ISSN NO: 2769-996X
Date of Publication: 07-05-2023

Understanding of Human Factors and Impact in Cybersecurity

Djurayev Musurmon Avlakulovich
Associate professor of the department of Mechanical Engineering,
Tashkent State Technical University named after Islam Karimov, Tashkent, Uzbekistan
Tuyboyov Oybek Valijonovich
Associate professor of the department of M echanical Engineering,
Tashkent State Technical University named after Islam Karimov, Tashkent, Uzbekistan
justoybek86@gmail.com
Rakhmonov Gayrat Ismatulloyevich
Department of Management and Marketing,
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
Tashkent, Uzbekistan.
raxmonovgayrat82@gmail.com

Abstract: In the mobile and digital age, technological advancements have provided numerous benefits in terms of information dissemination, education, remote work, and leisure activities. However, these advancements also bring the risk of data breaches and cyber threats at both individual and organizational levels. The ever-evolving nature of cyber threats highlights the importance of considering human factors in cybersecurity. This article provides an overview of the topic's significance and explores the common risks and impacts in the cybersecurity field. It further emphasizes the role of human factors in security and delves into behavioral approaches. The article concludes by stating the intention to conduct research on behavioral science theories to better understand the influence of human factors in cybersecurity.

Keywords: Cybersecurity, Risk, Human Factor, Human errors.

1.Introduction

As society becomes increasingly reliant on technology, it also becomes more vulnerable to cybercrime. This vulnerability has been highlighted during the COVID-19 pandemic, where healthcare organizations have become prime targets, leading to a five-fold increase in cyberattacks. Critical situations present ideal opportunities for cybercriminals, as they can exploit the weakest link in security: the human factor. In times of fear and uncertainty, individuals may become more susceptible to scams due to their lack of awareness, carelessness, and limited access to information [1-5]. Cybercriminals leverage these human factors to gain unauthorized access, steal credentials, and infect systems with malware. One alarming aspect of cyberattacks is their rising prevalence. Unlike physical attacks, cyberattacks are relatively inexpensive, not bound by geographical constraints, and difficult to trace and identify. Consequently, they have become more attractive and dangerous than their physical counterparts. Furthermore, malicious programs used in cyberattacks can be repurposed to target additional systems, multiplying the potential damage.

Overall, the increasing reliance on technology coupled with the exploitation of human factors in cybercrime poses a significant threat to individuals, organizations, and even society as a whole. It is crucial to raise awareness, promote cybersecurity education, and implement robust security measures to mitigate these risks and protect against cyber threats. In response to the evolving hacking methods employed by attackers, cybersecurity measures are continuously developing to combat a wide range of attack types [4]. Various approaches are used to enhance threat detection, including multi-factor authentication (MFA), Network Behavioral Analysis (NBA), Threat Intelligence, automatic updates, real-time protection, sandboxing, forensics, back-up and mirroring, and Web application firewalls.

However, despite these advancements, the increasing centralization of user data and personal information, as well as the availability of up-to-date data, have made social networking platforms an attractive target for both legitimate organizations and malicious actors. Additionally, the proliferation of the Internet of

ISSN NO: 2769-996X
Date of Publication: 07-05-2023

Things (IoT) and the ongoing digitalization of various aspects of life have created more opportunities for cybercriminals to exploit vulnerabilities [5-8]. Consequently, security remains a critical concern for individuals and organizations alike. It is essential for individuals and organizations to prioritize cybersecurity measures and stay vigilant against potential threats. This includes regularly updating security systems, implementing strong authentication practices, monitoring network behavior, leveraging threat intelligence, and maintaining backups of important data. By adopting a proactive approach to cybersecurity, we can mitigate risks and protect sensitive information from malicious attacks.

