

DOI: 10.18372/2225-5036.30.18604

CYBERSECURITY CHALLENGES AND SOLUTIONS FOR CRITICAL INFRASTRUCTURE PROTECTION

**Andrii Tkachov¹, Roman Korolov², Irada Rahimova³,
Iryna Aksonova⁴, Yelyzaveta Sevriukova⁵**

^{1, 2, 4} National Technical University "Kharkiv Polytechnic Institute", Ukraine

³ "Computer Technologies", Baku, Azerbaijan

^{1, 5} Kharkiv National University of Economics, Ukraine



TKACHOV Andrii, candidate of economic sciences, associate professor

Date and place of birth: 1974.

Education: Candidate of Technical Sciences, Senior Researcher.

Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Scientific interests: software development.

Publications: more than 70 scientific publications, including monographs, textbooks, articles and patents.

E-mail: andrii.tkachov@kxpi.edu.ua.

Orcid ID: 0000-0003-1428-0173.



KOROLOV Roman, Candidate of Technical Sciences, Associate Professor

Date and place of birth: 1974, Krasnyi Luch, Luhanska oblast.

Education: Kharkov Military University, 1999.

Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Scientific interests: information protection in socio-cyberphysical systems.

Publications: more than 80 scientific publications, including monographs, textbooks, articles and patents.

E-mail: korolevrv01@ukr.net.

Orcid ID: 0000-0002-7948-5914.



RAHIMOVA Irada, PhD in Technology, Assistant Professor

Date and place of birth: 1961, Baku, Azerbaijan.

Education: AzPI, 1978.

Position: Assistant Professor at the Department of "Computer Technologies", Baku, Azerbaijan.

Scientific interest: cybersecurity, artificial intelligence.

Publications: more than 90 scientific publications, 4 tutorials.

E-mail: irr1402@gmail.com.

Orcid ID: 0000-0003-3278-3225.



AKSONOVA Iryna, candidate of economic sciences, associate professor

Date and place of birth: 1973, R. Lozovaya, Dergachevsky district, Kharkov region.

Education: Kharkiv National University of Economics, 1995.

Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Scientific interests: quantitative methods for assessing and analyzing information.

Publications: more than 120 scientific publications, including monographs, textbooks, articles and copyrights.

E-mail: ivaksonova@gmail.com.

Orcid ID: 0000-0003-2605-0455.



SEVRIUKOVA Yelyzaveta, graduate student

Date and place of birth: 1997, Zmiyiv, Kharkiv region.

Education: Simon Kuznets Kharkiv National University of Economics, 2020.

Position: graduate student Department of Enterprise Economics and Business Organization, Simon Kuznets Kharkiv National University of Economics, Ukraine.

Scientific interests: economy and management of human resources, human capital.

Publications: more than 5 scientific publications, including articles.

E-mail: elizavetasevryukova@ukr.net.

Orcid ID: 0000-0002-0757-490X.

Abstract. Critical infrastructure can be vulnerable to attack from natural disasters or malicious actors such as hackers or terrorists. If these threats are not addressed quickly, they can lead to significant disruption in service delivery or even complete shutdowns which could have devastating consequences for those relying on them for their day-to-day activities. Therefore, it is important that governments take steps towards protecting critical infrastructure from potential threats by implementing comprehensive security measures both online and offline. Based on a comprehensive analysis of current issues, a decision has been made to ensure the cyber protection of critical infrastructure objects in infrastructure. An analysis of cyber threats was carried out in relation to the dynamics of historical retrospective in sectors of critical infrastructure objects. As more and more systems become connected to the internet and vulnerable to cyber-attacks, it is important for organizations to invest in robust cybersecurity defenses to protect their systems from malicious actors. By taking these measures, organizations can help protect their systems from cyber-attacks and ensure the safety of the public. Formulates a model of threats from spills of critical infrastructure objects to cyber-attacks with a breakdown of threats by type. A triad of main actions and approaches for protecting critical infrastructure has been seen. Existing problems in implementing countermeasures and major threats posed to cyberspace actors have been identified. Key factors have been identified to break the cycle of cyber-attacks on critical infrastructure. Based on a comprehensive analysis and formulated concepts, a comprehensive approach to the protection of critical infrastructure objects is proposed in accordance with the management of global trends in the development of threats, threat models, and vulnerabilities of the protection system, a triad of actions and approaches to breaking cycles of cyber-attacks on critical infrastructure.

Keywords: critical infrastructure, cybersecurity, security systems, information technologies.

Introduction

Critical infrastructure is defined as the systems and networks that are essential to the functioning of a country's economy and society. This includes everything from power grids and water systems to telecommunications networks and financial systems (fig. 1) [1]. These systems are vital to our way of life and are, therefore, of paramount importance. In order for our society to function properly, they must be secure and reliable.

