Cyber Security Controls and Countermeasures

Mohammed Mustafa Khan

Abstract *- Today's digital economy encompasses a conglomeration of devices, data, applications, and complex networks that can be hosted on-premises, in data centers or in cloud environments to support business functions. As a cybersecurity professional, you will be tasked to manage risks like cyber threats and data breaches in the workplace. The risks may emanate from the data that resides in the systems, like servers, computers or external drives and the physical assets themselves, like routers and switches. The onus is on preventing security events and limiting the damage or consequences of any event that might happen. Managing these risks in an organization can be achieved by implementing cyber security controls and countermeasures. Cyber security controls can be categorized into three distinct major groups: administrative control, physical control, and technological control. The administrative controls focus on security policies, guidelines, rules, procedures and standards designed by management to control access and utilization of confidential information. Physical control refers to a set of IT security controls deployed at the physical premise to prevent unauthorized physical access to data centres. Technical controls involve the use of systems and technical solutions to prevent security events in networks and cloud platforms. Additionally, when implementing security controls, the function of cyber security controls can be broadly divided into seven groups: directive, deterrent, preventive, compensating, corrective, detective, and recovery controls. Furthermore, security frameworks such as NIST, CIS controls COBIT, and ISO/IEC series form the cornerstone of cyber security controls and countermeasures. The aforementioned aspects will be discussed further in the later sections. For now, it is to provide a general picture of the cyber security controls and countermeasures.*

Keywords *– Security Controls, Countermeasures, Frameworks, Information Systems, Risk*

1.0 Introduction

Data that exists in an information system can be one of the three states of data. Data at rest that is stored in servers, hard drives, computers, among others or physically printed and stored in cabinet safe, data in motion or transit over the network or internet, and data in use involves active utilization of data either by the system like webserver or physical by an individual. It is the responsibility of an organization to ensure data is protected in different states. To achieve a high level of data protection, cyber security controls and countermeasures act as a standardized approach to data protection and even protect the IT systems that manage this data [1]. To ensure the cyber security of IT infrastructure, you do not have to reinvent the will but use the wheel. There are pre-existing cybersecurity controls and countermeasures that can be properly implemented. Organizations need to utilize cybersecurity controls and countermeasures as the baseline to enforce security. When it comes to the establishment of security controls, scoping and tailoring processes become fundamental aspects for cybersecurity professionals. Scoping determines what security controls apply to the underlying IT infrastructure, and you tailor the security controls either by adding, modifying, or removing them to benefit the protection needs of an organization. Additionally, scoping and tailoring help to classify the data based on its sensitivity. The most critical and sensitive data, such as credit cards, bank details, and intellectual property, need to be protected with superior security controls and countermeasures, whereas low and moderate data can be protected to attain data security [1]. The implementation of security controls and countermeasures needs stakeholder buy-in since stakeholders will spend time and money, and they need to be engaged in order to see the value of security controls and countermeasures. When implementing security controls and countermeasures, it is prudent to conduct a risk assessment analysis to determine the potential vulnerabilities and threats. This research paper discusses the defence in depth process for cyber security controls and countermeasures using administrative controls, physical controls, technological controls and existing frameworks.

2.0 Administrative Controls

Administrative controls comprise policies, guidelines, procedures, and rules that have been set up by the management to govern the access and usage of IT infrastructure. Many organizations have a policy document that acts as a standard operating procedure to guide employees on what they are expected to follow and things they are not supposed to do. Some employees have a certain level of privileges regarding the type of IT infrastructure they can access. The subsets of administrative controls entail user management, employee training and awareness, and privilege management. User management involves evaluating and monitoring user behaviour to ensure they adhere to the existing administrative controls. Training of employees is critical since it helps to sensitize and create a level of awareness. Modern threats, such as social engineering, target employees. When employees are not properly trained or educated, they fall prey to cybercriminals. According to the study done by Anwar et al. (2020) on the significance of employee training pertaining to cybersecurity, training improves the employees' intellectual capacity for cybersecurity.

3.0 Physical Control

Tangible IT assets of the organization, such as equipment housed in the data center or IT assets contained on the premises, are at high risk of being physically stolen or damaged. Additionally, the intruder may decide to walk into the data center or on-premise environment and plug in a rogue device that spies all the network traffic and transmits sensitive data back to the intruder [7]. These gadgets must be physically monitored to shield any unauthorized access that may result in devastating effects.

