Mesopotamian journal of Cybersecurity
Vol.2023, **pp**. 1–6
DOI: https://doi.org/10.58496/MJCS/2023/001; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Review Article

The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment

Maad M. Mijwil[1,*], Youssef Filali[2], Mohammad Aljanabi[3], Mariem Bounabi[2], Humam Al-Shahwani[4]

[1] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[2] *Department of Computer Science, Faculty of Sciences Dhar-Mahraz, University of Sidi Mohamed Ben Abdellah, Fez, Morocco*

[3] *Department of Computer, College of Education, Aliraqia University, Baghdad, Iraq*

[4] *Computer Science Department, College of Science, University of Baghdad, Baghdad, Iraq*

[5] *Open AI L.L.C., 3180 18th Street, San Francisco, CA 94110, USA*

ARTICLE INFO

Article History
Received 18 Dec 2022
Accepted 17 Jan 2023

Keywords
Cybersecurity
Digital transformation
Artificial intelligence
Governance
Cybercrime
ChatGPT

ABSTRACT

The process of digital transformation is considered one of the most influential matters in circulation at the present time, as it seeks to integrate computer-based technologies into the public services provided by companies or institutions. To achieve digital transformation, basics and points must be established, while relying on a set of employee skills and involving customers in developing this process. Today, all governments are seeking electronic transformation by converting all public services into digital, where changes in cybersecurity must be taken into account, which constitutes a large part of the priorities of nations and companies. The vulnerability to cyberspace, the development of technologies and devices, and the use of artificial intelligence in the growth of modern applications have led to the acceleration of the digital transformation process and the utilization of its services. To adopt straightforward programs and strategies to establish cybersecurity governance that can be trusted and practical in completing tasks without hacking and tampering with data and information. In this article, the importance of cybersecurity governance is highlighted in providing safe and effective technical means that have the ability to face all threats and challenges and preserve the data of individuals in various sectors.

1. INTRODUCTION

The digital space provides resources and advanced technology that supports individuals to make more profitable use of digital services in fulfilling their life requirements and assists in growing companies and institutions and meeting all the needs of citizens on a daily basis. Digital transformation provides tremendous development in economic, social, and political development and the protection of human data and rights by developing specific methods in preserving data and not allowing it to be tampered with by unauthorized persons and combating cybercrime in all its forms, which enhances a safe and stable digital environment that serves all citizens [1][2]. Cybersecurity is one of the most influential priorities followed by companies and institutions in providing secure electronic environments by developing clear strategies and relying on artificial intelligence techniques [3]. Cybersecurity is a set of technologies and processes designed to protect networks and computers from attack and data theft and to prevent unauthorized access by developing procedures to achieve complete protection from cybercrime [4][5]. In addition, cyber security seeks to put in place organizational procedures to ensure the protection of information in all its physical and electronic forms from various crimes and to prevent the access of unauthorized persons to manipulate the data of companies or institutions and exploit weaknesses in the systems of these companies. Information and data are among the most significant things that a hacker seeks to access in order to control the system and exploit customers. The cyber security system consists of three essential elements: Cyber force [6],

cyber defence [7], and cyber deterrence [8]. The primary position of cybersecurity is to put in place mechanisms to defend the computer network, protect the electronic environment, and ensure the safe transfer of information between government

*Corresponding author. Email: mr.maad.alnaimiy@baghdadcollege.edu.iq

institutions and agencies without the presence of unauthorized persons or malware software aimed at controlling and manipulating the system [9-11]. In addition, it concentrates on providing real-time responses to prevent attacks and threats and providing a flawless electronic structure to organize communications between devices and software without any issues. Companies or institutions must provide a cyber deterrent against malicious actions by unauthorized persons or a group of malicious software (viruses) [12-15]. In fact, it is a strategy developed by companies and institutions to defend their systems and electronic environments through the use of artificial intelligence techniques that have the ability to train on the practices of malicious programs or the paths taken by hackers [16-20]. These techniques contribute to making the right decision in real-time while taking measures in the event of any attack or penetration of the digital environment. The main objective of this article is to conduct a survey on the governance of cybersecurity and digital transformation and their significance in creating a digital environment free of hacks and data theft and serving all citizens in organizing their life better based on artificial intelligence techniques.

