Innovative: International Multi-disciplinary Journal of Applied Technology
(ISSN 2995-486X) VOLUME 03 ISSUE 09, 2025

Main Issues of Information Security and Their Solutions

Muxiddinov Navruzbek Muyassarovich
Independent Researcher, Uzbekistan
navruzbekislom@gmail.com

Abstract:
This paper examines the situation on informational security in Uzbekistan by drawing attention to importance of CYBERSECURITY as it is gaining significance at breakneck speed and a growing number of cyber threat incidents are being detected. Amid the India's digital push, having strong cybersecurity and information security systems has increasingly become crucial to protect sensitive personal data, national infrastructure and businesses. The study examines the political and technical progress in cybersecurity regulation made by Uzbekistan, with an emphasis on legislation that has been developed (including data protection laws) and national agencies established for cybersecurity such as the National Cyber security Center. The research adopts a mixed methods approach, applying qualitative interviews with IT professionals and quantitative surveys with respect to perceived appropriateness of security technologies involved, including the biometric authentication system. The results indicate progress in complying with fundamental cybersecurity measures like login and password policies, as well as increased use of biometric systems. But the study also illustrates persistent challenges, such as the growth of sophisticated cyberattacks like ransomware and phishing. The report ends with suggestions on how Uzbekistan can further develop its security infrastructure to safeguard against cyber warfare.Laying the Groundwork for the FutureOf course, this is just the beginning. These initiatives should guarantee the ongoing safety and viability of Uzbekistan's digital economy.
Keywords: Information security, cybersecurity, Uzbekistan, digitalization, biometric authentication, cyberattacks, data protection.

Introduction

Nowadays, the question of information security has gained seriousness with the increasing reliance of societies and economies on digital technologies. The inordinate popularity of information technology and the internet, as well as the wide-ranging data exchange have made protection of digital

information a major issue. Historically, data security largely focused on keeping classified materials and sensitive messages safe. With the penetration of digital technologies into society, security has become much more diverse than that now including personal data protection, intellectual property protection, financial operations and even national security. The explosive growth in cyber threats- penetrative hacking, malware epidemics, data breaches, cyber espionage- has created an even sharper need for strong information security systems.

The threats to data security have evolved significantly over time. In the early stages of the digital era, the biggest concern was that physical documents would be stolen or illicitly copied. Today, but companies are also faced with threats on a larger scale in the form of cyber-attacks against entire information systems. Such attacks typically result in unauthorized access, modification, destruction or theft of information stored on computers[1]. Accelerated growth in connecting everything, cloud-inspired software innovation and growing infrastructure complexity is creating new attack surfaces. What's more, cyber-attackers are increasingly sophisticated as they leverage tactics like phishing, ransomware and social engineering to exploit vulnerabilities in cybersecurity systems. Thus the information security domain is progressive in order to adapt to the new threats.

To deal with these increasing threats, information security has been addressed from two main perspectives: technical measures; and a legal framework. Technologically, numerous security tools have been developed such as firewalls, cryptographic algorithms, intrusion detection systems (IDS) and biometric authentication systems. Such devices exist in order to secure data that is sensitive and protect its integrity, as well as the confidentiality of communications. While legal systems are developed in response to concerns about data protection, privacy and control of digital systems. Laws, like the GDPR in Europe, try to set up a legal framework people's data. [2] These dual technical and legal strategies are the basis of current information security practices.

Over time, considering the rapid development of digital economy in Uzbekistan, issues of information security have also become paramount. As many industries, government, healthcare, finance, and education among others rely on the internet as well as digital technology hereopear the problematic phenomenon of Cyber threats. In reaction, the Uzbekistan government has adopted several measures to strengthen the national information security structure. New legislation has been introduced to help safeguard national infrastructure, our personal data and commercial secrets against a worldwide rise in cyber attacks. Nevertheless, the country is confronted with obstacles like deficiency of solid security culture, inadequate training for IT professionals and more advanced level of technology to face modern cyber threats. The paper is devoted to an analysis of information security level in Uzbekistan, evaluation of the TBS and recommendation on practical ways and measures how TBS can be improved in Uzbekistan.

Literature Review

Information security has long been an interest of study and discussion, here especially as advances in technology continue to expose new potential areas of vulnerability. Scholars argue how important it is to protect information in today's digital environment. For example, Anderson and Moore [describe the transition of threats to information security from physical to digital growing in both technical and legal dimensions, imply that a comprehensive cyber-security plan involves employing technological solutions as well as adopting appropriate laws[3]. Furthermore, research by Smith and Bishop indicate that information security issues are also vital to safeguarding critical national infrastructure, as they claim "Information security is not exclusively a technological issue

but is important for national security"[4]. These works pave the way for considering the multi-faceted aspects of information security and its importance in protecting digital as well as non-digital systems.

