A Socio-Technical Analysis and Critique of the NIST and NICE Cybersecurity Frameworks and How They Could Be Improved

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Samantha Jade Chiang

Spring 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

The field of cybersecurity is one that is fast paced and quickly evolving, to the point that methods and techniques from just a few years ago are already sorely outdated. The government aids in stressing the importance of cybersecurity by creating the National Institute of Standards and Technology (NIST) and tasking it with the job of creating a framework for companies to follow in order to "us[e] business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the organization's risk management processes … to improve cybersecurity risk management in critical infrastructure" ("Framework for improving critical infrastructure cybersecurity", 2018, p. vi). After an initial release in 2014, version 1.1 was drafted in 2017 before being released publicly in 2018. Since then, it has not seen any updates to combat the evolution of the field. In addition to being outdated, it is also often criticized for being hard to understand and does not properly stress the overall importance of cybersecurity. Despite this, many companies currently use this framework as a basis for their security plans. According to the Trends in Security Framework Adoption Survey, approximately 70% of companies surveyed incorporated it into their cybersecurity plans (Dark Reading Staff, 2016). This insecure method of protecting their systems and data could potentially lead to the leaking or loss of sensitive information and other potential losses. To best answer this pressing issue, I consulted research papers in the field of cybersecurity that talked at length about the NIST framework itself, as well as others that discussed the sphere of cybersecurity in its current form. I also reviewed the National Initiative for Cybersecurity Education (NICE) Framework, which aims to provide education about cybersecurity to individuals of an organization. Having been published later, in 2020, it does not provide additional information but only methods an employer can use to easily convey cybersecurity information to employees. In this paper, I argue

that the creation of a simplified, up-to-date, and extensive framework intended for use in both the private and public sector, will prove to be much more useful than the measures currently in place. Though the NIST framework has many flaws, this, and other similar guidelines (such as the NICE framework) provide a firm basis for a better framework. This paper indicates where the current measures and practices are lacking, particularly in the non-technical aspects and lack of consideration towards smaller companies. To support these claims, the paper will also delve into criticisms from experts in the field before proposing changes that would create a framework that suits the field of cybersecurity as it stands today.

The NIST Cybersecurity Framework and its Dominant Role in the Field

The NIST framework seeks to provide its target audience, typically companies in the private sector, with an outline of cybersecurity practices to be used in the company's plan of defense. To accomplish this task, the framework divides itself into three primary components, the Core, the Implementation Tiers, and the Profile. At its Core, it aims to fulfill five main functions: Identify, which aims to "[d]evelop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities"; Protect, with the purpose of "[d]evelop[ing] and implement[ing] the appropriate safeguards to ensure delivery of critical infrastructure services"; Detect, "[d]evelop and implement the appropriate activities to identify the occurrence of a cybersecurity threat"; Respond, "[d]evelop and implement the appropriate activities to take action regarding a detected cybersecurity event"; and Recover , "[d]evelop 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" ("Framework for improving critical infrastructure cybersecurity", 2018, p. 45-46). Each of these functions are further divided into categories and subcategories that more precisely define the role that each function hopes to

fulfill. For example, a category of the Protect function is Identity Management, Authentication, and Access Control (PRAC). Its goal is to ensure that only authorized users can access certain information and content. PRAC has seven further subcategories, each dealing with specific variables within the category, and contains references to further resources. These functions are not intended to be a step-by-step guide to follow in the event of a cybersecurity attack, but rather a sort of list to be referenced when developing a risk management process. This means, as an example, that the Respond function does not only become relevant when an attack does happen, but also should continuously be tested and run independently.

The Tiers define a set of four tiers, from Tier 1 (Partial), Tier 2 (Risk Informed), Tier 3 (Repeatable), and Tier 4 (Adaptive). These tiers describe a company's own cybersecurity methods, and to what extent it implements the practices described within the framework. It is heavily suggested to at least move up from Tier 1, but "the framework does not advocate that all organizations seek the most sophisticated tier; rather the framework indicates that an organization should select the tier that meets the organizations' objectives..." (Clark et al., 2018, p.42). In a cost-benefit analysis, a company must examine how much resources they are willing to invest into their cybersecurity plan, and what priority it holds over other factors or divisions. It is meant to answer such questions as: would having a lesser risk of an attack be a suitable payoff for not being to provide funding to other departments?