Literature analysis

Unfortunately, critical infrastructure can be vulnerable to attack from natural disasters or malicious actors such as hackers or terrorists. If these threats are not addressed quickly, they can lead to significant disruption in service delivery or even complete shutdowns which could have devastating consequences for those relying on them for their day-to-day activities.

Therefore, it is important that governments take steps towards protecting critical infrastructure from potential threats by implementing comprehensive security measures both online and offline.

The first step in securing critical infrastructure is understanding what assets need protection; this requires an extensive risk assessment which will identify any potential risks present within an organization's operations as well as its environment (e.g., physical location).

Purpose and statement of the task

Once the risks have been identified then appropriate countermeasures must be put into place including secure authentication protocols, encryption technologies, firewalls etc. Additionally, organizations should consider investing in cyber insurance policies which will help cover any damages incurred due to a successful attack on their system(s).

The main part of the study

An overview of cyber threats to critical infrastructure

Cybersecurity threats to critical infrastructure have the potential to cause significant and widespread disruption and economic damage. Data breaches, malicious software, and other forms of cyberattack can exploit vulnerabilities in computer systems, networks, and devices and cause serious harm to the organizations and individuals they affect.

The increasing prevalence of digital technologies in critical infrastructure sectors such as healthcare, transportation, aviation, and energy has made them particularly vulnerable to cyber threats (fig. 2).

These threats can come from a variety of sources, such as organized cyber criminals, state-sponsored hackers, or lone actors. They can target networks and systems,

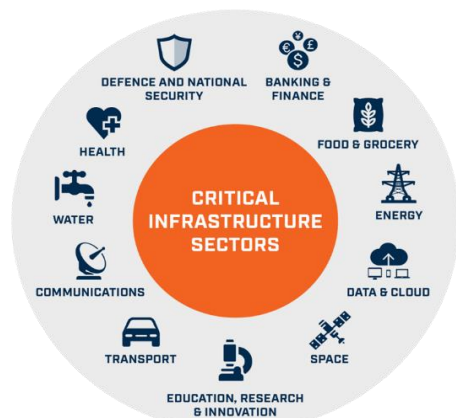


Fig. 1. Critical infrastructure sectors

steal confidential data, and cause financial losses by disrupting systems and operations.

Organizations in the critical infrastructure sectors must take steps to protect their systems from cyber threats, including implementing effective security controls, regularly monitoring networks for potential intrusions, and training employees to recognize and respond to potential cyber threats. Governments should also pro-

vide guidance and assistance to critical infrastructure sector organizations to help them mitigate cybersecurity risks.

Additionally, international and industry standards and best practices should be established and implemented, and regulatory frameworks should be put in place to ensure that organizations comply with cybersecurity requirements. [7].

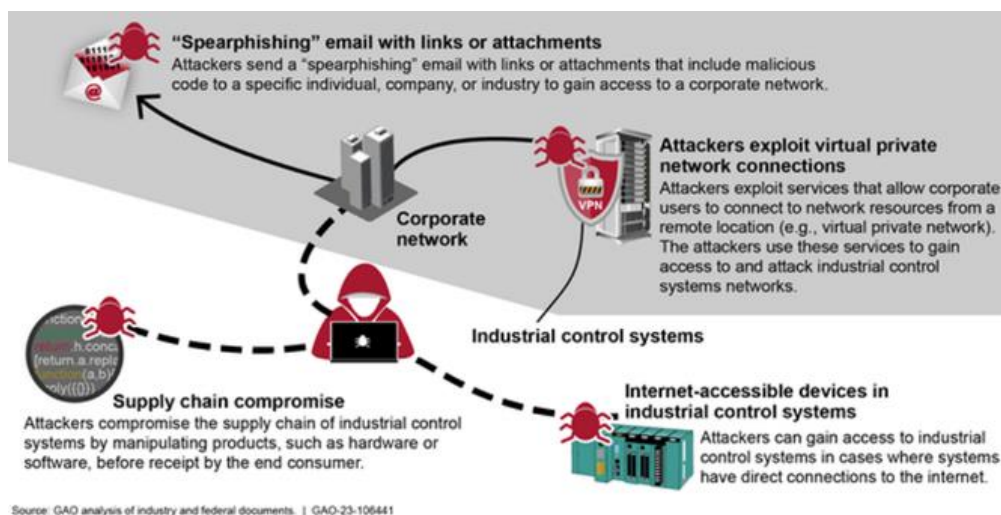


Fig. 2. Cyber threats for critical infrastructure

History of cyber-attacks on critical infrastructure

Cyberattacks against critical infrastructure systems are on the rise, and the damage and losses caused by these attacks can be devastating. According to US cybersecurity officials at Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), there were a total of 276 reported incidents in 2020, with 56% of energy utility facilities reporting at least one cyberattack that caused data loss or operations shutdown (fig. 3) [2, 10].