2. CYBERSECURITY GOVERNANCE

Digital transformation is the process of converting anything into digital through the use of modern applications and devices and storing it in a computer or in other media, and it can be skillfully transferred or modified. Also, cloud computing is used to transfer and save digital data and information. The term digital transformation refers to discovering ways to transform business models into new digital ones, and it is widely employed in many companies and institutions. Here, the term digitization appears to us, which benefits companies in transforming all their businesses into a digital environment employing computer-based methods [21][22]. The digitization process aims to enhance production processes, increase business opportunities, develop companies and institutions, and increase material resources. The digital transformation process is one of the most important things that are implemented and gives great opportunities to complete tasks and strengthen work mechanisms and helps customers benefit from all services provided by companies or institutions. In addition, it saves cost and effort, enhances operational efficiency, organizes it, and creates innovative and creative procedures that contribute to improving companies and satisfying clients. Companies work to deliver their services through websites or mobile applications, and this leads to publishing information on the Internet while preserving the privacy of users. Therefore, these verses tempt many unauthorized people to try to access, steal or manipulate this data. Therefore, companies or institutions should evaluate the performance of their applications, find technical ways to protect them, and take appropriate decisions in updating them and eliminating existing defects. In fact, the process of transition to digitization requires a great effort and is more challenging than many yearn for, as companies are required to have highly qualified employees to achieve this process. Moreover, companies or institutions must constantly discover and search for modern technology, provide services that help clients, and build a digital system free of defects or gaps. Therefore, the existence of cybersecurity governance requires control over electronic systems and not allowing unauthorized persons to enter or the presence of malicious programs inside, as well as the use of artificial intelligence techniques in accomplishing these complex tasks. Companies must follow and implement the key elements of cybersecurity governance in their business (see Figure 1).

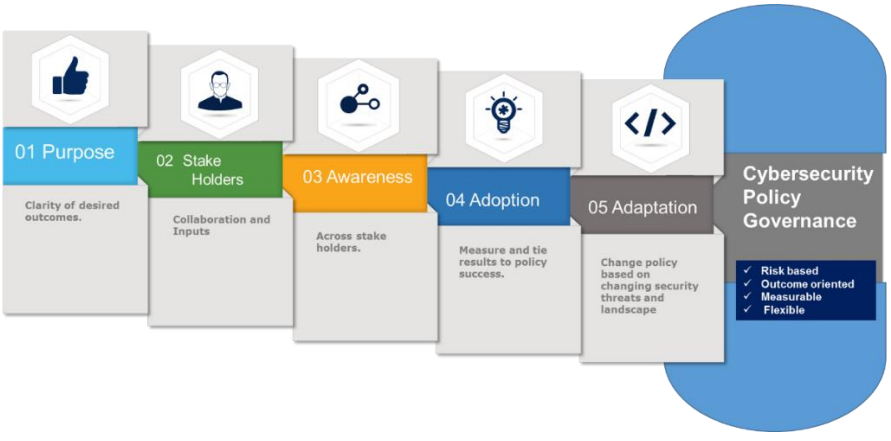

Fig. 1. Cybersecurity policy governance [23].