The final part of the framework, the Profile is the result that the company faces when selecting the Functions it desires to fulfill, and to what extent, including the categories and subcategories it selects. There is both a Current Profile, where the cybersecurity of the company is currently, and the Target Profile, which is the desired final stage. In this part of the framework, the most important categories and subcategories are identified and prioritized above others.

The document, at a full 55 pages (not including extended readings and references) does not tout itself as " a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure … Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks" ("Framework for improving critical infrastructure cybersecurity", 2018, p. vi). It reinforces the need for companies to use it in conjunction with their existing cybersecurity plans and efforts, as well as emphasizing the fact that unpredictable things may occur. One upside it does offer is that it is technology neutral. In other words, it does not cater to the use of a specific software to accomplish the goals that it sets out, forcing companies to invest in technologies when they already have a suitable substitute.

While there is no direct update to the NIST framework, NIST has published the NICE Framework. Instead of updating the actual cybersecurity practices themselves, it instead focuses on how to teach these practices in the workplace. It describes itself as a "fundamental reference for describing and sharing information about cybersecurity work [and] is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity education, training, and workforce development" (Peterson et. al., 2020, p. ii). In contrast to this NIST framework, the NICE framework is split into three main components, called Building Blocks: Tasks, Knowledge, and Skills (see Figure 1). It is also important to note the use of the terms "the learner," the employees to be implementing the practices being taught, and "the work," which are the practices themselves.

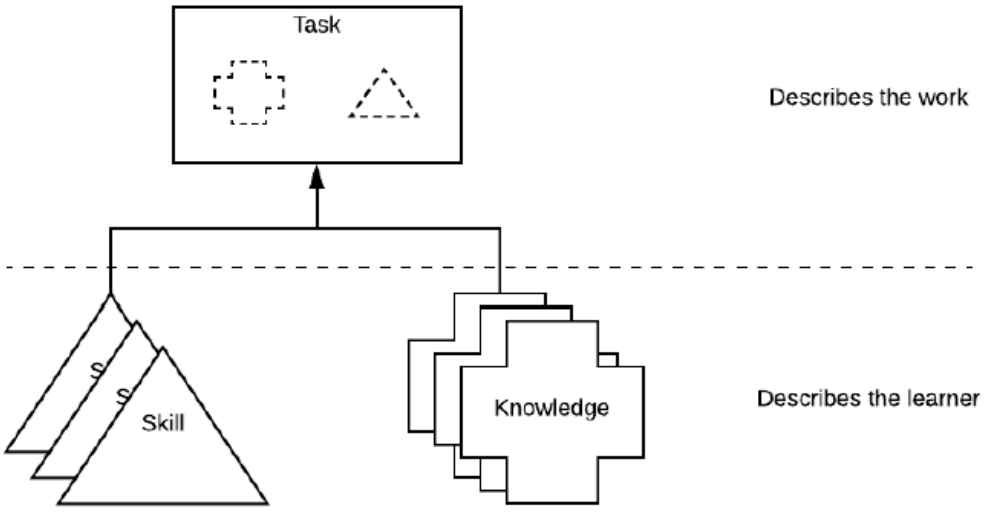

Figure 1 - The NICE Framework Building Blocks Approach *(Adapted from: Peterson et al. 2020, p. 1)*

The first building block is skills, which focuses on the learner and their ability to carry out a duty, whose consequences we can see. While in the context of cybersecurity, the skill can be technical and complex, such as determining the weakness exploited a bad actor exploited to gain access, or even as simple as being able to recognize phishing attempts in a sketchy email. Additionally, there is no limitation to how skills can be applied. It may take more than one to solve a single issue, and conversely, one skill can be used to solve multiple tasks, which we will discuss later.

Second, the knowledge building block, is the knowledge that a learner needs. This can range from an understanding of the general foundations of cybersecurity, down to the intricate details of a cybersecurity system. Similar to skills, it might take knowledge of multiple things to complete a task, or one could potentially solve many.

The previous two building blocks, skills and knowledge, come together to form the final block: tasks, as it takes both to be able to complete a task. Skills and knowledge have definitions

based upon the learner, while tasks centers on the context of the work. In short, it is the jobs that must be accomplished for a company to reach its Target Profile. tasks are not the final objective, but rather the work that needs to be done to accomplish that goal.