In addition to loss of data and disruption of operations, cyberattacks can cause significant financial losses. For example, in November 2022, a hacking group targeted Bahraini government websites with DDoS attacks prior the country's parliamentary and local elections [2]. The attack caused an estimated 50 million Bahraini dinars (about \$132 million) in damages and losses. Another significant cyberattack occurred in November 2022, when

hackers damaged Danish State Railways' network after targeting an IT subcontractor's software testing environment. The attack caused an estimated \$90 million in damages [3].

In February 2020, Saudi authorities reported that their public petroleum and natural gas company Saudi Aramco has seen an increase in cyber-attack attempts. This public enterprise suffered a huge cyber-attack back in the year 2012 when Shamoon Virus hit the facility and damaged around 30,000 computers [4].

New Zealand's central bank suffered a huge data breach, where commercially and individually sensitive information was stolen by cyber attackers. In another event, an electricity grid in the state of Maharashtra (India) was hit by a cyber-attack that resulted in a power outage. This incident took place in the month of October 2020 and the authorities suspect Chinese involvement in it [5].

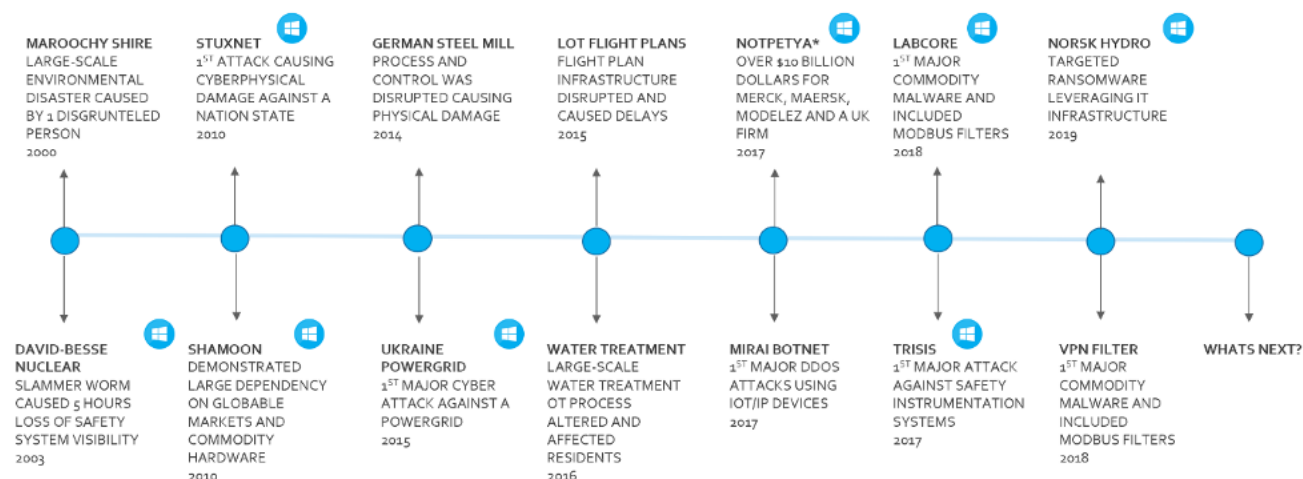


Fig. 3. Timeline of Cyber Attacks on Critical Infrastructure

These are just a few examples of the significant financial losses caused by cyberattacks on critical infrastructure. As more and more systems become connected to the internet and vulnerable to cyber-attacks, it is important for organizations to invest in robust cybersecurity defenses and cyber insurance policies to protect their systems from malicious actors. By taking these measures, organizations can help protect their systems from cyber-attacks and ensure the safety of the public.

Securing critical infrastructure from cyber threats is a complex task. As the infrastructure is interconnected, a security breach in one system can have a cascading effect, leading to multiple systems being compromised. Additionally, due to the critical nature of these systems, attackers can cause significant disruption and even physical damage if they are successful in their attacks (fig. 4, 5).

Another challenge is the fact that the infrastructure is aging and often outdated, meaning it lacks the robust

security measures that are necessary to protect it from cyber threats. Furthermore, as the infrastructure is often managed by multiple stakeholders, it can be difficult to ensure that all systems are adequately protected.

Finally, the cost associated with implementing and maintaining cybersecurity measures can be prohibitive, making it difficult for organizations to invest in the necessary safeguards [9].

