CYBERSECURITY AS A KEY FACTOR IN DEVELOPING A RESILIENT AND TRUSTWORTHY DIGITAL ECONOMY

Rasulova Sharifa Gaybullaevna
Associate professor of Jizzakh Polytechnic Institute
Islomov Elnurbek Najimiddin ugli
Student of Jizzakh Polytechnic Institute
https://doi.org/10.5281/zenodo.16891869

Annotation: This article explores the critical role of cybersecurity in fostering a resilient and trustworthy digital economy. It analyzes the main cyber threats that can undermine economic stability, including data breaches, ransomware attacks, and the misuse of personal and corporate information. The study highlights strategic measures for enhancing digital trust, such as implementing robust data protection policies, adopting advanced authentication systems, and fostering public-private cooperation in cybersecurity. Special attention is paid to the integration of cybersecurity practices into national digital transformation strategies. The findings can serve as a basis for creating sustainable and secure digital infrastructures that support economic growth and innovation.

Keywords: cybersecurity, digital economy, digital trust, data protection, cyber threats, resilience, innovation, secure infrastructure, national strategy, digital transformation.

Аннотатsiя: В данной статье рассматривается ключевая роль кибербезопасности в формировании устойчивой и надежной цифровой экономики. Анализируются основные киберугрозы, способные подорвать экономическую стабильность, включая утечки данных, атаки программ-вымогателей и неправомерное использование личной и корпоративной информатsии. В исследовании выделяются стратегические меры по укреплению цифрового доверия, такие как внедрение надежных политик защиты данных, использование современных систем аутентификатsии и развитие государственно-частного партнерства в сфере кибербезопасности. Особое внимание уделяется интегратsии практик киберзащиты в натsиональные стратегии цифровой трансформатsии. Полученные результаты могут служить основой для создания устойчивой и безопасной цифровой инфраструктуры, поддерживающей экономический рост и инноватsии.

Ключевые слова: кибербезопасность, цифровая экономика, цифровое доверие, защита данных, киберугрозы, устойчивость, инноватsии,

безопасная инфраструктура, natsіональная стратегия, цифровая трансформатsія.

Digital economy is strengthening in prominence and relevance in the era of increasingly connected world in the cyberspace. The boom in digital economy, however, is coupled with cyber threats and cyber risks for nations in the form of malware, escalating organized cybercrime, personal information and data breach, and Advanced Persistent Threat (APT). As such, nations need to prepare for the cyber threats from new frontiers namely Internet of Things (IOT), mobile and cloud technologies.

As the relevance of digital economy increases, the need for secured cyberspace increases. Cyber threats aspect is inescapable in digital progress. In the growth of cyber dominance, cybersecurity is a need. For nations to leverage and prosper in digital economy, national level strategy is developed to provide the necessary foundation and infrastructure to secure the cyberspace. Cybersecurity is a crucial element in national security. Nations need to balance the needs of digital economies and to ensure the reliability and security of the cyberspace. Protection against cyber threats had become top priority for nations across the globe. In 2015, UK government had affirmed cyber threats as Tier One risk in their 2015 National Security Strategy (NSS). The Department of Defense in US had developed its first cyber strategy in 2011, and released the updated Department of Defense Cyber Strategy in 2015. For national cybersecurity, it is vital to focus on critical infrastructure protection, combating cybercrime effectively and national defense capabilities.

When a person creates an online account, makes a purchase from a website or downloads an app, it's not just the exchange of data, goods or services taking place. It's a transaction in the ultimate currency: trust. Today, there is a real risk that trust in the digital economy is eroding.

The idea of regulating cyberspace by international law is not something remarkably novel. Since 1996, the efforts of formulating international law on cyberspace have already been continuously proposed (and refuted) by law experts, business actors, and states. There are three dominant ideas on how cyberspace should be regulated by international law: Liberal Institutionalists, Cyber libertarian, and Statists. Liberal institutionalists like Wu (1997) call for the importance of the international institution and rule-based multilateralism in managing cyberspace. While cyber libertarians like John Barlow (1996) are proponents of the idea that cyberspace should remain free from *tyranny* and *any oppressive rule that might hinder the internet liberty*. Statists, like James Lewis

(2010), believe that it is states' responsibility to formulate national and international law to govern cyberspace. These three mainstream ideas echo into the development of international law on cyberspace. Binding and well-functioning international law on cyberspace is still absent due to these ongoing contentious debates. These debates rest on to three major challenges on formulating international law on cyberspace are related to the core of principles and characteristics of international public law: jurisdiction, arbitration, and legal Instruments & jurisprudences.

