Cyber Threats and Prevention Methods in the Digital Economy

Anafiyaev Abdurashid Mamasidikovich
Senior Lecturer, justused02@gmail.com
Andijan Machine-Building Institute,
Uzbekistan, Andijan city

Shokirova Sarvinoz Oybekovna
3rd year student
justused02@gmail.com
Andijan Machine-Building Institute,
Uzbekistan, Andijan city

ABSTRACT

As the country's infrastructure quickly develops with a digital overlay over the next few decades, billions of sensors will be attached to highways, buildings, power plants, companies, and even residences. Increased digitalisation helps the government and commercial enterprises use data to manage this crucial infrastructure, but it also leaves them vulnerable to cybersecurity threats. This paper investigates cyber dangers in the digital economy and preventative methods.

Keywords: Digitalization, cybersecurity, digital economy, ICT.

Data security has become a requirement for digital economic supremacy, and governments throughout the world are increasing legal steps to better secure and manage data assets. The regulator (government) is working on a policy to encourage the growth of the data security business, which will support the orderly openness and in-depth use of data. While cyberthreats are now limited to information technology, this will change as 5G [5] rollouts enable Industry 4.0 - the ongoing fourth industrial revolution centered on automation, smart technology, interconnection, and machine learning - and the internet of things (IoT) in shop floors. Individuals are also at risk as the country's digital use grows. Cyber danger has increased tremendously for traditionally low-risk sectors such as small firms and individuals. This truly opens the Pandora's box. Everyone, from youngsters to the elderly, small street sellers to those in rural areas, uses digital means.

There are several risks to information systems, the most significant of which being the leaking of citizens' personal data. Among the threats are phishing—the sending of fraudulent emails and notifications; social engineering—psychological measures to gain access to confidential information; and various types of malicious software aimed at blocking system operation or stealing confidential data—account logins and passwords, as well as information on bank accounts and cards. Recently, there has been an increase in the activity of boot viruses: infected files disguised as legitimate software, cryptominer applications—programs that use the resources of an infected computer to mine cryptocurrencies—and so-called exploiters—programs that use system vulnerabilities to carry out attacks and gain access to them.

As individuals increasingly create, acquire, share, and consume data, public and private companies are acquiring huge and rising amounts of information assets. Businesses and individuals are increasingly reliant on information and technology assets to supply or buy goods, services, and information. At an increasing pace, businesses and individuals are entrusting their information to other businesses and individuals. Individuals in both high-income and underdeveloped nations are adopting digital technology. Between 2005 and 2020, the percentage of developing-country households having a home computer increased from 15.6% in 2005 to 36.1% in 2019, while the number of mobile phone subscriptions per 100 people increased thrice globally and fourfold in low- and middle-income countries. Furthermore, the number of registered mobile money accounts increased by 12.7% globally in 2020 to 1.21 billion accounts, more than double the projected growth rate [1].

Technological advancements aid in the integration of the Internet with conventional industries by allowing the network to connect a huge number of manufacturing equipment and control systems. The presence of two interrelated major networks: information and production (trade, transport) determines the complexity of digitized production (trade, transport) settings [2]. The ensuing interconnection in digital environments increases the attack surface and provides additional options for dissemination.

A cyberattack has the potential to propagate throughout the whole information network, causing considerable harm to both the information and production networks [3]. As a result of their interconnection, the harm produced by a cyberattack not only lowers the capability of the targeted network node but may also extend across both information and production networks. Furthermore, industrial control systems (ICS) have historically been used in isolated contexts. As information and communication technology and functional needs evolve, an increasing number of ICSs are being migrated to the public network to offer remote control and supervision of infrastructures [4]. This element raises the possibility of external harmful intrusion into corporate internal management systems.

The link between digital security and privacy risk has long been recognized, as evidenced by digital identity management and cryptography policy. However, greater and more exploited synergies between security and privacy policy approaches might be developed, and cooperation among key players could be strengthened. In contrast to digital security risk, which is addressed through national initiatives, law remains the primary reaction to digital privacy risk in many nations. While legal protection is necessary, privacy in an increasingly data-driven economy would benefit from a multidimensional strategy along the lines of digital security methods. This might increase protection while still providing the flexibility required to capitalize on upcoming technology. Such solutions would also aid efforts by privacy enforcement agencies and others to promote privacy risk management. Interoperable privacy techniques and frameworks can improve personal data protection across jurisdictions and eliminate ambiguity in cross-border data transfers.

The World Economic Forum's Global Cybersecurity Outlook 2022 research [6], co-created with Accenture, discovered that:

- only 19% of cyber executives are confidence in their company's cyber resilience.
- 58% believe their partners and suppliers are less resilient than their own company.
- 88% of respondents are concerned about the cyber resilience of their ecosystem's small and medium-sized firms (SMEs).

This does not have to be the case. If companies can transcend such self-limiting stigmas, they will benefit from their partners' joint understanding and united capabilities. As so many recent events have revealed, this is an essential response to the cascading repercussions that occur when delicate, interdependent ecosystems fail.