3.1 Video Surveillance

The surveillance video cameras must be deployed at the strategic point entrance and in any section of the room that houses tangible IT assets. Cameras will monitor the environment. Huge thanks to the advanced Internet of Things technology, which has enabled the development of motion sensor cameras that are embedded with alarm systems. Any suspicious movement is detected, and the appropriate person is notified to act accordingly [7]. Video surveillance provides real-time monitoring of events and records all the footage in a centralized place. In case of any data breach incidents, the footage can be reviewed and used as evidence.

3.2 Perimeter Security

Perimeter security entails protecting the external borders of an organization that houses the IT assets. It can be done by utilizing fences, bollards and barriers. Perimeter security can also involve access control measures at the entrance or exit points like gates and checkpoints. It prevents unauthorized access from stealing or vandalizing IT assets [7].

3.3 Access Control

Access control is the fundamental aspect of physical security control. There are various technologies, including smart cards, biometric authentication, and keypads, that can help to accomplish access control. Biometric lock door systems can be deployed to prevent unauthorized persons from assessing the rooms that house IT infrastructure [7]. Any visitor accessing the room must be uniquely identified by issuing them electronic identity cards. If the visitor carries a bag, it must be checked by passing it through the scanners or manually checking the bag, which is a basic security requirement. However, careful considerations must be taken when handling visitors. This will elevate the level of physical security and ensure data and IT assets are kept safe from unauthorized physical access.

3.4 Security Personnel

Security personnel is the pivotal component of any physical security strategy. Security guards monitor and oversee the physical environment. They provide assistance to visitors who want to access the premises [7]. They also keep an eye on the deployed video surveillance cameras, protecting them from being stolen or vandalized.

4.0 Technical Controls

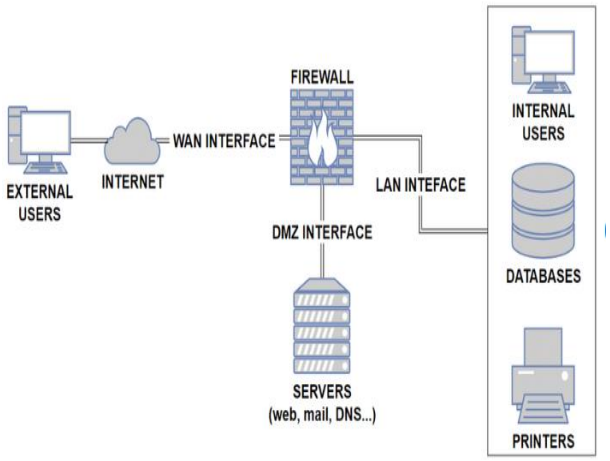
technical controls can be named logical controls. These controls are used to prevent or minimize attacks on software, hardware, network and cloud services. It involves the use of systems and technical solutions to prevent or reduce threats from exploiting the IT infrastructure. Weak security controls are prone to cyber-attacks. Attacks exploit weak security controls, gain access to the company's critical data and wreak havoc. It is crucial to implement strong security controls

that can help secure the organization's data and IT assets. There are various logical controls that are available to boost an organization's cyber resilience. some of these technical controls include;

- Firewalls
- Antivirus and antimalware software
- Encryption
- Authentication
- Security information and event management (SIEM)

4.1 Firewalls

Endpoint devices like servers, computers, and routers, to mention a few, can be protected by set-up firewalls. Strategic locations of networks where the corporate network interfacing with the internet needs deployment of firewalls. The role of a firewall is to filter the ingress and egress network traffic [3]. Any anomalous suspicious activities are investigated, and access is denied by blocking traffic. Properly configured firewall rules must be implemented when commissioning a firewall. Additionally, there are various manufacturers and vendors of firewalls. A firewall acquisition process must be conducted to ensure the standard industry firewall that conforms to compliance is selected. This will enable an organization to meet its intended objectives.



Source: https://www.researchgate.net/profile/Luis-Castro-Silva/publication/353368550/figure/fig1/AS:1048008447762434@1626876093465/Example-of-a-Corporate-Network-Architecture.ppm

Various types of firewalls exist in the market. Firewalls can be classified based on their functionalities. These include packet filtering firewalls, application-proxy gateway firewalls and stateful inspection firewalls. Packeting filtering firewalls helps in monitoring incoming and outgoing traffic regarding the source and destination. Application proxy gateway firewalls provide protection to the network resources by filtering traffic at the application level. Stateful inspection firewalls are used in monitoring active network connectivity to evaluate the packets to allow and deny [3].