2. Risks and Impacts in Cyber World

In the literature, there are various definitions of information security. However, the most widely recognized and influential model is the CIA security model, which was first mentioned in a publication by the National Institute of Standards and Technology (NIST) and is also referenced in the ISO/IEC standards (2018). The CIA security model is based on a triad of three fundamental elements that are essential for achieving comprehensive information security [3-9]. These elements are:

1. Confidentiality: Confidentiality ensures that sensitive information is protected from unauthorized access. It involves measures such as encryption, access controls, and data classification to prevent unauthorized individuals or entities from viewing or obtaining confidential data.
2. Integrity: Integrity ensures that information is accurate, complete, and unaltered. Measures like data validation, checksums, and digital signatures are implemented to detect and prevent unauthorized modifications, corruption, or tampering of data throughout its lifecycle.
3. Availability: Availability ensures that authorized users have timely and uninterrupted access to information and resources when needed. It involves measures such as redundancy, disaster recovery planning, and system resilience to ensure that systems and services remain operational and accessible, even in the face of disruptions or attacks.

These three elements of confidentiality, integrity, and availability form the core principles of the CIA security model. By addressing these aspects comprehensively, organizations can establish a robust framework for protecting their information assets and mitigating potential risks and vulnerabilities.

It's worth noting that there are other models and frameworks beyond the CIA model that provide additional dimensions and perspectives on information security, such as the extended CIA model (including authenticity, accountability, and non-repudiation) and the ISO/IEC 27001 standard, which provides a comprehensive approach to information security management systems [7].

When an attack is successfully executed, it has the potential to undermine the fundamental principles of confidentiality, integrity, and availability in information security. Theft and espionage can lead to significant losses of financial, proprietary, and personal information. The extent of risk reduction required varies across different sectors and organizations. For example, customer expectations for cybersecurity may be lower for a company operating in the entertainment industry compared to those for a hospital, bank, or government agency, which handle more sensitive data and have stricter security requirements.

To enhance our understanding of cyber risks and their implications, we utilize a classification system for categorizing malware and system vulnerabilities. This categorization enables us to better identify and analyze the various types of threats that exist. By organizing malware into distinct categories, such as viruses, worms, Trojans, ransomware, and spyware, we can develop targeted strategies for prevention, detection, and response. Similarly, identifying and categorizing system vulnerabilities, such as software flaws, misconfigurations, weak authentication mechanisms, and outdated security patches, allows us to prioritize and address these vulnerabilities effectively, thereby strengthening overall security measures.

2.1. Malware

In the present day, malware attacks are primarily utilized to illicitly obtain personal, business, and financial information for the benefit of malicious actors. These attacks commonly target government entities and organizational websites with the intent to disrupt operations or gather sensitive data. Additionally, attackers employ malware to steal individuals' personal information, including credit card numbers [10]. The widespread availability and convenience of Internet access have contributed to the increased usage of malware for profit-driven purposes. Cybersecurity experts are actively working to address the challenges posed by cybercrime and recognize the significant role that malware plays in the realm of cybersecurity.

ISSN NO: 2769-996X
Date of Publication: 07-05-2023

Malware attacks involve the surreptitious loading of malicious software onto a system without the knowledge or consent of the legitimate owner, with the aim of breaking or compromising the targeted system. The most prevalent forms of malware include viruses, worms, spyware, and bot executables. Hackers employ various methods to infect systems, such as directly targeting vulnerable machines, employing social engineering techniques to manipulate users into opening infected files, or convincing them to visit enticing websites [11-15]. Many of these malware strains are designed to gain control over victims' computers for nefarious purposes, including sending spam emails or monitoring users' web browsing behavior for exploitation in the black market. The most common categories of malware attacks can be classified as follows:

1. Spam: This type of malware involves the dissemination of irrelevant, inappropriate, and unsolicited messages to a list of recipients. In the second quarter of 2021, corporate accounts were particularly enticing targets for cybercriminals.
2. Phishing: Phishing attempts refer to the fraudulent practice of attempting to obtain users' credentials or bank account details by impersonating trusted entities. Cybercriminals have taken advantage of the COVID-19 pandemic, seeking to harvest account credentials and exploiting pandemic-related themes. They employ tactics such as embedding links in emails, perpetrating scams, and imitating emails from popular cloud services. Phishing methods often employ technical deception, such as creating email links and spoofed websites that mimic legitimate organizations.
3. Downloads: Drive-by downloads are a method employed by attackers to rapidly spread malware. These attacks do not require direct communication between the targeted endpoints and company servers. Users can inadvertently trigger these attacks by visiting a website while viewing an email message or clicking on deceptive pop-up windows. Research indicates that an increasing number of web pages have been infected, and various types of malware have been discovered. When a user visits a malicious website, malware is downloaded and automatically installed on the victim's machine without their knowledge.

2.2. System Vulnerabilities

When malware infiltrates a system, cybercriminals exploit existing vulnerabilities in various aspects of the system, including hardware, software, network infrastructure, and protocols. Hardware: The manipulation of hardware is considered a potent method for launching security attacks. Detecting hardware attacks is challenging due to the lack of adequate tools, leading to an increase in such attacks. Trojans are commonly used as hardware exploits, intentionally designed to compromise the integrity circuits in the hardware [16-19]. For example, a trojan embedded in the system's hardware can manipulate error detection modules to accept unauthorized inputs. It can also introduce additional buffers in chip interconnections, resulting in increased power consumption and reduced battery efficiency. Denial-of-Service (DoS) Trojans can disrupt specific functions or resources, depleting bandwidth, computation, and battery power. In some cases, these attacks can physically damage or alter the configuration of devices, such as control systems used in machinery like centrifuges, generators, and pumps.

Software: Cyber-attacks often leverage software errors, flaws, or faults in computer programs, including the operating system, external interface drivers, and applications. These issues, commonly referred to as bugs, enable attackers to manipulate systems and deviate from their intended behavior. Research has shown that many attacks exploit software vulnerabilities resulting from bugs and design flaws. Common areas of vulnerability include memory, user input validation, and user access privileges. Buffer overflow is a technique used by cybercriminals to disrupt existing process code [20]. Buffers are intended to store a limited amount of data, but when they contain excess information, it can overflow into adjacent memory, corrupting or overwriting valid data. Attackers can exploit this to interfere with the code execution and achieve their objectives. Another concern is the input validation process, which ensures that input data adheres to specific rules. Incorrect data validation can lead to data corruption, such as SQL injection, where a cybercriminal injects SQL commands from the web to manipulate a target database's content or gain access to sensitive information like passwords or credit card details.

Network infrastructure and protocols: Common network attacks exploit vulnerabilities in Internet Protocol (IP), Transmission Control Protocol (TCP), and Domain Name System (DNS). Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols were developed to provide secure communication between computers over TCP. The DNS protocol translates human-readable hostnames into 32-bit IP

ISSN NO: 2769-996X
Date of Publication: 07-05-2023

addresses, enabling routers to direct packets to the correct destination. However, DNS replies are not authenticated, allowing attackers to send malicious messages and gain unauthorized access to Internet servers. A successful attack on DNS can severely disrupt Internet communication [21-25]. Consequently, DNS has become a frequent target of Denial-of-Service attacks (DoS), which overwhelm web servers, networks, and systems with excessive traffic, rendering them inaccessible to legitimate users.

3. The Importance Of Human Factors

The importance of human factors in cybersecurity cannot be overstated. Despite the advancements in technology and information sciences, securing systems, services, organizations, and information relies heavily on human factors. If security holes are overlooked by process designers, IT systems can become weak and susceptible to repeated exploitation by attackers. Therefore, cybersecurity threats cannot be adequately addressed by focusing solely on technical issues.

Individuals are the ones who operate computers and interconnected devices, making the security of these devices and environments a matter of human and organizational factors. The adoption of security technologies alone has often failed to protect organizations from cyberattacks. Human and organizational factors are closely linked to computer and information security vulnerabilities (CIS). These factors can be classified into areas such as external influences, human error, management, organization, performance and resource management, policy issues, technology, and training.

