CYBERSECURITY ORGANIZATIONAL STRUCTURE & GOVERNANCE

Authored by:
David Stone, Principal

INTRODUCTION

Healthcare organizations are under constant threat of unauthorized access to their computing environments. Organizations face everything from monitoring by regulatory agencies to high penalties if unauthorized access and data breaches occur. As healthcare moves quickly to address computing environment threats, it is prudent to leverage the frameworks and models developed by non-healthcare entities to speed the deployment of effective solutions. In this paper we will examine two popular frameworks, the Three Lines of Defense Model and the National Institute of Standards and Technology (NIST) Cyber Security Framework, and how they can be leveraged to optimize an information security organizational and governance structure.

As healthcare organizations decide how best to address the constantly changing cybersecurity threat landscape, they have many important questions to answer:

- What gaps and vulnerabilities exist in the current information security program?
- What are the components of a complete information security program?
- How should roles and responsibilities be assigned?
- What is the most effective governance structure?
- How should an information security team be structured?
- What technologies should be deployed?

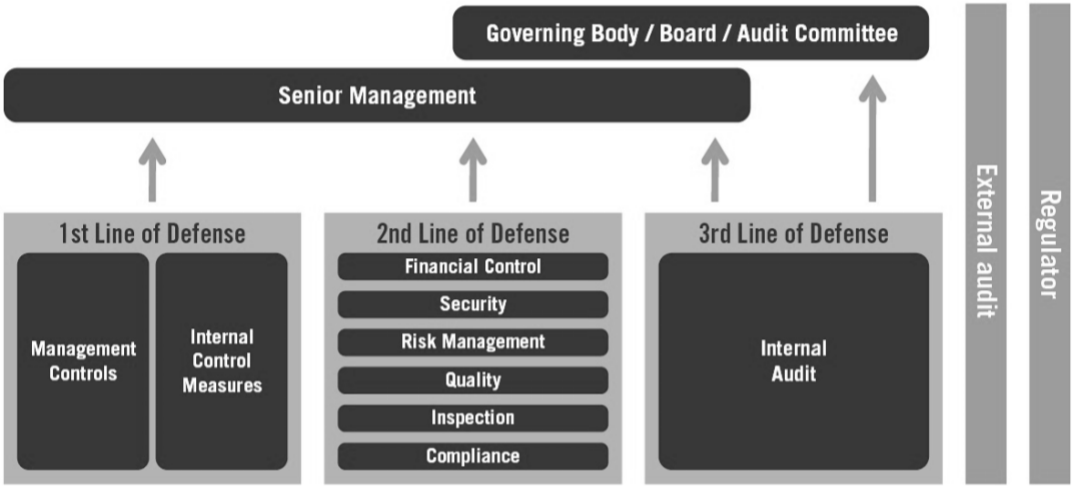
While healthcare information technology and security organizations have been aware of increasing issues and concerns, they have not been provided the attention or, more importantly, the funding needed to fully address security threats. With the recent attention healthcare is receiving from data thieves, regulatory agencies, and the media, healthcare executive management and boards of directors are demanding appropriate steps be taken to protect IT and data assets.

Other industries, particularly the financial industry, have dealt these issues and level of scrutiny for many years. Multiple industry groups have examined the issue of cybersecurity and developed different models and frameworks to assist their peers in deploying counter measures. When combined, the following two frameworks provide an excellent blueprint for establishing an effective information security program and an optimized organization.

The Three Lines of Defense Model

In 2013, the Institute of Internal Auditors (IIA) published a paper titled The Three Lines of Defense in Effective Risk Management and Control. The concept was again addressed in another paper issued in June 2017. Figure 1 is a graphical representation of this model.

Figure 1: Three Lines of Defense Model[1]



Line One – Own and Manage Risk

Line One conducts day to day security operations. This can be a dedicated security team, or it can be individuals or a team which typically performs another function. For instance, a network team has the primary task of ensuring the network is available and data flows to destinations as expected. However, there is also a security Line One function to ensure network equipment is up to date with security patching and to deploy access controls to keep unauthorized traffic from reaching unintended destinations.

