Cyber Security Standards

Mohammed Mustafa Khan

Abstract

Cybersecurity standards are guidelines or best practices that are used by organizations to improve their security posture. They use the standards to identify and implement appropriate measures to protect their data and systems from threats. Similarly, these mechanisms are guided by a set of cyber security standards. These standards are set to help improve the security of organizational networks, information technology infrastructure, and critical infrastructures. The assurance and functional requirements of a system, product, technology, or process are specified by these standards. Establishing a good cybersecurity standard assist in achieving uniformity in product development and is also useful when procuring security products. Similarly, they are critical in avoiding information leakage, securing vital information, and meeting regulatory requirements. The present work addresses the NIST Cybersecurity standard, ISO/IEC 27001, and CIS Critical Security Controls as some of the most crucial international cybersecurity standards. It also contains some specific types of standards, such as HIPAA, GDPR, FISMA, and PCI-DSS.

Keywords: Cybersecurity Standards, Information Security Management Systems (ISMS), ISO/IEC 27001, NIST Cybersecurity Framework, CIS Critical Security Controls, PCI-DSS, HIPAA, GDPR, FISMA, Regulatory Compliance, Risk Assessment, Data Protection, Encryption, Threat Detection, Incident Response, Artificial Intelligence in Cybersecurity, Compliance.

1.0 Introduction

Data and information protection is very paramount for any organization. Given the emergence of numerous complex technologies, the risk of cyber threats is high, and therefore, organizations may be affected. Thus, there is a need for proper cybersecurity protection that sustains and can protect organizational data and information. That is where cybersecurity standards come in. These standards assist organizations in developing adequate measures to deal with threats against their structures and information. All organizations typically use these frameworks irrespective of size, sector and industry. Thus, IT specialists utilize the standards and frameworks to organize further security and set the objectives that would help to address enterprise security issues appropriately. These standards guarantee security, ease advancement of integration and interoperability with other frameworks, ensure comparable measures, and offer the framework for new improvements. Cybersecurity standards are categorized into two parts: the specific standards for specific industries like finance and health; as a result, there are industrial standards on the international level. This document assesses cybersecurity measures, how they help organizations operate within the laws, and some problems organizations encounter whenever they adopt them.

Key International Cybersecurity Standards

a) ISO/IEC 27001

ISO/IEC 27001 is among most broadly adopted international information security management systems (ISMS) standards. The International Organization for Standardization developed it, and it can be applied to organizations of all types and sizes [4]. These standards provide world-class specifications for services, products, and computers to ensure efficiency, safety, and quality. These standards are very essential in conducting international trade. An organization that is ISO certified assures its customers, board, shareholders,

and partners that it is keen on cyber risk management [2]. Similarly, when a vendor is ISO certified, it demonstrates they have mature cybersecurity practices and controls. The two primary ISO standards are the ISO 27001 and 27002 [4].

Sources: https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/iso-27001-compliance-steps.png

These standards provide the framework and procedures for developing an information security management system. Compliance with ISO 2700 series standards is facilitated through an audit and certification process conducted by a third-party company that ISO and other accredited agencies approve.

The ISO 2700 series can be categorized into many types, such as the ISO 27001. This standard calls for the implementation, establishment, monitoring, maintenance, operation, and improvement of our ISMs using a process-based methodology [3]. The standard allows the company to prove to its stakeholders and customers that it is prudent and mindful of its confidential data and information security. The ISO27005 supports general concepts that are specified in 27001. The purpose of ISO 27005 is to offer recommendations for information security implementation that follow the risk management methodology. To understand this standard, one should completely understand the knowledge of models, concepts, terminologies, and processes described in 27001 and 27002. ISO 27032 is an international standard that provides guidelines on protecting information beyond an organization's orders, such as partnerships, collaborations, and other information-sharing arrangements with suppliers and clients [4]. It aids in managing the hazards connected with technology use and safeguarding enterprises against cyberattacks. Based on ISO 27001 criteria, the ISO/IEC 27701 standard outlines the specifications for a privacy information management system [4]. It can be used to extend the 27001 to improve organization security efforts and cover privacy management.