Cybersecurity governance is one of the means of managing information, organizing security systems applied within companies or institutions and preparing human resources to maintain the workflow in managing computer networks. It is an ongoing process that constitutes a large part of the culture of the company or organization and integrates risk management and sets conditions and strategies in achieving digital goals free from unauthorized operations by setting a set

of standards that must be followed within the institutions. In addition, the establishment of comprehensive security programs, the growth of security measures and controls within the organization, and the adoption of alternative plans to avoid the collapse of computers. There are many standards followed in the implementation of cybersecurity governance, the most famous of which is ISO/IEC 27001. This standard directs the company or institution to develop specific mechanisms for supervision, control, and mitigation of potential risks. It ensures the management of the implementation of all rules within the digital environment. Monitoring security services is one of the most meaningful measures followed in cybersecurity governance. Companies or institutions must be managed by reliable people who have sufficient experience in the process of managing the digital environment. Internet governance is considered one of the essential issues in cybersecurity governance, as it seeks to provide basic infrastructure and define Internet standards, mediation of information, and intellectual and property rights. These tasks are considered within the tasks of cybersecurity governance, with setting encryption standards, adopting regulations, correcting all security vulnerabilities in computer systems, and responding to security problems. In general, there is no effective and specific model for cybersecurity governance in organizing political, social, economic, and technical matters. Recent publications have confirmed that cybersecurity governance has many models for managing the digital environment and is controlled by technical experts or government agencies according to the standards applied in these models. Cyber governance relies on multiple patterns, including hierarchical patterns, which are distinguished for organizing tasks from top to bottom, and seek to search for the most common weaknesses in the system and try to control them. Other patterns make mechanisms work individually or collectively independently and obtain an application that is more suitable for the digital environment. Threats and penetration are in continuous development as companies and institutions seek to keep up with these penetrations and threats and know their behaviors and ways to combat them. Companies or institutions must put in place the necessary measures and anticipate the occurrence of a cyber-attack at any time. In addition, attention should be paid to artificial intelligence techniques, as they have a fundamental role in the development and growth of computer systems. These techniques had a significant and influential role in confronting the COVID-19 pandemic [24-26]. They proved to be powerful techniques in tracking the spread of the virus, predicting, and diagnosing cases of infection [27-32]. The digital environment is considered important in the economic development of countries through the establishment of digital cities that depend mainly on modern technologies in their management. Therefore, such cities require the presence of cybersecurity capable of deterring any attempt to penetrate or control them. Also, companies and institutions should constantly analyze cyber risks. When creating new models, all previous gaps they were exposed to must be addressed, with a mechanism for improving, monitoring, and measuring the performance of the work of all proposed models. Increasing awareness and adequate training on cybersecurity, because with training, a correct path has been reached in its performance within the digital environment.

3. THE IMPORTANCE OF CYBERSECURITY GOVERNANCE (by ChatGPT)

Cybersecurity governance is a critical aspect of an organization's overall risk management strategy. It involves the development and implementation of policies, procedures, and controls to protect the organization's information systems and data from cyber threats. This includes identifying and assessing risks, implementing technical and non-technical controls to mitigate those risks, and regularly reviewing and updating the organization's cybersecurity posture. Effective cybersecurity governance also requires active involvement from top management and clear communication throughout the organization to ensure that all employees understand their role in protecting the organization's assets. Additionally, compliance with laws and regulations is an important aspect of cybersecurity governance, as non-compliance can result in significant financial penalties and damage to an organization's reputation. Overall, a comprehensive and regularly reviewed cybersecurity governance program is necessary for organizations to effectively manage and mitigate the risks associated with cyber threats. Cybersecurity governance is the set of policies, procedures, and standards that an organization puts in place to ensure the protection of its information systems and data. It encompasses the management of both technical and non-technical controls to protect against cyber threats. This includes risk management, incident response planning, and compliance with laws and regulations. Effective cybersecurity governance requires the involvement of top management and a clear understanding of the organization's risk profile. It also involves regular review and updates to stay current with evolving cybersecurity threats and best practices. Effective cybersecurity governance involves implementing policies, procedures, and controls to prevent, detect, and respond to cybercrime. This includes identifying and assessing the organization's risk profile, implementing technical controls such as firewalls and intrusion detection systems, and implementing non-technical controls such as employee education and incident response plans. Additionally, compliance with laws and regulations related to cybersecurity is a critical aspect of cybersecurity governance, as non-compliance can result in significant financial penalties and damage to an organization's reputation. However, cybercrime is constantly evolving and becoming more sophisticated, so it's important for organizations to regularly review and update their cybersecurity governance program to stay current with evolving threats and best practices. This may include implementing advanced security technologies, regularly monitoring and reviewing logs and alerts, and conducting regular penetration

