The Matrix: A Cybersecurity Cross-mapping

Alex Assante

April 29th, 2022

Important Note:

The cross-mapping analysis of the program is too large to include in this document effectively. For evidence regarding the cross-mapping, the paper shall possess the line “[See Attached Document]." When referenced, please open, and use the EXCEL document: *The Matrix: A Cybersecurity Standards Cross-Mapping*

Abstract

This paper investigates a problem within our nation's various industries, namely the inefficient compliance process of Cybersecurity standards, and proposes the use of technology to remedy it. This study proposes that cybersecurity standards across the nation possess only modest divergence in requirements and cybersecurity practices. Furthermore, a practical implementation of cross-mapping research (consolidated as a tool in Microsoft Excel) can help companies optimize the process of adopting and maintaining cybersecurity standards compliance. This effort will help companies achieve a more mature compliance program while potentially improving their security posture and lessening security and business risk. The results of the study were significant even only when mapping three standards. The study and accompanying tool revealed significant overlap in cybersecurity standards' requirements and practices.

Introduction

This project exists to answer the question: “Do cybersecurity standards across the nation possess only modest divergence in requirements and cybersecurity practices?” The research begins with examining and learning standards and ends with cross-mapping analysis and the creation of an accompanying “tool.” The “tool” the project produces consists of the consolidation of cybersecurity standards cross-mapping research with functionality to aid in standard adoption. It allows users to access cybersecurity standards publications, understand the relationships between the different standards and work towards standard compliance. The tool utilizes various visualization techniques, data storage, resource mapping, and summary spreadsheets to achieve this end.

Background

I was first exposed to the world of cybersecurity standards during an internship I conducted through the Idaho National Labs in the CyberCore Division. During my time there, a project I worked on required me to do a shallow investigation into different standards in effect across the nation. As I began to look through various standards, I began to discover a few glaringly obvious issues. The first issue being the language across standards, the language used varies, even when referring to the same concepts. This causes the reader to spend time “decrypting” a standard’s language even if they are familiar with another standard. The second issue being overlap, with standards being so closely related there must be a more efficient way to analyze the information and adapt the standards. That is where our third issue comes in to play, being the inadequacy of current cross mapping. The existent cross mapping in the industry is

compiled in a confusing format, does not update frequently, does not map requirements and/or only maps two standards to each other.

With so many shareholders, clients, national organizations, federal agencies, and governments needing to be appeased for operation, companies, such as American Electric Power, often need to adopt multiple standards. The cost and time required to implement a standard become multiplied, even if the standard's requirements and practices are similar, causing the linear scaling of both time and cost to be quite damaging to the business model of these organizations. With the disorganized adoption process of new standards, companies cannot provide the resource necessary to support both standards' processes. The penalties of non-compliance can range from fines to massive lawsuits and even to cease and desist orders, adding more stress to the company's process. This burden causes a damaging shift in focus from where the organization's proper focus should lie in completing its objectives, for example, generating and supplying power to the populace.

After discussing with experts involved in cybersecurity standard compliance, I was encouraged to create a cross-mapping tool. Even though I have more experience in other data analysis and documentation applications, designing the tool in Microsoft Excel allowed ease of access as most companies possess and use Excel.

Purpose of the Study

The purpose of this study was to learn and conduct a cross-mapping analysis of the North American Electric Reliability Critical Infrastructure Protection (NERC CIP), Center for Internet Security 18 Critical Security Controls (CIS Controls), and National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework)

cybersecurity standards. This research attempts to determine if cybersecurity standards overlap to ease the standard adoption process for organizations. Additionally, the project also aimed to construct a tool to measure the progress of standard adoption. After the project, companies would ideally have the ability to use the cross-mapping to assist in adopting secondary and tertiary standards and use the tool to track their adoption progress.

Significance of the Study

The validity and generalizability of this project's results are limited due to only analyzing a few cybersecurity standards from the industry. Requests are being made to implement more cybersecurity standards in the cross-mapping, further increasing this study's significance. The research is significant on an organizational level because of the impact the results have in allowing an organization to ease the cybersecurity adoption process. For this discussion, let us assume the outcome of the research shows that cybersecurity standards possess only modest divergence in requirements/practices. If this is the case, the cross-mapping conducted by the study will allow for the optimization of multiple standard adoption processes undergone by organizations throughout the Bulk Electric System (BES) industry. For multiple reasons, organizations already compliant with a cybersecurity industry standard can be put in a position where they must also comply with a second cybersecurity standard. By analyzing the overlap and non-overlap between two standards' requirements, the data and processes needed to supplement the existing compliance program is found. This information can be used to alter the existing program to create a singular compliance program working for both standards, effectively killing two birds with one stone. This project’s true significance lies in its prospective ability to give organizations the ability to streamline the cybersecurity standard adoption process,

potentially saving hundreds of thousands of dollars and months of time and human resources. By making information shareable, more easily understood, and "less painful" to implement, this project ultimately makes the BES industry, the power grid, and the world safer and more secure.