To overcome this long-standing distrust, companies must leverage a different type of critical vulnerability than what cyber specialists are used to—the vulnerability of an organization to be fully seen. They must embrace the willingness to be upfront about gaps in their cyber resilience posture inside their business and ecosystem. They should establish realistic exposure expectations and offer clear information about the systemic repercussions of disruptions. They should be open about their encounters with disruptive occurrences and share the lessons they learnt as a consequence.

When security preventative methods fail, cyber resilience takes over. The capacity to withstand cyber disruption separates market leaders in the digital economy. Organizations that transform their vulnerability into strength will be more willing to take healthy risks.

It is not easy to transform institutional weakness into organizational strength. Fortunately, the World Economic Forum's recently launched Cyber Resilience Index Framework [7] - created in conjunction with Accenture - outlines the six principles for cultivating a resilient culture:

- On a regular basis, assess and prioritize cyber risk.
- Establish and uphold basic security standards.
- Integrate cybersecurity governance into company strategy.
- To promote systemic resilience and ecosystem-wide cooperation
- Ascertain that the design promotes cyber resilience.
- Develop a resilient culture.

Two aspects in particular have long been undervalued: developing a culture of cyber resilience and supporting systemic resilience and collaboration. Both of these ideas offer companies a starting point for transforming vulnerability into cyber resilience. The concepts are implemented as follows:

- *Develop a resilient culture.*
- *Promote systemic resilience and ecosystem-wide cooperation.*

Develop a resilient culture.

Employees are given the tools they need to comprehend and embody cyber-resilient behaviors. This idea is implemented as follows:

- *Earn trust by being accountable and transparent:* Management communicates the cyber resilience strategy, processes, operations, achievements, and failures on a frequent, clear, and transparent basis. This foster and sustains knowledge, trust, transparency, and ownership of organizational performance.
- *Leadership that is cyber resilient:* Leadership possesses the knowledge and authority to manage the organization's cyber resilience in accordance with best practices, and it is encouraged to enhance its skills in response to changes in the landscape.
- *Culture is shaped through leadership:* Leadership establishes the tone and implements organizational processes to foster a culture of capacity and accountability for cyber resilience at all levels of the company.
- *Encourage positive employee behavior:* Employees are aware of the established cyber resilience objectives, feel accountable for the organization's cyber resilience, and are empowered to engage in cyber resilient behavior in their everyday contacts without fear of repercussions.
- *Provide ongoing training:* Employees are trained about cyber resilience ideas and best practices, as well as the necessity of cyber resilience in everyday tasks. They put these lessons to the test on a regular basis, as the cyber resilience landscape changes. Furthermore, they receive immediate feedback on their efforts.

Promote systemic resilience and ecosystem-wide cooperation.

The organization recognizes the interdependence of its ecosystem, collaborates with other organizations, and does its part in ensuring the overall ecosystem's resilience. This idea is implemented as follows:

- *Trust is built via information, accountability, and openness:* The organization maintains transparency with its ecosystem partners in its procedures, operations, achievements, and failures, and shares best practices to develop a more resilient collective.
- *Collaboration across the ecosystem:* Knowledge management fosters a collaborative culture and establishes

strategic goals for knowledge and information exchange. It also discovers, comprehends, and mitigates cyber hazards in the ecosystem. In addition, the group regularly engages with colleagues in the industry and government.

- *Cyber resilience capabilities throughout the ecosystem:* The organization is constantly improving collective cyber-resilience skills in collaboration with other ecosystem participants in order to exchange information, promote awareness, and elevate general standards of conduct. This improves the collective capacity of all ecosystem participants while balancing innovation, readiness, protection, reaction, and recovery.

References

1. The role of cybersecurity and data security in the digital economy. UNCDF Policy Accelerator. URL: https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/62082f066a25c62651a9ae40/1644703527175/EN-UNCDF-Brief-CyberSecurity-2022.pdf
2. Estimating the impact of IT security incidents in digitized production environments / O. Burger [et al.] // Decision Support Systems. 2019. No. 127 (10). P. 11. DOI: 10.1016/j.dss.2019.113144.
3. Kumar N., Mallick P. Blockchain technology for security issues and challenges in IoT // International Conference on Computational Intelligence and Data Science (ICCIDS 2018). Procedia Computer Science. 2018. No. 132. P. 1815-1823. DOI: 10.1016/j.procs.2018.05.140.
4. Asghar M., Hu Q., Zeadally S. Cybersecurity in industrial control systems: Issues, technologies, and challenges // Computer Networks. 2019. No. 165. P. 16. DOI: 10.1016/j.comnet.2019.106946.
5. The Economic Times. URL: https://economictimes.indiatimes.com/topic/5g
6. Global Cybersecurity Outlook 2022. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2022
7. The Cyber Resilience Index: Advancing Organizational Cyber Resilience WHITE PAPER JULY 2022. In collaboration with Accenture. URL: https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf