Udipto Chowdhury

Prof. Kennedy

FCM 761

03/27/2023

Midterm Part 2

NIST (National Institute of Standards and Technology), is a United States Department of Commerce agency whose mission is to promote American innovation and industrial competitiveness. In February 2013, The Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - when it comes to reducing cyber risks to critical infrastructure. Because it was created through collaboration between industry and government, the voluntary Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure, which in turn helps the companies to be prioritized, a flexible, repeatable, and cost-effective approach to the Framework. Which in turn helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

Thanks to the NIST CSF Framework, the University of Pittsburgh has successfully improvised its situations regarding streamlining awareness as well as gaining a better perspective of security risks and compliance issues across the university, resulting in units proactively seeking security support from the Information Technology department on issues that are considered broader than federal grant management requirements. What this is conveying is that NIST is observing and surveilling certain companies and educational institutions regarding cybersecurity and IT framework much like NYC DOE (Department of Education) in which the Chancellor and the Supervisor attend specific public schools when it comes to academics, extracurriculars, student body, and reputation. NIST CSF was possibly selected because not only it is government-based but also it assists organizations by providing context on how an organization views cybersecurity risk management clearly and concisely.

Methodology-wise, a goal-based approach was used. Since it is a method used to determine the actual outcome of a project when compared to the goals of the original plan. This helps the position of the evaluation that was taken to understand the position as well as knowing the do's and don'ts when it comes to improving the employers' and employees' awareness when it comes to dealing with cybersecurity infrastructure.

In terms of the maturity scale, it has to be on level 4 because the organization is capable when it comes to integrating with other business value-creating activities. Along with the capabilities which are aimed at being dynamic to meet changing business needs with additional capabilities that may exhibit improvement through an iterative process or innovation. The reason it has to be set to level 4 is that, even though the organization is somewhat above average, it has the potential to become a company with world-class standards.

On one hand, 'Detect' is the most vital asset of our company with ratings of: 4.6 on anomalies, 4.1 on continuous, and 4.4 on detection. Since 'Detect' is understanding the development and implementation of appropriate activities when identifying any symptoms that can lead to infecting a cybersecurity event. Additionally, 'Protect' and 'Respond' are not the most vital assets but are not the liabilities as well. Since the company scored 3.9 on 'Awareness and Training', employees and employers know that they must ensure that they work smarter to uphold the company's reputation. As for 'Respond', the company scored 4.5 and 5 on Response

Plan and Improvement. Again, the employers and employees know what they are doing but in the future, they need to start coordinating with each other since it is important to ensure that the enterprise’s response plans and updates for the key stakeholders and external service providers remain satisfied with the company's expectations along with their investments. In the end, the concepts of 'Protect' and 'Respond' will help the company to ensure delivery of service as well as take proper action regarding a cybersecurity event as long as the employees' and employers' heads are above the water.

On the other hand, 'Identify' and 'Recover' scored 2.5 and 2.8 based on the company's evaluation. Respectively, 'Identify' does have some understanding when it comes to risk assessment/management along with asset management. At the same time, the company knows how to approach recovery planning even though the employees and the employers are not communicating fashionably. To put it in simple terms, the company has the motivation to improve the company's reputation. The company can improve gradually when it comes to better performance under 'Identify' and 'Recover' in which the company will develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities along with developing and implementing the appropriate activities to take action regarding a detected cybersecurity event.

In general, this company will prosper as long as the executives, the employers, and the employees know what they are doing to uphold the company's reputation as well as gain respect from other companies through hard work and determination as long as they follow the NIST CSF Framework and demonstrate the ability to maintain their work responsibilities.

To conclude, the general key suggestions and timelines in which I have to propose to raise the maturity are to ensure that there is an integrated capability framework with real-time monitoring for the sake of continuous improvement. And the fact that sub-areas of "Identify' and "Recover' needs to be improved for the company to uphold its reputation along with ensuring the company's employers, employees, and executives are doing their best to serve others when it comes to cybersecurity infrastructure along with software inventory. In addition, the company will gain mastery when it comes to developing an understanding to manage cybersecurity risks, ensuring the delivery of services promptly, mitigating the symptoms that will cripple a cybersecurity event, creating an action plan for the company's reputation to go into the right direction, and creating a backup drive for the sake of preparing any unexpected events in addition to ensuring the employees and the employers are doing the right thing when it comes to upholding the company's reputation. Therefore, Hence, the company shall be named 'Trenton-Stanford'. And the company's motto is "Start Today, Finish Tomorrow". Hopefully, this company can prosper when it comes to ensuring the success of the company's reputation. With the fact that this company has the motivation to arrive at Successful Boulevard.