Line One has the ultimate responsibility to deploy effective controls based on what's specified by the governance process at Line Two. To operate effective security controls, Line One also needs to ensure monitoring is in place to validate that controls are operating as intended.

Line One Managers:

- Own and manage risks and implement corrective actions to address process and control deficiencies.
- Guide the development and implementation of internal policies and procedures and ensure activities are consistent with goals and objectives.
- Implement and manage managerial and supervisory functions to maintain compliance and to highlight control breakdown, inadequate processes, and unexpected events.

Line Two – Oversee Risk

Line Two of defense provides security governance (policies and standards) and oversight by monitoring the controls deployed by Line One. Governance is essential as it presents clear expectations to all workforce members. Monitoring serves as an oversight function reporting both up and down the lines, as well as to senior management, that security controls are operating properly. In cases where Line One is providing monitoring, the Line Two function may merely provide oversight that the monitoring solution is in place and is effective. The same holds true where Line Two performs the primary monitoring of Line One controls – it is not necessary for both lines to perform monitoring as long as Line Two provides the oversight.

Line Two activities, which are typically performed by the information security team, include:

- Support management policies, define roles and responsibilities, and set goals for implementation.
- Provide risk management frameworks.
- Identify known and emerging issues and shifts in the organization's implicit risk tolerance.
- Assist management in developing processes and controls to manage risks and issues.
- Provide guidance and training on risk management processes.
- Facilitate and monitor implementation of effective risk management practices by operational management.
- Alert operational management to emerging issues and changing regulatory and risk scenarios.
- Monitor the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.

Line Three – Provide Independent Assurance

Line Three of defense is assurance, which is typically provided by the internal or external audit function. In this line of defense, security controls are validated by testing both their design and effectiveness. As an independent function, Line Three provides assurance to senior management and the Board of Directors that security monitoring, and the entire security program, are effective.

Line Three activities, which are typically performed by internal or external IT auditors, include:

- Report how well the first and second lines adhere to the organization's cyber risk framework
- Independently validate the IT organization's asset inventory and associated risk profiles
- Evaluate third party risks
- Conduct independent penetration tests and vulnerability assessments
- Review internal audit procedures and enhance, where appropriate, with cybersecurity considerations

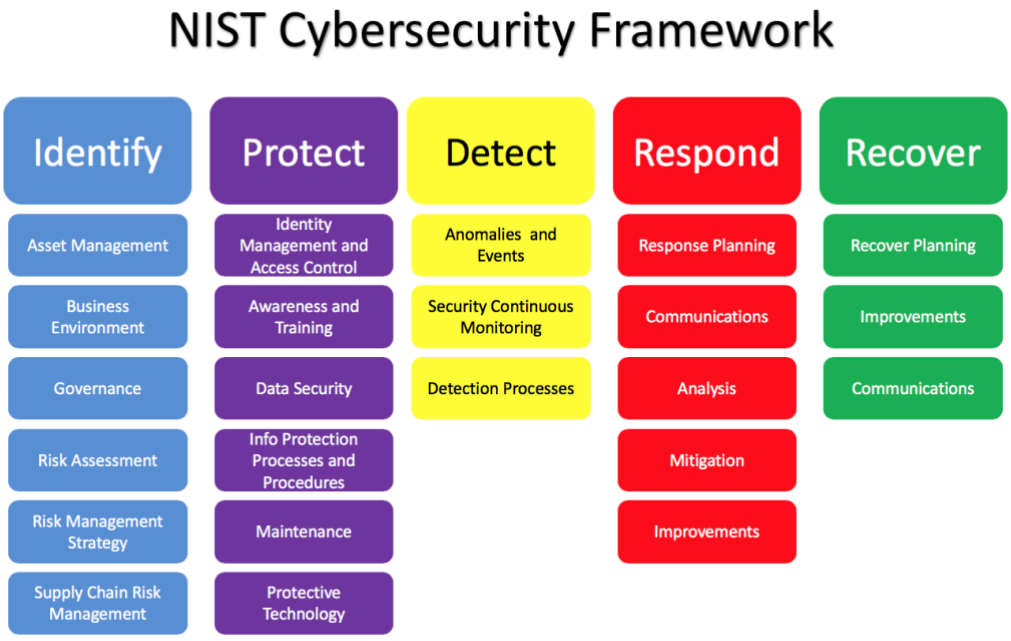
It is important to note that for the Three Lines of Defense model to be most effective, the functions of each line must be performed by separate groups. That is, the day to day deployment and management of security controls should not be done by the same group who sets the policies and standards and provides oversight that the controls are operating effectively.