The need to improve the cybersecurity of critical infrastructure

Given the wide range of cyber threats faced by critical infrastructure, it is clear that improved cybersecurity measures are needed. In order to protect critical infrastructure from cyber-attacks, organizations must take a proactive approach to security and ensure that their systems are adequately protected. This means implementing robust security measures such as firewalls, intrusion detection systems, and antivirus software.




| Type of threat | Description |
|--|--|
| Physical  | <ul style="list-style-type: none"> Natural occurrences, such as hurricanes, floods, and ice storms Human-made occurrences, such as explosive, chemical, biological, or radiological contaminant attacks on communications network infrastructure and personnel |
| Cyber-related  | <ul style="list-style-type: none"> Malicious actors, such as adversaries who intentionally disrupt the systems on a communications network Nonmalicious actors, such as employees that accidentally alter a communication network's configuration, negatively affecting the network's ability to function properly |
| Human  | <ul style="list-style-type: none"> Threats to a communications network due to the failure of employees to plan for security incidents and implement protocols to protect networks from the impacts of such incidents |

Fig. 4. Types of cyber threats for critical infrastructure

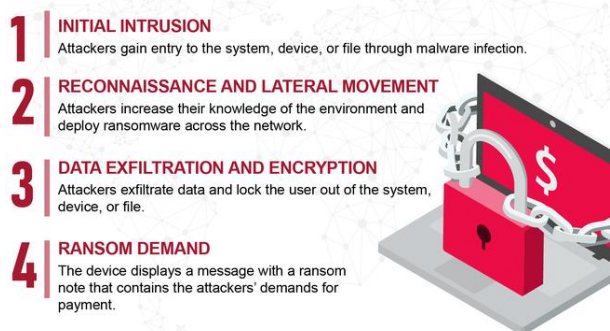


Fig. 5. Security breach in critical infrastructure after cyber attacks

Organizations must also ensure that their systems are regularly updated and patched to address any vulnerabilities that may be present. Additionally, they must have in place procedures for responding to security incidents and for recovering from an attack. Finally, organizations should ensure that their staff are adequately trained in cybersecurity and are aware of the threats posed.

Current measures for securing critical infrastructure

Currently, there are a number of measures that can be taken to secure critical infrastructure from cyber-attacks. The basic triad of current measures for securing critical infrastructure involves people, processes, and technology. It would include guarding against legal, contractual, and third-party risks, as well as instituting

continuous compliance monitoring for cyber threats and associated countermeasures. These include the implementation of robust security measures such as firewalls, intrusion detection systems, and antivirus software. Additionally, organizations should ensure that their systems are regularly updated and patched to address any vulnerabilities that may be present.

Organizations must also put in place procedures for responding to security incidents and for recovering from an attack. Finally, they should ensure that their staff are adequately trained in cybersecurity and are aware of the threats posed [6, 7]:

1. At the organizational level, some of the following measures can help in stopping cyber-attacks from affecting the enterprise infrastructure;

2. Access Management – access management is the first basic measure that organizations should take to protect their control systems. Identity Access Management in databases and other important IT infrastructure is necessary to limit access and prevent the misuse or leak of information;

3. Awareness as Defense – one very effective way of preventing cyber-attacks on an enterprise is to train the employees in the basics of cyber security. Cyber aware employees form a major defense against attempted cyber-attacks on the enterprise. An increase in the overall cyber security awareness can be achieved through cyber security awareness tools;

4. Email Domain Security – to ensure the security of an organization, it is imperative to address the cyber

threats originating from its email domain. Using email domain security tools can be very effective in stopping spoofing of the email domain to protect the enterprise against spear-phishing attacks;

5. Data Backup – frequent data backup in offline locations in a segmented manner is the best approach to defend against ransomware attacks;

6. Incident Response – use of incident response tools can facilitate quick detection of and response to a cyber-attack. A phishing incident response tool can be

quite helpful in identifying and removing phishing emails from the employees' inboxes;

7. Strong Password Policy – employees should be encouraged to use strong passwords. This applies to both their work emails and other credentials used for accessing information and operations of critical systems in the enterprise (Fig. 6) [11].

By taking the necessary steps to protect their systems from cyber-attacks, organizations can help ensure the safety of the public [9].