testing. Overall, a comprehensive cybersecurity governance program is necessary for organizations to effectively protect themselves from cybercrime and mitigate the risks associated with cyber threats. Some common themes that have emerged in the literature include the importance of involving top management and creating a culture of cybersecurity within the organization, the need for regular risk assessments and incident response planning, and the importance of compliance with laws and regulations. Many studies have also emphasized the need for a holistic approach to cybersecurity governance, which takes into account both technical and non-technical controls. This includes implementing technical controls such as firewalls and intrusion detection systems, as well as non-technical controls such as employee education and incident response plans. Additionally, there are many studies that focus on the importance of communication and collaboration within an organization to ensure that all employees understand their role in protecting the organization's assets. In the recent years, industry-specific frameworks, such as NIST, ISO 27001 and COBIT, have been proposed to provide guidance to the organizations on cybersecurity governance. These frameworks are widely adopted and recognized in different sectors. Overall, the literature on cybersecurity governance highlights the importance of a comprehensive and regularly reviewed program to effectively manage and mitigate the risks associated with cyber threats.

4. CONCLUSIONS

The massive growth of technology in all domains, especially information and communication technology, the diversity of electronic content and services, the presence of artificial intelligence, the Internet of Things and cloud computing, have led to positive industry development and enhanced interaction between companies and clients. At the same time, the emergence of cyber threats and risks, the development of malicious software that seeks to destroy data, and the development of spying and data theft mechanisms. Cybersecurity is one of the challenges that many governments face during the development of hacking operations, malicious software, and technologies that contribute to making gaps in computer networks. Spreading the culture of the concept of cybersecurity governance in companies and institutions because its absence leads to a lack of confidence in their applications and services. Relying heavily on artificial intelligence techniques in developing the digital environment and preserving data because these technologies have the ability to study the behavior of unauthorized persons and malicious programs. Relying on international standards in determining work mechanisms and satisfying from the experiences of other companies in applying standards and communicating with them. Not dealing with unreliable parties and always striving to conduct an evaluation of the work organization and involving clients in the evaluation process. In the future, more manuscripts will be made on the importance and effective role of artificial intelligence techniques in cybersecurity governance.

Conflicts Of Interest

authors declare no conflicts of interest.

Acknowledgment

Authors would like to thank the anonymous reviewers for their efforts.

References

[1] Rosário A. T. and Dias J. C., “Sustainability and the Digital Transition: A Literature Review,” *Sustainability*, vol.14, no.7, pp:1-18, March 2022. https://doi.org/10.3390/su14074072

[2] Brauner P., Dalibor M., Jarke M., Kunze I., Koren I., et al., “A Computer Science Perspective on Digital Transformation in Production,” *ACM Transactions on Internet of Things*, vol.3, no.2, pp:1-32, May 2022. https://doi.org/10.1145/3502265

[3] Agrawal S., Sahu A., and Kumar G., “A conceptual framework for the implementation of Industry 4.0 in legal informatics,” *Sustainable Computing: Informatics and Systems*, vol.33, pp:100650, January 2022. https://doi.org/10.1016/j.suscom.2021.100650

[4] Mijwil M. M., Sadıkoğlu E., Cengiz E., and Candan H., “Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme,” *Veri Bilimi*, vol.5, no.2 pp:97-105, December 2022.

