Global Journal of Engineering and Technology Advances, 2020, 02(03), 016–021

Global Journal of Engineering and Technology Advances

Cross Ref DOI: 10.30574/gjeta

Journal homepage: http://www.gjeta.com

(RESEARCH ARTICLE)

Cybersecurity for higher education institutions: adopting regulatory framework

Custodio Eunice Bondoc [1, 2, *] and Tumibay Gilbert Malawit [2]

[1] *Bulacan State University, City of Malolos, Bulacan, Philippines.*
[2] *Angeles University Foundation, Graduate School, Angeles City, Philippines.*

Publication history: Received on 18 February 2020; revised on 24 February 2020; accepted on 25 February 2020

Article DOI: https://doi.org/10.30574/gjeta.2020.2.3.0013

Abstract

Cybersecurity is defined as the protection of networks, data and systems in the cyberspace. It should have the ability to protect or defend an organization's use of cyberspace from any attack, conducted via cyberspace with the intention of disrupting, disabling, destroying, or maliciously controlling a computing environment and even destroying the integrity of the data or stealing controlled information. As the rapid technological developments have provided vast opportunities and potential sources of efficiency to every organization, these new technologies have also brought unprecedented threats and could be a critical issue for every organization.

In this study, Phase I delved into the different Cybersecurity frameworks and regulatory environments presented through review of related literature. One of the frameworks is the Cybersecurity Framework released in 2014 by the National Institute of Standards and Technology (NIST). Establishing an internal cyber security policies and procedures, management of cyber security risk and the alignment to international information security standards will be the highlight of the literature review of this study. The Phase II will focus on the design, and analysis of a specific cyber security dealings guided by the standard regulatory framework intended for selected State Universities in Region III in the Philippines. Facing the threat of cyber-attacks, the researchers believed that educational administrators and leaders need to implement the right solutions to protect their resources from cyber threats. All organizations need to understand these cyber threats they face. The challenge now is the establishment of imperative tasks related to preservation of confidentiality, integrity and availability of information in the Cyberspace while facilitating an essential operating function.

Keywords: Cybersecurity; Framework; Cyber-attacks; Regulatory Framework; Confidentiality

1. Introduction

Countries heavily rely on cyberspace for everything, and everyone is vulnerable. Computer code connects millions of objects to the Internet which shapes the communication between the cyber and physical world. Our reliance on the confidentiality, availability, and integrity of data stands in stark contrast to the inadequacy of our Cybersecurity. The rapid growth of the information and communication technology networks in cyberspace according to Schjolberg and Ghernaouti-Hélie [1] has created new opportunities for criminals in perpetrating crime, and to exploit online vulnerabilities and attack countries' critical information infrastructure.

The Internet was not originally designed with security in mind, but as an open system that allows scientists, researchers, educators and anyone to send data to one another quickly. Without strong investments in Cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack. Malicious actors use cyberspace to steal data and intellectual property for their own economic or political goals. And an actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems.

* Corresponding author: Custodio Eunice Bondoc

Leaders must take steps to mitigate cyber risks. Governments, companies, and organizations should carefully prioritize the systems and data that they need to protect, assess risks and hazards, and make prudent investments in Cybersecurity and cyber defense capabilities to achieve their security goals and objectives. Behind these defense investments, organizations of every kind must build business continuity plans and be ready to operate in a degraded cyber environment where access to networks and data is uncertain. To mitigate risks in cyberspace requires a comprehensive strategy to counter and if necessary withstand disruptive and destructive attacks.

In this study, the researchers looked into the different Cybersecurity frameworks, the standards and its implementation in reducing cyber risks. According to the National Institute of Standards and Technology (NIST) [2], a framework is not a "one-size-fits-all" approach to managing cyber security risk. Organizations will continue to have unique risks, different threats, different risk tolerances, different vulnerabilities and how they implement the practices in the framework also vary.

The proliferation of cyber threats [3] and the effects of cyber-attacks [4] impelled the implementation of a Cybersecurity framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments. Even Universities wanted to secure important data from all the transactions that can be done online, like the research of Custodio and Castro [5], the Bulacan State University's prioritization of pre-enrollment procedure, online registration and grade evaluation system. As the framework is put into practice, lessons learned will be integrated into future versions. This will ensure if it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions of higher education institutions in the Philippines.

It is believes the Cybersecurity framework is an excellent way to approach the fundamentals of Cybersecurity which can provide foundation upon which the public sector can build greater protection against cyber threats and to have collaborative Cybersecurity partnerships among all levels of government.

