Journal of Modern Technology and Engineering
Vol.9, No.2, 2024, pp.94-101
https://doi.org/10.62476/jmte9294

CYBER HYGIENE IN PUBLIC ADMINISTRATION OF AZERBAIJAN: ENSURING DATA SECURITY

Elvin I. Azizbayov, Gulnar R. Mirzayeva*

Department of Management of Intelligent Systems, The Academy of Public Administration under the President of the Republic of Azerbaijan, Baku, Azerbaijan

Abstract. The Republic of Azerbaijan public administration holds sensitive data about citizens, including personal and financial information. The increasing frequency and sophistication of cyber-attacks make it essential for public administration to implement robust cyber hygiene practices to protect this data. This article discusses the importance of cyber hygiene in the public administration of Azerbaijan and outlines best practices for ensuring data security. Cyber hygiene similarly refers to practices meant to prevent malware infections, as well as cyber intrusions and data loss or corruption, and maintain a healthy cyber environment. This ensures the health of systems and improves cybersecurity in the same way routine handwashing helps prevent the spread of disease. Given that all organizations use information systems to do business today, all are at risk of exposure to various cyberattacks that can prevent the functioning of information systems or block access to data. Thus, every organization must protect its information system(s), establish procedures and policies, and offer regular training, to establish adequate cyber hygiene practices.

Keywords: Cyber hygien, cyber security, digital public administration.

Corresponding author: Gulnar R. Mirzayeva, The Academy of Public Administration under the President of the Republic of Azerbaijan, 74, Lermontov Str., Az 1001, Baku, Azerbaijan, e-mail: *gulnar.mirzayeva@gmail.com*

Received: 12 April 2024; Revised: 5 June 2024; Accepted: 12 July 2024; Published: 30 August 2024.

1 Introduction and problem formulation

Cyber hygiene is often compared to personal hygiene. An individual engages in certain personal hygiene practices to maintain good health and well-being, cyber hygiene practices can keep data safe and well-protected. In turn, this aids in maintaining properly functioning devices by protecting them from outside attacks, such as malware, which can hinder functionality. Cyber hygiene relates to the practices and precautions users take to keep sensitive data organized, safe, and secure from theft and outside attacks (Digital Guardian, 2023).

Definition of Cyber Hygiene. Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.

Benefits of Cyber Hygiene. Having a routine cyber hygiene procedure in place for your computers and software is beneficial for two distinct reasons – maintenance and security.

How to cite (APA): Azizbayov, E.I., Mirzayeva G.R. (2024). Cyber hygiene in public administration of Azerbaijan: Ensuring data security. *Journal of Modern Technology and Engineering*, *9*(2), 94-101 https://doi.org/10.62476/jmte9294

Maintenance is necessary for computers and software to run at peak efficiency. Files become fragmented and programs become outdated, increasing the risk of vulnerabilities. Routines that include maintenance are likely to spot many of these issues early and prevent serious issues from occurring. A well-maintained system is less likely to be vulnerable to cyber security risks.

Security is perhaps the most important reason to incorporate a cyber hygiene routine. Hackers, identity thieves, advanced viruses, and intelligent malware are all part of the hostile threat landscape. While predicting threats can be challenging, preparing and preventing them becomes feasible with sound cyber hygiene practices.

Common Cyber Hygiene Problems. Enterprises often have multiple elements in need of cyber hygiene. All hardware (computers, phones, connected devices), software programs, and online applications used should be included in a regular, ongoing maintenance program. Each of these systems has specific vulnerabilities that can lead to different problems. Some of these problems include:

- Loss of Data: Hard drives and online cloud storage that aren't backed up or maintained are vulnerable to hacking, corruption, and other problems that could result in the loss of information.

- Misplaced Data: Poor cyber hygiene could mean losing data in other ways. The information may not be corrupted or gone for good, but with so many places to store data, misplaced files are becoming increasingly commonplace in the modern enterprise.

- Security Breach: There are constant and immediate threats to all enterprise data. Phishing, hackers, malware, spam, viruses, and a variety of other threats exist in the modern threat landscape, which is constantly in a state of flux.

- Out of Date Software: Software applications should be updated regularly, ensuring that the latest security patches and most current versions are in use across the enterprise – for all applications. Out-of-date software is more vulnerable to attacks and malware.