[5] Mijwil M. M., Doshi R., Hiran K. K., Al-Mistarehi AH, and Gök M., “Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects,” *Mesopotamian journal of cybersecurity*, vol.2022, pp:1-4, 2022. https://doi.org/10.58496/MJCS/2022/001

[6] Ji-Young K., In L. J., and Gon K. K., "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," In Proceedings of International on Cyber Conflict, pp:1-6, Tallinn, Estonia, 28-31 May 2019. https://doi.org/10.23919/CYCON.2019.8756954

[7] Oreyomi M. and Jahankhani H., "Challenges and Opportunities of Autonomous Cyber Defence (ACyD) Against Cyber Attacks," In Blockchain and Other Emerging Technologies for Digital Business Strategies, pp:239–269, May 2022. https://doi.org/10.1007/978-3-030-98225-6_9

[8] Welburn J., Grana J., and Schwindt K., "Cyber deterrence with imperfect attribution and unverifiable signaling," *European Journal of Operational Research*, In press, July 2022. https://doi.org/10.1016/j.ejor.2022.07.021

[9] Skopik F., Settanni G., and Fiedler R., "A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing," *Computers & Security*, vol.60, pp:154-176, July 2016. https://doi.org/10.1016/j.cose.2016.04.003

[10] Gunduz M. Z. and Das R., "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol.169, pp:107094, March 2020. https://doi.org/10.1016/j.comnet.2019.107094

[11] Salem I. E., Mijwil M. M., Abdulqader A. W., Ismaeel M. M., Alkhazraji A., and Alaabdin A. M. Z., "Introduction to The Data Mining Techniques in Cybersecurity," *Mesopotamian Journal of Cybersecurity*, vol.2022, pp:28-37, May 2022. https://doi.org/10.58496/MJCS/2022/004

[12] Al Azzam S. B. N., "The AI algorithm for text encryption using Steganography," *Mesopotamian Journal of Cybersecurity*, vol.2020, pp:18-27, 2020. https://doi.org/10.58496/MJCS/2022/003

[13] Alwan A. H. and Kashmar A. H., "FCNN Model for Diagnosis and Analysis of Symmetric Key Cryptosystem," *Iraqi Journal For Computer Science and Mathematics*, vol. 4, no. 1, pp. 53–61, November 2022. https://doi.org/10.52866/ijcsm.2023.01.01.006

[14] Salem I. E., Salman A. M., and Mijwil M. M., "A Survey: Cryptographic Hash Functions for Digital Stamping," *Journal of Southwest Jiaotong University*, vol.54, no.6, pp.1-11, December 2019. https://doi.org/10.35741/issn.0258-2724.54.6.2.

[15] Sabah N., Sagheer A., and Dawood O., "Survey: (Blockchain-Based Solution for COVID-19 and Smart Contract Healthcare Certification)," *Iraqi Journal For Computer Science and Mathematics*, vol. 2, no. 1, pp. 1–8, January 2021. https://doi.org/10.52866/ijcsm.2021.02.01.001

[16] Venkatraman S., Alazab M., and Vinayakumar R., "A hybrid deep learning image-based analysis for effective malware detection," *Journal of Information Security and Applications*, vol.47, pp:377-389. August 2019. https://doi.org/10.1016/j.jisa.2019.06.006

[17] Aggarwal, K., Mijwil, M. M., Sonia, Al-Mistarehi, AH., Alomari, S., Gök M., Alaabdin, A. M., and Abdulrhman, S. H., "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," *Iraqi Journal for Computer Science and Mathematics*, vol.3, no.1, pp:115-123, January 2022. https://doi.org/10.52866/ijcsm.2022.01.01.013

[18] Li S., Li Y., Han W., Du X.,Guizani M., and Tian Z., "Malicious mining code detection based on ensemble learning in cloud computing environment," *Simulation Modelling Practice and Theory*, vol.113, pp:102391, December 2021. https://doi.org/10.1016/j.simpat.2021.102391

[19] Capuano N., Fenza G., Loia V., Stanzione C.," Explainable Artificial Intelligence in CyberSecurity: A Survey," *IEEE Access*, vol.10, pp:93575 - 93600, September 2022. https://doi.org/10.1109/ACCESS.2022.3204171

