Cybersecurity Regulation and Governance

Amerah M. Alelayani, Fatimah M. Al Zahrani, Asmaa M. Munshi, Roaa M. Monshi and Shahad A. Al-sofyani

shahadalsofyani92@gmail.com

[1]Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

Abstract

This study discusses cybersecurity regulation and governance, as cybersecurity has become very important for government organizations, agencies, and companies, as well as for end users. Cybersecurity governance is needed by establishing a set of responsibilities and practices that are applied to provide strategic direction for cybersecurity, ensuring that cybersecurity objectives are achieved, and ascertaining that cyber risks are managed appropriately. In addition, we discuss the cybersecurity regulation and governance framework. Every country is responsible for establishing regulations which are a set of policies and standards that will protect the rights of citizens and their information in all electronic transactions and operations. We also discuss international cybersecurity laws and regulations in the European Union, Canada, and China. This is followed by a discussion of cybersecurity regulation and governance in Saudi Arabia. Subsequently, we discuss challenges for cybersecurity regulation and governance in managing data, responding to change, and defining risk posture. Finally, we highlight the importance of cybersecurity awareness and outline best practices for enhancing awareness and implementing the regulation process.

Key words:

Cybersecurity, CIA triad, Governance, Regulations, Policies, Standards, Laws

1. Introduction

With the development of the Internet and technology, more risks, challenges, and violations are arising. Many countries have become a victim of these violations, which make it necessary for the governments to implement cybersecurity and enforce policies, procedures, and strict punishments that are regulated by law. Cybersecurity covers all systems, technology, mechanisms, tools, measures, software, hardware, processes, protocols, policies, procedures, safeguards, guidelines, strategies, approaches, actions, training, assurance, and best practices that provide and preserve the basic security objectives, which are known as the CIA triad: Confidentiality, integrity, and availability. Confidentiality means the assets are only accessible by the authorized person, and these assets are protected against any disclosure. Integrity means ensuring assets are not being modified or manipulated. Availability means these assets exist when the authorized person requires them (Eugen and Petru, n.d.).

Cybersecurity has become the most critical issue in every country, and it has become a strategic war between many countries. Therefore, each government is keeping up with this trend by providing the appropriate defense regulations and policies, establishing a cybersecurity framework, adopting important control strategies and procedures to meet security requirements, ensuring compliance by implementing applicable auditing measures and standards and training the stockholders to ensure they have the necessary qualification and skill, as well as improving awareness among citizens (Lewis, 2005).

This article discusses cybersecurity regulation and governance. First, it outlines a framework of cybersecurity regulation and governance. Next, it discusses international cybersecurity regulation and governance, as well as cybersecurity regulation and governance in Saudi Arabia. Subsequently, it discusses some challenges and weaknesses of cybersecurity regulation and governance in general. The article concludes by providing some suggestions regarding best practices and solutions.

2. Cybersecurity Regulation and Governance Framework

Cybersecurity governance is the term that means directing and controlling everything related to cybersecurity by establishing the rules and policies to face all associated issues that arise due to the increased utilization of electronic information and transactions all over the world. Every country is responsible for establishing regulations which are a set of policies and standards that will protect the rights of citizens and their information in all electronic transactions and operations. At the organization level, the board of directors of each organization must identify, document, and support its own policies, and these policies should be in line with the relevant regulatory requirements and governance policies established by the government, as well as international standards issued by international information security institutions such as the International Organization for Standardization , the International Electrotechnical Commission, the National Institute of Standards and Technology, and the Information Security Forum. To ensure the effectiveness of these policies and standards, it is the

Manuscript received May 5, 2020
Manuscript revised May 20, 2020

responsibility of each organization to adhere to the periodic audit and assessment process to make sure that these regulations and standards are implemented and followed (Pernice, 2017; Ellis and Mohan, 2019). Applying cybersecurity governance in the organizations requires implementing a plan, creating a cybersecurity department independent of the information and communications technology department, publishing these regulations for the stakeholders, and ensuring clear roles and responsibilities are identified for all parties involved in implementing the cybersecurity governance (National Cybersecurity Authority, 2020). Implementing cybersecurity governance in companies will increase investor confidence in the company or organization and consequently increase the investment and financial revenue, help in carrying out efficient and effective risk management and process improvement, and increase the rapid response to information security incidents, thus improving trust in customer relationships, protecting the company's reputation, and reducing the risk of privacy violations (Pernice, 2018).