Research Method

The research project consisted of learning the three aforementioned standards and cross-mapping them. Similar cross-mappings exist; however, the primary goal was to learn the standards and conduct independent cross-mappings. Over a semester, the research project analyzed the NERC CIP, CIS Controls, and NIST framework standards. The project has two main phases: learning the standards and building the cross-mapping and tracking “tool." Throughout the first phase, I set aside a month or two per standard to thoroughly read and work to understand all of the primary and supporting material. Throughout the second phase, time splits between conducting the cross-mapping analysis and building the tracking “tool” with a time emphasis spent on the analysis. As for technologies used in creating the project, the cross-mapping/implementation tracking “tool” was built in Microsoft Excel. Excel was used to house the project due to the program's data organization and analysis capabilities and ease of information sharing.

Definition of Key Terms

Cybersecurity Standard: For this study, a Cybersecurity Standard is an amalgamation of best practices compiled by Cybersecurity experts to protect organizations from cyber threats.

Requirements: For this study, cybersecurity practices and requirements are interchangeable [2 – 15, 17].

Map To: For this study, when two or more cybersecurity standards' requirements "map to" each other, they are equivalent in either language or intent.

Requirements and Controls and Subcategories: These three terms are interchangeable; NERC CIP uses the term "requirements" to refer to cybersecurity practices, while CIS uses "controls" and NIST uses "subcategories" [2 – 15, 17].

Limitations of the Study

The primary restricting factor of this study was the short time frame. The study was limited in the number of standards analyzed and cross-mapped. Within the constraints of the time frame, three cybersecurity standards were selected to be learned and analyzed. The focus was shown on the NIST Framework, CIS Controls, and NERC CIP standards due to their significant presence throughout the cybersecurity industry [2,3,17]. Choosing these three standards also allowed for the comparison of both voluntary and mandatory compliance standards, helping reduce any data biases, and making the research well-rounded. These three standards have a total of 502 requirements; of those, 171 requirements were mapped. The short time frame, coupled with learning the standards themselves, greatly constrained the amount of time available to conduct the cross-mapping. In order to conduct the most thorough mapping possible, in the time frame given, the 108 NIST subcategories and the eighteen CIS Controls were mapped to the 49 NERC CIP requirements. Given a longer time frame, a more thorough (deeper) cross-mapping could have been conducted, and a larger sample size could have been

collected. Had more time been given to the study, better overall results could have been expected.

Summary

Overall, this semester-long research project consisted of learning and analyzing the NERC CIP, CIS Controls, and NIST framework cybersecurity standards. After learning the standards, the knowledge gained was used to implement a cross-mapping analysis of the standards and construct an accompanying standard adoption tool.

Research Methodology

Setting

The research project's goal is to uncover if there exists a significant overlap in requirements across Cybersecurity Standards. The subjects of this research were the NERC CIP, NIST Framework, and CIS Controls cybersecurity standards. This project focuses on these three standards for their presence in the cybersecurity industry and their varied applicability. The CIS Controls and the NIST Framework are voluntary for industry; however, the NIST Framework is mandatory for US federal government agencies [2, 17]. The use of the NERC CIP standards is mandatory for entities owning, managing, or using bulk power system assets part of the US and Canadian power grid [3]. These standards were chosen to well round the research and eliminate bias by analyzing standards that are both voluntary and mandatory throughout the cybersecurity industry.

Research Design

This research project was designed with the continuation of work in mind by implementing one or more standards into the cross-mapping. To replicate and/or continue this work, a researcher would start by creating and populating a cybersecurity standard(s) overview worksheet. The researcher would then add the new standard(s) to the cross-mapping and conduct all the proper analysis/matching. The procedure for the standard's cross-mapping is conducted upon two primary principles. First, NERC CIP was chosen as the "main" set of standards, meaning that the other standards are mapped to NERC CIP. Second, the standards map to one another based upon equivalence of language or intent of their requirements. Finally, the researcher would create and build a "controls implemented" worksheet for the new standard(s) [See Attached Document].

Summary

Altogether, the setting and research design are structured to provide the results with clarity and accuracy. The choice of standards used in the project was well researched to ensure accurate data. The mapping criteria are defined succinctly as to be applied equally across current and yet-to-be-mapped standards. Given the defined mapping criteria and setting, this study could be replicated and continued by other researchers.