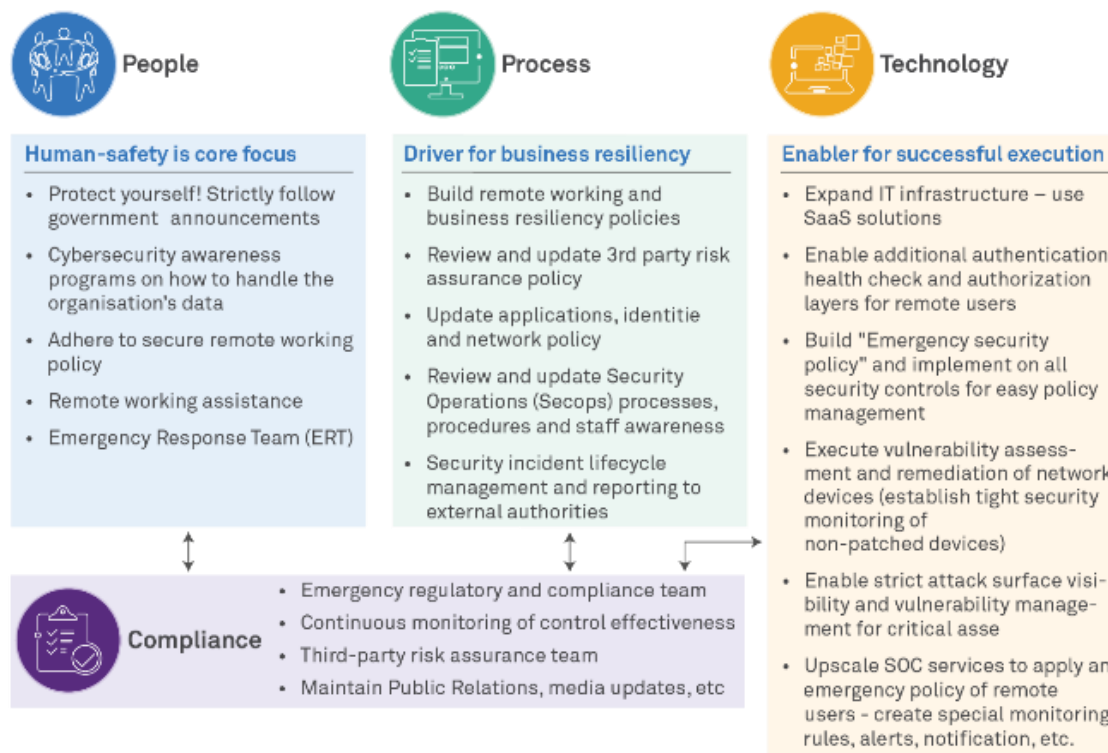


Fig. 6. Basic triad of current measures for securing critical infrastructure

How to create a secure cyber environment for critical infrastructure

In order to create a secure cyber environment for critical infrastructure, organizations must take a holistic approach to security. This means implementing a range of measures to protect the infrastructure from cyber threats, including robust security measures such as firewalls, intrusion detection systems, and antivirus software. Additionally, organizations should ensure that their systems are regularly updated and patched to address any vulnerabilities that may be present.

Organizations must also have in place procedures for responding to security incidents and for recovering from an attack. Finally, they should ensure that their staff are adequately trained in cybersecurity and are aware of the threats posed.

The security of critical infrastructure systems is of paramount importance to the safety and security of our society. Organizations must take steps to ensure that their systems are adequately protected from cyber-attacks [12]. The following are some of the key steps that organizations can take to create a secure cyber environment for their critical infrastructure:

1. Implement Robust Security Policies: organizations should develop and implement comprehensive

security policies that outline acceptable use, access controls, and other security-related topics. These policies should be regularly reviewed and updated to ensure that they are in line with the latest best practices;

2. Implement Security Controls: organizations should implement security controls such as firewalls, antivirus software, and intrusion prevention systems to protect their systems from malicious actors;

3. Train Employees: organizations should provide regular security training to their employees to ensure that they are aware of the risks posed by cyber-attacks and have the necessary skills to protect against them;

4. Monitor Activity: organizations should monitor their systems for suspicious activity, such as unauthorized access attempts, to ensure that their systems are not being compromised.

By taking these measures, organizations can help create a secure cyber environment for their critical infrastructure and ensure the safety of the public.

The role of artificial intelligence in improving critical infrastructure security

The prevalence of mobility combined with faster internet has expanded the reach of connected systems. Apps that used to be on-premises apps, with access limited to company-approved devices, are now "Apps" and

"Clouds" for anytime, anywhere, anywhere access device. This transformation has narrowed business boundaries and moved users, data, and devices beyond the company. The threat landscape, as a result, has changed. Fraudsters have developed sophisticated skills and capabilities, and the lack of cybersecurity professionals-with the requisite skills and knowledge to counteract cyber-attacks-poses a challenge.

Cybersecurity involves multiple issues related to people, process and technology (fig. 7).



Fig. 7. Cybersecurity issues related to people, process and technology

Cyber defenders are grappling with traditional, commercial off-the-shelf security solutions that are built as one-size-fits-all, for all industries and segments. These security solutions heavily rely on predefined signatures for detection and prevention, and totally lack the context for human behavior. Fraudsters have found sophisticated ways to evade signature-based technology and are exploiting humans to gain access to the enterprise [13].

The use of artificial intelligence (AI) is becoming increasingly common in cybersecurity. AI-based systems are able to detect and respond to cyber threats in real-time, allowing organizations to quickly detect and mitigate any potential threats.

Additionally, AI-based systems can be used to automate mundane security tasks, freeing up security personnel to focus on more complex tasks.