3. International Cybersecurity Laws and Regulations

Countries have fought against cybercrime by implementing laws and regulations to control the usage of information in the communications, financial and medical fields and all electronic transactions. In the past, cybercrime only comprised copyright and software piracy. However, serious crimes have emerged, which requires specific laws for every field and in all countries to limit the spread of these crimes (Ellis and Mohan, 2019). Moreover, it has become difficult to implement laws that keep pace with the rapid development of technology. There is also a relationship between these laws and human rights, as countries adopt many measures to monitor the online activity of Internet users, which constitutes a breach of privacy in some cases. Countries are studying this issue to try to create a balance in a manner that preserves human rights and state rights by protecting their citizens and their security. Therefore, it is necessary for those who develop these laws and regulations and technologists and scientists who understand the nature of the technology to exchange experiences and information (Brivat, 2017).

Because of the increase in cybercrime, in 2016, the European Union established the General Data Protection Regulation (GDPR), a legal framework that contains guidelines of how to process, transfer, and deal with personal information for people who live in European Union countries and in the European Economic Area which was adopted in 2018. These regulations apply to sites visited or used by European Union residents regardless of whether these sites are restricted to these residents or others from around the world. GDPR unifies and regulates all laws relating to the protection of data for European Union residents and thus makes it easier for companies and websites to access and follow these laws (Kosseff, 2019).

In Canada, the Canadian Parliament established the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000. This is a federal privacy law that enables private sector organizations to protect the information of the Canadian citizens in a manner that preserves their privacy by taking into account the needs of the organization. Similar to GDPR, PIPEDA unifies all laws related to personal data and allows individuals to access their personal information in organizations, find out who is responsible for this data, and verify its authenticity. In 2017, the Canadian government reported that it had reached a level equivalent to data privacy in European Union law, which allows the easy and safe exchange of data between the European Union and Canada (Kosseff, 2019).

In China, despite the existence of laws implemented by the government for companies and individuals regarding data protection and privacy, there is no governmental organization dedicated to these laws as there is in the European Union and Canada. However, in 2016, the Standing Committee of the 12th National People's Congress established the law of the cybersecurity of the Republic of China, which contains 79 articles stipulating the protection of personal information and the most important cyber problems. This law was officially implemented in 2017 (Kosseff, 2019).

In the United States (U.S.), several laws and regulations are concerned with the field of cybersecurity, though few of them mention cybersecurity by name. The Federal Trade Commission is the federal agency that deals with these cybersecurity laws, including data security, hacking, electronic and privacy monitoring, and notification of data breach (Kosseff, 2019). Some of the major U.S. federal cybersecurity laws are outlined below. The Health Insurance Portability and Accountability Act (HIPAA) was established in 1996 and approved by President Bill Clinton to protect the personal data of individuals in the medical field. These data include medical history, the name and telephone number of the patient, and all that would reveal the patient's identity. The Gramm-Leach-Bliley Act (GLBA), which was established in 1999, is a development of the Glass-Steagall Act. GLBA requires customers' data in the companies to be protected. It also sets laws for companies regarding their systems and computers to ensure that customer data is not exposed (Guiora, 2017). The Cybersecurity and Infrastructure Security Agency Act, which was signed by President Trump in 2018, aims to create a cybersecurity agency under the National Security Act (that was signed by President George W. Bush after the September 11, 2002 attacks) to embrace all issues related to cybersecurity within the U.S. and assist organizations to analyze and handle cyber threats and establish laws for all emerging issues in the field of cybersecurity (cisa.gov, 2020).

4. Cybersecurity Regulation and Governance in Saudi Arabia

In 2018, the National Cybersecurity Authority published the minimum requirements of cybersecurity for Saudi government organizations. The Essential Cybersecurity Controls (ECCs) consist of 114 cybersecurity controls linked to national and international regulatory requirements organized into five main areas: governance, cybersecurity defense, cybersecurity resilience, third-party & cloud computing cybersecurity, and industrial control systems cybersecurity (National Cybersecurity Authority, 2020). These controls aim to provide a minimum level of basic requirements for cybersecurity based on best practices and standards to reduce cyber risks to the information and technology assets of entities from internal and external threats. Protecting the information and technology assets of the entity requires focusing on the primary objectives of protection, which are confidentiality, integrity, and availability of information (Alkahtani, 2017). ECC's governance requirements are considering, developing and implementing a cybersecurity strategy that contributes to compliance with relevant laws and regulations. ECC's specifies the personnel, operations, and other steps that organizations need to achieve effective cybersecurity (Alsmadi and Zarour, 2018). Cybersecurity strategy and cybersecurity management come under the governance of cybersecurity. Policies, procedures, and publication of cybersecurity requirements are established according to the regulatory business requirements of the entity. The roles and responsibilities of cybersecurity and risk management are defined in a systematic way aimed at protecting the information and technology assets of the entity (Alkahtani, 2017). It is vital to ensure that the requirements of cybersecurity are included in the methodology and procedures of the entity's projects to protect the confidentiality and integrity of the information and technology assets of the entity. Commitment to cybersecurity legislation, regulations and standards is considered a part of the cybersecurity governance (National Cybersecurity Authority, 2020). It is necessary to review and periodically audit cybersecurity in addition to ensuring that the cybersecurity risks and requirements related to workers (employees and contractors) in the entity are dealt with effectively before and during their work and when their work ends (Alabdulatif, 2018). A program to raise awareness of cybersecurity should be developed and implemented periodically through multiple channels to build a positive culture of cybersecurity (National Cybersecurity Authority, 2020).