Results

An overlap of cybersecurity practices and requirements was shown upon conducting a cross-mapping and analyzing the NERC CIP, NIST Framework, and CIS Controls cybersecurity standards. Of the 171 practices and requirements analyzed, only 15 did not map to another

standard. Although a shallow depth cross-mapping was conducted (as mentioned in the limitations), the results showed a 91.23% overlap in practices/requirements across standards [See Attached Document].

Discussion

Research Question

RQ: Was there a significant overlap in requirements across Cybersecurity Standards?

An overlap in requirements across cybersecurity standards are defined as an equivalence of language or equivalence of intent of two or more standards' requirements. For example [See Attached Document]: The NERC CIP-002 Requirement 1 requires the user to identify and inventory bulk electric system (BES) cyber systems assets. The NIST Framework Identify Function Asset Management (ID.AM) category requires identifying and managing organizational assets. The CIS Control 1 requires the inventory of and active management and control of enterprise assets. All three requirements listed possess similar language and the exact intent of creating and managing an enterprise asset inventory; as such, we can map these three requirements to each other. This process of "matching" the standards' requirements' languages and intents is the most fundamental aspect of creating an accurate cross-mapping analysis and measuring overlap across standards [See Attached Document].

91.23% of the requirements analyzed for the cross-mapping matched one or more other standards' requirements, compared to 8.77% of requirements that did not match other requirements [See Attached Document]. Although this is a significant overlap of practices and requirements across cybersecurity standards, the intended results and further project revision should be conducted for better results.

Intent vs. Execution

The initial proposed project state varies significantly from the current executed state of the research project. The project's original intent remains the same (learn and cross-map cybersecurity standards), but the execution of the project had to be changed. As I mentioned previously in the limitations of this project, the number of requirements analyzed to be mapped was changed. Counting all requirements, sub-requirements, and sub-sub requirements, the three standards have a combined total of 502 requirements. Two reasons exist for not including all said requirements in the cross-mapping analysis: the restricted time frame, as stated previously, and data organization. Mapping some of the existing sub-sub requirements by themselves would be illogical as it would be difficult and would not yield a different result than mapping only the parent requirements.

The early project plan was to create and build the cross-mapping/implementation tracking "tool" in an excel workbook alongside several other features. Those features included: standards access, data analysis, data storage, file storage, resource mapping, violation mapping, and summary spreadsheets. The executed project still includes the cross-mapping, implementation tracking, cybersecurity standards access, and data analysis/summary spreadsheets; but is missing data storage, file storage, resource mapping, and violation mapping. Of the missing features, data storage, file storage, and resource mapping (asset inventories) were removed under the realization that it is not practical to store the necessary amount of information and other files needed for standard compliancy within the workbook. Instead, the data and files could be stored alongside the project in a computer system. Violation mapping was removed from the project because of standard violations' unpredictable and dangerous nature. Auditors determine standard violations and their severity during an audit. While auditors are supposed to be fair and unbiased

human nature causes this to be the case rarely. Therefore, if violations and their severity can be determined/interpreted by an individual auditor, some auditors will find violations where others will not. Tracking potential violations become unpredictable; and dangerous if used in a business setting. Suppose an organization hires a consultant to prepare for an audit and they find no violations using a potential violation tracker. If a blatant violation is then found under audit, the consultant risks losing the client's business and legal ramifications.

Roadblocks

The time spent undertaking the research project did not come without a burden. Throughout the study, multiple roadblocks were encountered and overcome. The "learning" part of the project in itself was a roadblock. The NERC CIPs, NIST Framework, and CIS Controls are written professionally and are often verbose with specific industry jargon. An even more significant challenge presents itself when 100s to 1000s of pages of the confusing/complex language have to be read. Taking the time to learn and understand this new vocabulary was challenging and took time.

The "developing" part of the project saw multiple roadblocks; however, many were minor. The first significant roadblock experienced was importing information. For the cross-mapping and the "tool" to work, much information was necessary inside the excel workbook. That roadblock was overcome by importing all the information by hand, as there was no other way to do so. The second roadblock experienced in the development phase was table formatting. In order to run the data analysis, formulas had to run on an excel table. The problem lay in my initial data layout; I custom-designed tables for better readability and separation of information. However, I could not run the analysis on any of those tables. I had to make new excel tables and

transfer all the data between tables by hand. The final roadblock experienced was implementing working excel functions in the implementation tracking pages. Some of the equations, written only to count for "x" in cells, took hours of troubleshooting and twenty-plus iterations to work correctly. This roadblock was overcome through trial and error and by learning the syntax and behavior of specific excel functions.

