International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Framework for Improving Critical Infrastructure Cyber Security

Naby Nouhou Nassou Conde[1], Jamaludin Bin Abrahim[2]

[1]Department of Information System, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

[2]Professor, Department of Information System, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

Abstract: ***Cyber security are becoming vital in the national critical infrastructure systems. Due to the rapid increase of sophisticated cyber threats with exponentially destructive effects, security systems become systematically evolve. The security aspects of ICS are broad, ranging from security for, hardware/firmware used in industrial control systems to system aspects of ICS such as secure architectures and vulnerability screening to the human aspects of cyber security and training. Both research and practical aspects of security considerations in systems are in interest. In this paper, this special issue focuses on innovative methods and techniques called framework in order to address unique security issues relating to ICS.***

Keywords: Critical, Infrastructure, Cybersecurity, Framework, protection, cyber, crime

1. Introduction

The national and economic security depend on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure (Obama, 2013), every nation has to improve the Critical Infrastructure Cybersecurity. To better protect these systems, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013. This Executive Order calls for the development of a voluntary Cybersecurity Framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk and to have a consistent and iterative approach to identify, assess, and manage cybersecurity risk.

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to (National Institute of Standards and Technology, February 12, 2014);

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state;
- Communicate among internal and external stakeholders aboutcybersecurity risk.

The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology (IT) and industrial control systems (ICS). This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organization's business, assets, health and safety of individuals, and the environment should be considered. To manage cybersecurity risks, a clear understanding of the organization's business drivers and security considerations specific to its use of IT and ICS is required. Because each organization's risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary.

1.1 Framework Core

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by industry as helpful in managing cybersecurity risk. The Core comprises four elements: Functions, Categories, Subcategories, and Informative References, depicted below.



Figure 1: Framework Core Structure (NIST, February 12, 2014)

The Framework Core elements work together as follows (National Institute of Standards and Technology, January 10, 2017):

a) **Functions** organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by

Licensed Under Creative Commons Attribution CC BY

organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.

The five Framework Core Functions are defined below. These Functions are not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.

- **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The respond function supports the ability to contain the impact of a potential cybersecurity event.
- **Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements and communication.

b) **Categories** are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include Asset Management, Access Control, and detection processes.

c) **Subcategories** further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include External information systems are catalogued, Data-at-rest is protected, and Notifications from detection systems are investigated.

d) **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the framework development process.

1.2 Framework Profile

The Framework Profile is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile 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. Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

1.3 Framework Implementation Tiers

The Framework Implementation Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor and sophistication in cybersecurity risk management practices and the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.

The Tier definitions are as follows:

Tier 1: Partial

- Risk Management Process: Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Integrated Risk Management Program: There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.

Licensed Under Creative Commons Attribution CC BY

- External Participation: An organization may not have the processes in place to participate in coordination or collaboration with other entities.

Tier 2: Risk Informed

- Risk Management Process Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/ mission requirements.
- Integrated Risk Management Program: There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.
- External Participation: The organization knows its role in the larger ecosystem, but has not formalized his capabilities to interact and share information externally.

Tier 3: Repeatable

- Risk Management Process: The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- Integrated Risk Management Program: There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
- External Participation: The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.

Tier 4: Adaptive

- Risk Management Process: The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- Integrated Risk Management Program: There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
- External Participation: The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.

1.4 Coordination of Framework Implementation

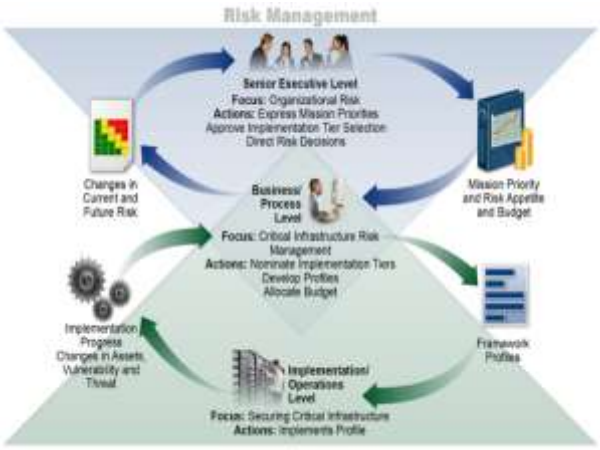

Figure 2: National Information and Decision Flows within an Organization (National Institute of Standards and Technology, January 10, 2017).

Figure 2 describes a common flow of information and decisions at the following levels within an Organization:

- Executive
- Business/Process
- Implementation/Operations

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into the risk management process, and then collaborates with the implementation/operations level to communicate business needs and create a Profile. The implementation/operations level communicates the Profile implementation progress to the business/process level. The business/process level uses this information to perform an impact assessment. Business/process level management reports the outcomes of that impact assessment to the executive level to inform the organization's overall risk management process and to the implementation/operations level for awareness of business impact.

1.5 How to Use the Framework (Ross et al, November 2016).

An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk. The Framework is not designed to replace existing processes; an organization can use its current process and overlay it onto the Framework to determine gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Utilizing the Framework as a cybersecurity risk management tool, an organization can determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.

Licensed Under Creative Commons Attribution CC BY

The Framework is designed to complement existing business and cybersecurity operations. It can serve as the foundation for a new cybersecurity program or a mechanism for improving an existing program. The Framework provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization's cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program. The following sections present different ways in which organizations can use the Framework.

2. Conclusion

The descriptive study so far done above carries some concluding remarks. Owners and operators of critical infrastructure have the primary responsibility for the security of their networks and have proven motivated and effective in addressing increasing and evolving cyber threats. Moving forward, continuation of a voluntary public-private partnership model will be key to provide the flexibility needed to address threats as they evolve. Developing countries will have to embrace technology in order to supplement traditional methods of communication. This will allow vital information to be communicated in the event that traditional modes are unavailable. For instance, should communication via email not be possible, information could be exchanged via SMS messages or fax. When it comes to cybersecurity, industry recognizes that everyone, governments, ICT manufacturers, owners and operators are in this fight together, with industry participants setting aside their own competitive interests to solve a problem that concerns all.

Finally, developing nations have to invest in broad-based awareness programs to ensure that new users are aware of the risks associated with their activities in cyber space. Such programs benefit users as well as the nation as a whole. Critical systems are connected by the same networks that are used by the general public reducing threats and vulnerabilities at the user end helps protect critical systems as well as underlying information infrastructure. Modern critical systems rely heavily on information infrastructures in order to operate efficiently this is true for developed countries as well as developing countries.

References

[1] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
[2] *NIST. (2014).* Framework for improving critical infrastructure cybersecurity. Retrieved February 6, 2015, from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
[3] NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Boyens et al, April 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 161.pdf
[4] NIST Special Publication 800-160: System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Ross et al, November 2016, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
[5] Karchefsky S., Rao H.R. (2017) Toward a Safer Tomorrow: Cybersecurity and Critical Infrastructure. In: Ellermann H., Kreutter P., Messner W. (Eds) The Palgrave Handbook of Managing Continuous Business Transformation. Palgrave Macmillan, London.
[6] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity retrieved January 10, 2017, from https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf

Licensed Under Creative Commons Attribution CC BY