[20] Muhammad T. and Ghafory H., "SQL Injection Attack Detection Using Machine Learning Algorithm," *Mesopotamian journal of cybersecurity*, vol.2022, pp:5-17, 2022. https://doi.org/10.58496/MJCS/2022/002

[21] Mijwil M. M., Faieq A. K., and Al-Mistarehi AH., "The Significance of Digitalisation and Artificial Intelligence in The Healthcare Sector: A Review," *Asian Journal of Pharmacy, Nursing and Medical Sciences*, vol.10, no. 3, pp: 25-32, November 2022. https://doi.org/10.24203/ajpnms.v10i3.7065

[22] Mijwil M. M., Mutar D. S., Filali Y., Aggarwal K., and Al-Shahwani H., "Comparison Between Expert Systems, Machine Learning, and Big Data: An Overview," *Asian Journal of Applied Sciences*, vol.10, no.1, pp:83-88, March 2022. https://doi.org/10.24203/ajas.v10i1.6930

[23] Venu Y., "Cyber Security Policy considerations and Governance," *LinkedIn*, 2018. https://www.linkedin.com/pulse/cyber-security-policy-considerations-governance-venu-yedugondla/

[24] Mijwil M. M., Aggarwal K., Doshi R., Hiran K. K., Sundaravadivazhagan B. "Deep Learning Techniques for COVID-19 Detection Based on Chest X-ray and CT-scan Images: A Short Review and Future Perspective," *Asian Journal of Applied Sciences*, vol.10, no.3, pp:224-231, July 2022. https://doi.org/10.24203/ajas.v10i3.6998

[25] Ismael A. M. and Şengür A., "Deep learning approaches for COVID-19 detection based on chest X-ray images," *Expert Systems with Applications*, vol.164, pp:114054, February 2021. https://doi.org/10.1016/j.eswa.2020.114054

[26] Zhou T., Lu H., Yang Z., Qiu S., Huo B., and Dong Y., "The ensemble deep learning model for novel COVID-19 on CT images," *Applied Soft Computing*, vol.98, pp:106885, January 2021. https://doi.org/10.1016/j.asoc.2020.106885

[27] Jain R., Gupta M., Taneja S., and Hemanth D. J., "Deep learning based detection and analysis of COVID-19 on chest X-ray images," *Applied Intelligence*, vol. 51, pp:1690-1700, October 2020. https://doi.org/10.1007/s10489-020-01902-1

[28] Vaid S., Kalantar R., and Bhandari M., "Deep learning COVID-19 detection bias: accuracy through artificial intelligence," *International Orthopaedics*, vol. 44, pp: 1539-1542, May 2020. https://doi.org/10.1007/s00264-020-04609-7

[29] Wang L., Lin Z. Q., and Wong A.," COVID-Net: a tailored deep convolutional neural network design for detection of COVID-19 cases from chest X-ray images," *Scientific Reports*, vol. 10, no.19549, pp:1-12, November 2020. https://doi.org/10.1038/s41598-020-76550-z

[30] Mijwil M. M., Aggarwal K., Doshi R., Hiran K. K., and Gök M., "The Distinction between R-CNN and Fast R-CNN in Image Analysis: A Performance Comparison," *Asian Journal of Applied Sciences*, vol.10, no.5, pp:429-437, November 2022. https://doi.org/10.24203/ajas.v10i5.7064

[31] Fagbola T. M., Fagbola F. I., Aroba O. J., Doshi R., Hiran K. K., and Thakur S. C., "Smart Face Masks for Covid-19 Pandemic Management: A Concise Review of Emerging Architectures, Challenges and Future Research Directions," *IEEE Sensors Journal*, pp:1-6, December 2022. https://doi.org/10.1109/JSEN.2022.3225067

[32] Mijwil M. M., Salem I. E., and Ismaeel M. M., "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," *Iraqi Journal For Computer Science and Mathematics*, vol.4, no.1, In press, January 2023. https://doi.org/10.52866/ijcsm.2023.01.01.008