Within all these components themselves, it emphasizes the four main ideas: Agility, being able to change and evolve to keep up with the cybersecurity world; Flexibility, the capability to adapt to different solutions to similar problems; Interoperability, the means to exchange information; and Modularity, the engagement with other departments not directly related to cybersecurity.

Similar to the NIST framework, the NICE framework also emphasizes the importance of constant growth, especially for "those who are (or will be) performing work [who are] are continually learning and achieving objectives and can be found in any part of the learning lifecycle" (Peterson et al., 2020, p. 1). The employer should not assume that employees will reach an apex of understanding of cybersecurity, but rather should also encourage constant growth and learning.

Undoubtedly, the strength of a business's cybersecurity plan is reliant on the actions on all of its employees, not just that of its security team. This being said, it is abundantly clear the important role that the NICE framework plays. It does not fill all the gaps that are in the NIST framework, but the two in conjunction form a solid foundation for a solution to the most pressing matter: that the NIST framework is almost four years out of date. In order to most efficiently update these standards to best upgrade both private and public security, a new framework, based on the previous work done by both the NIST and NICE frameworks, should be formed.

If things are left as is, the impact could be tremendous on the digital sphere. Many companies use the framework, and it has even been translated to a multitude of languages, so its

reach is farther than that of just firms within the United States. As the world moves more towards an online learning and working environment, more sensitive information is being placed online that could cost companies an unforseen amount in losses if their systems are breached by bad actors. This does not even take into account the damage it will do to an individual if their information is compromised. We will now delve further into the research and the methods of analysis for this evidence.

Analyzing the Flaws in the Literature Through the Lens of Socio-Technical Landscape

The approach I used to structure my analysis of the research is "Multi-Level Perspective on Sustainability Transitions", put forth by Frank W. Geels. It outlines its method of analysis by basing its focus on technology and its interaction in the sociotechnical world. In particular, it centers on its evolution, and how society responds to it, both positive and negative. The NIST framework begins in the Niche level, as the framework was the first literature, and thus standardization of a field that previously lacked such structure. It transitions to the Regime level as it ages as, since its conception, become a prevalent practice within the cybersecurity field. The literature that criticizes the framework can be looked at through the Niche level, as it challenges the Regime in place and supports innovation within the field to replace it.

In his paper, "Limitations of Cybersecurity Frameworks that Cybersecurity Specialists Must Understand to Reduce Cybersecurity Breaches", Hitchcox highlighted four major criticisms of this policy that he discovered during his research: "(a) guidance too high-level and outdated, (b) limitations negatively affect guidance implementation, (c) lacking understanding of cybersecurity importance, and (d) compliance is not security" (Hitchcox, 2020, p. ii). This came as a result of Hitchcox's interviews with eleven experts who work within the cybersecurity industry and had worked with the NIST framework on some level. They were asked a series of

questions regarding their qualifications, as well as their personal insights, based on their work, about the guidance provided in the framework. One of these such questions, which helped form the aforementioned four criticisms, was "Could you describe your negative or positive perceptions of NIST cybersecurity guidance beneficial contribution to the organization's cybersecurity posture?" (Hitchcox, 2020, p. 62). A majority of respondents, seven out of the eleven total interviewees, noted that the framework was severely outdated and much too high level for most to understand, requiring a cybersecurity professional to translate the language used into text that would be more understandable. One profession stated "There is so much information out there, and it is so technical and so complex, and the NIST guidance generally is specific … You cannot open a NIST document and immediately know how to implement a program. As I start to focus on smaller businesses, for example, it is not something that a person that does not have a security background could easily digest and know what to do" (Hitchcox, 2020, p. 64-65). This insight in particular highlights this disparity in cybersecurity resources between small and large companies. While a large company will have the resources to have a cybersecurity team decipher the NIST document in order to implement it, a smaller company might not have those capabilities to dedicate valuable time and effort into such a task.

Another perceptive question that the researchers ask is "Without providing specifics of a company related cybersecurity incident (using generalities), could you describe an experience where NIST cybersecurity guidance failed to adequately capture and mitigate risk?" (Hitchcox, 2020, p. 74). Incidents cannot be directly attributed towards the framework itself, as the document does not describe how to actually implement the guidance that it provides. However, many of the participants shared similar ideas that the framework simply did not provide enough information to adequately protect company systems, and can leave many factors up to

interpretation. For example, the NIST framework suggests that enterprises perform exercises, but do not say what sort of exercises, and what things are to be learned from such experiences.