Project Takeaway

After graduation, I am beginning work in this field, so regardless of the outcome, the main goal of the research project was to serve as a learning experience for me. This project was just that; I learned much more than I bargained for. Besides hoping to further my Excel proficiency, when I began the project, I had hoped to and did learn professional data analysis, cross-mapping analysis techniques, and the cybersecurity standards themselves (NERC CIPs, NIST Framework, and CIS Controls).

However, besides the standards, the most beneficial things I learned were professional and technical skills. By reading the three standards and all accompanying information, I learned how to professionally “decipher” technical and confusing language. The reading process led me to learn all about the BES and cybersecurity industry. However, more importantly, it taught me how to properly search for information to further my understanding of the field. When extremely niche and technical terms are used, google might not have a definition for you. I had to learn how to find and piece together information in my field to gain an understanding of the work being done.

Throughout the project, I used and exhausted every resource I could to learn new information and skills that would be beneficial for my new career. I learned and practiced

professional communication skills when asking soon-to-be coworkers to explain a tricky subject. Though it might sound silly, I learned professional time management. Having so much work to complete in a semester forced me to suppress my procrastination habit and instead work on and ahead of schedule. The most important thing I learned was professional drafting and problem-solving. I had coworkers look at my project and my process throughout the project and give me feedback. This helped prepare me and gave me experience in taking professional, constructive criticism and learning project drafting techniques before I begin work full time. No matter the outcome, the senior project has been nothing but an eye-opening, enjoyable, and tremendous learning experience for me.

Conclusions

In conclusion, the overarching goal of this project was to create a comprehensive cross-mapping analysis of prominent cybersecurity standards to allow organizations to optimize and streamline the cybersecurity adoption and compliance process. By analyzing the connections between the NERC CIP, NIST Framework, and CIS Control standards, we can begin to further share and understand the information in the BES industry, ultimately creating a safer and more secure environment. A research goal was adapted by learning and analyzing the relationships between cybersecurity standards and creating a research methodology. As a result, a cross-mapping of standards is constructed, providing quantifiable results comparable to other studies done with a larger pool of cybersecurity standards. This research proved to be effective and a stepping stone down the path toward a safer and more secure future.

Recommendations and Implications for Theory, Research, and Practice

More cybersecurity standards can be implemented for further implementation and research data to increase the sample size and add more diversity to achieve more results and cross-mappings. This study would have to be updated upon new version releases of the standards to ensure the cross-mapping still holds its validity. I believe that it would be helpful to have others review this study's cross-mappings or conduct their own to reaffirm the study's results. However, overall, this study showed only modest divergence in cybersecurity practices and requirements in cybersecurity standards.

References

[1] CIS. CIS Critical Security Controls: Implementation Groups. Retrieved from https://www.cisecurity.org/controls/implementation-groups.

[2] CIS. CIS Security Controls. Retrieved from https://www.cisecurity.org/controls.

[3] NERC. CIP Standards. Retrieved from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[4] NERC. *CIP-002 Cyber Security – BES Cyber System Categorization* (5.1a ed.). Retrieved from https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization&Jurisdiction=United%20States.

[5] NERC. *CIP-003 Cyber Security – Security Management Controls* (8th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-003-8.pdf.

[6] NERC. *CIP-004 Cyber Security – Personnel & Training* (6th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-004-6.pdf.

[7] NERC. *CIP-005 Cyber Security – Electronic Security Perimeter(s)* (6th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-6.pdf.

[8] NERC. *CIP-006 Cyber Security – Physical Security of BES Cyber Systems* (6th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-006-6.pdf.

[9] NERC. *CIP-007 Cyber Security – System Security Management* (6th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-6.pdf.

[10] NERC. *CIP-008 Incident Reporting and Response Planning* (6th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-008-6.pdf.

[11] NERC. *CIP-009 Cyber Security – Recovery Plans for BES Cyber Systems* (6th ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-009-6.pdf.

[12] NERC. *CIP-010 Cyber Security – Configuration Change Management and Vulnerability* (3rd ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf.

[13] NERC. *CIP-011 Cyber Security – Information Protection* (2nd ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-011-2.pdf.

[14] NERC. *CIP-013 Cyber Security – Supply Chain Risk Management* (1st ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

[15] NERC. *CIP-014 Physical Security* (2nd ed.). Retrieved from https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf.

[16] NERC. Updated March 29th, 2022. *Glossary of Terms used in NERC Reliability Standards*. Retrieved from https://www.nerc.com/files/glossary_of_terms.pdf.

[17] NIST. NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/cyberframework/framework.