AI-based systems can also be used to identify anomalous behavior within systems and networks, allowing organizations to detect and respond to threats before they become a problem. Finally, AI-based systems can be used to analyze large amounts of data and identify patterns that may indicate a security breach.

AI has become an increasingly important tool in protecting these critical assets from malicious actors due to its ability to process large amounts of data quickly while learning from past experiences. AI can be used in various ways when it comes to improving critical infrastructure security including detection of anomalies or suspicious activity; monitoring for signs of attack or tampering; identifying vulnerabilities; optimizing access control measures; providing predictive analytics on potential threats; coordinating responses between different agen-

cies/organizations involved in protecting the asset(s); as well as aiding with incident response efforts should an attack occur.

One example of how AI can be used in this capacity is through anomaly detection algorithms which detect unusual behavior within a system by analyzing patterns over time. These algorithms have been proven effective at detecting intrusions into computer networks which may otherwise go unnoticed by traditional methods such as signature-based intrusion detection systems.

Additionally, AI can also be utilized for cybersecurity tasks such as malware identification by scanning files for signs of malicious code or analyzing network traffic for abnormal communication patterns indicative of an ongoing attack attempt.

By leveraging machine learning techniques trained on historical data sets collected over long periods of time these algorithms are able to accurately identify potential risks before they cause any damage or disruption to operations.

Another area where AI technology can help enhance security measures around critical infrastructure is through optimization strategies designed specifically around access control mechanisms like authentication processes or authorization rulesets governing who can access certain resources within a system/network environment etc. Similarly rule-sets governing resource access could also benefit from similar optimization strategies allowing admins greater flexibility when creating policies that best suit their organization's specific needs without sacrificing overall security integrity level unnecessarily either way.

Key factor to breaking the cycle of cyberattacks on critical infrastructure

Cyberattacks on critical infrastructure have become increasingly frequent, posing a serious threat to national security. Experts agree that the most effective way to break this cycle is through incentives for organizations to increase their security measures and invest in cyber protection.

One key factor contributing to this problem is the lack of incentives for companies operating critical infrastructure to invest in cybersecurity measures. In some cases, companies may be reluctant to invest due to cost considerations; however, in many cases it can also be attributed to misaligned incentives between operators and regulators. This misalignment means that even when operators do spend money on cybersecurity measures, they may not be rewarded for doing so; instead, they might suffer financial penalties if their system fails despite having invested in protective measures. As such, operators may feel like any investment into security will simply result in increased costs with no benefit – leaving them vulnerable targets for hackers looking exploit these weaknesses.

Incentives provide a way forward when attempting break this cycle of cyberattacks on critical infrastructure. By providing both short-term benefits (such as reduced costs) and long-term rewards (like increased trust), incentive structures can help encourage operators make the necessary investments into protection against attacks – thus reducing risk levels across whole industries at once. However, designing effective incentive structures isn't easy; different approaches will work best depending on

factors such as industry size/complexity and local regulatory environments. As such policy makers must consider multiple forms of incentivization when crafting strategies aimed at breaking this dangerous cycle once and for all. One approach policy maker should consider is offering financial rewards those who successfully defend against cyberattacks – both directly through cash payments or indirectly through tax breaks etc. Such rewards act as an immediate incentive encouraging those responsible protect their systems. Another option involves using public recognition programs reward successful defense efforts against attack attempts. Here companies would receive awards/certifications acknowledging their hard work protecting customers data etc., creating positive publicity around organization.

The first incentive that can be used to encourage organizations to invest in cyber protection is the provision of financial rewards. While this may seem counterintuitive, providing financial incentives for organizations to increase their security measures can provide a strong motivation for them to do so.

Another form of incentive structure which has been gaining traction is public recognition programs. These programs recognize organizations who have taken steps towards improving their cybersecurity posture by investing in protective technologies, training personnel, and developing policies and procedures around handling sensitive data and information systems.

A third type of incentive involves government regulation requiring certain levels of cybersecurity protections within critical infrastructure networks such as power grids or water supply systems.

Governments can subtle encouragement through design choices to promote better cybersecurity practices among private sector actors by making it easier for them access resources like training materials or expert advice on how improve their defenses against cyberattacks on critical infrastructure networks. By increasing awareness about available resources, governments can create more visible pathways toward improved security postures without having force compliance through heavy-handed regulations or fines – allowing companies greater flexibility when deciding what works best for their organization while still moving closer towards achieving national goals around protecting our critical infrastructure from attacks.

Incentives are an important tool when attempting break the cycle of cyberattacks on critical infrastructure because they provide both short-term benefits (such as reduced costs) and long-term rewards (like increased trust). However, there is no one size fits all approach when designing effective incentives structures; different approaches will work best depending on factors such as industry size/complexity and local regulatory environments. As such, it's important that policy makers consider multiple forms incentives - from financial rewards, to public recognition programs - when crafting strategies aimed at breaking this dangerous cycle once and for all [14, 15, 16].