4.2 Antivirus and antimalware software

Antivirus and antimalware software discover and eliminate computer viruses and other types of malware, such as spyware, rootkits, trojan horses, and worms, to mention a few [3]. The marketplace is flooded with numerous antivirus and antimalware software. Some notable providers included Avira, McAfee, and Kaspersky. It is important to install and implement superior antivirus and antimalware software on all workstation devices.

4.3 Authentication and password policy

Authentication is the practice whereby an application, service or individual ought to provide their identity prior to gaining access to the digital systems. The most common method of authentication is the user's name and password credentials [6]. An entity that claims to access the digital system must provide the correct credentials for validation by the system. Password policy best practices must be enforced to enhance computer security. The advancement of technology has enabled the adoption of multifactor authentication that forces a user to provide another verification identity apart from a password, which may be a password. Additionally, cryptography has enabled the use of digital self-assigned certificates to prove the real identity of an entity. All these controls have the objective of countering cybersecurity incidents.

4.4 Encryption

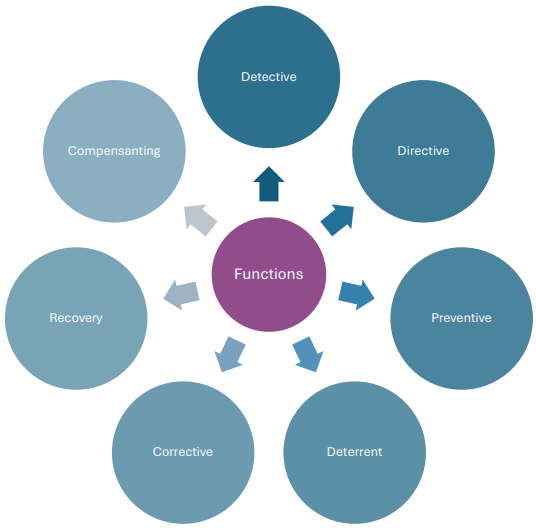
In our earlier discussions, we examined the three states in which data can exist. Data in any state must be kept protected. The best practice to ensure data is safe at any of the stages, specifically in transit and storage, is through encryption. Encryption masks the data by converting readable plaintext data into unreadable ciphertext, preventing information leakage even when the cybercriminals intercept the communication channel. Anyone who reads the data will need a decryption key. It is important to use industry-standard encryption algorithms such as the

advanced encryption standard (AES) that provides a high level of security [9]. Avoid using traditional encryption technologies that are prone to threats. In the study conducted by Bosnjak et al. (2018), the data encryption standard (DES) is susceptible to brute force attacks.

4.5 SIEM

SIEM is an integrated system that aggregates data, discovers variations from the norm, and recommends appropriate actions to be taken. Organizations need to enhance their security controls by implementing SIEM solutions. SIEM is an essential solution that is an integral part of data security strategy. The solution collects data from various sources of the network and stores the data in a centralized location database that enables the security team to view security logs in a single pane of glass [5]. SIEM adheres to various forms of regulatory compliance requirements by the HIPAA Hospital Insurance Portability and Accountability Act, GDPR (General Data Protection Regulation), and PCI-DSS (Payment Card Industry Data Security Standard) and various regulatory standards.

5.0 Functions of Cyber Security Controls and Countermeasures



This can be classified into seven categories

- Directive controls provide guidance to all the staff to follow the established standard operating procedures regarding the use of IT infrastructure. It entails policies and rules contained in a document [8].
- The main objective of deterrent controls is to discourage employees from assisting cybercriminals in launching attacks [8].
- Detective controls are used to discover any suspicious activities or unusual network traffic and signal the appropriate person to counteract the event [8].
- Corrective controls are utilized in the mitigation or remediation of security impact. It entails methods that mitigate and prevent similar issues from happening again [8].
- Preventive controls are used to curb security data breach incidents. It involves good cyber hygiene, user authentication, and network segmentation.
- Recovery controls are employed in the event of a cyber disaster to ensure there is business continuity. It involves recovering and restoring files and systems.
- Compensating controls are alternative strategies put in place to support the primary security controls. Their purpose is to maintain a comparable level of protection, even if the main security measure has been compromised by an attacker [8].