The current regulatory environment for data protection is highly fragmented:

✓ Outdated or incompatible legal frameworks;

✓ New pieces of legislation introduced may be incompatible;

✓ Enforcement of privacy and security obligations is often inadequate;

✓ Many developing countries still lack data protection and privacy legislation altogether;

✓ The lack of clarity creates uncertainty for consumers and businesses, and limits the scope for cross-border exchange and growth.

But today, the Internet is facing many challenges. Malicious cybercriminals threaten the security of the digital economy, which becomes more fragile with each attack. The Internet, which was once a tool for information sharing and communication, has grown increasingly complex, and new, digital innovations are outpacing the ability to keep it secure. Trust in our digital economy now hangs in the balance, putting significant value at risk.

For CEOs, the task is clear: Build a trustworthy digital economy that safeguards our future prosperity.

CEOs must demonstrate decisive and, at times, unconventional leadership if they're going to restore security to the digital economy. For guidance, they should look to the oil and gas industry. In doing so, they might soon begin to see how reinventing the Internet for trust will require both *above-ground* and *below-ground* solutions.

Executives in the oil and gas industry often focus on figuring out how to best get production out of the ground an issue that comes down to engineering below ground. However, they also have to keep an eye on issues that occur above ground, ranging from strategy to politics to macroeconomics. CEOs need to demonstrate the ability to handle the technical expertise of digging down to solve a problem while also addressing concerns around pricing, supply and demand and other factors that fall into the category of business and operating

models. When it comes to securing the digital economy, the oil and gas industry acts as a powerful analogy for CEOs. Updating the Internet's *below-ground* infrastructure to keep pace with today's innovations is obviously important, but many of the issues and opportunities for CEOs are occurring above ground. Security-first solutions, execution of cybersecurity strategies, digitally fueled operating models all of these are issues that corporate leaders can own.

Here are 3 obvious and effective steps that CEOs are supposed to consider:

Above the ground steps:

1. Take the lead on the issue of Internet governance and stewardship:

When leaders realize that prioritizing a trustworthy digital economy is a win-win situation, businesses, consumers and governments all benefit. Chief executives should band together to create a code of ethical conduct for each industry and principle-based standards for Internet security.

2. Embed security into your business architecture:

When security is a foundational requirement through the company's value chain from suppliers to customers your business partner won't become your greatest vulnerability. With this approach, security is not an "add-on" feature for products and services. That's why CEOs should articulate a vision of "security-by-design" from the earliest stages of development.

Below the ground:

3. Address the vulnerabilities of Internet technology:

To some, the technical deficiencies of Internet infrastructure are the "elephant in the room." But with the guidance that our research provides, business leaders can exert their influence to address these issues. Then the tech community can truly commit to strengthening not just security on devices, but also for networks and the Internet's basic protocols.

The benefits of a secure, trustworthy Internet economy are clear.

CEOs have an opportunity to drive meaningful change today and develop a foundation of trust for tomorrow's digital economy. Unfortunately, just one attack is all it takes to damage an organization.

The actions of CEOs driving above ground and influencing below ground matter. By joining forces with other CEOs, public sector leaders and regulators, they can develop much-needed guidelines and oversight mechanisms. By protecting their own organization and extending protection through its value chain, they will safeguard the business ecosystem. By embracing and developing technologies that can advance their businesses and enhance digital safety, CEO

engagement can drive a trust turnaround for the Internet and secure the future of the digital economy.

References:

1. Gaybullayevna, R. S. ., & Musurmangulov. (2024). THE IMPORTANCE OF TIME MANAGEMENT IN ENSURING EFFICIENCY IN CONSTRUCTION. JOURNAL OF ECONOMY, TOURISM AND SERVICE, 3(1), 28-31.
2. Gaybullayevna, R. S. (2023). THE STATE OF THE DIGITAL ECONOMY TODAY: PROBLEMS AND SOLUTIONS. JOURNAL OF ECONOMY, TOURISM AND SERVICE, 2(12), 38-42.