The ISO 27001 and The NIST Framework: Strengths and Weaknesses

Information Security has many frameworks that can be utilized by organizations to make a cybersecurity plan. Preserving the confidentiality, integrity, and availability of information can be a difficult task. Organizations are often very complex, and it is difficult to ensure that all possible risks are identified, and that the best measures are in place to counteract them. Frameworks simplify the process, providing guidelines, best practices, and even the opportunity for certifications. In this essay, I will discuss the pros and cons of the NIST Framework for Improving Critical Infrastructure Security and the ISO 27001, as well as how they relate to an organization in the health industry.

The structure of the NIST Cybersecurity Framework consists of three main parts; the Framework Core, tiers, and profiles. The core itself is divided into five subcomponents called "functions." These functions are identify, protect, detect, respond and recover, and are meant to be performed continuously and concurrently. Performing the functions in this way is necessary in order to secure a system, and none should be neglected or left out. The functions are further divided into categories and subcategories that specify what activities are necessary to perform each core function (Winter, 2014).

Tiers describe an organization's approach and level of immersion with regards to cybersecurity. There are four tiers, ranging from the most basic level of security at tier one, to a very comprehensive security approach at level four. Depending on the amount of resources an organization is willing to put aside for cybersecurity, as well at the value of the information it is protecting, the organization would select the tier that is most appropriate for it. These tiers then direct the organization with guidelines for meeting its goals (Winter, 2014).

Profiles are the third component of the NIST Framework. These combine the core functions with the organization’s risk tolerance, resources, and industry requirements in order to construct a cybersecurity plan. The organization can create a current profile as well as a target one. The former refers to a profile that describes what the organization is currently doing, while the target profile describes what the organization aims to do in the future. These profiles serve as a guide for the organization’s efforts (Winter, 2014).

The biggest advantage of the NIST Framework is its flexibility. The Framework does not tell an organization exactly how to implement cybersecurity. Instead, it guides the organization towards figuring out what it needs, what goals to set, and how to meet its objectives. The suggestions and best practices within the Framework are guidelines and provide a high level of customization. The tiers, for example, allow an organization to choose a level of security based on its available resources and tolerance for risk. This makes it usable by almost any organization, big or small (Chaput, 2017).

The adaptability of the NIST Framework makes collaboration between different industries much easier. A health organization might have a need for collaboration with the financial industry, the IT sector, and other sectors that it is dependent on. Having a common framework facilitates this process, while ensuring that there are no gaps in security (Chaput, 2017).

One drawback of the NIST Framework is its potential for redundancy. Cybersecurity risks are becoming more complicated and expensive to manage, which leads to organizations relying on third parties to assist with security. However, when multiple different organizations are implementing the same policies, they are using more resources from these third parties than they would if they collaborated. Putting strain on limited resources is never a good thing, and the guidelines within the NIST Framework have the potential to discourage coordination rather than encourage it (Leithauser, 2013).

Similarly, the NIST Framework is not universal or used internationally, which can cause issues when communicating or working with an organization in another country. According to Leithauser, "Cybersecurity approaches that differ dramatically by country—a policy patchwork—not only present potentially negative consequences for security, but also disrupt global commerce and ignore the borderless nature of the Internet" (2013). This is fine for organizations that operate solely in the United States, and as mentioned above, the adaptability of the NIST Framework may even present an advantage for them. However, organizations that collaborate internationally are likely to run into issues. For example, online retailers may want to adhere more closely to international standards. Organizations like those should choose a different framework that is more globally relevant in order to smoothly incorporate international standards (Leithauser, 2013).

Additionally, some organizations already have security measures in place before beginning to use the NIST Framework, and they might end up with overlapping measures as a result of implementing it. Because of this, it is important to make sure that the NIST Framework is fully integrated into an organization's security policies instead of being slapped on top of them (Leithauser, 2013). This might require amending or eliminating parts of the system that contradict each other or are redundant. It may even be easier to scrap the existing system and start from scratch in order to ensure that it runs smoothly and covers all its bases. However, this can be costly and time-consuming, and many organizations elect to take the easier route.