6.0 Cybersecurity Frameworks

We can not discuss the cybersecurity controls and countermeasures without pointing out the cybersecurity frameworks. This is like trying to reinvent the wheel, yet everything has been done. Our goal is just to use the existing cyber security controls and countermeasures to protect the organizational IT infrastructure. Frameworks are the backbone of developing and implementing cyber security controls and countermeasures. They enable an organization to manage security controls in various types of assets using accepted and proven methodology. Some of the cybersecurity frameworks and standards include the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and Center for Internet Security (CIS) Controls, among others [4].

6.1 NIST CSF

This framework was created by the National Institute of Standards and Technology in 2014. The framework provides a roadmap to organizations on how to prevent, detect, and respond to cyber threats. The methods of assessment and procedures help to evaluate how the security controls and countermeasures of an organization have been implemented and work as expected [4]. The frameworks ensure the desired

outcomes pertaining to the security of IT infrastructure have been met as intended. Furthermore, this framework is updated regularly to show their proactive approach regarding advancement in the cyber security threat landscape.

6.2 CIS Controls

The Center for Internet Security established a list of controls and safeguards that help organizations implement each control and safeguard step by step to ensure the protection of IT infrastructure. Initially, 20 CIS controls were developed, but they were later reduced to 18 CIS controls to keep pace with technological advancement. As business were shifting their operations from on-premise to hybrid clouds, it necessitated the SANS Institute to adopt the modern ways of businesses [4]. The CIS controls are effective in thwarting modern threats since they are derived from the most common attack patterns outlined in the most leading reports and validated with a broad community of industry practitioners and government.

7.0 Conclusion

The main objective of cybersecurity controls and countermeasures is to protect data and information systems. Various approaches may be used by organizations to ensure data protection and that the information systems that house data are kept secure. It is crucial to understand the different states in data that exist to ensure appropriate security controls and countermeasures are applied accordingly. The defence in-depth approach is a standardized way of protecting even the information systems that store the data. It is not tenable to focus only on data without also focusing on the IT assets. Comprehending the various functions of security controls will help to appreciate the benefits of security controls and countermeasures. Various cybersecurity frameworks exist. Organizations need to review these two frameworks and any other frameworks to tailor their security controls and countermeasures to align with the business objectives. This multi-layered approach will enable organizations to successfully develop and implement cyber security controls and countermeasures that appropriately suit the organizational needs.

8.0 Reference:

[1] Anwar, Yuan, and Ivan, "Improving employees' intellectual capacity for cybersecurity through evidence-based malware training," May. 2020. https://www.emerald.com/insight/content/doi/10.1108/JIC-05-2019-0112/full/html

[2] L. Bosnjak, J. Sres, and B. Brumen, "Brute-force and dictionary attack on hashed real-world passwords," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, May 2018, doi: https://doi.org/10.23919/mipro.2018.8400211.

[3] Centers for Disease Control and Prevention, "Information Systems Security Controls Guidance: Application Systems | Compliance | Federal Select Agent Program," *www.selectagents.gov*, Sep. 09, 2020. https://www.selectagents.gov/compliance/guidance/information-systems/app-systems.htm

[4] A. Amiruddin, H. Nugroho, and A. HG, "Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8 | IEEE Conference Publication | IEEE Xplore," *ieeexplore.ieee.org*, Oct. 2021. https://ieeexplore.ieee.org/abstract/document/9699337/

[5] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021, doi: https://doi.org/10.3390/s21144759.

[6] CISA, "Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA," *Cybersecurity and Infrastructure Security Agency CISA*, May 17, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a

[7] Center for Development of Security Excellence, "Introduction to Physical Security Student Guide Introduction to Physical Security Student Guide," Sep. 2017. Available:

https://www.cdse.edu/Portals/124/Documents/student-guides/PY011-guide.pdf

[8] The National Cyber Security Society, "How To Select Access Controls DID YOU KNOW?," May 2019. Accessed: 1BC. [Online]. Available: https://nationalcybersecuritysociety.org/wp-content/uploads/2019/05/HOW2-Select-Controls-FINAL.pdf

[9] M. Ocenas, I. Homoliak, P. Hanacek, and K. Malinka, "Security and Encryption at Modern Databases," *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, Jan. 2020, doi: https://doi.org/10.1145/3377644.3377662.

[10] J. T. Force, "Security and Privacy Controls for Information Systems and Organizations," *csrc.nist.gov*, Aug. 15, 2017. https://csrc.nist.gov/pubs/sp/800/53/r5/ipd