NIST Cybersecurity Framework

In 2014, responding to the increasing risk to the nation's information technology infrastructure, NIST developed a framework for establishing and maintaining an information security program. The framework was updated in April 2018.

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce information security risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and security management communications amongst both internal and external organizational stakeholders. Figure 2 below shows the NIST categories and associated subcategories.

Figure 2: Graphical representation of the NIST framework, version 1.1[2]



Source: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018

Below is an overview of each of the five facets of the NIST Cybersecurity Framework:

1. Identify

The activities in the Identify Function are foundational for an information security program. This function relates directly to the development of organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. As it relates to the business and clinical context, the resources that support critical functions and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of supporting activities are asset management, governance, and risk assessment and management.

2. Protect

The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. It establishes the appropriate safeguards to ensure delivery of critical infrastructure services. Examples of supporting activities include access control, awareness and training, data security, and use of protective technology.

3. Detect

The Detect Function facilitates the timely discovery of cybersecurity events. It is intended to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Examples of supporting activities include intrusion detection and behavior analysis.

4. Respond

The Respond Function supports the ability to contain the impact of a potential cybersecurity event. This function ensures the appropriate activities to take action regarding a detected cybersecurity event are developed and implemented. Examples of supporting activities include response planning and communications.

5. Recover

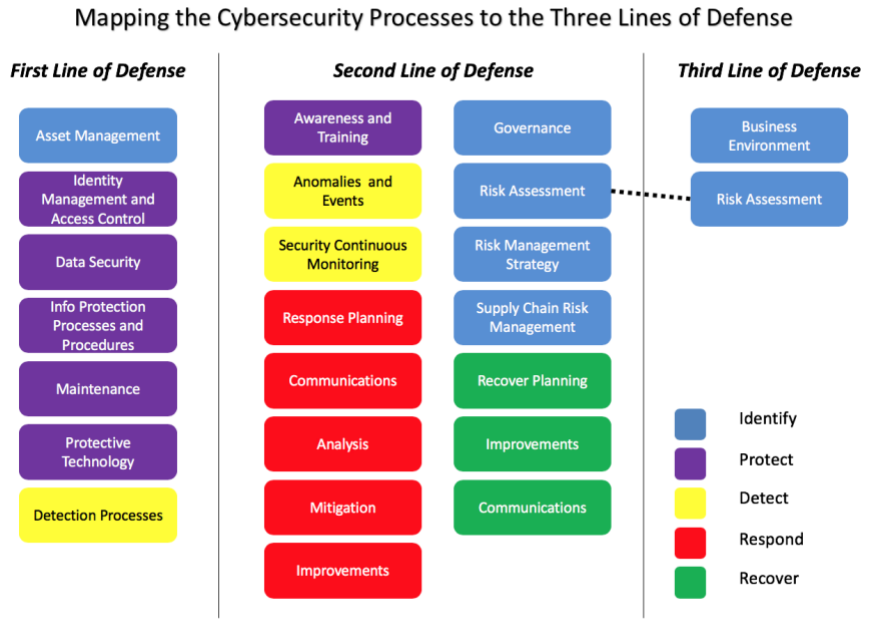
The Recover Function supports timely recovery to normal operations to reduce impact from a cybersecurity event. The purpose of this function is to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Examples of supporting activities include disaster recovery planning and business contingency planning.

