Practical Application of the NIST Cybersecurity Framework Across Enterprise Environments

Parker Daudt
x17118379
MSc Internship in Cyber Security

30th August 2018

Abstract

Described as one the of most serious challenges facing U.S. national security, an increasing number of attacks on critical infrastructure lead to the creation of the National Institute for Standards and Technology's Cybersecurity Framework. Created from the consolidation of recommendations and input from industry-leading organisations and researchers over several years, the NIST Framework has received both continued praise and criticism. Designed as a voluntary tool for organisations across every domain in both the public and private sector, the Framework has seen adoption by enterprises such as Intel, Seattle Children's Hospital, and The University of Chicago. To determine the extent to which the NIST Framework is a beneficial tool for organisations that choose to implement it, an analysis of use case documents and case studies was conducted. Additionally, a hands-on review of EY's cybersecurity-related services was conducted through a three-month internship to determine how the Framework had impacted their business decisions. From this analysis, it was concluded that the NIST Framework serves as a powerful tool for organisations looking to evaluate their current cybersecurity program, or implement a new one. From this information a cybersecurity program assessment tool was created. This tool utilises a series of activities and tasks for organisations to assess or introduce cybersecurity procedures and communicate them through a concise dashboard.

1 Introduction

Described by then United States President Barack Obama as "one of the most serious national security challenges we must confront," the continuous attacks on critical infrastructure services established the necessity for improved and modernised cybersecurity (Obama; 2013). The year 2013 saw a rise of cybersecurity-related attacks. From the attempted hacking of the government-run health-care exchange, to the theft of over $45 million from a New York bank, numerous infrastructure services, across various domains, faced severe attacks from countless sources[1]. With more opportunities to learn defensive and offensive tactics, including formal and informal training, than previously seen,

[1]https://www.cnbc.com/2013/12/27/top-2013-cybersecurity-stories-and-what-to-watch-for-in-2014.html

the number of cybersecurity-conscious individuals is at an all-time high. With potential threats ranging from nation-sponsored attacks looking for information or to cause disruption, to a single individual looking to test his knowledge and skills, many companies struggle to determine the best place to start when it comes to cybersecurity and information technology service. To assist in combating this struggle, the introduction of the Cybersecurity Framework from the US's National Institute for Standards and Technology (NIST) has frequently been used as a starting point.

Comprised partially of private-sector industry best practices, the Framework for Improving Critical Infrastructure (Framework) aligns standards and best practices to provide, as argued by its supporters, a cost-effective and flexible approach to improving cybersecurity programs. Prior to President Obama's 2013 Executive Order 13636, efforts to update governmental regulations stalled with initiatives such as the Cybersecurity Act of 2012 due to opposition from the private-sector (Shackelford, Proia, Martell and Craig; 2015). In the time since its publication in 2014, the NIST Framework has received support from U.S. government and industry officials, described by Shackelford et al. as "an example of leveraging public-private partnerships" to develop a comprehensive cybersecurity policy. As broader adoption of the framework occurs both within the U.S. and globally, with IT leaders promoting the Framework through industry associations and with governments themselves, it is crucial that we understand the impact the Framework has already demonstrated in the companies who have chosen to adopt it into their organisation. Therefore, we proposed the following research question: **To what extent is the National Institute for Standards and Technology's Cybersecurity Framework a beneficial tool when integrating with an enterprise's currently existing, or when developing a new cybersecurity program?**

In an effort to explore the development of the NIST Framework and its application in enterprises across various domains including education, healthcare, technology, and finance, both directly and indirectly in new or preexisting programs, this paper is structured as follows. Section II establishes the context of the NIST Framework, discussing its origin and evolution. Section III outlines reasoning behind the observations and analysis that occur in Section IV, including the key questions and areas of interest. Section IV then outlines and analyses the programs in place at organisations across the various domains in an effort to determine what impact the NIST Framework had on shaping their cybersecurity programs or practices. This analysis is done through the collection of information answering the questions outlined in Section III. Finally, Section V analyses the findings from Section IV to highlight any overall challenges or benefits that the Framework has been able to provide.

2 Related Work

To fully understand the impact of the NIST Framework across various domains, it is important to understand the context in which the framework was founded, and evolved. To establish this context, a review and analysis of documentation provided by sources including NIST, Presidents of the United States, industry-leading organisations and cybersecurity academics was conducted. These sources provided the necessary information to understand how the framework was introduced, how it had evolved, and how it had been received.

2.1 Framework Introduction

In February 2014, the National Security Council of the United States unveiled the Framework for Improving Critical Infrastructure, aimed at improving the cybersecurity of critical infrastructure across the country (Sedgewick; 2014). Stemming from the 2013 Presidential Executive Order 13636, former United States president, Barack Obama, expressed the need to strengthen the security and resilience of critical infrastructure to combat the threats to personal privacy and other serious issues (Obama; 2013). The Executive Order tasked cooperation between the United States' National Institute for Standards and Technology and private sector corporations to highlight standards and industry best-practices that could be incorporated into a standardised, voluntary cybersecurity framework. This newly created framework was intended to be useful regardless of any implemented technology, promote the adoption of the best cybersecurity practices, increase the quality, volume, and speed of information sharing related to cyber-threats, and incorporate strong protections into every governmental initiative necessary in securing critical infrastructure. Additionally, the broader impact of this framework allowed for its implementation in organisations and industries outside the scope of a governmental sector. The presidential administration recognised the impracticality of a "one-size-fits-all approach to managing cybersecurity risk," as the solution for one company may not be effective or appropriate for other companies in a similar or different industry (Sedgewick; 2014). To address this limitation, the purpose of the Framework served to drive companies to ask the appropriate questions, and to implement the right solutions for their unique industrial and organisational requirements.

