THE UTILISATION OF NIST AS A CYBERSECURITY FRAMEWORK IN HIGHER EDUCATION INSTITUTES DURING COVID-19

Project Report

by

Thomas Hughes

C00231519

APRIL 29, 2022

Supervisor: Christopher Staff

Table of Contents

Introduction

General Issues

Problems encountered & how resolved

The general issues I faced during the project can be identified by each segment of the work that I was doing.

The Survey posed a couple of issues, namely the timing of the project and the availability of the HEIs I was contacting. One of the main reasons I switched focus during the mid-way point of the project was due to an inconvenient timing issue – a cyber survey had been sent out during production of my survey. While in the final stages of preparing my cybersecurity readiness survey, quite literally as I was about to send the completed draft out, I heard from an HEI that they had received a similar project from the HEAnet, the service provider for HEIs. The survey they had conducted was quite similar in nature to mine, and my supervisor and I decided that HEIs would be less likely to answer a survey so soon after one they had answered – one with less relevance to their interest. This was resolved by proceeding forwards as originally planned. I sent the survey to my 10 HEIs, but decided to focus on a gap analysis method, which was the NIST CSF audit.

Communications with the HEI also seemed to be an issue initially. During the preparation of the survey, I had sent out a few preliminary emails to HEIs regarding them answering this survey. I received only one reply from the list of 10. This was a worrying response from the target audience that I was meant to be in contact with. This was resolved by maintaining contact with the HEI which received the NIST audit by keeping close and contacting them regularly. They were kind enough to allow this project to go ahead and helped me avoid a large setback in my project.

Another large element of the survey was the issue of privacy in the survey. During the research process of this project, A question came up: will HEIs want to answer a survey where they are giving out their cybersecurity vulnerabilities? This was something I had to mull over when creating the survey. If I was to compare all results together, there would have to be an insurance for those HEIs who were willing to give out these details in the first place. This was resolved by anonymizing all survey results and providing a disclaimer at the start of the survey. This was possible with a feature that could be enabled with the SurveyMonkey suite.

Overall, I consider my project a success. Following the metrics detailed in the Functional Specification -

The following metrics for the UTILISATION OF NIST AS A CYBERSECURITY FRAMEWORK IN HIGHER EDUCATION INSTITUTES DURING COVID-19 project are;

- Understand in greater detail the cybersecurity preparedness of Higher Education Institutes in Ireland during the COVID-19 period
- Understand how well the HEIs conform to the NIST cybersecurity framework when comparing their current setup using a NIST CSF audit

- Establish contact with HEIs, specifically IT employees, and gain information on the current cybersecurity landscape
- Report any findings in this research, process this, and develop responses and recommendations to help improve these HEIs
- Finish all documents and submit within the timeframe

To comment on this, I would consider myself much better versed in the knowledge of how HEIs operate with their cybersecurity in the COVID 19 period after the extensive research and NIST audit carried out over the last 6 months of the project. I got a better understanding with how HEIs fare in the NIST measurement with the successful audit and a more general knowledge acquired through the survey. Contact was established with HEIs, more reliably with some than others, and reported the findings in my final document.

What was not achieved

The main element not achieved was the depth of the survey results analysis. This was originally meant to be one of the aims of the survey. While a results were accumulated and analysed, they lacked the depth I wanted from the beginning. There were plans to include visual data, graphs and pie charts to represent it effectively. During the creation of this however, there was a change of plans due to unforeseen circumstances. This meant more effort was spent on the NIST cybersecurity audit, thus leaving less time to complete this section. While complete, it definatly could've benefited from more fleshing out.

What I learned

I believe I managed to get a strong grasp of the NIST CSF framework – how it is applied, how often it's utilized by organisations who subscribe to it. One of the most interesting things about the NIST framework is how often you will use it in day-to-day business decisions once you have began applying it. For example, an order of new laptops in your organisations doesn't just mean a flashy new tech for your employees. You must first consider your new assets – are they compliant with asset management? Is your asset management register kept up to date? Does it account for all vital info of your assets e.g. asset ID, network, OS, used ports, Mac address. Once these are documented, how do monitor and protect them? What softwares do we have to use on this machine? Are they fully license, documented and accounted for? Now, how will they be used? If brought home, is there an updated BYOD policy to allow this? Is this within the means of the risk assessment of the company? Are stakeholders satisfied with this? This is just a single scenario with more elements to consider, so understanding the intricacies of what an application of this framework has been very informative to me.

I found a lot of information based on the legislative side of the research too. Understanding the EUs directive NIS having been created was something I was not originally aware of. During my research, I had noticed how lacking in some areas the HEIs were, specifically guidance-wise. To know that there were laws and directives in place to protect Irish organisations was rather informative.

I learned the importance of time management, and how long-term projects require a greater level of time management. I found juggling certain documents and researching to be challenging, but it certainly helped me understand the importance of prioritizing time and

understanding better time management. As someone who worked full-time while completing this project, I found this to be a necessity.

What would be differently

The main changes I would make to the project if I was starting again are;

- Focus on the NIST Audit straight away. More time spent on the audit means better familiarity with both the HEI and the NIST framework + NIST publications. This extra time would allow more personalised recommendations according to the HEIs specific needs.
- Making and maintaining contact from the get-go. Having contact halfway through the project certainly made things a bit tighter on the deadline. Allowing more time for myself would help the project overall.
- Send out the survey earlier. One of my issues in this project was the timing of which the survey was sent out, clashing with another formal survey. While this could not have been predicted without prior knowledge, for this instance of the project that I achieved, that is a change I would make.

Technical Issues

A main difference to note was the drafts that were part of the survey process. Originally, there were more question in the first draft – about 22 in total. These questions were satisfactory content-wise: they asked NIST-based questions; however, it didn't have a natural flow. Each question seemed to jump from topic to topic and didn't flow well in this style. This was brought up from feedback from the HEI which received the NIST audit. Having taken this onboard, drafts were tested until the final product was used, the one seen in the final project.