Source: https://static.isms.online/app/uploads/2023/08/ISO-27002-New-Controls.png

b) NIST Cybersecurity Framework

The National Institute of Standards and Technology Cybersecurity Framework provides a set of guidelines and procedures for managing cybersecurity risks. It helps organizations identify, assess, and effectively manage their cybersecurity risks. Nevertheless, this framework is not mandatory for organizations, but numerous organizations are adopting it as a voluntary measure to improve their cybersecurity posture [5]. In February 2013, the framework was created in accordance with Executive Order 13636. The standard addressed US critical infrastructure such as water and food supplies, energy production, healthcare delivery, communications, and transportation. The framework's security controls are founded upon the five phases of risk management, namely identification, detection, protection, response, and recovery. It is suitable for both private and public sectors [7].

Source: https://www.nist.gov/sites/default/files/images/2018/04/16/framework-01.png

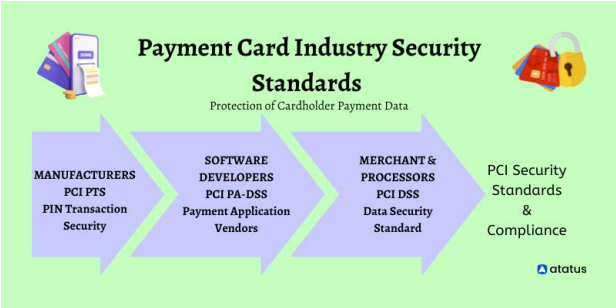
c) CIS Critical Security Controls

The Center for Internet Security CIS Critical Security Controls are guidelines that are prioritized to properly position an organization against cyber-attacks and form an in-depth defense of specific and actionable best practices to mitigate the attacks [6]. The framework is essential because it focuses on the small number of actions that can be worked upon to prevent or reduce cybersecurity risk. The SANA Institute initially developed the framework [6]. However, it is currently managed by the Center for Internet Security and produced by technology experts to create a globally accepted security best practice.

2. Industry-Specific Cybersecurity Standards

a) PCI-DSS (Payment Card Industry Data Security Standard)

The PCI-DSS standard is a widely acceptable set of guidelines that provide procedures and policies on optimizing the security of cash, debit, and credit card transactions to protect cardholders against misuse of their personal information [7]. This standard focuses on encryption, access control, and regular network monitoring to prevent data breaches during transactions. In addition, it provides comprehensive frameworks, tools, support resources, and measurements to ensure that the information of cardholders is safe [7]. PCI-DSS is mandatory for organizations such as financial institutions, service providers, as well as merchants that process, store, or transmit credit card data. Failure to comply with the standards leads to severe penalties in the form of legal action.



Source: https://www.atatus.com/blog/content/images/2022/08/defining.png

b) HIPAA (Health Insurance Portability and Accountability Act)

The Health Insurance Portability and Accountability Act sets rules that set the standard for protecting sensitive patient data. Additionally, to ensure companies comply with HIPPA, they must have a physical network and apply security measures to the network to protect patient data and follow the security measures [8]. Furthermore, all the parties involved in the health sector should comply with HIPPA. These include the people providing treatment, operations in healthcare and payment, and anyone who aids the hospital and has access to patient information. A set of regulations and guidelines for the electronic exchange of health information was established by HIPAA. It also established standards the code sets that are applied to medical coding and billing. HIPAA officially accepts CPT, HCPCS and ICD codes to submit claims. A uniform means of communication for all parties involved in healthcare, including providers, insurance payers, governmental organizations, and clearinghouses, was the aim of the regulations [8]. All HIPAA-covered organizations must follow these transactional criteria. Title II mandates that the Electronic Data Interchange (EDI) standard type of electronic transaction be used for all transactions. The technology is extensively used in all commercial transactions, including ATMs. Healthcare providers and payers are required to utilize the EDI that has been authorized by the Accredited Standards Committee X12 (ASC X12) [12]. National Provider Identifier (NPI) numbers must be used per Title II regulations. The numbers are ten in length, may contain alphanumeric characters, and are never reusable. NPIs offer a proper global abbreviation for identifying.