Immediately following the initial executive order released in 2013, additional governmental policies and decrees reinforced the commitment made by the United States government to improve and standardise cybersecurity policies and procedures. Throughout 2013 NIST released a series of Requests for Information[2], collecting information relating to current standards and their effectiveness. From these requests, over 270 responses were received. In addition to the Requests for Information, multiple workshops were held across the country, attracting as many participants from as many industries as possible. These workshops aimed to raise awareness, gain a clearer understanding from industries regarding areas of promise, those needing additional guidance, and areas that should be avoided. Following discussions and additional workshops, by early 2014, Version 1.0 of the voluntary cybersecurity Framework was released. Created from the consolidation of over 15,000[3] recommendations from individuals and groups across the globe, the Framework can be easily divided into three main components: Core, Profiles, and Tiers.

The Framework's Core consists of a set of activities and references that are common across the critical infrastructure sectors. These activities are grouped under five functions and provides the organisation with a high-level view of their cyber risk management techniques: Identify, Protect, Detect, Respond, and Recover. The function Identify serves to develop an organisation's understanding to manage cybersecurity risks to its assets and Protect is used to implement the necessary safeguards used in the delivery of infrastructure services. While the function Detect develops activities for identifying a security event, Respond is used when implementing activities for addressing a detected event. Recover is used when implementing activities to build resilience and restore services af-

[2]https://www.federalregister.gov/documents/2013/10/29/2013-25566/request-for-comments-on-the-preliminary-cybersecurity-framework

[3]https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

fected by a security event. Additionally, the Framework Core provides both categories and subcategories for each function. These provide additional context and clarification for each function and makes implementing the Framework easier.

The Framework's Tiers are used to provide an organisation context on how they identify and understand cybersecurity risks, and describe the processes used in their risk management practices. While an unofficial Tier 0 describes static solutions to high-impact items, Tiers are ranked on a level ranging from Partial (Tier 1) to Adaptive (Tier 4) as described in Figure 1. These levels serve as an informal measurement of maturity that can be used to evaluate process integration into the organisation's overall risk management practices, and identifies the extent to which the needs of the business shape their cybersecurity risks. While smaller business and even some larger organisations may fall into Tier 1, by getting executives interested in cybersecurity, Tier 2 can be achieved. However, this is often an arduous task. While Tiers provide organisations a tool to evaluate their cybersecurity program and make informed business decisions to address the necessary changes while moving forward, by advancing from Tier 1 to Tier 2, accountability widens to include management and executive levels, improving motivation and successful integration.

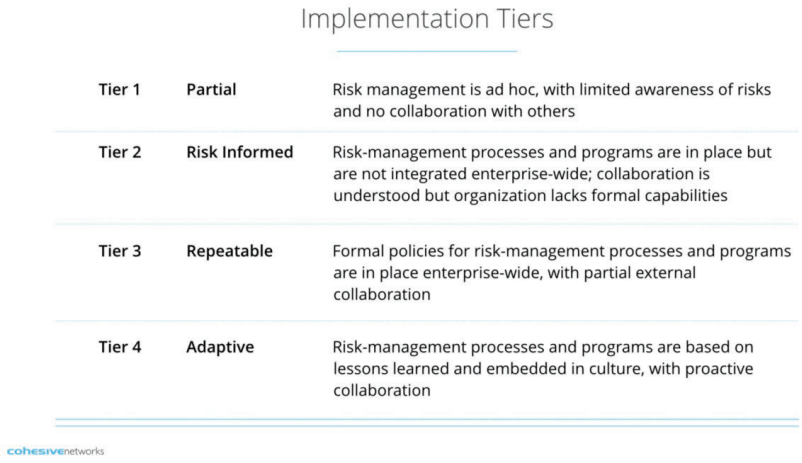

Figure 1: NIST Framework's Implementation Tiers[4]

Lastly, due to the Framework's flexible and customisable nature, Profiles help organisations align individual business objectives, resources, and the management of threats with their unique cybersecurity environment. Policies associated with each Profile, used in conjunction with Tiers, can be used to help an organisation determine the state of their current cybersecurity program, measure progress towards a targeted goal, and support improvement prioritisation. As part of the adoption or integration of the Framework within a new or preexisting program, Profiles can be used to form the foundation of prioritising, budgeting, and conducting gap analysis. While the Framework provides numerous resources, including Core, Tiers, and Profiles, for organisations to introduce or improve cybersecurity policies, due to the constant changes in both the organisational and threat landscapes, continuous research and development of the Framework is necessary to keep it relevant and beneficial.

