Hoya Inc. Framework Selection

Clara Kellermann-Bryant, Evan Rapson, Jefferson Mondestin, Denis Gallagher

Module 3: Hoya Inc. Project Group 3

MPCR-5661-101

Professor Sumera Baker

September 18, 2024

Abstract

Hoya Inc. is a large manufacturer of technical devices which spans transnationally and has international suppliers. The broad and multifaceted company needs strong cybersecurity capabilities and most importantly an updated cyber risk management framework. After reviewing cybersecurity frameworks such as ISO/IEC 27001, COBIT, and HITRUST, our group recommends that Hoyas Inc. implements the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

NIST CSF was created for any sort of business to manage and reduce their level of risk, regardless of size, industry, or sector (NIST, 2024). It defines itself as descriptive rather than prescriptive. We are attracted to this choice because it emphasizes organizational self-awareness and communicability to stakeholders, which fits Hoyas Inc's demands regarding internal systems, multinational regulations, and business relationships. By following the framework, Hoyas Inc. will gain the abilities to prioritize Core functions like Identify, Detect, and Respond, write Organizational Profiles, and recognize Tiered cybersecurity demands (NIST, 2024). NIST CSF allows the entire organizational hierarchy, from executives to engineers, to understand and reduce risks. Because Hoya Inc. has international suppliers and operates on various platforms such as the Cloud, risks are highly variable. Therefore, due to its vendor and technology neutral stance (NIST, 2024), the NIST CSF will meet the wide array of cybersecurity risk management demands facing Hoyas Inc.

In this paper we will review how the utilization of NIST CSF Core Functions, Organizational Profiles, and CSF Tiers can benefit Hoya Inc. (NIST, 2024). We will address the remedial controls relevant to Hoyas Inc.'s use of legacy systems, international operations, and

remote workers that utilize mobile phones for sales and management tasks. Lastly, we will explore how NIST CSF fits into the broader realm of Enterprise Risk Management Framework.

Why is NIST CSF the best for Hoya Inc.? Understanding the CSF Core.

The NIST CSF is a highly adaptable and vendor neutral cybersecurity framework that works for a wide range of business types (NIST, 2024). NIST CSF has three main components, beginning with the CSF Core. The Core provides high-level cybersecurity outcomes that allows an organization to understand and manage their cyber risk (NIST, 2024). Next are CSF Organizational Profiles, which describe the organization's posture from the CSF core outcomes (NIST, 2024). Lastly are the CSF Tiers, which describe the emphasis that an organization puts on their cybersecurity risk and at what level of importance is cybersecurity risk compared with other components in the business (Jha, 2024a). Combining these elements allows an organization to map out and evaluate, identify, and respond to any sort of cybersecurity risk with the end goal of reducing the overall risk to their assets in the organization.

Hoya Inc. has a multitude of different components that can increase the risk of their operations. Using the CSF Core functions allows Hoya Inc. to map out their risk management strategy and evaluate the outcomes from this process. The 2024 NIST CSF document categorizes Core functions in an understandable and actionable way (NIST, 2024). The list of Core functions starts with Identify. This involves making an inventory of the company’s assets and assessing their risk implications (NIST, 2024). Hoya Inc. has assets all over the world, from information systems to phones, which each have their own vulnerabilities and organizational risks. The next core function, Protect, is meant to develop safeguards and controls against cyber security incidents and to ensure that critical assets are operational and secure (Bresnahan, 2019). This function includes categories such as Identity Management, Data Security, Awareness and Training, etc… (NIST, 2024). All these categories are vital for Hoya Inc. as they deal with various systems in their organization. For Hoyas Inc., The Technology and Infrastructure Resilience (PR.IR) category deserves prioritization due to the fact that they use two cloud providers. Hoya Inc. must ensure that availability is maintained and proper security procedures are being followed by the cloud providers (NIST, 2024). Failure by cloud providers to follow best practices and protocols to adequately protect assets and servers jeopardizes Hoya's Inc.'s data.

The primary purpose of the Detect function is to develop and implement actions to identify and respond to a cyber incident (Bresnahan, 2019). Hoya Inc. already has a Security Operation Center (SOC), meaning they have a control in place (in this case a department) dedicated to responding to cyber incidents. However, they do not have a cyber threat intelligence center, meaning there is no function to collect, process and analyze data to understand the threat actors' tactics, techniques and procedures (TTPs) (CrowdStrike, 2023). The Adverse Event Analysis (DE.AE) category states that "Cyber threat intelligence and other contextual information are integrated into the analysis" (NIST, 2024). Therefore, for Hoyas Inc. to understand their cyber threat landscape they should follow the explicit NIST CSF Detect function suggestion for a cyber threat intelligence center.