Organizational: Mapping the Framework to the Model

Deciding how to combine the NIST Framework to the Three Lines of Defense Model is not a simple process of placing each Framework Category in the appropriate Line of Defense. You must examine each subcategory and, based on the maturity of your IT and information security organizations, determine (1) which line of defense is appropriate and (2) who within your organization should have this specific responsibility. The mapping presented in Figure 3 should serve as a good starting point.

As you move through this process for your organization, you may have to accept the fact that your current IT and/or information security organizations are inadequate or may be incompatible with the Three Lines of Defense model. In these instances, I would recommend taking a fresh look at your current organizational and governance structures and consider a significant restructuring. These models have been used successfully by many organizations to implement cybersecurity protections and controls and are considered to be best practice.

Figure 3: Mapping the Framework to the Model [2]



Source: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018

Technology and Process: Mapping the Framework to the Model

A frequent question, along with the most effective organizational structure, is what supporting processes and technologies should be implemented to support the information security program. The models themselves do not specify technologies but identify needed functionality and capabilities. Figure 4 presents an overview of the processes and technologies that can support each line of defense.

An important consideration is the need for formal, written policies, standards and procedures. These written documents provide the tools to audit and measure the effectiveness of the information security program. NIST Special Publication 800-53[3] can be very helpful in identifying the areas for which policies, standards and procedures are needed.

Policies are clear, simple statements which provide direction to the organization in order to conduct its services, actions or business. A policy provides definitive requirements to help with decision-making; it should identify issues and scope and address "why" it is a requirement.

Example: *Establish principles that will safeguard access to the information systems and data, including sensitive systems and data (i.e., PHI, PCI, etc.), to ensure the confidentiality, integrity, and availability of business data and help minimize exposure to unauthorized disclosure or theft of information, fraud, and possible litigation.*

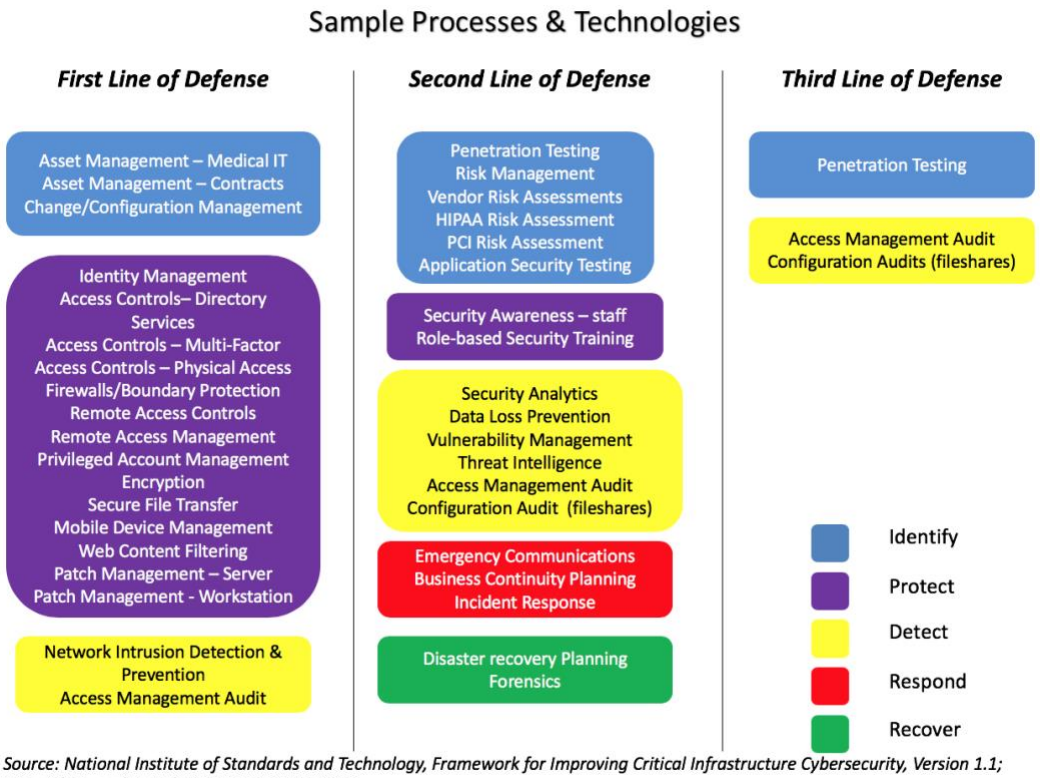
Standards detail the fundamental provisions or requirements of the policy. A standard assigns specific, mandatory controls; it addresses "what" is required.