- Older Security Software: Antivirus software and other security software must be updated continuously to keep pace with the ever-changing threat landscape. Outdated security software – even software that has gone a few months without an update – can't protect the enterprise against the latest threats.

In an increasingly digital world, the legal framework of a country plays a crucial role in addressing cyber threats and ensuring the security of its digital infrastructure. Azerbaijan, a country at the crossroads of Europe and Asia, has recognized the importance of robust legislation to combat cyber threats and protect its citizens, businesses, and critical infrastructure. This article analyzes Azerbaijan's legal framework for addressing cyber threats, highlighting key laws and regulations enacted to tackle cybercrime and enhance cybersecurity (Gavin Dennis, 2023). Incident-based statistics include data reported by citizens, private organizations, independent cyber security companies and collected by the Electronic Security Service Analytical Report, 2022):

1. Cybersecurity Law: Azerbaijan enacted the Cybersecurity Law in 2018, which serves as a comprehensive legal framework for addressing cyber threats. The law establishes the legal basis for cybersecurity measures, outlines the responsibilities of relevant entities, and sets out procedures for incident reporting and response. It also emphasizes the protection of critical information infrastructure, the prevention of cyber-attacks, and the facilitation of international cooperation in combating cybercrime.

2. Criminal Code Amendments: Azerbaijan's Criminal Code has been amended to include provisions specific to cybercrime. These amendments define cyber offenses, such as unauthorized access to computer systems, data theft, computer fraud, and the distribution

of malicious software. The inclusion of these provisions allows for the prosecution and punishment of individuals involved in cybercriminal activities, thereby deterring potential offenders.

3. Data Protection Laws: Azerbaijan has implemented data protection laws to safeguard the privacy and security of personal information. The Law on Personal Data Protection, adopted in 2019, establishes the principles and requirements for the collection, processing, storage, and transfer of personal data. It provides individuals with rights over their personal information and mandates organizations to implement appropriate security measures to protect data from unauthorized access or disclosure.

4. Electronic Signature and Authentication: To facilitate secure electronic transactions and enhance digital trust, Azerbaijan has enacted laws governing electronic signatures and authentication. The Law on Electronic Signature and the Law on Electronic Commerce provide the legal framework for the use and recognition of electronic signatures, ensuring their validity and integrity. These laws also establish requirements for secure authentication methods, promoting secure online transactions.

5. Cooperation with International Organizations: Azerbaijan recognizes the transnational nature of cyber threats and the importance of international cooperation in combating cybercrime. The country actively collaborates with international organizations such as the Council of Europe, the United Nations, and the International Telecommunication Union (ITU) to exchange information, share best practices, and participate in capacity-building programs. These collaborations enhance Azerbaijan's ability to address cyber threats effectively and align its legal framework with international standards.

6. Public-Private Partnerships: Azerbaijan emphasizes the importance of public-private partnerships in addressing cyber threats. The government collaborates with private sector entities to exchange information, share intelligence, and develop joint initiatives to enhance cybersecurity. This partnership approach allows for the collective sharing of expertise, resources, and best practices, fostering a collaborative environment for addressing cyber threats effectively.

7. Awareness and Education: Recognizing the need for cybersecurity awareness and education, Azerbaijan has taken steps to promote cybersecurity knowledge among its citizens. The government conducts awareness campaigns, workshops, and training programs to educate individuals about cyber threats, safe online practices, and the importance of adhering to cybersecurity regulations. These initiatives empower individuals to take proactive measures to protect themselves and contribute to a cyber-resilient society.

Most successful attacks leverage well-known security problems. Reporting from the UK Government's CESG (the part of GCHQ tasked with protecting the nation) indicates that around 80 of cyber-attacks result from poor cyber habits within the victim organizations.

A cyber hygiene strategy that emphasizes the importance of carrying out regular, low-impact security measures should be implemented to address this. This will minimize the risks of becoming a victim of a cyber attack or spreading the impact of a cyber-attack to other organizations.

Cyber-attacks are growing in both frequency and impact. The repercussions of security mistakes often become headline news and can cause significant harm to the victim organization. However, there is a perception that only big, global, corporations are at risk, and, as a result, thousands of attacks against the Small – Medium business sector go largely unreported (Smith, 2019; Blokdyk, 2018).