5. Cybersecurity Regulation and Governance Challenges

With the increasing number and complexity of cybersecurity threats, governments decided to create regulation as well as governance for cybersecurity. However, many cases of internal and external governance mechanisms that affect cybersecurity are discarded or managed ineffectively. The consequences of such actions are the reason for the increase in financial and operational risks to the organizations.

In this section, we will discuss some of the challenges that cybersecurity governance and regulation might face. The first challenge is defining risk posture. Developing a cybersecurity governance strategy requires understanding the environment of the organization and defining its risk posture. Many organizations are utilizing outdated strategies in specifying risks that treat all risks equally without prioritizing, which could lead to massive risk. The second challenge is managing data on an equal basis without prioritizing. As we know, data are divided into categories such as financials, citizens records, and intellectual property. All those data have different levels of security and are accessible to many custodians. Some data are categorized as critical data which are not allowed to be modified or changed under any circumstances to maintain their integrity at the highest level. Furthermore, operations or processes should maintain access to those data by authorized individuals. The categorization standards will play a vital role in achieving this by applying levels of protection to the data based on their sensitivity. In fact, most organizations add an unnecessary burden to their process by adding misplaced security. To have an effective governance strategy, the organizations must categorize their data by the level of sensitivity to reduce the load of protecting massive quantities of data through the network. The third challenge is responding to change. As we know, the business processes and technology are developing continuously, and therefore the challenge for the cybersecurity governance and regulation is to be compatible with those developments. The most significant challenge facing organizations due to this rapid development of technology is complying with those regulations. Whenever the organization tries to implement the regulations, some new threats appear. As a result, new regulations should be created to control those threats, and governments have to edit their current regulations continuously to keep up with those threats (Hellwig, 2017).

In general, the technology sector is evolving very rapidly. Due to this fast growth, the regulatory step behind and the cyber risks become the biggest hazard for the organizations. Most boards of directors do not believe they have sufficient preparations for cyberattacks. Moreover, the regulations become more sophisticated as the minimum obligations are no longer enough. Furthermore, the current Internet infrastructure and regulations are lagging behind the current technology because of the fast growth of the digital world

and its design that does not have the ability to handle the massive amount of data and number of attackers (Iannone and Omar, 2015).

The challenges we have discussed above may affect the compliance with regulation and governance. Consequently, the organizations have to be able to identify their challenges and then try to find solutions to ensure their work continues smoothly without violations.

6. Cybersecurity Regulation and Governance Best Practices

Sensitive data such as critical government-related information and valuable assets are the most secure and protected by the governments. Therefore, most of the enemies and attackers direct their focus and attention toward a human element which is the most sensitive and weak part of many systems and organizations. The enemies and attackers exploit the human-related vulnerabilities, especially the lack of cybersecurity awareness and its regulations (Abawajy, 2014). Most of the previous studies confirm that 90% of the cybersecurity crimes were the result of a lack of cybersecurity knowledge and insufficient awareness (Kemper, 2019).

Governments now realize that cybersecurity awareness can be improved through education, training, and best practices, and they have been making an effort to change citizens' behaviors and attitudes toward the importance of cybersecurity. They have started to implement laws and regulations related to cybersecurity crimes to eliminate risks and threats and impose disciplinary sanctions and financial penalties. These regulations should not be constant and must be up to date with the modern technology and its risk. They should be comprehensive, flexible, and applicable to new attacks in the cybersecurity field, as well as reviewed in a manner to ensure their enhancement with the interest of organizations and citizens. Moreover, they should take into account human rights and privacy when establishing these regulations and laws, as well as how they measure the seriousness of the information when monitoring any local electronic activity and establishing controls for legally qualified authorities who are responsible for the monitoring process. To obtain a safe and creative environment, these regulations must be knowledgeable to the citizens, who must be aware of their importance on a personal and public level, by embedding cybersecurity concepts in the curriculum and organizing training and awareness programs which are supported by the governments, as well as spreading cybersecurity awareness and its regulations on internet platforms.