[4]https://www.nist.gov/cyberframework/online-learning/components-framework

2.2 Framework Evolution

Early changes to the proposed framework helped to widen the scope of development from a sole focus on critical governmental systems involving energy, healthcare, and other critical areas, to the inclusion of consensus and industry-based guidelines. Almost immediately after the release of Version 1.0 of the Framework, continued refinement took place. Several workshops were held to address the growing concerns around individual privacy, civil liberties, and improved privacy through system design. Additionally, NIST held a second Request for Information[5], asking about the ways in which the Framework had been used to improve cybersecurity risk management, how best practices for using the Framework had been shared, the value of the Framework, and the possible need for an update. This request saw a response from over one hundred individuals and organisations focusing on ideas such as improved awareness, improved industry resources, and whether an update would be necessary or desired. Additional updates and changes made to the framework between 2013 and 2017 aimed to clarify key terms, introduced cybersecurity measurement methods and a comprehensive approach to identity management, detailed the necessity to manage supply chain risks, and improved usability through clarification and refinement. By January 2017, a draft of Version 1.1 was released, to mixed reception.

A Request for Comments held after the draft release saw mixed review from over 125[6] responses. These responses included statements and reviews from IBM, Amazon Web Services, Symantec, Ernst & Young, and European Central Bank. While many comments noted the many benefits the Framework had provided, and the positive reception of the changes made between Version 1.0 and the Version 1.1 draft, the concerns could not be ignored. Comments included those by Symantec's Jeffrey Greene (2017) that stated, "...the Framework does not provide guidance on how to conduct the required risk assessment...Less mature organisations could choose not to use the Framework or if they do use it, they may not take full advantage of it." Also, Intel and McAfee's Kent Landfield (2017) believed that, "there are two crucial and fundamental areas missing from the Framework: threat intelligence and vulnerability disclosure" echo the concern that businesses may not recognise how they can benefit from the framework, or that critical areas are entirely absent. Leading up to the official release of Version 1.1 in April 2018, further workshops and requests for comments were held, additional revisions were made, and US President, Donald J. Trump, reiterated the need for strengthened cybersecurity (Trump; 2017). The most notable updates found in Version 1.1 included clarifications and refinements making the Framework easier to use, a new section focused on relating cybersecurity risk management to organisation objectives, expanding supply chain risk mitigation guidance, addressing vulnerability disclosure, emerging technology risks, and a life-cycle approach to cybersecurity (Barrett; 2018). The numerous requests for information and comments allowed industries to raise concerns, address areas of interest, and provide feedback that could make the Framework easier to use across multiple industries.

2.3 Reception Across Various Domains

Despite stemming from a presidential executive order, and an initial aim to be applied to internal infrastructure services within the private sector, the broader impact

[5]https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity

[6]https://www.nist.gov/cyberframework/rfc-cybersecurity-framework-draft-version-11

of the Framework was recognised almost immediately. Since the first Request for Information in 2015[7], companies and organisations[8] including Boeing, RSA, Rapid7, Microsoft, and CERT have provided insight and feedback into the development process. As a result of the broad range of references from both public and private enterprises, the framework has since seen mandatory implementation in all U.S. government agencies, adoption by lower-level governmental bodies including The State of California and the State of Michigan for non-critical infrastructure use, and public companies including Intel, AT&T, and JPMorgan Chase & Co. Early popularity within the U.S. could even be seen in a 2015 Gartner poll which stated that the Framework had seen adoption by 30% of United States public and private enterprises, with an expected increase to 50% by 2020 (Pratap and Perkins; 2015). Additionally, international reception of the framework has been strong, seeing multiple adaptations for use by numerous countries[9] including use in Japan's Information-Technology Promotion Agency, Italy's National Framework for Cybersecurity, and use by the governments of the United Kingdom, Bermuda, Israel, and Uruguay.

As reflected by the numerous adoptions, the Cybersecurity Framework has received praise from researchers and companies across a wide range of domains. Many adopters note the Framework's development as organisations can continue to achieve their desired goals. Described by Threat Sketch as "a great way to protect your company from cyber attack" and "a comprehensive technical reference for solving specific problems," the Framework has been viewed as a well-rounded solution for both large and small organisations looking to manage their cyber risks (ThreatSketch; n.d.). PwC has continued to recommend the Framework as it "offers potential advances for organisations across industries" and allows for improved internal and external discussion of cybersecurity issues (PwC; 2014). Outside of private industry, academic researchers have expressed praise for the Framework both inside the U.S. and abroad. In a comparison of several global cybersecurity frameworks, Shackelford, Proia, Martell and Craig (2015) have noted that the NIST Framework has shaped the field of cybersecurity and has been referenced in numerous debates. Additionally, Lei Shen of TheSciTech Lawyer makes note of several potential benefits of the Framework, both financial and organisational. Shen (2014) proposed that the Framework could improve security along the supply chain as organisations working with the U.S. government are required to adopt the framework, and their own suppliers may be required to adopt the framework as well. He also notes that insurance could be shaped by the Framework, creating a benchmark when drafting contracts. These benefits may not only result in an increase in adoption, but also in several financial incentives.

In addition to the positive reception received following the release of Version 1.0, continued praise had been received during the numerous periods of revision. Companies including SANS and PwC continued to hold the Framework in high regard, with PwC advising numerous clients of the potential benefits[10], while companies such as Symantec continued to integrate the Framework into several aspects of their own business (Greene; 2017). Additionally, the Center for Internet Security[11], the FIDO Alliance[12], and Cyber

[7]https://www.federalregister.gov/documents/2015/12/11/2015-31217/views-on-the-framework-for-improving-critical-infrastructure-cybersecurity

[8]https://www.nist.gov/cyberframework/rfi-framework-reducing-cyber-risks-critical-infrastructure

[9]https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

[10]https://www.nist.gov/sites/default/files/documents/2018/02/01/2018-01-19$_{-p}wc_{c}ybersecurity.pdf$

[11]https://www.nist.gov/sites/default/files/documents/2017/04/20/2017-04-10$_{-c}is.pdf$

[12]https://www.nist.gov/document/2017-04-10-fidoalliancepdf

Threat Alliance[13] demonstrated dedicated support for the framework. Despite the successful integration and praise from numerous enterprises, the Framework has not failed to receive its share of criticism.