Example: *The System Owner shall create a process for notifying account managers when temporary accounts are no longer required and when workforce members are terminated, transferred, or need-to-know/need-to-share changes.*

Procedures specify the tasks required to deliver the controls stated in the standards. Procedures are susceptible to change, particularly when new technologies or best practices emerge; they address "how" a requirement is implemented or enforced.

Example: *Upon termination notice given by a Workforce Member, access to applications will be revoked and suspended based on the end date provided in the termination notice is completed and submitted by the Workforce Member's supervisor or manager.*

Figure 4: Sample Processes and Technologies [2]



Source: National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018

CONCLUSION

Every organization has its own unique challenges and organizational realities. The information presented in this paper can be very helpful in assessing your current organization and identifying functionality gaps. To get started:

- Review and, where necessary, strengthen your governance structure around cybersecurity. Security is the responsibility of all areas within the organization, so there needs to be involvement by all major business and clinical areas.
- Use the 17 security control families from the NIST Special Publication 800-53[3] to verify policies are in place for all subject areas within a comprehensive information security program.
- Review you current catalog of services and make sure all of the identified functional areas are addressed.
- Review how roles and responsibilities are divided. Properly separating Line One and Line Two functionality can be confusing and requires consensus between Line One and Line Two teams.
- Identify where technology can add real value. You need to avoid being tool rich with overlapping functionality and expensive "shelfware."

Establishing an effective organization that supports an information security program is hard. Hopefully, the intersection of these two models will provide a framework for success.

To discuss how the NIST Cybersecurity Framework and the Three Lines of Defense Model could help your organization, contact me at David.stone@divurgent.com.

ABOUT THE AUTHOR

David Stone, Principal
www.divurgent.com | Follow David on LinkedIn
As Principal, David leads Divurgent's strategic information technology and cybersecurity projects and a diverse portfolio in each area. With over 40 years of IT experience, over 20 of those years are in healthcare, David leverages his multi-industry experience to provide new perspectives on the use of information technology within a healthcare setting.

With expertise ranging from establishing IT organization from the ground up, optimizing EHR platforms, managing large-scale, complex technology projects, applying data-driven analytics, to leveraging clinical data to improve clinical processes and quality of care and establishing security processes, procedures, and policies.

David has held numerous positions including CIO, Information Security Officer, Program Manager, Project Manager, and Director of Applications, where he's been able to apply his years of dynamic experience in information technology and apply innovation solutions to today's top-of-mind IT challenges. When David is part of the consulting team, an organization gets more than just the knowledge and expertise to complete his assignment, they also get access to an experienced IT executive that can and will provide other value add expertise and guidance to the organization.

While David's healthcare experience spans multiple ambulatory and acute care settings, he has a strong focus in pediatric facilities.

REFERENCES

1. *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control; The Institute of Internal Auditors, January 2013; https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf*
2. *National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1; https://doi.org/10.6028/NIST.CSWP.04162018*
3. *National Institute of Standards and Technology Special Publication 800-53 Revision 4; Security and Privacy Controls for Federal Information Systems and Organizations; Joint Task Force Transformation Initiative; http://dx.doi.org/10.6028/NIST.SP.800-53r4*