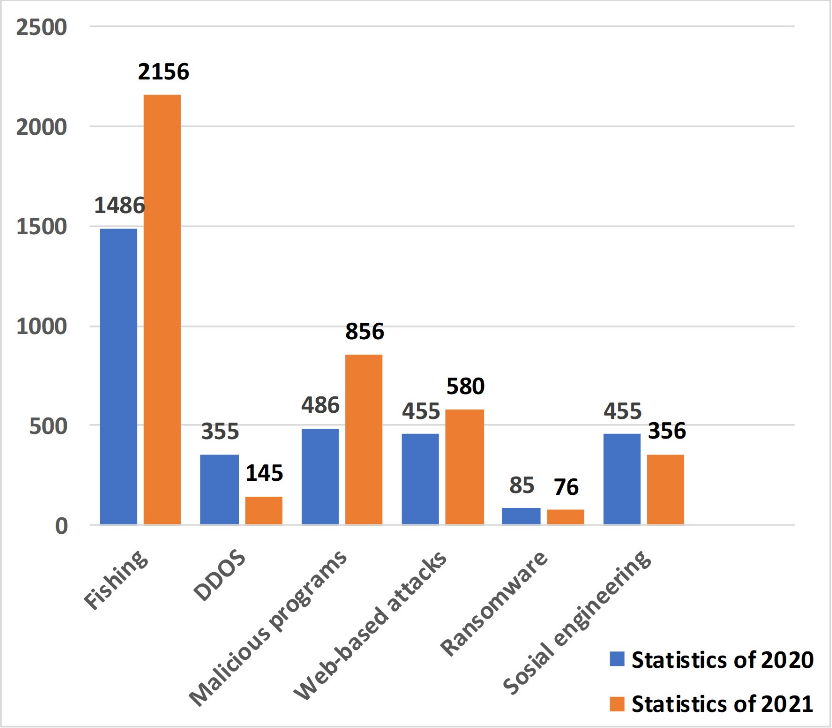

Figure 1: Statistics of cyber security incidents in Azerbaijan for 2020-2021 `https://stm.az/storage/common/1682925330.KIBERCINAYET2022.pdf`

In this context, cyber hygiene should be viewed in the same manner as personal hygiene and, once properly integrated into an organization will be simple daily routines, good behaviors, and occasional checkups to make sure the organization's online health is in optimum condition.

As businesses across Europe become more connected, with multi-level supply chains for even the smallest organization, this last point becomes quite significant. The attack on the US Target corporation in 2013, for example, was the result of a compromised vendor within their supply chain `https://redriver.com/security/target-data-breach`. While this has highlighted the need to secure the supply chain, most SMEs struggle to have the resources, access, or knowledge to do this properly.

In 2020, ”Kaspersky” noted a significant increase in attacks made over the RDP (Remote Desktop Protocol) protocol intended for organizing remote work. Sputnik Azerbaijan reports that according to the company's ”Remote work - story of the year” report, 2.2 million such attacks were registered in Azerbaijan between January and November. This is 2.6 times more than in the same period of 2019.

The public administration of the Republic of Azerbaijan is responsible for collecting and holding sensitive data about citizens. Cyber security threats, such as ransomware, phishing, and social engineering, pose a significant risk to the confidentiality and integrity of this data. Adequate cyber security measures are essential to safeguard this data and maintain public trust. This article discusses the importance of cyber hygiene in the public administration of the Republic of Azerbaijan and best practices for ensuring data security `www.enisa.europa.eu`.

Achieving a healthy and safe cyberspace is impossible without involving other states in bilateral and multilateral cooperation. In parallel with the unilateral initiatives, the state bodies of Azerbaijan are active in establishing relations with the states on improving global cyber security mechanisms. In other words, Azerbaijan is interested in learning and applying advanced practice in the field of cyber security, and it is making constant efforts in the field of international cooperation. In this direction, since 2009, close cooperation relations have been established with Estonia, which ranks third in terms of digital solutions among European countries. As one of the best examples, the implementation of ”Easy signature” in Azerbaijan, formed within the framework of a partnership with Estonia, can be mentioned. The mobile identity service and the digital function of ”Easy signature” provide secure access to public and private electronic services anywhere. The digital mobile signature is considered equal to the national identity at the legislative level. Cyberspace protection is also one of the main directions of Azerbaijan-Romania bilateral relations. In addition, Azerbaijan has started international cooperation with the computer emergency response teams of more than twenty countries, including Georgia and the Czech Republic.