Criticism of the NIST Cybersecurity Framework starts at the highest level, the United States government. Claims made against the U.S. government state that a voluntary framework is not feasible. Robert Gyenes from the University of Pittsburgh believes that the framework "creates a financial burden" on the organisations that choose to implement it (Gyenes; 2013). Gyenes also believes that voluntary guidelines may cause executives to question whether the framework will become an industry standard. His remedy is for the government to provide financial incentives for integrating the framework, while simultaneously mandating liability for companies that suffer security failures. He believes this shift would drive adoption, while still allowing corporate independence. Gyenes is not alone in his criticism of the lack of adoption incentives as many other critics have noted this as a major concern for many standardized frameworks (Fischer; 2005). Lei Shen notes that while incentives would make adoption "very attractive" for the companies that choose to adopt the Framework, these incentives may require federal legislation or grants (Shen; 2014).

Criticism of the Framework is not limited to a lack of incentives; many critics also focus on its voluntary nature. Shackelford, Russell and Haut (2015) argue that the governmental push behind the NIST Framework will cause the once-voluntary framework to become the de facto legal standard for cybersecurity practices. Such legal standards may cause turmoil as organisations rush to implement the Framework as quickly as possible to avoid any penalties, rather than implement the practices that best fit their requirements. Following Executive Order 13800, the United States government made the framework a mandatory requirement for every governmental agency, and this requirement extends to any organisation interacting with these agencies (Trump; 2017). These requirements have a potential domino effect that has major implications, shifting the framework from voluntary to mandatory. Additionally, Dolezilek and Hussey (2011) have continued to argue that cybersecurity requirements or recommendations imposed by legislation are typically unclear. They state that "it may not be clear that requirements that apply to one set of entities may not apply to another set of entities" (Dolezilek and Hussey; 2011). This combination of uncertainty can lead to legal confusion, causing difficulties for both small and large organisations attempting to adopt the Framework into their operation. Critics of the Framework point out the known problems with a reliance on information sharing, something described as both critical yet ineffective. The problem with using best practices is the difficulty in mapping the NIST Framework to other models when measuring a security process' maturity. Again, Gyenes (2013) notes that a lack of government transparency will limit the information sharing process, and the uncertainty of defined framework compliance will cause needless confusion.

3 Methodology

Due to the mixed reception, concerns, and criticism raised regarding the NIST Cybersecurity Framework, there was a need for an in-depth review of multiple independent

[13] https://www.nist.gov/sites/default/files/documents/2018/01/31/2018-01-19_cyber_threat_alliance.pdf

organisations' experiences with the Framework. To appropriately evaluate the extent to which the NIST Cybersecurity Framework has been a beneficial tool when integrating with an organisation's currently existing program or in developing a new one, it is necessary to review case studies and use case documents provided by enterprises that have chosen to adopt the Framework. The case studies and use case documents necessary to provide a fuller picture must serve as a more-accurate representation of the private and public sector. They must be selected from enterprises across different industry domains in both the public and private sector, and must capture either the Framework's integration into a current cybersecurity program, or its use in creating a new one. This review serves to better evaluate the Framework's usability in a wide range of enterprise domains, highlight any challenges or benefits that the Framework has presented, and to determine the impact of the Framework. To accomplish this task, studies and reports published by organisations in industries ranging from a multinational technology company and a health care organisation, to an educational institution were examined. These case studies and use case documents were gathered from publicly available sources, directly from the enterprise that performed the study, or directly from the National Institute of Standards and Technology's website. These case studies were then analysed to provide answers to several questions to obtain crucial pieces of information:

- What background information can give insight into the state of the organisation's cybersecurity program before the use of the NIST Cybersecurity Framework?
- What is the organisation's reasoning behind the selection of the NIST Cybersecurity Framework?
- What steps were taken to implement the Cybersecurity Framework into an already existing program (if applicable)?
- What steps were taken to use the Cybersecurity Frameworks in developing a new program (if applicable)?
- What are the results of the use of the Framework?
- What concluding observations were made by the organisation?

In addition to the review of case studies and use case documents, a hands-on analysis of the integration and application of the NIST Cybersecurity Framework at the professional services firm, EY, was conducted. Over a three-month internship, the integration of the Framework into EY's auditing services was observed and analysed. These observations were made with the following questions in mind:

- Does EY directly or indirectly use the NIST Cybersecurity Framework?
- How does the Cybersecurity Framework shape the decisions made by EY?
- What challenges have arisen due to the use of the Cybersecurity Framework?
- What benefits have been provided by the Cybersecurity Framework?

As the Framework can be used in a range of capacities, including the establishment of an entirely new cybersecurity program or in an already existing one, it is important that the level of integration is identified. As such, the purpose of the initial question was

used to ensure that the scope of use was determined. The additional questions were used to determine how the Framework has impacted the company's practices and to ensure that the praises and criticisms of the Cybersecurity Framework were considered when observing the processes used and opinions held by EY.

