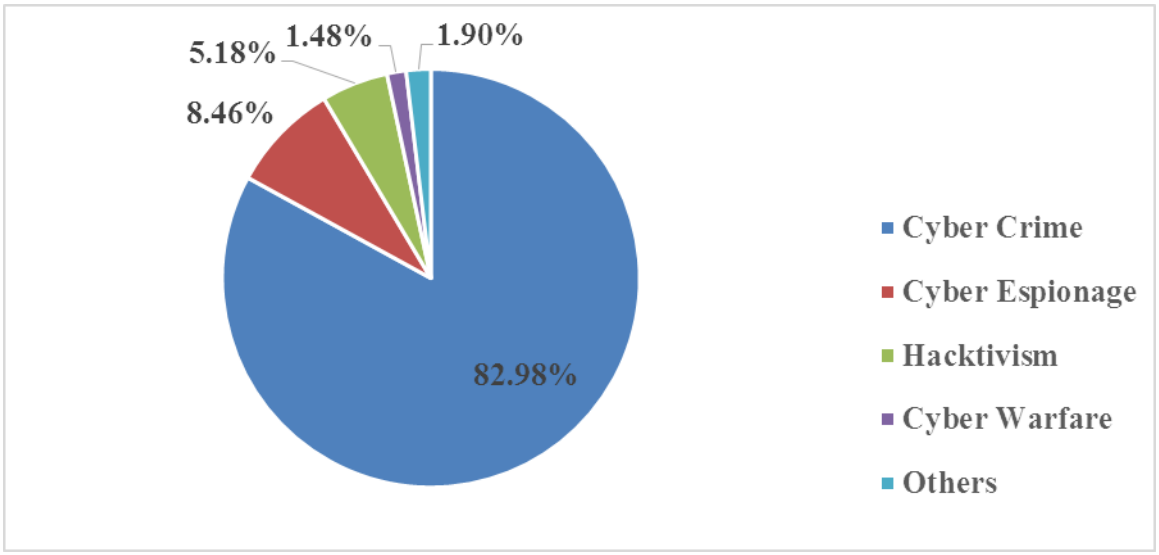
In general, subjects of cybersecurity have the statutory duty to notify the DXX about the cybersecurity incidents and cybercrimes that have occurred, and corresponding duties:

- to take measures to prevent the loss of relevant digital traces to fully disclose these incidents;
- to ensure the permanent storage of information necessary for analyzing cybersecurity incidents and investigating cybercrime (Paragraph 4 Part 2 Article 16 of the Law on Cybersecurity); and
- to notify the DXX on the results of investigation of the owner of an information resource or system in which a cybersecurity incident occurred (Part 2 of Article 22 of the Law on Cybersecurity).

Cybersecurity has become increasingly important recently as governments, corporations, and people collect, process, and store vast amounts of confidential information and transmit that data across networks.

Data breaches have become almost commonplace in recent years.

Authors have aggregated the statistics created from the cyber-attacks timelines published in the first three months of 2023. In total authors have collected 946 events (10.51 events per day), a noticeable decrease (nearly **30%**) from the 646 events that we collected in first quarter 2022.



Fig, 1. Distribution of cyber-attacks motivations Q1 2023 [3]

Cyber-crime continues to lead the Motivations chart with 82.9%, definitely an important increase from 70.3% of Q1 2022 and back to values closer to Q1 2021 (86%). Similarly, malware continues to lead the Attack Techniques chart with 38.7% up from 31.3% of 2022 and 32.3% of two years ago. The Target Distribution chart confirms Multiple industries at the first place with 22.9& down from 25.9% of 2022 and up from 16,7% of two years ago.