2. Methodology

The main purpose of this study is to review related literature on Cybersecurity. Literature review on the policies and procedures, management of cyber security risk and the alignment to international information security standards will be the basis in proposing Cybersecurity framework intended for educational institutions specifically for higher education with online transactions. The researchers believe that every organization whether public or private, will continue to have unique risks, different threats, risk tolerances and vulnerabilities that are needed to be addressed. Policies, guidelines and procedure in the implementation of the proposed framework will concentrate essentially on the needs of the network infrastructure of higher education institutions.

3. Results and discussion

This section presents literature review on Cybersecurity framework, procedure, policies and implementation.

3.1. Perspectives on Cybersecurity Framework

Cybersecurity involves protecting information and systems from major cyber threats, such as cyber warfare, cyber terrorism, and cyber espionage. In their most disruptive form, cyber threats take aim at secret, political, military, or infrastructural assets of a particular nation or even its people. Therefore, Cybersecurity is a critical part of any governments' security strategy. Many countries are investing on infrastructure and allotting budget for Cybersecurity.

A framework can be used to align Cybersecurity decisions to mission objectives; 1) organize security requirements originating from legislation, policy, regulation, and industry best practice; 2) communicate Cybersecurity requirements with stakeholders, integrate privacy and civil liberties risk management into Cybersecurity activities; 3) measure current state and express desired state; 4) prioritize Cybersecurity resources and activities; 5) and analyze trade-offs between expenditure and risk [2]. The framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. As the framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

The NIST Cybersecurity Framework is a government's high-profile program to help private organizations in their Cybersecurity strategies. The framework addresses standards, guidelines and best practices to promote the protection of information and information systems.

The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. Version 1.0 of the framework was released on Feb. 12, 2014, along with a roadmap for future work. Based on the Executive Order, the Cybersecurity Framework must include the following: (a) include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks; (b) provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk; (c) identify areas for improvement to be addressed through future collaboration with particular sectors and standards-developing organizations; and (4) be consistent with voluntary international standards [2]. These are models presenting the process and procedure of the Cybersecurity Framework [6]:

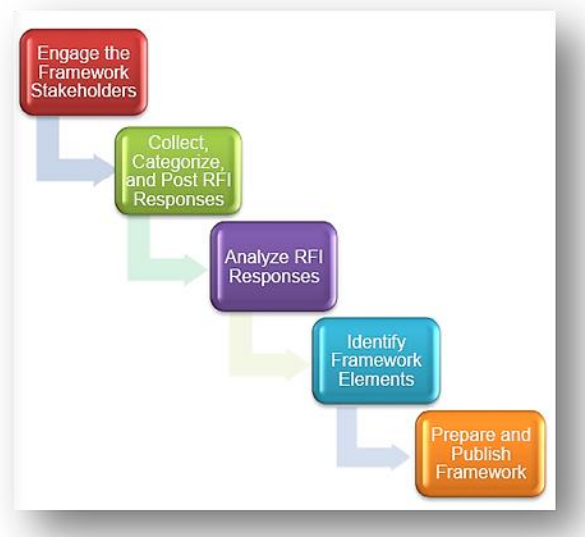

Figure 1 Framework Development

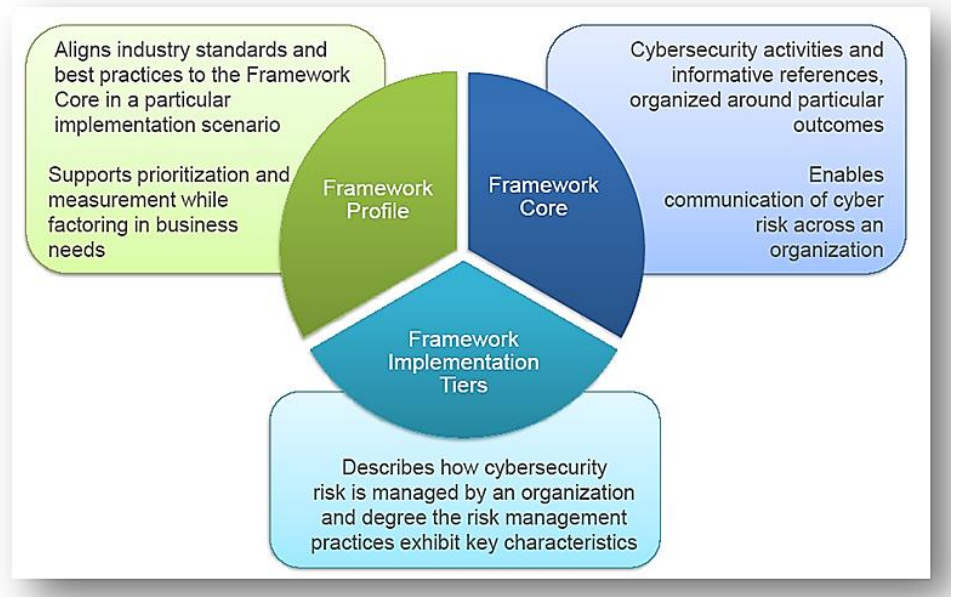

Figure 2 Framework Components

The framework components presents the alignment of functions, categories, and subcategories with business requirements, risk tolerance, and resources of the organization. Enables organizations to establish a roadmap for reducing Cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. Can be used to describe current state or desired target state of Cybersecurity activities [6].

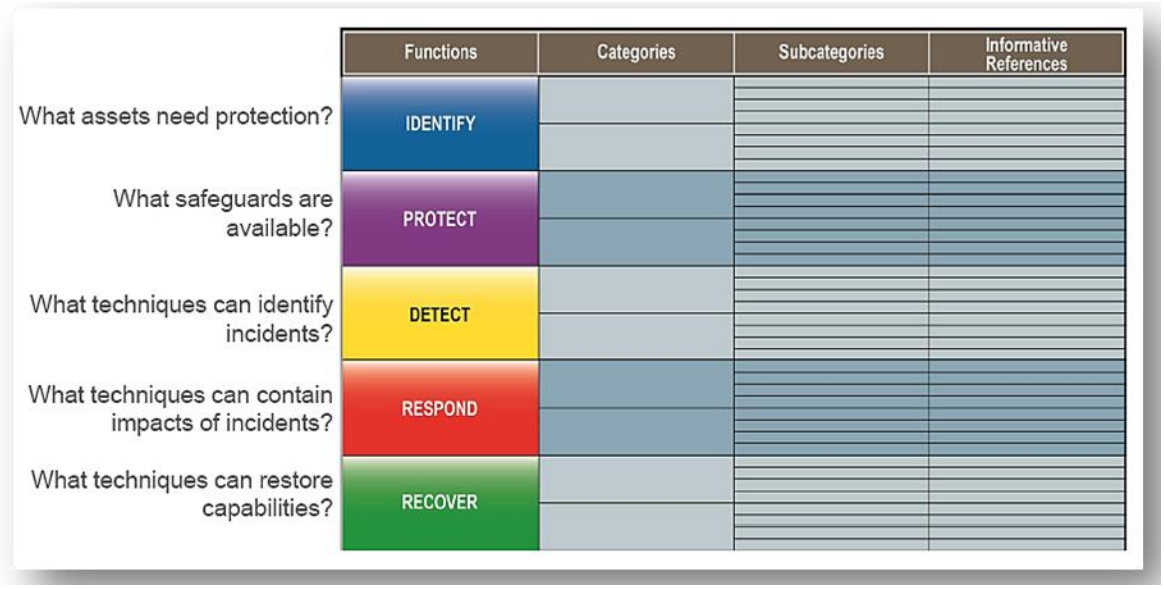

Figure 3 Framework Core

The Framework is designed to complement existing business and Cybersecurity operations, and can be used to: 1) Understand security status. Establish and Improve a Cybersecurity program, 2) Communicate Cybersecurity requirements with stakeholders, including partners and suppliers, 3) Identify opportunities for new or revised standards. Identify tools and technologies to help organizations use the Framework, and 4) Integrate privacy and civil liberties considerations into a Cybersecurity program [6].

The NIST Cybersecurity Framework (NIST CSF) provides a high level taxonomy of Cybersecurity outcomes and a methodology to assess and manage those outcomes. It is intended to help private sector organizations that provide critical infrastructure with guidance on how to protect it, along with relevant protections for privacy and civil liberties.

The NIST Cybersecurity framework provides a workable approach to protecting our bulk transmission system and are pleased to have been part of the development effort. Through collaboration, NIST aims at continuing to work with the federal government, companies in the electric industry and other stakeholders to advance its capabilities in protecting the assets.

3.2. Cybersecurity Strategy Framework

The newly created Department of Information and Communications Technology in the Philippines, through its attached agency the Cybercrime Investigation and Coordination Center (CICC), adapts to the new paradigm with the comprehensive National Cybersecurity Strategy Framework. The development of this framework expected to institutionalize the adoption and implementation of the information security governance as well as the risk management approaches. These globally recognized standards shall provide the government a systematic and methodical practice of ensuring the protection of all the critical and non-critical infrastructure from cyber-attacks through effective coordination with law enforcement agencies. The government shall build up its capability and capacity for quick response and recovery through the establishment of the National Computer Emergency Response Team (NCERT) [7].