4 Implementation

This section discusses the findings from the application of the methodology outlined in Section III. The questions outlined in Section III were applied to use case documents, presentations, and case studies to determine the organisation's cybersecurity program, their use of the NIST Framework, and observations made following its application.

4.1 Intel

As an organisation that has recognised the importance of security, by early 2014, Intel had formed a dedicated business division to advance their focus on security. Composed of a combination of McAfee, a subsidiary of Intel, and other internal security resources, this division focuses on evolving defence against security risks affecting businesses, people, and governments. Prior to the integration of the NIST Framework, Intel's mature cybersecurity division, Intel IT, made up of numerous cybersecurity experts and consisting of a robust cybersecurity program, was chosen as the most beneficial internal resource for integration assistance. As Intel IT had initially implemented a cybersecurity solution that divided the organisation into five functional environments (Design, Office, Manufacturing, Enterprise, and Services), an independent evaluation by experts could be expected, and Intel believed their assistance would further simplify the integration process (Casey et al.; 2015). The NIST Framework was chosen based on early support and dedication since the initial inception of the Framework. This support included active participation in public comment periods, calls for information, and workshop attendance. By using the Framework, Intel hoped to harmonise risk management practices, communication, and technologies across the organisation, and hoped to identify existing strengths and areas for improvement.

Rather than integrate the Framework across the entire organisation, the Office and Enterprise environments were chosen as they contained similar risk management requirements, and most closely aligned with the Framework's categories. Initially, the Framework was used to perform a high-level risk assessment across both environments and to foster communication with executives and stakeholders to ensure resources were available (Casey; 2015). This assessment was conducted to establish an alignment of risk tolerance objectives, to inform processes for budget planning and prioritisation, to communicate cybersecurity risks to leadership, and to create organisational tools and best practices to better assess infrastructure risks while using the Framework. Taking place over a seven-month period, a four-phase plan was put in place: establishment of target scores, assessment of the current status, analysis of the results, and communication of the results. Each phase divided the integration process into organised objectives with a greater likelihood for success.

Through establishing target scores, Intel was able to agree on descriptions for their process maturity and methodologies. Intel then validated Framework functions and

categories, defined new Intel-specific subcategories and tier maturity descriptions that better-aligned to their programs, capabilities, and processes. They were then able to assign target scores to the validated functions and categories. The establishment of these scores were followed by the identification of 8-10 subject matter experts and security program managers to conduct the assessment, online training sessions, and the actual individual assessments. The training sessions comprised of an introduction to the NIST Framework, the reasoning behind Intel's choice to implement it, and how the assessment would fit into Intel's decision-making process. Additionally, training on the Intel-specific descriptions, the difference between the target and assessment scores, and how risk discussions are handled was provided. Following the training session, senior subject matter experts performed the assessment, scoring the Categories and noting opportunities for improvement. Overall, each assessment, including training, was completed in less than three hours (Casey et al.; 2015).

Following the completion of their assessments, the scores and results given by the subject matter experts and program managers were analysed and compared. This comparison was done to identify any visibility issues identified by significant scoring differences. Additionally, a heat map was generated from these scores to examine areas of concern and to identify areas for improvement, shown at the subcategory level. Once the results were analysed, findings were communicated to both the Chief Information Security Officer (CISO) and staff. This communication fostered dialog between the CISO and other key stakeholders and helped with an agreement on risk tolerance and prioritisation, while also providing information for process owners impacted by the assessment results. Once the assessment had been completed, numerous benefits were noted. The integration of the Framework into the assessment process allowed the organisation to develop reusable tools including risk worksheets, heat maps, and customised tier definitions, enhance training material, improve dialogue, improve category understanding through Intel-specific subcategories, and the creation of a heat map that identified outliers, variances, and improved risk landscape visibility.

4.2 University of Chicago

As an educational organisation in the United States, the University of Chicago's Biological Sciences Division (BSD) focuses on basic and clinical research, education, and patient care. With 5,000 faculty and staff across 23 departments, information technology resources drive discoveries in fields including genome and cancer research. The University of Chicago's BSD, driven by research and education, implemented a decentralised resource model, using local IT staff and technology to meet specific department needs. While a decentralised model provided each department flexibility and customised management and governance processes, several security challenges were also introduced. These include risks due to gaps in security controls between departments and inconsistent application of the controls, the potential for a duplication of effort, and an increase in security spending (Martinov; 2018). To combat increasing cybersecurity threats, in a cost-effective and systematic manner, the Biological Sciences Division determined the use of an existing framework would be required. Described by Plamen Martinov, Chief Information Security Officer of the BSD as "well-aligned with our main objective" the NIST Framework was selected to "establish a common language for communicating cybersecurity risks" across the BSD. As Martinov, hired to institute an information security program to protect

the academic and research functionality of the BSD, alongside the BSD's Chief Research Informatics Officer, Robert Grossman, both believed the NIST Framework to be the best fit (Martinov; 2018).