ISO 27001 is more specific in its requirements than NIST's Framework. It guides an organization through a risk analysis in order to identify what needs to be protected. It also includes requirements for security and defines how each one must be implemented. An example requirement has to do with an organization's "performance evaluation," under which ISO defines the ways in which security must be monitored, measured, managed, and reviewed. ISO lists fourteen domains that security controls fall under, including access control, cryptography, compliance, and communications security. A total of 114 controls fall under these categories; organizations are expected to choose the ones that best fit their risks and needs ("What is ISO 27001?," 2020).

ISO 27001 is comprehensive and provides organizations with many pre-defined options. Its list of domains encompasses every aspect of an organization that would need to be protected in a holistic security system. The regulations within the framework are structured so that the organization will end up with a security plan that protects every part of the organization (Kenyon, 2019). It walks an organization through the process and makes choosing security controls fairly simple by categorizing them and presenting them in a table, similar to a menu. Doing this makes it possible for even less experienced organizations to create a comprehensive security plan ("What is ISO 27001?," 2020).

However, this strength can also be a weakness. Unlike the NIST Framework, ISO 27001 does not have the same level of flexibility. An organization attempting to create a cybersecurity plan that cannot or does not want to adhere to ISO 27001's strict requirements would need to use a different, more flexible framework (Kenyon, 2019). A framework that is too rigid cannot be effectively adapted to situations it does not fit. While its list of controls is long and provides many options, there are still requirements to be met that can be constraining for an organization that wants to take a different approach.

Its usage internationally is one strength of ISO 27001. Organizations from all over the world use it, which facilitates collaboration between them even when they belong to different countries. This is different from the NIST Framework, which is exclusively used in the United States. Because of this difference, organizations that regularly communicate and work with organizations in other countries would find ISO 27001 to be more effective and less likely to create gaps in security (Everett, 2011).

ISO 27001 also provides the potential for certification. An organization that becomes certified by ISO must be compliant with its requirements. Being certified by ISO is an advantage for any organization because the certification is a verifiable way of proving to customers, clients, and business partners that the organization has security controls in place. Because ISO 27001 is so comprehensive, the requirements for certification ensure that a very reliable security plan is in place (“What is ISO 27001?,” 2020).

The biggest drawback to ISO 27001 is its costliness. Unlike the NIST Framework, compliance with ISO 27001 involves a higher minimum level of security that must be implemented throughout the entire organization, not just specific parts of it. For smaller organizations, the cost for this level of security can be an issue. For larger organizations, the fact that the required policies and procedures must be implemented throughout makes it time-consuming and difficult. Organizations have less wiggle-room when it comes to deciding how much they want to spend on ensuring security (Everett, 2011).

Either of these frameworks are usable by a public health organization. However, I believe that ISO 27001 is the better fit. A health organization has lots of sensitive patient information and the cost of implementing a more rigid security plan is worth the protection it would provide. Additionally, complying to international standards might provide them with an advantage over using the NIST Framework. While they likely aren’t communicating with organizations in other countries as much as, for example, an online retailer might, there still is enough communication that ISO 27001 might be beneficial. Finally, an ISO certification adds an extra level of trust between patients and the organization. While it may take months or years to make sure that policies are properly implemented across the organization, the payoff is worth the amount of time invested.

References

Chaput, B. (2017). NIST cybersecurity framework offers both integration and customization. Health Management Technology, 38(11), 24. Retrieved from http://proxy.lib.odu.edu/login?url=https://www-proquest-com.proxy.lib.odu.edu/docview/1970110109?accountid=12967

Everett, C. (2011). Is ISO 27001 worth it? Computer Fraud & Security, 2011(1), 5-7.

Kenyon, B. (2019). ISO 27001 controls – A guide to implementing and auditing (1st ed.). IT Governance Publishing.

Leithauser, T. (2013). REDUNDANCY, GLOBAL VARIATIONS CITED AS HAZARDS FOR NIST's CYBER FRAMEWORK. Cybersecurity Policy Report, , 1. Retrieved from http://proxy.lib.odu.edu/login?url=https://www-proquest-com.proxy.lib.odu.edu/docview/1352742214?accountid=12967

What is ISO 27001? A beginner's guide. (2020, July 17). Retrieved October 12, 2020, from https://advisera.com/27001academy/what-is-iso-27001/

Winter, K. (2014). Technology: Dissecting the first version of the NIST's cybersecurity framework. Inside Counsel.Breaking News, Retrieved from http://proxy.lib.odu.edu/login?url=https://www-proquest-com.proxy.lib.odu.edu/docview/1504934944?accountid=12967