After reading Hitchcox's criticisms of the NIST framework, it becomes easier to analyze the literature through Geel's multi-level perspective (MLP). As previously stated, criticisms of the framework fall into the niche layer of the MLP. After interviewing cybersecurity experts, Hitchcox creates new expectations that an up-to-date and extensive framework should contain, challenging the socio-technical regime that the NIST framework has previously established. By gathering information from multiple different sources, he shows where the regime is lacking and the gaps that must be filled by the innovation of a new niche framework.

Another publication that presents relevant information is the book *Nordic Conference on Secure IT Systems,* which catalogs papers presented at the 23rd Nordic Conference on Secure IT Systems, NordSec, that occurred during November 28th-29th 2018. One of particular interest is "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework". The paper analyzes the EU's recent instructions on cybersecurity, based heavily on the NIST framework; how well the framework was implemented; and the gaps that the researchers identified within the NIST literature that make the EU's implementation flawed as well. This is conducted through a literature review of 56 papers that were carefully curated by cybersecurity experts and were related to metrics and controls. From these, 1,378 units (either metrics or controls) were identified.

When comparing the literature studied, several topics were identified that the NIST framework did not address, or addressed briefly with a noticeable lack of detail. The paper does not elaborate on each individual topic, but highlights "five uncovered topic areas, which are

either prevailing the analysis (i.e., organizational climate, monetary aspects, executive involvement, ethics) or highly important in the context of critical infrastructure cybersecurity (i.e., natural disasters)" (Krumay et al., 2018, p. 379). A full table of topics provided by the paper is shown below in Table 1.

Topic areas	Representative examples	U	M	C
Organizational climate	M: "Degree of organizational climate satisfaction" [17] C: "Enhance individual/group pride in the organization" [29]	65	13	52
Monetary aspects	M: "Cost of image rebuilt after information security accidents" [33] C: "Security budget segregation" [17]	59	41	18
Executive involvement	M: "Leaderships' involvement in information security planning" [18] C: "Develop a management team that leads by example" [29]	25	5	20
Ethics	C: "Create an organizational code of ethics" [29]	23	0	23
General management	M: "documents scheduled for that month must be received within five business days of due date" [34] C: "Ensure a right balance between centralization and decentralization" [29]	23	12	11
IT Service Levels	M: "Customer Satisfaction" [33] C: "SLA covers all the aspects of security when there is a third party providing other services" [35]	22	11	11
Cognitive response	C: "Instill a fear of consequences" [29]	18	0	18
Procurement	M: "Testing ICT before acquisition" [18] C: "Procure IT Resources" [36]	14	4	10
Business value	C: "Contribution to the overall business" [32]	10	0	10
Natural disasters	M: "Intensity of the extreme weather event" [37] C: "Fire, voltage and flood protection of buildings and premises" [18]	10	3	7

Table 1: Uncovered topic area with examples (U = Units, M = Metrics, C = Controls) *(Adapted from: Krumay et al., 2018, p. 378)*

The topic covered most within the literature (i.e. the topic with the most units associated with it) and not within the framework is organizational climate, which are things such as an employee's level of job satisfaction and drive to continue working. Though this does not relate

directly to technical subject matter, it is still a concern that the NIST framework fails to touch upon it at all. Organizational climate can heavily influence the level at which an employee will perform, and their composition during work. The researchers note how "[t]he detected underrepresentation of organizational climate and social aspects [in the NIST framework] is surprising. Academic literature has long established that in particular social norms and organizational climate affect behavior and are influential in achieving compliance" (Krumay et al., 2018, p.380). This oversight, among many others, in the framework points to a need for new regulations to be put into place to protect both companies and individuals.

The Proposed Benefits of a Thorough and Updated Framework

After analyzing the evidence presented, we can easily identify the way in which the NIST framework fails to properly prepare a company for the cybersecurity risks that it will almost undoubtedly face. In addition to proving the need for an updated framework through exploring the multitudes of oversights in the framework, I also learned other faults that I had not previously considered as well as rare cases in which using the framework helped a company when developing their risk management strategy.