In the event and detection of a breach of the information security regime, payment system operators and payment service providers are obliged to promptly inform the Central Bank of the Republic of Uzbekistan ('CBU') of this and the measures taken to minimize its consequences. The CBU

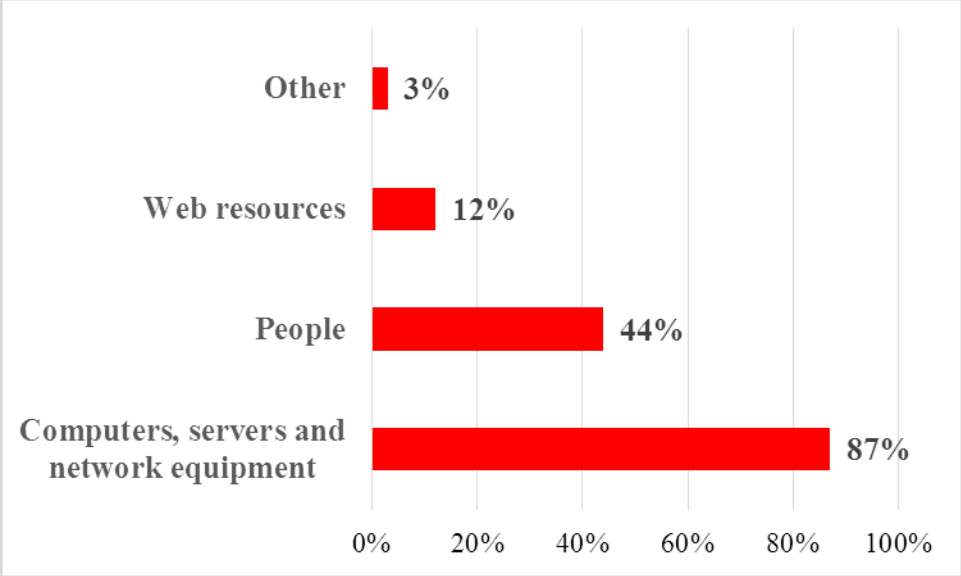
maintains a database of violations of the information security regime of payment systems (Article 57 of the Law on Payment Systems).

If irregular use of information exchange tools is detected, such as erroneous commands, as well as commands caused by unauthorized actions of service personnel or other persons, or false information is discovered, the owner of these tools must inform the control authorities for the implementation of the information exchange (Item 11.3 of the Decree of the Cabinet of Ministers No. 137).

It should be noted that of the successful attacks, 87% were directed at computers, servers and network equipment - the main targets of ransomware.

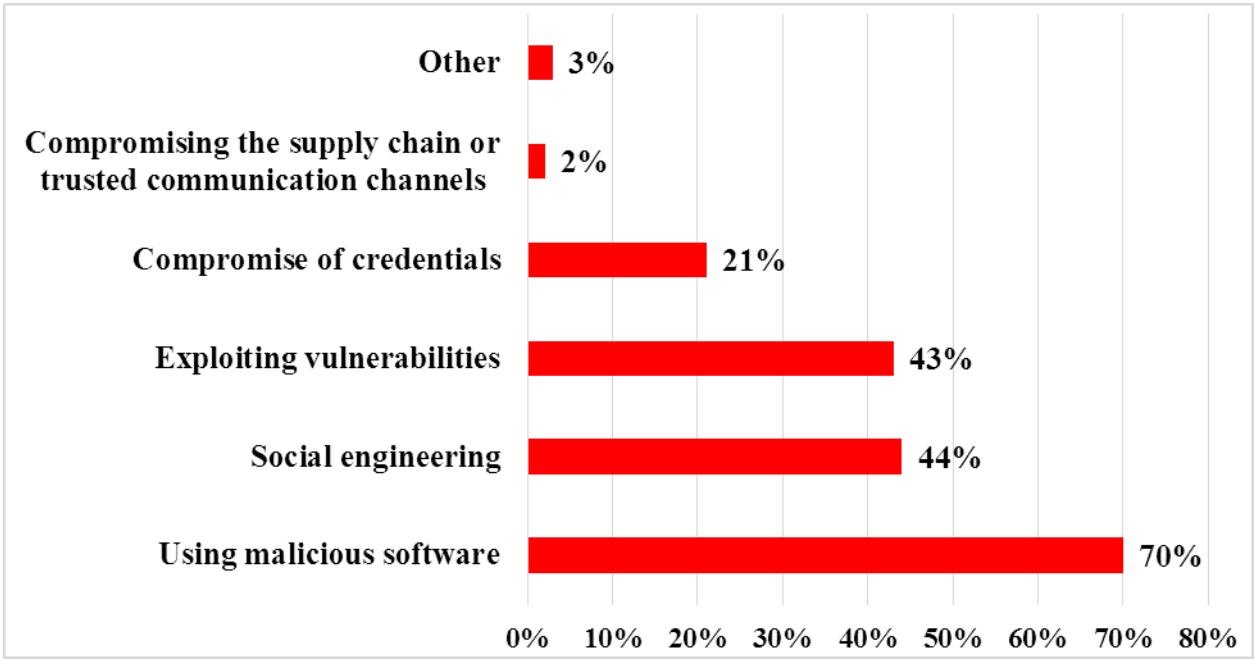
In 44% of cases, attackers carried out attacks on the personnel of industrial organizations using malicious email newsletters (94%) and phishing sites (10%).