7. Conclusion

In conclusion, we discussed the cybersecurity regulation and governance framework, and then provided details of international regulations and regulations in Saudi Arabia. Furthermore, we highlighted some challenges facing cybersecurity regulations and governance, such as defining risk posture and managing data, and discussed the most important challenge, which is the inability of the regulations to keep up with the rapidly evolving technology and threats. Moreover, we discussed awareness and the best practices. We conclude the paper by highlighting that those cybersecurity regulations and governance could be a strong backbone for all organizations and governments, and they should be comprehensive, flexible, updated, and applicable to new attacks on the cybersecurity and take into account human rights and privacy.

References

[1] Eugen, P. and Petruț, D., 2018. Exploring the new era of cybersecurity governance. Ovidius University Annals, Economic Sciences Series, 18(1), pp.358-363.

[2] Lewis, J.A., 2005. Aux armes, citoyens: Cyber security and regulation in the United States. Telecommunications Policy, 29(11), pp.821-830.

[3] Ellis, R. and Mohan, V. eds., 2019. Rewired: Cybersecurity governance. John Wiley & Sons.

[4] Pernice, I., 2017. Cybersecurity governance: Making cyberspace a safer place.

[5] National Cybersecurity Authority, 2020. Essential cybersecurity controls. [online] Available at: <https://nca.gov.sa/files/ecc-ar.pdf> [Accessed 30 March 2020].

[6] Pernice, I., 2018. Global cybersecurity governance: A constitutionalist analysis. Global Constitutionalism, 7(1), pp. 112–141.

[7] Brivat, B., 2017. Cyber security, cultural security and the cyber gap: Lessons from Middle Eastern policy makers cultural security: Concepts and applications. Al-Ameed Journal, 6(4), pp. 58–81.

[8] Kosseff, J., 2019. Cybersecurity law. John Wiley & Sons.

[9] Guiora, A.N., 2017. Cybersecurity: Geopolitics, law and policy. CRC Press.

[10] cisa.gov, 2020. About CISA [online] Available at: <https://www.cisa.gov/about-cisa> [Accessed 30 March 2020].

[11] Alkahtani, F.S., 2017. Saudi Anti-cybercrime Law of 2007: A comparative study looking at the United Arab Emirates' Combating Cybercrimes Law of 2006 amended in 2012. Majallat al-Nadwah lil-Dirāsāt al-Qānūnīyah, 239(6128), pp. 1–20.

[12] Alsmadi, I. and Zarour, M., 2018, April. Cybersecurity Programs in Saudi Arabia: Issues and Recommendations. In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-5). IEEE.

[13] Alabdulatif, A., 2018. Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia (Doctoral dissertation).

[14] Hellwig, C., 2017. New perspectives on cyber security: The regulatory challenge. [online] Global Risk Insights. Available

at: <https://globalriskinsights.com/2017/05/new-perspectives-cyber-security-regulatory-challenge/> [Accessed 27 March 2020].
[15] Iannone, P & Omar, A 2015, CYBERSECURITY GOVERNANCE Five Reasons Your Cybersecurity Governance Strategy May be Flawed and How to Fix It The Changing Faces of Cybersecurity Governance, American University Washington .DC, March.
[16] Abawajy, J., 2012. User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), pp. 237–248.
[17] Kemper, G., 2019. Improving employees' cyber security awareness. Computer Fraud & Security, 2019(8), pp.11-14
[18] Glance, C.R.A.A., 2017. Kingdom of Saudi Arabia.
[19] Style Iqbal, Z. and Khan, M.K., 2019. Saudi Women in Cybersecurity Narrowing the Gap of Human Capital Crisis. Global Foundation for Cyber Studies and Research.
[20] Aboul Enein, S., 2017. Cybersecurity challenges in the Middle East.
[21] Dawson, M., Unprepared for cybersecurity in Saudi Arabia: Argument for a shift towards cyber readiness.
[22] Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M., 2016, December. A survey of cyber-security awareness in Saudi Arabia. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 154-158). IEEE.
[23] Authority, S.A.M., 2017. Cyber security framework.
[24] Ajmi, L., Alqahtani, N., Rahman, A.U. and Mahmud, M., 2019, May. A Novel Cybersecurity Framework for Countermeasure of SME's in Saudi Arabia. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-9). IEEE.