In Uzbekistan, data information security have been given importance recently and there is on-going legislative and policy initiatives targeting the enhancing of country's cyber security infrastructure. Scholars such as Karimov and Ismailov discuss the effects of digitalization on security in Uzbekistan, focusing on threats arising from growing numbers of cyber risk[5]. In addition, Jalilov s study is evidence of the importance to apply international best practices with respect to information security management in order to reducing the threats related to data breach and cyber-attack[6]. These studies provide valuable insights on the particular security issues facing Uzbekistan, particularly as it undergoes a digital transition. Research gaps to the current work are complemented by findings and suggestions from these works, which help shape a common understanding of the context, as well as enabling an argueable basis for evaluating what has been done in bolstering information security efforts within Uganda.

Methodology

This study is implemented using mixed methods to evaluate information security in Uzbekistan in the context of biometric-based authentication systems and its relevant security technologies. The mixed-methods approach helped to collect both qualitative and quantitative data for a better understanding of IK violation.

Survey and interview with 150 IT people, cyber experts and policy makers has been taken as primary data. Recursive interviews were used to obtain in-depth understanding of security problems and solutions, while the surveys produced only quantitative data about patterns and effects-of-use as well as reuse of biometric technology and other technologies for security. Quote secondary information was derived from academic papers, government reports and any other related source available to put thigs in perspective.

Qualitative interview and open-ended survey data were thematically analyzed to delineate themes that related to security technologies. Quantitative data were descriptively analyzed and correlation made to express trends and relationships existing among variables.

Case studies of few selected organizations have also been carried out to explore the real life practices of biometric systems in terms of integration issues and security results.

Ethical consideration This study adhered to ethical principles aimed at ensuring participant voluntariness, protecting participant privacy and obtaining informed consent from the participants.

Results

The findings of the study in relation to the use and importance of information security solutions and technologies in Uzbekistan are discussed in this section, concerning with popular cybersecurity approaches which would be reasonable both from compliance requirement and technical feasibility. The results indicated that the advent of digital technologies has increased information security program requirements among a variety of industries but seems most apparent in corporations, where cyber-related attacks are becoming relatively familiar. Demand for robust Information security measures has increased Digitalization spreads, as confirmed by the rising utilization of Information Security Software.

Amongst the findings, use of basic cybersecurity measures are being widely used (such as login and password systems which are critical to protecting user data). 95% of Uzbek organizations have implemented login authentication systems, which are significant in securing access to sensitive information[7]. Adoption of such fundamental IT security practices is important as the nation

proceeds with its digital transformation. This is further proof that Uzbekistan has advanced in terms of its cybersecurity readiness over the past few years, primarily thanks to stricter legislative frameworks and the formulation of national policy documents related to cybersecurity. In particular, the promulgation of laws and regulations on privacy protection of person information, and the setting up of specialized agencies for information security are essential to strengthen the cybersecurity infrastructures.

The study also found that the volume of cyber incidents such as hacking and phishing is rising. In 2019 first quarter, more than 200 cyberattacks were recorded. Nevertheless, the study reported that the impact of these attacks decreased at the end of 2020 due to stronger defensive measures among which: strengthened firewall solutions and improved antivirus security protocols [8]. The analysis also noted the need to remain on guard, as new forms of cyberattacks - in particular, ransomware - are proliferating at a staggering pace. With proactive government intervention in the way of these threats, key sectors and institutions such as the Central Bank and the Ministry of Justice has seen its level of safeguarding improved with them seated among the creme-de-le-creme organizations around with regards to cyber defense.

In addition, the study also showed that information security practices were integrating biometric authentication systems. such systems, which are more secure than classical ones, are now widely used in the public and private sectors[9]. The addition of biometric validation was also remarked upon as a step to improve data security and prevent access by unauthorized personnel. This suggests that these types of technologies are effectively addressing the risks associated with unauthorized loss of data, although practical and technical issues still need to be resolved before being thus widely adopted.

The research also looked at cybersecurity in Uzbekistan by and large, stating that the Government has made significant efforts to enhance its cybersecurity readiness. The creation of the National Cybersecurity Center and the ongoing work to better cyber information security standards has been very helpful for a country vulnerable to cyber attacks. These new initiatives, together with the implementation of international cybersecurity guidelines, should help to improve further Uzbekistan’s capacity to tackle new cybersecurity threats. Yet, the findings indicate that additional cybersecurity preparedness by both citizens and private institutions is required to adequately protect the digital infrastructure of Uzbekistan[10].

In summary, conclusions of the research emphasize the growing role of information security in Uzbekistan, especially when rapid digitalization takes place. Although much headway has been made to achieve enhanced cybersecurity, work remains in order to combat the latest threats and maintain security of sensitive information in key industrial sectors. The findings underscore the importance of both technical and legal measures in determining its cybersecurity ecology and resilience against new cyber threats.

Discussion

The findings of the study imply certain achievements in information security state in Uzbekistan which were adopted due to growing requirements for digitization and the scale of cyber threats surge. One of the principal results is the exposure of a stronger regulatory environment for information security that has been emerging in Uzbekistan. New cybersecurity laws and regulations, specifically those related to protection of personal data have had a huge impact on developing the nation's security overall[11-12]. The institutional basis has been further enhanced through the establishment of key national institutions such as the National Cybersecurity Center coordinating information security efforts between public and private entities.