Two major groups of factors have been identified: those belonging to the user and those belonging to management. User-related factors include risky behavior, belief systems, lack of motivation, and inadequate use of technology. Management-related factors include workload and inadequate staffing. People may deny the use of security technologies, fail to follow security protocols, engage in harmful activities, and underestimate the likelihood of falling victim to a cybersecurity breach. Understanding the role of human factors in cybersecurity is crucial due to these challenges.

Human factors significantly influence people's interaction with information security, introducing various risks. Human weaknesses can inadvertently lead to harm for an organization, but increasing awareness levels can help mitigate these weaknesses. Security solutions that focus solely on hardware and software have been found to be ineffective. To develop effective cybersecurity measures, an integrated human factors methodology is essential. Studying user behaviors that contribute to security risks is of great interest, and mobile device security solutions should prioritize understanding user behavior rather than purely technical issues.

Studies comparing the security behaviors of college students and IT professionals have shown that both groups often fail to properly secure their mobile devices, putting themselves at risk. Aligning user behavior with security practices is crucial for mitigating security issues. Research has suggested monitoring the applications used and installed on devices and implementing authentication tokens as effective data security measures. However, there is still a lack of research on users' security behaviors and their correct application.

Decision-makers in IT security may prioritize out-of-pocket losses over making the right decision in terms of security. Considering all costs in the IT security field as opportunity costs is important. Organizations implement measures, yet accidents and security breaches continue to occur. Training programs and awareness initiatives are being integrated, but more work is needed. Human behavior is purpose-driven, aiming to adapt to systems and external conditions. Understanding what is considered better in terms of security and ensuring that individuals know, understand, and apply it correctly is essential.

When analyzing the human side of cybersecurity, cultural differences should also be considered. Some societies perform better than others, with trust levels and social virtues differing between nations. Therefore, it is necessary to take into account and work with the human side and its influencing factors to achieve better cybersecurity outcomes.

4. Conclusions

In conclusion, the rapid advancement of technology has increased our reliance on information technology, making cyber-attacks more appealing to malicious actors. While some attacks may have minimal impact, those targeting critical infrastructure can have severe consequences for national security, the economy,

ISSN NO: 2769-996X
Date of Publication: 07-05-2023

and the safety of individuals. Therefore, infrequent successful attacks with significant impacts pose a greater risk than ordinary attacks with lower influence.

Our research has highlighted the crucial role of human factors in cybersecurity. It has been established that technology alone cannot fully address the complexity of cyber-attacks. We have identified human weaknesses that contribute to security issues and emphasized that understanding the human side is essential in mitigating security risks associated with human behavior. To address these challenges, it is proposed that collaboration among private organizations, public entities, and academia is necessary. By working together, these stakeholders can cultivate positive security behaviors and promote a culture of cybersecurity. This collaboration can help bridge the gap between technological solutions and the human factors that influence cybersecurity.

In conclusion, recognizing the importance of human factors, alongside technological solutions, is vital in effectively managing cybersecurity risks. The collaboration between private, public, and academic sectors is key to fostering positive security behaviors and enhancing overall cybersecurity posture. By understanding and addressing human characteristics, we can better protect ourselves and our critical systems from cyber threats.