Best practices for protecting critical infrastructure from cyber attacks

Organizations must take a proactive approach to protecting their critical infrastructure from cyber threats. This means implementing robust security measures such

as firewalls, intrusion detection systems, and antivirus software. Additionally, organizations should ensure that their systems are regularly updated and patched to address any vulnerabilities that may be present. Hacker attacks present a major threat to the security of critical infrastructure and can have a severe impact on the safety and security of the public. As such, organizations must take steps to protect their critical infrastructure from hackers [15].

The most effective approach to protecting critical infrastructure from hacker attacks is to implement a combination of preventive measures and response plans.

Preventive Measures: Preventive measures are designed to reduce the risk of a successful attack by implementing security controls such as firewalls, antivirus software, intrusion prevention systems, and access controls. These measures can help organizations identify and neutralize potential threats before they can cause any damage.

Response Plans: Organizations should also develop an effective response plan in the event of a successful attack. This plan should include steps to mitigate any damage, investigate the attack, and prevent future attacks.

By taking these measures, organizations can help protect their critical infrastructure from hacker attacks and ensure the safety of the public.

Organizations must also have in place procedures for responding to security incidents and for recovering from an attack. Additionally, they should ensure that their staff are adequately trained in cybersecurity and are aware of the threats posed. Finally, organizations should consider leveraging AI-based systems to detect and respond to cyber threats in real-time.

Conclusions. Critical infrastructure is important base of modern technologies - it is the foundation upon which all other technologies are built and relies on for their successful operation. Critical infrastructure includes power grids, communication networks, transportation systems, water supplies, financial institutions, and other vital services that enable businesses and citizens to go about their daily lives with minimal disruption. In today's digital world where almost, everything is connected in some way or another, critical infrastructure plays an even more important role as it provides a basis.

In order to do this, organizations must take a proactive approach to security and ensure that their systems are adequately protected. This means implementing robust security measures such as firewalls, intrusion detection systems, and antivirus software.

Additionally, organizations should ensure that their systems are regularly updated and patched to address any vulnerabilities that may be present. Organizations must also have in place procedures for responding to security incidents and for recovering from an attack. Finally, they should consider leveraging AI-based systems to detect and respond to cyber threats in real-time. By taking the necessary steps to protect their critical infrastructure, organizations can ensure that their systems remain secure and reliable.

References

[1]. Critical Infrastructure Cyber Security Solutions. Huntsman. (2021, May 6). Retrieved February 13, 2023, from <https://www.huntsmansecurity.com/industries/critical-infrastructure>.

- [2]. Cyber-attacks on Critical Infrastructure. AGCS Global. Retrieved February 2, 2023, from <https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html>
- [3]. Significant cyber incidents: Strategic technologies program. CSIS. Retrieved February 2, 2023, from <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- [4]. Weinberg, A. (2022, October 2). Analysis of top 11 cyber-attacks on critical infrastructure. FirstPoint. Retrieved February 3, 2023, from <https://www.firstpointmg.com/blog/analysis-of-top-11-cyber-attacks-on-critical-infrastructure/>.
- [5]. Khemani, R. (2021, April 7). Cyber Security for Critical Infrastructure: Challenges and Solutions. Security Boulevard. Retrieved February 3, 2023, from <https://securityboulevard.com/2021/04/cyber-security-for-critical-infrastructure-challenges-and-solutions/>.
- [6]. Protecting critical infrastructure. Cybersecurity and Infrastructure Security Agency CISA. Retrieved February 3, 2023, from <https://www.cisa.gov/protecting-critical-infrastructure>.
- [7]. Infrastructure security. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). Retrieved February 3, 2023, from <https://www.cisa.gov/infrastructure-security>.
- [8]. Llc, L., & Pires, A. (2021, September 10). Cybersecurity threats to critical infrastructure. LIFARS, a Security Scorecard company. Retrieved February 4, 2023, from <https://www.lifars.com/2021/09/cybersecurity-threats-to-critical-infrastructure>.
- [9]. Office, U. S. G. A. Cybersecurity high-risk series: Challenges in protecting Cyber Critical Infrastructure. Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure / U.S. GAO. Retrieved February 4, 2023, from <https://www.gao.gov/products/gao-23-106441>.
- [10]. Brash, R. (2022, December 1). How 20 years of cyber security incidents inform future strategy. Verve Industrial. Retrieved February 5, 2023, from <https://verveindustrial.com/resources/blog/how-20-years-of-cyber-security-incidents-inform-future-strategy/>.
- [11]. Cybersecurity strategies for adjusting to covid-19. Retrieved February 5, 2023, from <https://www.wipro.com/blogs/amit-kothari/cybersecurity-strategies-for-adjusting-to-covid-19/>.
- [12]. Eytan, D. O. (2021, April 14). Council post: Six key guidelines to protect critical infrastructure from cyber threats. Forbes. Retrieved February 6, 2023, from <https://www.forbes.com/sites/forbestechcouncil/2021/04/14/six-key-guidelines-to-protect-critical-infrastructure-from-cyber-threats/>.
- [13]. Transforming the future of cybersecurity with an AI-driven approach. Retrieved February 13, 2023, from <https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence>.
- [14]. Dow Jones & Company. (2022, June 8). Reshaping incentives to protect critical infrastructure from cyberattacks. The Wall Street Journal. Retrieved February 7, 2023, from <https://deloitte.wsj.com/articles/reshaping-incentives-to-protect-critical-infrastructure-from-cyberattacks-01654630416>.
- [15]. Protecting critical infrastructure from cyberattacks – nationally and internationally. EU Policy Blog. (2022, September 12). Retrieved February 7, 2023, from <https://blogs.microsoft.com/eupolicy/2022/07/28/protecting-critical-infrastructure-from-cyberattacks/>.
- [16]. Tagabe, P. M. (2022, November 8). How to protect critical infrastructure from Cyber Threats. Infrastructure Magazine. Retrieved February 8, 2023, from <https://infrastructuremagazine.com.au/2022/11/04/how-to-protect-critical-infrastructure-from-cyber-threats/>.