Through my research I discovered more lapses in the framework than I had initially expected. My line of thinking was directed towards problems in the technical aspects that were presented, such as such guidance being outdated or overly complicated, but other non-technical issues became abundantly clear. Though technical capabilities are the foundation of any good cybersecurity system, aspects such as the monetary feasibility as well as the role of other employees outside of the cybersecurity team are also important in these systems. For example, in terms of monetary feasibility of the NIST framework, carrying out the advice proposed can put a strain on company finances. Though the framework does in fact state that implementation could

be costly, it was not written with a reasonable budget in mind, which can be especially harmful if a smaller company with less resources and personnel wishes to follow the framework's guidance. There are several levels of implementation that are outlined, and a strict adherence does not necessarily mean a better cybersecurity system, but the document does not state what aspects are most important when considering only a partial implementation.

The paper proposed by Krumay et al. extensively covered such non-technical topics, though they did not necessarily only search for non-technical topics when looking for blind spots in the NIST framework. The research conducted also highlighted how prevalent these subjects were in a multitude of papers dealing with cybersecurity, possibly alluding to a lack of research done or time to conduct such research occurring when the framework was created. An update to the framework would consider these at a much greater length. Though they might not fit into the predefined functions that the framework defines, it is important to address them as they can drastically impact the effectiveness of one's cybersecurity.

Some aspects of the NIST framework are actually beneficial, though I believe, after reading the multitudes of papers on the framework's flaws versus the small amount that states otherwise, that such a case is rare. It is undoubtedly possible. A potential benefit could occur in the circumstance where "...someone tries to sue organizations that have implemented the Framework … the response could be 'Hey, we've got this Framework in place, we've done all the things that were recommended.' It makes it easier for [organizations] to defend themselves in court against potential lawsuits" (Scofield, 2016, p.28). However, this sort of attitude towards cybersecurity is dangerous. A company should prioritize the security of its systems and sensitive information (both theirs and their customers), rather than trying to cover their own bases in the event a lawsuit could occur. When creating a risk assessment plan, the top priority should be the

mitigation and prevention of such an attack, not the legal defense one can present in the case that something occurs. Additionally, the framework is not designed to be the end all be all.

Despite the support of the framework being useful, there is more evidence to the contrary. In some cases, this evidence even directly refutes some of the claims that Scofield writes about. For example, the idea that someone who is not an expert in technology could use the guidance provided is a statement that has been heavily contested by those working in the cybersecurity field. One participant in a study covered in "The Cybersecurity Framework as an Effective Information Security Baseline: A Qualitative Exploration" noted how "[people with little or no technical training] get very overwhelmed because they don't have the technical expertise and they don't know what to do..." (Troia, 2018, p. 82). Some things, such as the way the framework is organized into functions, Core, and Tiers can make sense in layman's terms, but going further into technical details can quickly become confusing.

Overall, there are many aspects of the NIST framework in need of changing, but I believe that the most pressing matter to address is the lack of details and examples. This is one of the shortfalls presented during Hitchcox's research, and nine out of the eleven cybersecurity professionals interviewed agreed that this was a major problem. Not only is the framework written in a generalized fashion, but it does not provide examples of the techniques that it talks about. It can be argued that the lack of detail helps it to remain neutral to specific applications or technology, but this also makes the guidance harder to follow. One participant, when asked about improvements to the framework suggested adding "[s]pecific examples of good implementations that are adequate in reducing risk and examples of partial implementation and also very bad implementations to mitigate risk, examples of each control, and how they should be implemented as well as measured and managed" (Hitchcox, 2020, p. 90). This would be helpful when a

company is implementing things suggested by the framework, and can also direct focus towards edge cases and other more unusual occurrences that might not normally be considered when dealing with a specific situation.

Another important issue deals with the framework's accessibility. This is in addition to the monetary problems previously discussed, where they do not have the resources to implement the full framework. This leaves smaller companies to flounder and having inadequate protections. They can choose what aspects to apply to their own systems, but the framework does not give guidance on what steps are the most critical to take, and what can be skipped without compromising too much security. One expert that took part in Troia's study summarizes the problem: "From NIST it's really hard to compare, it literally is almost [like] you're either doing it or you're not. You can have these really big, gaping holes and it really doesn't give you the overall impact of how you rank … Is there anyone that's any more important than another?" (Troia, 2018, p. 84). This is a huge oversight on NIST's part, and makes it inaccessible to small companies. It is to the point that a cybersecurity evaluation tool (CET) has been proposed that would specifically suit the needs of small and medium-sized enterprises (SMEs). In a time where SMEs are the most vulnerable to cybersecurity attacks, the NIST framework leaves its most important audience behind.