Referance

1. Rajaboevich, G. S., Baxtiyarovich, N. N., & Salimovna, F. D. (2020, November). Methods and intelligent mechanisms for constructing cyberattack detection components on distance-learning systems. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
2. Bakhodir, Y., Nurbek, N., & Odiljon, Z. (2019). Methods for applying of scheme of packet filtering rules. International Journal of Innovative Technology and Exploring Engineering, 8(11), 1014-1019.
3. Safoev, Nuriddin, and Jun-Cheol Jeon. "Area efficient QCA Barrel shifter." *Advanced Science and Technology Letters* (2017): 51-57.
4. Safoev, Nuriddin, and Jun-Cheol Jeon. "Full adder based on quantum-dot cellular automata." *Proceedings of international conference of trends in engineering and technology*. 2017.
5. Safoev, N., and J. C. Jeon. "Reliable design of reversible universal gate based on QCA." *Advanced Science Letters* 23.10 (2017): 9818-9823.
6. Safoev, Nuriddin, and Jun-Cheol Jeon. "Coplanar QCA adders for arithmetic circuits." *International Journal of Engineering & Technology* 7.4.4 (2018): 15-16.
7. Gulomov, S. R., & Bakhtiyorovich, N. N. (2016, November). Method for security monitoring and special filtering traffic mode in info communication systems. In 2016 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.
8. Malikovich, K. M., Rajaboevich, G. S., & Karamatovich, Y. B. (2019, November). Method of constucting packet filtering rules. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
9. Насруллаев, Н. Б., & Файзиева, Д. С. (2020). Анализ средств службы информационной безопасности в дистанционном обучении. Молодой ученый, (31), 14-18.
10. Baxtiyorovich, N. N., & Ubaydullaevna, H. I. (2019, November). Method of analyzing of antivirus errors when audit provides. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-3). IEEE.
11. Safoev, N., and J. C. Jeon. "Peres gate realization in QCA for reversible binary incrementer." *Advanced Science Letters* 23.10 (2017): 9812-9817.
12. Komil, T., & Nurbek, N. (2015). Development method of code detection system on based racewalk algorithm on platform FPGA. In Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE) (p. 278). International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE).
13. Safoev, N., & Nasrullaev, N. (2021, November). Low area QCA Demultiplexer Design. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 01-05). IEEE.

ISSN NO: 2769-996X
Date of Publication: 07-05-2023

14. Yakubdjanovna, I. D., Bakhtiyarovich, N. N., & lqbol Ubaydullayevna, X. (2020, November). Implementation of intercorporate correlation of information security messages and audits. In 2020 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
15. Cohen, M. I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. digital investigation, 8, S101-S110.
16. Mrdovic, S., Huseinovic, A., & Zajko, E. (2009, October). Combining static and live digital forensic analysis in virtual environment. In 2009 XXII International Symposium on Information, Communication and Automation Technologies (pp. 1-6). IEEE.
17. Hay, B., Bishop, M., & Nance, K. (2009). Live analysis: Progress and challenges. IEEE Security & Privacy, 7(2), 30-37.
18. Wang, L., Zhang, R., & Zhang, S. (2009, December). A model of computer live forensics based on physical memory analysis. In 2009 First International Conference on Information Science and Engineering (pp. 4647-4649). IEEE.
19. Alazab, M., Venkatraman, S., & Watters, P. (2009, June). Digital forensic techniques for static analysis of NTFS images. In Proceedings of ICIT2009, Fourth International Conference on Information Technology, IEEE Xplore.
20. Sherzod Rajaboevich, G., Dilmurod Gulamovich, A., & Nurbek Bakhtiyorovich, N. (2019). Method for determination of the probabilities of functioning states of information of protection on cloud computing. International Journal of Mechanical Engineering and Technology, 10(3).
21. Safoev, N., and J. C. Jeon. "Cell interaction based QCA multiplexer for complex circuit design." *Advanced Science Letters* 23.10 (2017): 10097-10101.
22. Shakarov, M., Safoev, N., & Nasrullaev, N. (2022). Обеспечение безопасности интернет вещей в промышленности 4.0 с использованием WAF. Research and Education, 1(9), 386-393.
23. Насруллаев, Н., Муминова, С., Сейдуллаев, М., & Сафоев, Н. (2022). Внедрение DMZ для повышения сетевой безопасности веб-тестирования. *Scientific Collection «InterConf»*, (110), 641-649.
24. Rajaboevich, G. S., Baxtiyorovich, N. N., & Komilovich, T. S. (2021, November). A model for preventing malicious traffic in DNS servers using machine learning. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-4). IEEE.
25. Safoev, N., and J. C. Jeon. "Low complexity design of conservative QCA with two-pair error checker." *Advanced Science Letters* 23.10 (2017): 10077-10081.