Source: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSWjmafEKyfq3SjoyljljmD6Q7lyFwpEfbJzg&s

c). NERC-CIP

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standards are a set of policies and practices focused on ensuring the protection and security of the bulk electric system within North America [9]. These were drafted following information on the need for better safety systems, especially regarding attacks on the power grid. NERC-CIP paints minimum standards for protecting various components, such as the power plants, the interconnected transmission systems, and associated control

facilities [13]. It includes many standards that address such questions as how to protect and defend assets properly, what has to be done regarding incidents, what training ought to be provided to employees, and how to assist clients in a calamity [9]. Other aspects of such focus are electronic perimeter security management, vulnerability management, and physical logic access management.

All the organizations engaged in critical electric infrastructure operations must comply with NERC-CIP regulations. Such organizations may be fined heavily for violations and susceptible to cyber-attacks. Similarly, it is easy to reformulate the norms as new threats appear [9]. Hence, the energy sector can cope with new challenges without falling behind. Following these norms will allow power companies to operate the grid with reliability and safety.

3. Regulatory Compliance and Governance

a) GDPR (General Data Protection Regulation)

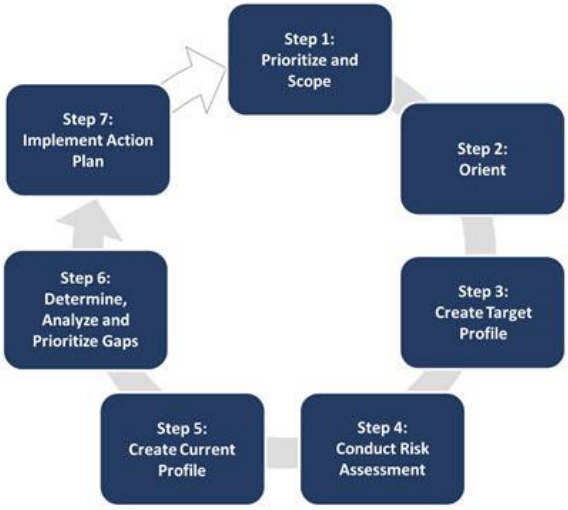
One of the strictest privacy and security regulations in the world is the GDPR. It was drafted and approved by the European Union. It requires organizations globally to adhere to it to protect the security of EU citizen's personnel information [10]. A few of the framework's controls are those that limit unwanted access to data that has been stored, as well as access control methods including multifactor authentication and role-based access [10]. It governs how personal data of the individual states should be transmitted. This includes listing the data subject's rights giving individuals more control over their data. When it comes to organizations, the framework requires them to provide notification on personal data breaches and appoint data protection officers[1].

Source: https://www.investopedia.com/thmb/j-Te5s88JZF_96k1qCoB2RwoNtU=/1500x0/filters:no_upscale():max_bytes(150000):strip_icc()/general-data-protection-regulation-gdpr.asp-final-1b12e02aa4d149b9af4fcd8aec409a89.png

b) FISMA (Federal Information Security Management Act)

The FISMA framework offers security guidelines for safeguarding federal government information and systems, and it closely resembles the NIST Risk Framework. Its goal is to make government agencies' information security stronger. The 2002 introduction of the framework was followed by an upgrade in 2014. FISMA was passed in 2002 as part of the E-Government Act [11]. The policy mandates government agencies, contractors, third parties, and vendors to design and implement security policies and practices that protect the safety of their information and systems. Among the things they may do are keep an eye on its IT infrastructure and perform frequent security assessments [12]. The act defines the three main objectives to enhance cybersecurity: confidentiality, integrity, and availability.

4. Development and Implementation of Cybersecurity Standards



Source: https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/PublishingImages/figure2.jpg

Developing and implementing an effective cybersecurity policy is very important for any organization. Below are the various requirements for an organization to create and implement a robust cybersecurity standard.