To apply the NIST Framework across the Biological Sciences Division, subject matter experts from G2, a small cybersecurity-focused business with previous experience in developing and deploying the Framework, and BSD security analysts developed a four-stage implementation process using a combination of risk management and Framework principles: Current State, Risk Assessment, Target State, and Road Map. Stage 1 primarily focused on the identification of priorities, compliance requirements, vulnerabilities, and risk events. Additionally, stakeholders and management were interviewed to determine previously used processes, individual department priorities, necessary requirements to ensure research information could be shared remotely, and to establish a broad understanding of all needs. Finally, a customised profile was created to aid in the development of internal management tools, best practices, and to establish the BSD's current profile. Following these developments, a comprehensive review of the current profile was conducted to identify potential vulnerabilities. The comprehensive risk assessment conducted by BSD and G2 aimed to identify threats, review discovered vulnerabilities, determine their likelihood and probability of exploitation, categorise the discovered risks, and create a risk heat map. The several hundred discovered vulnerabilities resulting from the profile development identified unique operational threats, and the team found that the associated threats were not only a risk to technology, but also extended to people and procedures (Martinov; 2018). These risks were then plotted onto a heat map that provided a complete view of the organisation's exposure, and identified fundamental risk factors.

Following the risk and current state assessment, BSD determined their target goals. By identifying mitigation strategies and desired outcomes, they outlined their security priorities and determined high-level approaches to mitigate each risk. To integrate the preexisting processes and information sharing activities, BSD translated these approaches into additional desired outcomes by utilising the Framework's Profile categories and subcategories as a guiding reference. Following this integration, a secondary review was performed to ensure that the created outcomes were consistent with the NIST Framework and would be able to achieve the desired goals in a cost-effective manner, establishing the BSD's target profile (Martinov; 2018). Once the profile had been defined, the BSD was left with a better understanding of its current state, and what processes would properly handle the established risks. By utilising this information, a baseline was established, and goals were determined based on the organisation's budget, resources, priorities. In comparing the current state with the targeted goals, BSD established practical targets, obtainable within the available budget. To allow for continued improvements, the BSD developed a collaboration tool to provide the information necessary to perform periodic self-assessments, supporting questionnaires, and activities and processes for staff and external partners. Described by Martinov as "a journey, not a destination" the continued improvement of a successful cybersecurity program requires consistent tools and procedures (Martinov; 2018).

4.3 Seattle Children's Hospital

As a high-ranking children's hospital in Seattle, Washington, the Seattle Children's Hospital is a large organisation that includes academia, a research institute, and a found-

ation to assist in patient financial support. As a complex organisation, Seattle Children's Hospital was required to identify and understand not only cybersecurity risks, but those introduced by the entire organisation. To support the security of the hospital, Seattle Children's implemented the Health Information Trust Alliance's (HITRUST) framework. Dr. Cris Ewell, Chief Information Security Officer at Seattle Children's Hospital, believed that the security of an organisation does not come solely from information security or compliance, but also from understanding the business and organisational risks in a continually evolving manner. The implementation of the HITRUST framework ensured that risk awareness and understanding was integrated into operational and business practices, communication with executive management was integrated, and showed how risk management was incorporated into key business aspects such as IT, research, and the foundation.

As a healthcare organisation containing a research institute, a pharmacy, and a financial foundation, Seattle Children's Hospital fell under several regulations including PCI DSS for financial processing, HIPPA for health information privacy, and FISMA for information security. The hospital required a framework that could ensure that all regulatory requirements were met. As a result, Seattle Children's chose to implement the HITRUST Framework, a healthcare-specific framework created as a direct response to the multiple industry compliance requirements, offering scalability and improved internal organisational communication (Curren et al.; 2015). In addition to the HITRUST Framework, Seattle Children's also chose to integrate the NIST Cybersecurity Framework to improve mapping, alignment, reporting, and communication. To integrate the NIST Framework, a requirements profile was created, structuring the requirements of each regulation in addition to organisation requirements. This profile is organised into 6 separate categories: Confidentiality, Integrity, Availability, Strategic, Tactical, and Organisational. By breaking down the profile into these categories, it became easier to communicate how policies and procedures are implemented. Additionally, the created profile allows the policies and procedures to be labelled under thirteen categories including: Operational Management, Technical Security and Access Control, and Incident Management. This allowed them to be related back to the NIST and HITRUST frameworks and applicable regulations (Curren et al.; 2015).

The incorporation of the NIST Framework with the current security program was conducted through a three-year project. Over the three-year period, the hospital performed an in-depth threat assessment across every application and key data element, performed an organisation-wide vulnerability assessment, and inventory asset management. Integrating the NIST Framework initially started with risk determination, conversations with key risk officers to determine current adversary behaviour, identifying what risks are acceptable to ensure the business and compliance needs are met, and what risks must be addressed to ensure the business remains operational. Following this, the identification of key assets including intellectual property, key people, applications, products, and data was carried out. As described by Ewell during a HITRUST NIST Framework Guidance Webinar, "my entire program is built on assets... I believe that's what our adversaries are after." Following these procedures, dashboards and diagrams were generated that could be used to understand risks. To understand threat areas or to mature any under-developed area, outside information is brought in to track any particular asset or vulnerability to develop a method to identify areas of interest. From these dashboards, operational and actionable information can be produced for the IT and business departments. Additionally, from this gathered information, an executive report could be delivered to the board

of directors that consolidates the information to give an organisation-wide risk picture Curren et al. (2015).

4.4 EY (Formerly Ernst & Young)

As a global provider of advisory products, EY[14] offers numerous cybersecurity-focused services[15] including vulnerability assessment, penetration testing, program maturity assessment, and control-based auditing. Conducted over a three-month internship at their Cyber Hub in Dublin, Ireland, the assessment of EY's integration of the NIST Framework established how EY had directly and indirectly utilised the framework. It also established how they had shaped decisions around it, identified several challenges that had arisen during its use, and the numerous benefits that it had provided.