There is an initiative known as the National Cybersecurity Plan 2022 [8] which primarily seeks to safeguard the ICT environment of the country through the establishment of a robust Cybersecurity infrastructure. Based on globally recognized standards, the framework will be able to institutionalize the adoption and implementation of information security governance and risk management approaches. It also aims to establish the NCERT to build the capability and capacity of the government for quick response and recovery during the hacking incidents and other cyber-attacks.

Domingo [9] said that cyber-attacks will continue to grow in number, scope, and impact; he pointed out that performing such attacks are less difficult than physical violence, and puts forward a valid observation that anonymity may be a factor in choosing to perpetrate crime or fraud, destruction and disruption, or enter into conflict via cyber-attacks over conventional means.

The Department of Justice (DOJ), Philippine National Police (PNP) and the National Bureau of Investigation (NBI) are the lead agencies for the investigation and prosecution of cybercrimes as well as the enforcement of Cybersecurity laws. While, the Department of National Defense (DND) will be in charge of defending the country from cyber-attacks; intelligence gathering of foreign cyber threats; securing national security and military systems and investigation of cybercrimes under military jurisdiction. Whereas, the Cybercrime Investigation and Coordination Center (CICC), one of the attached agencies of DICT, is mandated to establish Cybersecurity measures that would guard the country against cyber threats. It will enforce, evaluate and constantly monitor these Cybersecurity policies through regular assessment and compliance activities, conduct of annual cyber drills and exercises and Cybersecurity education and awareness program.

The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks. These published materials consist of collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies.

3.3. Cybersecurity Standards

Cybersecurity standards are techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. This environment includes users themselves, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks.

When identifying the most useful best-practice standards and guidance for implementing effective cyber security, it is important to establish the role that each fulfils, its scope and how it interacts with other standards and guidance. Cybersecurity standards are generally applicable to all organizations regardless of their size or the industry and sector in which they operate.

Protecting the Cybersecurity of our critical infrastructure is a top priority for every Nation. The Executive Order (EO) 13636 (2013) entitled *"Improving Critical Infrastructure Cybersecurity".* One of the major components of the E.O. is the development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to help critical infrastructure sectors and organizations reduce and manage their cyber risk regardless of size or Cybersecurity sophistication.

4. Conclusion

Effective Cybersecurity presents a complex challenge requiring collaboration from across the entire Internet environment. The Cybersecurity Framework builds in the necessary flexibility for effective implementation and continued innovation. This flexibility is vital, as it allows organizations to adapt and evolve as the threat landscape continuously shifts. The Cybersecurity Framework can shows international leadership by demonstrating that an effective partnership between government and industry which is the most effective way to fight cyber-attacks.

Establishing a framework of best practices and standards is an important step toward improving the country's critical infrastructure and security posture. Lastly, Cybersecurity framework is aimed at reducing and better managing Cybersecurity risks. The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation.

Compliance with ethical standards

Acknowledgments

The authors would like to express their gratitude and thanks to Angeles University Foundation and to Bulacan State University Administration for all the kind support and help. Thanks and appreciations to their family, colleagues, friends and relatives who supported them for the completion of this study and to the Almighty God who is always there to guide and help them.

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Schjolberg and Ghernaouti-Hélie. (2009). A global treaty on cybersecurity and cybercrime. 2nd edition.

[2] National Institute of Standards and Technology (NIST) Cybersecurity Framework. (2017).

[3] Walsh E. (2011).The cyber proliferation threats.

[4] What are the most common cyber-attacks? (2017).

[5] Custodio EB and Castro MDB. (2016).Advancing pre-enrollment procedure through online registration and grade evaluation system. International Journal of Signal Processing Systems, 4, 5.

[6] Framework for improving critical infrastructure cybersecurity. (2016).

[7] National Computer Emergency Response Team (NCERT). (2018). National Cybersecurity Plan 2022.

[8] Government launches National Cybersecurity Plan. (2016).

[9] Domingo F. (2013).Debunking Errors in a Proposed Philippine Cybersecurity Framework, Philippine Daily Inquirer.

How to cite this article

Custodio EB and Tumibay GM. (2020). Cybersecurity for higher education institutions: adopting regulatory framework. Global Journal of Engineering and Technology Advances, 2(3), 16-21.