Conclusion

For a document that has been used by so many companies across the world, the NIST framework brings a disappointing document to the table. Not only does it fail to cover some of the most basic and crucial topics, such as outlining which steps are most important or the role of executives in their cybersecurity teams, but it is even lacking in the subjects that it does provide guidance on. Following the advice provided by this framework would inevitably lead to a

company facing cyberattacks not described in the document and having to not only deal with repercussions, but find another source of information to protect against this attack in the future. Additionally, it pushes out smaller companies by being too expensive to implement in its entirety, yet does not offer solutions for partial implementation.

A new framework would correct these pressing issues and could use the old document as a basis. Nonetheless, there are many potential roadblocks. Creating this new framework would undoubtedly be costly in both time and money. It could soon also face a similar fate to the old NIST framework of becoming outdated, as the field evolves so rapidly. This would require frequent updates in order to stay relevant, which would also add to the costs. However, I believe that such an effort is well worth it. Not only is cybersecurity crucial in protecting the systems run by companies, but it also protects the information of the everyday consumer. Businesses have a responsibility to protect the assets of not just themselves, but those of their customers as well.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5-14. doi:10.22215/timreview/861

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for nist cyber security framework. *Computer Science & Information Technology (CS & IT)*. doi:10.5121/csit.2017.70305

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for smes. *Business Horizons, 63*(4), 531-540. doi:10.1016/j.bushor.2020.03.010

Clark, R. M., & Hakim, S. (2018). *Cyber-Physical Security Protecting Critical Infrastructure at the State and Local Level*. Cham: Springer International Publishing.

Fischer, E. A. (2016, August 12). Cybersecurity issues and challenges: In brief. Retrieved March 23, 2021, from https://fas.org/sgp/crs/misc/R43831.pdf

Framework for improving critical infrastructure cybersecurity, version 1.1. (2018). doi:10.6028/nist.cswp.04162018

Geels, F. W. (n.d.). Multi-Level perspective on SYSTEM Innovation: Relevance for industrial transformation. *Environment & Policy,* 163-186. doi:10.1007/1-4020-4418-6_9

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST CYBERSECURITY framework via the GORDON–LOEB MODEL. *Journal of Cybersecurity, 6*(1). doi:10.1093/cybsec/tyaa005

Gruschka, N. (2018). *Secure IT systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, proceedings*. Cham, Switzerland: Springer.

Harknett, R. J., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management, 6*(1). doi:10.2202/1547-7355.1649

Hitchcox, Z. (2020). Limitations of Cybersecurity Frameworks that Cybersecurity Specialists Must Understand to Reduce Cybersecurity Breaches.

Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the nist cybersecurity framework. *Secure IT Systems,* 369-384. doi:10.1007/978-3-030-03638-6_23

Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). doi:10.6028/nist.sp.800-181r1-draft

Rodin, D. N. (2015). THE CYBERSECURITY PARTNERSHIP: A PROPOSAL FOR CYBERTHREAT INFORMATION SHARING BETWEEN CONTRACTORS AND THE FEDERAL GOVERNMENT. *Public Contract Law Journal, 44*(3), 505-528. Retrieved March 20, 2021, from https://www.jstor.org/stable/26419479.

Scofield, M. (2016). Benefiting from the NIST Cybersecurity Framework. *Information Management, 50*(2), 25-28, 47. doi:http://proxy01.its.virginia.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fbenefiting-nist-cybersecurity-framework%2Fdocview%2F1779940925%2Fse-2%3Faccountid%3D14678

Staff, D. (2016, March 30). NIST cybersecurity framework Adoption hampered by Costs, survey finds. Retrieved April 21, 2021, from https://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901

Troia, V. (2018). The cybersecurity framework as an effective information security baseline: A qualitative exploration. Retrieved March 22, 2021, from http://proxy01.its.virginia.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fdissertations-theses%2Fcybersecurity-framework-as-effective-information%2Fdocview%2F2126637538%2Fse-2%3Faccountid%3D14678