2 Importance of cyber hygiene in the public administration of Azerbaijan

Analyze systems and establish procedures and policies [4] Babić & Bratić (2022);
Asset inventory;
Maintain a hardware & software inventory;

Managing IT hardware and software (IT assets) can be an overwhelming task, especially if equipment and personnel constantly move or change, but it is essential. Hardware, software, and all network and non-network devices count as assets for this purpose.

Maintaining a hardware and software inventory will support different processes in your organization, such as:

- Incident management
- Problem management
- Change management

And in these processes, similar questions are asked:

- What does this IT asset do?
- What kind of Operating System does it use?
- What applications are stored on/in the asset?
- What is the network topology?
- Who has access to the asset?
- Who is accountable for it?

To provide answers, a centralized information base is needed. Thus, the first step in establishing cyber hygiene practices is standardizing the inventory of software and hardware by:

1. Documenting the baseline security posture of the organization
2. Standardizing this across the organization based on policy and procedures
3. Monitoring and responding to deviations
4. Reducing any vulnerabilities introduced by rogue hardware and software

The benefits of maintaining a software and hardware inventory are quickly evident and include:

- Control of the IT environment

- Control of software assets (version, patch, dependency, accountability, proof of concept (PoC))
- Control of hardware assets (version, criticality, PoC, dependency)
- Effective Governance
- Better MTTRS (Mean time to restore service)

Protects Sensitive Data: Public administration organizations in the Republic of Azerbaijan hold sensitive data about citizens, including personal data and financial information. Cyber hygiene practices can help protect this data from cyber threats and prevent data breaches.

Compliance with Regulations: Public administration organizations of the Republic of Azerbaijan are subject to data protection regulations, such as the Law on Personal Data. Implementing cyber hygiene practices can help ensure compliance with these regulations and avoid legal consequences.

Public Trust: Citizens trust the public administration of Azerbaijan to protect their sensitive data. A data breach can erode public trust, resulting in reputational damage and loss of confidence in the organization.

Regular Employee Training: Train employees on cyber security best practices and policies, including password management, software updates, and phishing awareness. Regular training can help employees understand the importance of cyber hygiene and the consequences of a data breach.

Access Controls: Restrict access to sensitive data to authorized personnel only. Use role-based access control (RBAC) to ensure that employees only have access to the data they need to perform their job responsibilities.

Network Security: Implement appropriate network security measures, including firewalls, intrusion detection and prevention systems, and network segmentation. Regularly scan for vulnerabilities and perform penetration testing to identify weaknesses in the network.

Incident Response Plan: Develop an incident response plan to address cybersecurity incidents. The plan should include procedures for identifying, containing, and mitigating the impact of a cyber-attack.

Data Backups: Regularly back up all data to an offsite location. Backups can help recover data in case of a ransomware attack or other cyber incident.

This article, which evaluates the level of cyber security of the states in 5 main areas - legal basis, technical preparation, organizational issues, personnel potential, as well as communication and cooperation directions, assesses the level of cyber security between countries, identifies gaps and challenges for each country, sets priorities for development, and also, is of great importance for the exchange of knowledge between countries with the identification of weak and strong sides.

According to the "Global Cyber Security Index 2020" (GCI) report of the International Telecommunication Union, which is considered one of the most pioneering reports at the international level, Azerbaijan moved up 15 places and rose to 40th place this year. With a total of 89.31 points, our country ranks 3rd among the CIS countries after Russia and Kazakhstan. Leaving behind Georgia and Ukraine from the CIS countries, Switzerland, Ireland, Iceland, Slovenia, and the Czech Republic from the European countries, Azerbaijan is demonstrating continuous development by implementing international cooperation in this field and applying the best global examples. It is no coincidence that Estonia, with which our country closely cooperates in the field of digital solutions, ranks 3rd among European countries according to the index this year. The first place in the rating was taken by the United States, and the second place was taken by Great Britain and Saudi Arabia `www.enisa.europa.eu`.