УДК 004.056:004.7:656.7

Ткачов А., Корольов Р., Рагімова І., Аксьонова І., Севрюкова Є. Проблеми кібербезпеки та рішення для захисту критичної інфраструктури

Анотація. Критична інфраструктура може бути вразливою до атак стихійних лих або зловмисників, таких як хакери чи терористи. Якщо ці загрози не усунути швидко, вони можуть призвести до значних збоїв у наданні послуг або навіть до повної зупинки, що може мати руйнівні наслідки для тих, хто покладається на них у своїй повсякденній діяльності. Тому важливо, щоб уряди вжили заходів для захисту критичної інфраструктури від потенційних загроз шляхом впровадження комплексних заходів безпеки як онлайн, так і офлайн. На основі комплексного аналізу актуальних проблем прийнято рішення щодо забезпечення кіберзахисту інфраструктури об'єктів критичної інфраструктури. Проведено аналіз кіберзагроз у зв'язку з динамікою історичної ретроспективи в секторах об'єктів критичної інфраструктури. Оскільки все більше і більше систем стають підключеними до Інтернету та вразливими до кібератак, організаціям важливо інвестувати в надійні засоби кібербезпеки, щоб захистити свої системи від зловмисників. Вживаючи цих заходів, організації можуть допомогти захистити свої системи від кібератак і забезпечити безпеку населення. Сформульовано модель загрози від розливу об'єктів критичної інфраструктури до кібератак із розбивкою загрози за типами. Розглянуто тріаду основних дій і підходів для захисту критичної інфраструктури. Визначено існуючі проблеми в реалізації заходів протидії та основні загрози для суб'єктів кіберпростору. Було визначено ключові фактори, які розривають цикл кібератак на критичну інфраструктуру. На основі комплексного аналізу та сформульованих концепцій запропоновано комплексний підхід до захисту об'єктів критичної інфраструктури відповідно до управління глобальними тенденціями розвитку загроз, моделей загрози та вразливостей системи захисту, тріади дій та підходи до розриву циклів кібератак на критичну інфраструктуру.

Ключові слова: критична інфраструктура, кібербезпека, системи безпеки, інформаційні технології.

Ткачов Андрій Михайлович, кандидат економічних наук, доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.

Andrii Tkachov, candidate of economic sciences, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Корольов Роман Володимирович, кандидат технічних наук, доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.

Roman Korolov, candidate of technical sciences, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Ірада Рагімова, кандидат технічних наук, доцент кафедри комп'ютерних технологій, Баку, Азербайджан.

Irada Rahimova, PhD in technology, assistant professor at the Department of "Computer Technologies", Baku, Azerbaijan.

Аксьонова Ірина Вікторівна, кандидат економічних наук, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.

Iryna Aksonova, candidate of economic sciences, associate professor of cybersecurity department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Севрюкова Єлизавета Олександрівна, аспірант кафедри економіки підприємства та організації бізнесу Харківського національного економічного університету імені Симона Кузнеця, Україна.

Yelyzaveta Sevriukova, graduate student of the Department of Enterprise Economics and Business Organization, Simon Kuznets Kharkiv National University of Economics, Ukraine.

Отримано 7 лютого 2024 року, затверджено редколегією 1 квітня 2024 року