Initial observations of EY's cybersecurity program showed that the NIST Framework had been implemented in both an indirect and direct manner. The Cybersecurity Programme Maturity (CPM) Framework, employed by EY during many of its cybersecurity assessments, is a NIST-based cybersecurity framework that assists in the understanding of an organisation's exposure to risk, establishment of current program maturity, and identification of areas for improvement. These assessments are typically accomplished through a questionnaire-based interview, documentation review, and executive discussions. Additionally, these are typically conducted in part with a penetration test or cyber-incident exercise to address control implementation, responsibility distribution, and management systems. In their Programme Maturity Assessment process, EYs CPM Framework is aligned to the NIST Framework's Core profiles. In this alignment, EY mapped several key business practices to each profile. Examples of this alignment are the mapping of NIST's Identify profile to categories including asset management, metrics and reporting, third party management, and strategy. The Protect profile was mapped to categories including awareness, data protection, network and software security, and vulnerability identification and remediation. From this mapping technique EY was able to develop an in-depth and industry-tailored questionnaire that applied the NIST subcategories to relevant organisational practices and activities. In addition to the integration into their proprietary CPM Framework, the NIST Framework has typically been used by EY as a comparative tool during maturity assessments, offering a reference point for other organisations unfamiliar with their framework during the discussion of current practices.

Through the hands-on experience with working on a Cybersecurity Programme Assessment (CPA) engagement with EY cybersecurity professionals, numerous benefits and limitations of the NIST-based CPM Framework were uncovered. While working with a multi-national healthcare service provider several limitations and challenges were faced. When conducting the initial stages of the maturity assessment, collection of requested process and procedure documentation to establish the current status of the items outlined in the questionnaire, several hurdles were encountered. When communicating with departments across several different countries, it was determined that the received documents were often incomplete, inaccurate, or completely missing. When investigating the cause, it was revealed that many departments found the request to be difficult or unclear. For some organisations the questions were unclear, resulting in the delivery of documents based on each departments interpretation of the questions, or no evidence was provided

[14]https://www.ey.com/

[15]https://www.ey.com/gl/en/services/advisory/ey-cybersecurity

as it is difficult to provide documents for something that is not properly understood. Other departments faced additional issues such as requiring further explanation, being unaware of where documents and procedures were applicable, or missing the documentation entirely. Additional complications arose during the collection and organisation of the received files. Using an online cloud-based document management system, each department uploaded their available documents. However, the lack of a specified upload format often led to difficulty in determining what documentation was present, what was missing, and to which activity or activities the document was applicable.

5 Evaluation

Following the analysis of the programs implemented at enterprise environments outlined in Section IV, the impact of the NIST Framework across various domains was discovered.

5.1 Intel

Following the completion of the four-phase plan, Intel concluded that for organisations looking to integrate or implement the NIST Framework, the most crucial factor is to tailor the Framework to meet organisational requirements and to start where they are most comfortable. Additionally, Intel plans to extend the Framework into the other business environments and is committed to improving the Framework.

5.2 University of Chicago

By ensuring that the business objectives are aligned with the most impactful activities, reducing the risks to the important research and educational programs, the Framework, and the information it provides, ensures the most value to BSD. Through the use of the NIST Framework, the University of Chicago's Biological Sciences Division was able to identify their security requirements as a set of target goals, while allowing each department to maintain the processes and procedures necessary to reach these goals. As the Framework allows for an individualised approach, each department can customise its approach to best meet their specific requirements and communicate these approaches across departments.

5.3 Seattle Children's Hospital

As a result of the integration of the NIST Framework with their current HITUST-based risk assessment procedures, Seattle Children's Hospital identified several key elements to success. To ensure that frameworks can be integrated successfully, it is crucial that the organisation understand the frameworks themselves. As the HITRUST Framework was chosen based on its healthcare-specific nature, created specifically to address the multiple compliance requirements, prescriptive application, and required scalability, the NIST Framework allowed for integration as it shares many similar features. As HITRUST

and NIST have become a popular framework combination, implementation guidance and certification is now available (BusinessWire; 2018).

Additionally, it is necessary to identify and focus on the most important aspects of the organisation; identifying key assets, the associated risks and controls, and knowing what needs to adjust or mature. Finally, continued improvements are critical, as prioritisation and balance are necessary to ensure business and security needs are considered.

5.4 EY (Formerly Ernst & Young)

Following the analysis of EY's CPA engagement process and CPM Framework documentation, EY has demonstrated remarkable success with their integration and implementation of the NIST Framework. From the creation of their own CPM Framework, to the use of the Framework as a point of reference to improve communication and discussions, EY has been able to successfully use the NIST Framework to perform maturity assessments and improve cybersecurity programs across countless organisations. To accomplish this level of success, EY has utilised resources such as their tailored questionnaire and internal threat intelligence program, and their experience with numerous companies across several domains to continually improve and adapt their framework to address the latest organisational risks and newly implemented best practices. While the issues faced during the CPA engagement demonstrated a need for refinement of the CPM procedure and highlight a known criticism of the NIST Framework, the possibility for misinterpretation due to its broad approach to security, these challenges could be addressed through questionnaire refinement and additional information provided during the maturity assessment process.