A). Risk Assessment

Conducting a risk assessment is the most critical step in developing a robust cybersecurity policy. It involves a comprehensive evaluation of the organization, including assets and systems, and understanding each process [2]. First, the organizational susceptibility to various cyber-attacks must be evaluated. It is essential to consider both internal and external risks. After identifying the assets, map every asset, where they are located, both in the network and physically, who has access to it, and how it is currently protected. Sort risks according to likelihood of occurrence and possible impact.

B). Set Your Security Goals

Use the previous step realizations to drive the security goals. Determine the organization's security maturity, understand the risk appetite, and set reasonable expectations. These aspects are essential in shaping a realistic and practical cybersecurity policy.

C). Evaluate The Technology In Use

The next step is to evaluate the organization's current technology infrastructure. Understand the effectiveness of the existing tools and systems and how they are safeguarded. Next, create a list of all software and hardware utilities for each technology that determine their security and ensure that they are updated [3]. The process involves assessing whether the particular organization possesses the necessary resources, including the budget and staffing levels required to manage and maintain the related platforms. Subsequently, the existing technology staff should be evaluated to determine whether they are capable and trained enough to handle such technologies[8].

d). Review your security policies

The next step is to review the current cyber security policies and establishing whether these policies are up to date and adequately implemented. List down the policies that have been developed and consider whether these are useful in the present technological environment and threats.

E). Create A Risk Management Plan

This process is critical in the development of cyber security policy. It helps strengthen the organizational cybersecurity posture. The plan should be comprehensive and actionable to identify all the potential risks and align with all the security goals highlighted in the previous stages. To create an effective plan, combine the

risk assessment findings, define risk management objectives, develop risk mitigation strategies, implement risk controls such as enhancing network security and updating policies, establish a monitoring and reviewing process, plan for incident process and recovery, document and communicate the plan, regularly review and update the risk management plan to ensure it is up to date.

F). Implementation And Evaluation

After planning the cybersecurity strategy and policies that have been created, it is now proper to implement them. It involves putting into action the strategies and policies that have been developed. Proper Implementation involves a multifaceted approach combining employee involvement, strategic planning, continuous improvement, and technology integration [4].

5. Challenges in Implementing Cybersecurity Standards

Deploying cybersecurity tools is not as easy as mentioned above. Various obstacles can significantly affect efficiency and security. One of the major problems is the availability of too many security tools, which gives management a headache due to a lack of compatibility and may clash with existing systems. Similarly, the costs of implementing the solutions are very high, making small businesses struggle with the Implementation. Next is the technical challenge involved with implementing the solutions. To integrate the systems, a company needs the necessary expertise due to complexity [12]. These systems are required to work with new and old systems, which may be challenging for the experts. For a cybersecurity policy to be effective, employees in the organization need to be adequately trained to avoid mistakes and make it work [3]. However, this is challenging because some employees might be reluctant to embrace and trust the new changes. Similarly, it costs the organization money and time to train their staff on the new solutions.

6. Best Practices in Cybersecurity Standard Compliance

Organizations must carry out security audits and vulnerability assessments periodically to achieve full-fledged compliance with the prescribed cybersecurity norms. The use of automated systems for security monitoring helps identify security policy breaches on time, allowing for a quicker response. Organizations must also ensure that third-party vendors abide by security measures since such violations at the vendor level can affect the entire supply chain [2]. Also, there is a constant necessity to follow guidelines concerning human-trained behavior, as human error is prominent in security breaches.

7. Future Trends in Cybersecurity Standards

Cyber threats are evolving with the evolving technology. Attacks are becoming more sophisticated and complex. Additionally, with the over-reliance on technology for communication, critical infrastructure, and commerce, it is very important to be updated with emerging trends [2]. Cyber threats are increasing in sophistication and the attackers are developing and launching new tactics and mechanisms to pass the gatekeepers and turn off important service delivery. This has been made possible with powerful hacking tools, making the hacking process more accessible. Similarly, there are new threats and novel attacks since numerous IoT gadgets are already on the market [13]. These devices embody several risks that are pretty dangerous for any organization. Lastly, AI and machine learning are new trends within the field of study. Today's cyber attackers are using these aspects of new technologies to improve their attack execution.