Directed to the web resources (sites) of industrial organizations sectors were 12% of attacks.(fig.2)



Fig, 2. Objects of attacks on organizations (share of attacks) 2022 [3]

Wherein In most successful attacks (70%) on industrial organizations, attackers used malware. Almost half of the cyberattacks (44%) on industry were used methods of social engineering. The share of attacks in which software vulnerabilities were exploited was 43%. (fig.3).



Fig, 3. Methods of attacks on enterprises (share of attacks) 2022 [3]

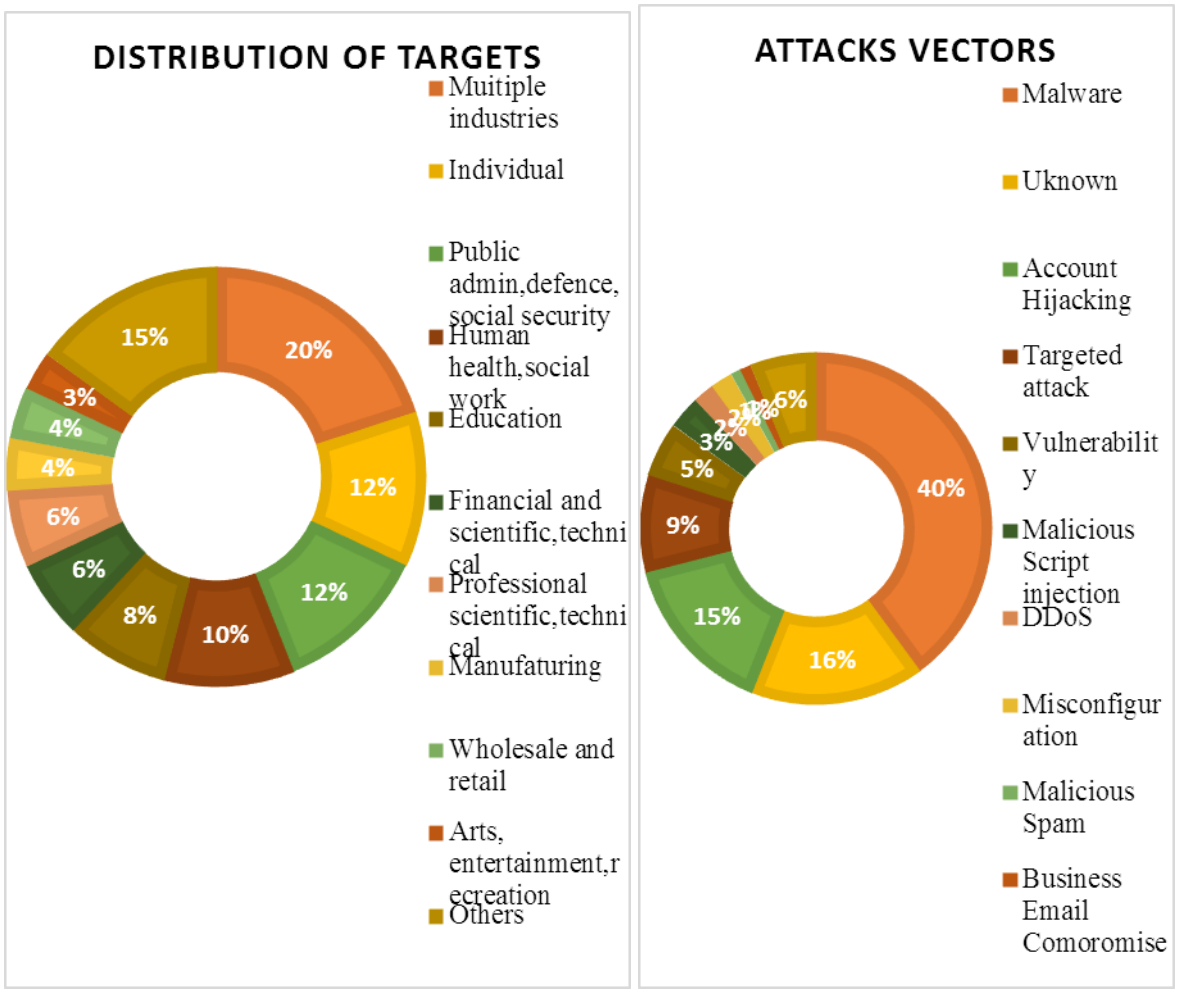
Over the last few years, high-profile cases of cyber hacks have increased the demand for sophisticated software and security products. Companies across the globe are growing more aware of the potential threat which is leading to a greater allocation of resources towards companies that help mitigate such risks.