5.5 Discussion

From the analysis of enterprise cybersecurity programs across various domains, the NIST Framework has served as a powerful tool when auditing and strengthening existing processes and procedures, and when introducing entirely new ones. Regardless of the domain to which it has been applied, the NIST Framework has shown the importance of cross-organisation communication, the identification of key business assets, the establishment of achievable goals, and program maintenance and evolution. From the creation of new tools and procedures, to the integration within other preexisting frameworks, NIST has developed a powerful tool to aid any organisation. Following the review of multiple enterprise environments, it appears that the key factors for successful implementation occur during communication and the establishment of a starting point. To assist organisations in taking the steps towards successful use of the NIST Framework, a security program assessment tool (See Configuration Manual) has been created based on the information gathered from the review of successful industry practices and tools. This mapping tool consists of a series of activities, mapped to NIST subcategories, that an organisation can undertake to audit or establish their security procedures. The activities are intended to produce or record documentation or procedures that establish an organisation-wide consensus for security practices and communicate the preferred way by which they are documented.

6 Conclusion and Future Work

Through the review of published documents from governmental agencies and reports from academic researchers, and the analysis of various enterprise programs across multiple domains, the history, evolution, and numerous features of the NIST Framework has been established. The review of published documents and reports outlined the initial establishment of the NIST Framework, and how it has evolved since the initial release in 2014, and its reception across various domains. Since the time of its inception in Executive Order 13636, and through requests for comments and numerous revisions, the Framework has received its share of praise and criticism. These critiques and praise were vital when the case study, use case documents, and internship observation analysis questions were designed. By highlighting concerns such as a lack of incentives, impact, and consistency difficulties, the analysis and observations were shaped to ensure these concerns were addressed. Ultimately, we have argued that the NIST Framework has been a useful and beneficial tool for the organisations that have implemented it. While the Framework has been established as a voluntary governmental tool, the immense support from both the public and private sector has driven its popularity both within the United States and internationally. One of the limitations of this analysis has been the inclusion of only a small subset of use case documents, a small number case studies across few domains, and a single hands-on organisational analysis. Future research could use a greater number of case studies, a larger breadth of domains, or a hands-on analysis of multiple organisations. This work could help evaluate and lead the continued evolution of the Framework by identifying new areas of concern and developing new best practices and procedures as new cybersecurity threats arise. As a framework with input from thousands of individuals, years of revisions, and support from the public and private sector, the NIST Cybersecurity Framework has demonstrated its ability to be an influential tool when integrated with an in-use or newly created cybersecurity program.

References

Barrett, M. P. (2018). The framework for improving critical infrastructure cybersecurity version 1.1, National Institute of Standards and Technology.

BusinessWire (2018). Hitrust provides nist cybersecurity framework certification. [Online; posted 22-May-2018].
URL: *https://www.businesswire.com/news/home/20180522005533/en/*

Casey, T. (2015). Implementing the u.s. cybersecurity framework at intel - a case study, RSA Conference.

Casey, T., Fiftal, K., Landfield, K., Miller, J., Morgan, D. and Willis, B. (2015). The cybersecurity framework in action: An intel use case, *Intel Corporation* pp. 1–10.

Curren, S., Wolf, L. K., Stine, K., Bryan, C., Mehta, R. and Ewell, C. (2015). Health industry implementation of the nist cybersecurity framework.

Dolezilek, D. and Hussey, L. (2011). Requirements or recommendations? sorting out nerc cip, nist, and doe cybersecurity, *Protective Relay Engineers, 2011 64th Annual Conference for*, IEEE, pp. 328–333.

Fischer, E. A. (2005). Creating a national framework for cybersecurity: An analysis of issues and options, LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Greene, J. (2017). private communication.
URL: *https://www.nist.gov/sites/default/files/documents/2017/04/19/2017-04-10_symantec.pdf*

Gyenes, R. (2013). A voluntary cybersecurity framework is unworkable-government must crack the whip, *Pitt. J. Tech. L. & Pol'y* **14**: 293.

Landfield, K. (2017). private communication.
URL: *https://www.nist.gov/sites/default/files/documents/2017/04/19/2017-04-10_intel.pdf*

Martinov, P. (2018). Applying the cybersecurity framework at the university of chicago an education case study, *Technical report*, University of Chicago.

Obama, B. (2013). Executive order 13636: Improving critical infrastructure cybersecurity, *The White House, Washington, DC* .

Pratap, K. and Perkins, E. (2015). Using the nist cybersecurity framework. Gartner Security & Risk Management Summit.

PwC (2014). Why you should adopt the nist cybersecurity framework.
URL: *https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf*

Sedgewick, A. (2014). Framework for improving critical infrastructure cybersecurity, version 1.0, *Technical report*.

Shackelford, S. J., Proia, A. A., Martell, B. and Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices, *Tex. Int'l LJ* **50**: 305.

Shackelford, S. J., Russell, S. and Haut, J. (2015). Bottoms up: A comparison of voluntary cybersecurity frameworks, *UC Davis Bus. LJ* **16**: 217.

Shen, L. (2014). The nist cybersecurity framework: Overview and potential impacts, *The SciTech Lawyer* **10**: 16–19.

ThreatSketch (n.d.). A 10 minute guide to the nist cybersecurity framework, *Technical report*.

Trump, D. J. (2017). Executive order 13800: Strengthening the cybersecurity of federal networks and critical infrastructure, *The White House, Washington, DC* .