Discussion on the implementation of the NIST Cybersecurity Framework by Intel

Author: Mohammed Sadiq Abuwala
Student ID: 45921407
Date: 14/03/2021

Introduction

The national Institute of Standards and Technology (NIST) is a U.S. government agency that provides standards and recommendations for the security controls of Information Systems. Complying with the NIST cybersecurity framework helps an organization to protect itself against cyber attacks and threats such as viruses, ransomware, and malware. The NIST Cybersecurity Framework is one such standard that has been widely adopted since its inception. In this report, we discuss the benefits and limitations of using this framework in the context of the Intel case study. Finally, we also discuss the appropriateness of the implementation of such a framework for the purpose of this project.

Benefits of implementing the NIST Cybersecurity Framework

First, let us discuss the unique aspects of introducing such a framework in an organization. The framework provides a common language and systematic methodology for managing cybersecurity risks (Uses and Benefits of the Framework, 2021). Furthermore, it does not disrupt the existing cybersecurity program of an organization but is meant to complement existing standards. This is ideal for Intel which already possesses cybersecurity apparatus. This means that less time is spent tailoring the NIST framework at Intel. The high customizability allows the framework to be adopted by a large variety of industries. This customizability is offered due to the profile section of the framework. The profile feature allows organizations to align cybersecurity processes based on their individual business needs, available resources and tolerance for risks.

Implementation of the NIST framework allows an organization to possess adequate risk assessment of their processes. This means that upon successful implementation of this cybersecurity framework, Intel can identify existing processes that need to be made more secure and also predict new processes that may be required. The framework makes it possible for Intel to manage their cybersecurity and risks in the long term. Hence, the organization becomes adaptive, responsive, and in continuous compliance.

As more regulators also begin encouraging the use of the NIST cybersecurity framework, Intel's integration of it in their organization allows them to be on par with current and future compliance requirements in IT security.

Finally, the NIST cybersecurity framework is available for free and does not require a subscription, license, or certification. This makes it cost effective for organizations of all sizes to implement it.

Limitations of the framework

The framework only provides a high level operation and a security assessment in line with the framework can be open to interpretation by various organizations. This can lead some organizations to incorrectly measure their security risks and provide a false sense of security. Furthermore, self certification may also provide a cost effective way to implement the framework but incorrect analysis by the organization can further compound to a false sense of security.

By complying, organizations are assumed to have less risk. But the framework does not help to measure risk (Is the NIST Cybersecurity Framework Enough to Protect Your Organization?, 2021). Furthermore, the framework does show that improvements occur as the organization progresses among the tiers but it is not able to measure the exact return of investment (ROI) of any improvements implemented.

While implementation of such a framework might be beneficial to a U.S based organization such as Intel, it may not be considered as valuable for organizations based outside the U.S. This is because the NIST cybersecurity framework is not highly acknowledged outside the U.S.

Conclusion

The large number of benefits clearly show that the implementation of the NIST cybersecurity framework allowed Intel to considerably improve their organizational cybersecurity posture. The framework provides a common language to address cybersecurity needs. It allows Intel to make more cost effective use of their security budget. Significant and irrelevant cybersecurity measures can be identified. Furthermore, risks present in supply chains can also be identified. Finally, implementing the framework allows the organization to maintain a continuous and adaptive cybersecurity posture.

References

NIST. 2021. Uses and Benefits of the Framework. [online] Available at: <https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework#:~:text=The%20Framework%20provides%20a%20common,to%20meet%20any%20organization's%20needs.> [Accessed 14 March 2021].

ISACA. 2021. Is the NIST Cybersecurity Framework Enough to Protect Your Organization?. [online] Available at: <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization> [Accessed 14 March 2021].