Many organizations, including the International Telecommunication Union, have grappled with new challenges stemming from remote work.

Cybersecurity is fundamentally intertwined with remote work, from managing video call participants, to making sure that documents are shared safely. International Telecommunication Union has therefore continued to work together with countries to be more efficient, more active, and deliver impact in the areas where we are needed the most

The Global Cybersecurity Index (GCI) is a joint project, undertaken by ABI Research and the International Telecommunication Union, which assesses the level of participation of independent states in the field of cybersecurity.

Based on the International Telecommunication Union Global Cybersecurity Agenda, the GIC assesses the level of commitments in five areas: legal measures, technical measures, organizational measures, capacity development and international cooperation. The performance is then aggregated into an overall score.



Fig, 4.- Targets and types of cyberattacks [3]

Since 2016, Uzbekistan has improved Global Cybersecurity Index in this rating from 0.1471 to 0.666 and rose from 93rd to 52nd place among 175 countries.

The two charts below break down the attacks to highlight toward whom the attacks were targeted as well as the ways in which the attacks occurred (fig 4.).

The fig.4 illustrate that multiple industries, governments, and individuals were the most affected by cyberattacks in 2022 and that most of those attacks were done via malware or account hijacking. In most instances, corporations are hesitant to reveal breaches and cyberattacks that they've been exposed to, primarily for fear of reputational damage. As such, Cybersecurity Ventures is predicting slightly higher growth rates, at about 12-15% year-over- year through 2025, which is higher than the 8-10% being predicted by other industry analysts.

As a result, the actual spending on cybersecurity may be far more than what's revealed publicly, as companies may be understating their cybersecurity budgets to protect their reputation.

Individuals and organizations across the globe are dedicating unprecedented resources to protecting their data with worldwide spending expected to reach $151 billion by 2023. That rapid growth has led to a rise of companies providing cybersecurity services.

In Uzbekistan in 2022, more than 27,000,000 events of malicious network activity were detected in the context of leading telecommunications network operators and cybersecurity events in the context of communication operators (fig 5.).