Conclusion

There is a need for cybersecurity standards in the modern world since different systems are integrated at various levels. Cybersecurity standards provide organizations with a guide to reducing risks and protecting their information. Implementing international frameworks like ISO/IEC 27001 or NIST or Industrial demands like PCI-DSS and HIPAA helps to build proper protection from cybersecurity risks. However, since it is

essential to follow such standards, inhibitors such as lack of resources and complexity in compliance must be addressed. Because these cyber security threats are dynamic, organizations should constantly learn about new cyber security phenomena, such as using artificial intelligence in threat detection and the zero-trust model. The evolution of these standards will be required to effectively respond to potential security threats from, for instance, IoT technology. When organizations focus on achieving IT standards, their security in protecting information resources and dealing with challenges is bound to be better.
References

8. References

1. J. Srinivas, A. K. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” Future Generation Computer Systems, vol. 92, no. 1, pp. 178–188, Mar. 2019, doi: https://doi.org/10.1016/j.future.2018.09.063.
2. R. Leszczyna, “A review of standards with cybersecurity requirements for smart grid,” Computers & Security, vol. 77, pp. 262–276, Aug. 2018, doi: https://doi.org/10.1016/j.cose.2018.03.011.
3. I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, “Standardising a Moving Target: The Development and Evolution of IoT Security Standards,” SSRN Electronic Journal, 2018, doi: https://doi.org/10.2139/ssrn.3437681.
4. B. Barafort, A.-L. Mesquida, and A. Mas, “Integrating risk management in IT settings from ISO standards and management systems perspectives,” Computer Standards & Interfaces, vol. 54, pp. 176–185, Nov. 2017, doi: https://doi.org/10.1016/j.csi.2016.11.010.
5. A. Qusef and H. Alkilani, “The effect of ISO/IEC 27001 standard over open-source intelligence,” PeerJ Computer Science, vol. 8, p. e810, Jan. 2022, doi: https://doi.org/10.7717/peerj-cs.810.
6. M. Frayssinet Delgado, D. Esenarro, F. F. Juárez Regalado, and M. Díaz Reátegui, “Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations,” 3C TIC: Cuadernos de desarrollo aplicados a las TIC, vol. 10, no. 2, pp. 123–141, Jun. 2021, doi: https://doi.org/10.17993/3ctic.2021.102.123-141.
7. M. N. M. Bhutta et al., “Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS),” Wireless Communications and Mobile Computing, vol. 2022, no. 1, pp. 1–10, Jan. 2022, doi: https://doi.org/10.1155/2022/9942270.
8. B. Chinmoy, C. H. Ho, and R. T. Brodell, “Time to revisit HIPAA? Accelerated telehealth adoption during the COVID-19 pandemic,” Journal of the American Academy of Dermatology, vol. 83, no. 4, Jun. 2020, doi: https://doi.org/10.1016/j.jaad.2020.06.989.
9. T. Chang et al., “Development and Implementation of Practical Processes for NERC CIP-010 Compliance Evaluation,” Mar. 2022, doi: https://doi.org/10.1109/cpre55809.2022.9776559.
10. M. Syafrizal, S. R. Selamat, and N. A. Zakaria, "Analysis of cybersecurity standard and framework components," *International Journal of Communication Networks and Information Security*, vol. 12, no. 3, pp. 417-432, 2020.
11. R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, “A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM),” 2017 International Conference on Information Systems and Computer Science (INCISCOS), Nov. 2017, doi: https://doi.org/10.1109/inciscos.2017.20.
12. L. Axon, K. Fletcher, M. Stolz, A. E. Kaafarani, and S. Creese, “Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda IIoT Capability Gaps,” Digital Threats: Research and Practice, Mar. 2022, doi: https://doi.org/10.1145/3503920.
13. A. Adeyemi, “Assessing The Impact Of The EU General Data Protection Regulation (GDPR) On Businesses In Nigeria,” SSRN Electronic Journal, 2018, doi: https://doi.org/10.2139/ssrn.3393959.