Another interesting revelation is that different organizations are also heavily relying on different cyber-security tools and elements. The study has indicated that basic security procedures such as a login authentication system (successful in protecting users personal data) have been introduced into 95% of all Uzbek companies[13]. And these measures formed an important part of the country's improved security situation. But despite these improvements, the research showed that the threat of attack remains strong, particularly from more advanced threats – such as ransomware and phishing attacks. Over 200 cyber attack cases were reported just in the first quarter of 2020, but its total influence declined at the end of year due to implementation of better security system[14],[15].

Conclusion

Conclusion Uzbekistan has come a long way to develop its Information Security infrastructure thanks to the new technologies and comprehensive legislative reforms. The country's effort to improve cybersecurity is reflected in the creation of dedicated legislation as well as government-led initiatives intended to protect digital infrastructure. Yet despite its efforts, the country still faces significant threats — most notably the increase of sophisticated cyber threats and attacks that could hamper a blossoming digital economy. The research also highlights the importance of ongoing diligence in keeping up-to-date with cyber security policies and practices.

Adoption of the best global practices with active cooperation with world-leading IT security organizations will be essential to counter new threats." What's more, the investment in education and training of talent and specialists as well as raising public awareness on cyber risks are important for building a healthy and secure digital environment. To ensure the resilience of the country's information systems, there are increasingly requirements in place for measures to manage risks effectively as well for enhanced cooperation between public and private sectors. From now on, it is necessary to pursue a policy of a well-though balance between the further development and protection of Uzbekistan's digital environment by enhancing legal and technological base, reliable information security systems and proactive coordination.

REFERENCES:

[1] R. Anderson and T. Moore, "The Economics of Information Security," *Science, Technology, & Human Values*, vol. 31, no. 2, pp. 104-119, 2006.

[2] R. E. Smith and P. Bishop, *Cybersecurity: Protecting Critical Infrastructures from Cyber Threats*, New York: Wiley & Sons, 2015.

[3] R. Karimov and F. Ismailov, "Digitalization and Information Security in Uzbekistan: Challenges and Solutions," *Journal of Information Security*, vol. 6, no. 3, pp. 45-57, 2019.

[4] O. Jalilov, "Adoption of International Best Practices in Cybersecurity: A Case Study of Uzbekistan," *Uzbekistan Journal of Cybersecurity*, vol. 12, no. 1, pp. 78-92, 2020.

[5] S. Kumar and A. Singh, "Cybersecurity Challenges in Developing Economies: A Case Study of Uzbekistan," *International Journal of Information Security*, vol. 14, no. 4, pp. 123-134, 2018.

[6] J. Brown and L. White, "The Role of GDPR in Enhancing Data Protection in Central Asia," *Cybersecurity and Privacy Law Review*, vol. 7, pp. 55-70, 2019.

[7] J. Smith and L. Zhao, "Biometric Authentication in the Private Sector: A Case Study in Uzbekistan," *International Journal of Biometric Systems*, vol. 12, no. 2, pp. 87-96, 2020.

[8] H. Clark and R. Patel, "The State of Cybersecurity in Uzbekistan: Emerging Threats and Protective Measures," *Journal of Cybersecurity Studies*, vol. 10, no. 3, pp. 233-245, 2021.

[9] M. Jackson and G. Williams, "Cybercrime and Countermeasures in Uzbekistan's Digital Economy," *Journal of Digital Security*, vol. 5, no. 1, pp. 99-112, 2018.
[10] P. Garcia and A. Lopez, "Global Cybersecurity Practices and Their Applicability to Uzbekistan," *Journal of International Cyber Law*, vol. 4, pp. 123-134, 2019.
[11] E. Hasanov and R. Turdikulov, "The Development of Cybersecurity Frameworks in Uzbekistan: A Progress Report," *Uzbekistan Journal of Information Technology*, vol. 9, no. 2, pp. 58-70, 2021.
[12] J. Wright and Y. Chen, "The Role of Firewalls in Strengthening Cyber Defenses in Uzbekistan," *Network Security Journal*, vol. 15, no. 4, pp. 220-230, 2020.
[13] T. Stewart and D. Martin, "Building National Cybersecurity Infrastructure: Lessons from Uzbekistan," *Global Cybersecurity Review*, vol. 8, pp. 77-89, 2021.
[14] K. Shah and P. Kumar, "Ransomware and Phishing: Emerging Threats to Uzbekistan's Information Systems," *International Journal of Cyber Defense*, vol. 19, no. 1, pp. 45-55, 2022.
[15] F. Ahmad, "Cybersecurity Awareness and Training in Uzbekistan: Current Status and Future Challenges," *Journal of Cybersecurity Education and Practice*, vol. 3, no. 1, pp. 56-69, 2021.