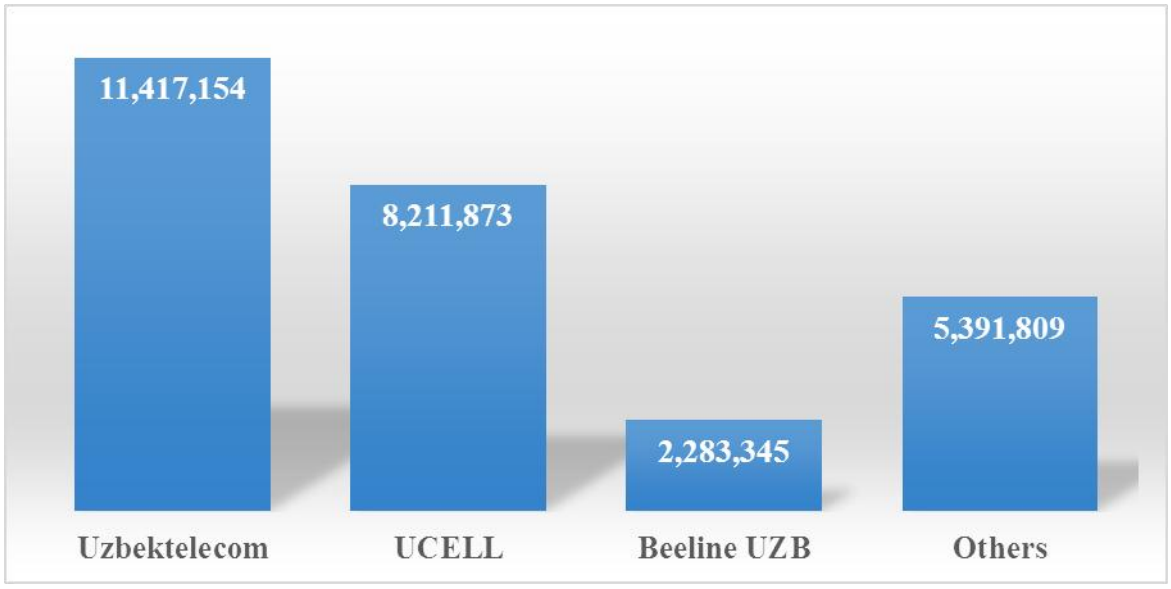


Fig. 5. - Cybersecurity events in the context of communication operators of Uzbekistan in 2021[5]

Cybersecurity Index gives investors a simple way to incorporate this theme into their portfolios through companies protecting data from data breaches and cyberattacks.

Cyber-attacks on all businesses, but particularly small to medium sized businesses, are becoming more frequent, targeted, and complex. According to Accenture's Cost of Cybercrime Study, 43% of cyber-attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

The most common types of attacks on small businesses include:

- Phishing/Social Engineering: 57%
- Compromised/Stolen Devices: 33%
- Credential Theft: 30%

Not only does a cyber-attack disrupt normal operations, but it may cause damage to important IT assets and infrastructure that can be impossible to recover from without the budget or resources to do so.

The global cyber security market was worth 173.5 billion dollars in 2022.

It is expected to grow at a compound annual growth rate of 8.9% to reach 266.2 billion dollars by 2027.

The cybersecurity market growth includes increased number of data breaches across the globe, rising digitalization and increased sophisticated cyber intrusions. However, difficulties in addressing complexity of advanced threats and implementation challenges during the deployment of cybersecurity solutions are expected to hinder the market growth.

Nevertheless, some issues about cybersecurity for the future can be drawn:

- Lagging corporate governance: although there has been significant improvement in the priority organizations place on cybersecurity in recent years, many firms still have not placed cybersecurity specialists and keep cybersecurity separate from organizational objectives.
- Lack of investment, preparedness, and resilience: both public and private sectors are still insufficiently prepared for a cybersecurity disaster due to incomplete and imperfect data, lack of crisis preparedness, disaster recovery, and business continuity planning, failure to conduct crisis exercises and planning, vendor risk concentration and insufficient third-party assurance capabilities, the escalating cost of cyber insurance, and chronic poor cyber hygiene and security awareness among the general public.
- Vulnerable infrastructure: critical infrastructure remains vulnerable as organizations "rely heavily on state and local agencies and third- and fourth-party vendors who may lack necessary cybersecurity controls," particularly in the finance, utilities, and government services sectors, which often run on unpatched and outdated code and legacy systems.

To sum up, we can conclude that the industry outlook for cybersecurity is generally positive. Due to the increasing number of cyberattacks the expectations for cybersecurity spending going forward remain very high.

Some of the key growth areas within cybersecurity, such as cloud-based security, will help sustain overall growth, even if other areas decelerate. The rising costs of cyber-attacks and corporations' willingness to invest time and money into various cybersecurity initiatives - further justify the elevated growth expectations for the industry, as well as the likelihood of it remaining a profitable investment for the foreseeable future.

References

1. Law of the Republic of Uzbekistan «Cybersecurity Law»: 03/22/764/0313-04/16/2022 RK-764
2. Resolution of the President of the Republic of Uzbekistan "“Digital Uzbekistan-2030” Strategy " (No. PP-4996, 05.10.2020).
3. https://www.hackmageddon.com/2023/04/21/q1-2023-cyber-attacks-statistics/
4. Development of the digital economy in Uzbekistan 06.05.2022
5. https://www.hackmageddon.com/2022/01/13/2020- cyber-attacks-statistics/
6. https://www.csec.uz
7. Cybersecurity Ventures. □
8. State Committee on Statistics of the Republic of Uzbekistan