Almost all cyberattacks take advantage of conditions that fall under the umbrella of poor cyber hygiene. This includes missing patches, bad configurations, and poor user awareness. A lack of consistent cyber hygiene is therefore one of the most pernicious threats that can emanate from inside an organization. To foster good cyber hygiene across your organization:

- Provide employees ample training to identify and report suspicious cyber activity.
- Ensure that all servers, workstations, smartphones, and other devices used by employees receive frequent security updates.
- Implement a strong system access management policy requiring multi-factor authentication whenever possible and strict password standards.
- Invest in systems and solutions that enable clear visibility and granular control access to the organization's entire network infrastructure.

While it may seem that complexity would be the enemy of cybercriminals, it is in fact the enemy of your own cybersecurity. In a complicated and dynamic digital world, your best defense is getting back to the basics.

To improve cyber hygiene and scale it up, it is not enough for an organization to simply offer examples to employees and declare the importance of cybersecurity. In any organization, cyber hygiene must be specifically defined and then supported through metrics and education.

- A security framework is a great starting point, but it should be: Right-sized to your organizational needs
- Aligned with your unique regulatory requirements
- Complemented by training that is available & affordable for your organization
- Maintainable/repeatable with your organizational resources
- In support of your business and operational goals

3 Conclusion

Cyber hygiene is essential for public administration organizations in the Republic of Azerbaijan to protect their sensitive data from cyber threats. Public administration organizations can reduce the risk of data breaches and maintain public trust by adopting best practices such as regular employee training, access controls, network security, incident response planning, and data backups. Cyber hygiene is an ongoing process, and staying vigilant and proactive in safeguarding sensitive data is essential. With proper implementation of cyber hygiene practices, the public administration can ensure the security of sensitive data and meet regulatory requirements.

Ultimately, bad cyber habits – or poor cyber hygiene – are the cause of most successful cyberattacks. This is why it is so important for organizations to develop a culture of good cyber hygiene. However, the measures recommended in this article, though presented mostly through the lens of organizational security, apply to both organizations and individuals. Organizations should thus emphasize to employees that they consider implementing cyber hygiene habits at home as well. Moreover, we are all safer in the cyber world when a culture of cyber hygiene extends across both personal and professional spaces.

In conclusion, Azerbaijan's legal framework for addressing cyber threats demonstrates the country's commitment to cybersecurity and the protection of its digital infrastructure. The Cybersecurity Law, Criminal Code amendments, data protection laws, and regulations on electronic signatures provide the foundation for combating cybercrime and enhancing cybersecurity. Collaboration with international organizations, public-private partnerships, and initiatives focused on awareness and education further strengthen Azerbaijan's legal framework. By continuously updating and improving its laws and regulations, Azerbaijan can effectively mitigate cyber threats and safeguard its digital landscape.

4 Acknowledgement

The authors sincerely thank the anonymous reviewers at Journal of Modern Technology and Engineering for their careful reading and constructive suggestions.

References

Analytical Report. (2022). Cybercrime and cyber security barometer in Azerbaijan. `https://stm.az/storage/common/1682925330.KIBERCINAYET2022.pdf`

Babić, V., Bratić, A. (2022). *Cyber Hygiene for Public Institutions and SMEs.* Guidebook on Staying Safe Online, Geneva Centre for Security Sector Governance.

Blokdyk, G. (2003). *Cyber hygiene.* Emereo Publishing.

Digital Guardian. (2023). A Digital Guardian's Blog. `https://www.digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more`

Gavin Dennis. (2023). An Analysis of Azerbaijan's Legal Framework for Addressing Cyber Threats. `https://blog.gavindennis.com/an-analysis-of-azerbaijans-legal-framework-for-addressing-cyber-threats/`

Jones, C. (2021). *Think red.* `https://redriver.com/security/target-data-breach`

Review of Cyber Hygiene Practices. (2016). European Union Agency for Network and Information Security, `www.enisa.europa.eu`.

Smith, R.E. (2019). *Elementary information security.* Jones & Bartlett Learning.