Lastly, the two functions of Respond and Recover go hand in hand. The Respond function is meant to develop and implement actions to remediate a cybersecurity incident (Bresnahan, 2019). The Recover Function is meant to restore and repair capabilities that were affected by the cybersecurity incident (Breshahan, 2019). Hoya Inc. has a SOC implemented in their organization which helps them with responding to incidents, however NIST CSF goes further into communication in the event of a cyber incident. Respond Category “Incident Response Reporting and Communication (RS.CO)” emphasizes the aspect of communicating with internal and external stakeholders so that they are aware of the incident (NIST, 2024). Effective communication is essential to remediate incidents efficiently.

All of these core functions revolve around the last function, Govern. The Govern Function is meant to establish the organization’s cybersecurity risk management strategy, expectations and policy (NIST, 2024). The Govern function is vital as it incorporates cybersecurity risk into the organization’s overarching Enterprise Risk Management (ERM) strategy (NIST, 2024). In the ever-evolving technology landscape and with an outdated 2019 Risk Management Framework, Hoyas Inc. must change and adopt the NIST CSF.

CSF Organizational Profiles

The NIST CSF is used to describe desired outcomes. The second element in the CSF is an Organizational Profile. An effective CSF Organizational Profile translates Core goal outcomes into specific organizational terms. A Profile considers the context of the organization’s ‘mission objectives, stakeholder expectations, threat landscape, and requirements’ (NIST 2024). This element of the CSF makes cybersecurity objectives more specific, actionable, and communicable.

The framework outlines how to draft Organizational Profiles. This begins with defining the scope of the profile, which can vary in size from the entire organization down to specific systems. Next, the profile must consider and compile the information relevant to cybersecurity Core goals. Examples of considerations include ‘organizational policies, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirements and standards, and work roles' (NIST 2024). Once a Profile is drafted, it has several uses.

Organizational Profiles serve several useful purposes, many of which are relevant to Hoyas Inc. The CSF suggests the benefit of outlining a 'Current' Profile and comparing it to a 'Target' Profile, which might point out gaps and illuminate courses of action. A CSF Organizational Profile is also useful as a communication tool. It can outline capabilities to stakeholders like business partners and customers. It can streamline compliance. Additionally, it can express expectations to new parties. All of these Profile use cases present Hoyas Inc. with potential value and improved security and risk management.

CSF Tiers

The four NIST CSF tiers that are to be incorporated into Hoyas Inc. include partial, risk-informed, repeatable, and adaptive tiers that determine awareness and proper risk management implementation (Jha, 2024b). Tier 1 organizations lack basic security awareness and tier 2 organizations lack appropriate risk management. Tier 3 organizations have obtained executive approval, and tier 4 implements high-technology solutions (Jha, 2024b).

Within the four NIST CSF tiers, these aspects can also be aligned to the Hoyas Inc. manufacturing profile. For example, the aspects can incorporate environmental safety, personnel safety, production goals, product quality, and sensitive information maintenance (Stouffer et al., 2020). Subcategories including asset management, business environment, governance, and supply chain management are to be aligned with the tiers as well (Stouffer et al., 2020). Continuous manufacturing and batch manufacturing are the last aspects to be considered for the four NIST CSF tiers (Stouffer et al., 2020).

NIST CSF and Hoya Inc’s ERM Incorporation

The rapid adoption of diverse technologies and society's growing reliance on cloud services have introduced significant risks to Hoya Inc.'s governance and IT security. Key concerns include the use of legacy systems, the complexity of international operations, and the growing number of remote workers using mobile devices for sales and management tasks. To address these challenges, we propose integrating two essential frameworks—the NIST Cybersecurity Framework (CSF) for managing cybersecurity risks and Hoya Inc.'s Enterprise Risk Management (ERM) for a comprehensive, organization-wide risk approach. Together, these frameworks offer a holistic solution to strengthen Hoya Inc.'s risk governance and cybersecurity posture. The NIST CSF is flexible and adaptable for organizations of any size, particularly those with critical infrastructure (e.g., sensitive government contracts). It emphasizes continuous improvement and aligns well with global standards. This framework focuses on five key areas: identify, protect, detect, respond, and recover (NIST, 2024).

To further enhance its effectiveness, Hoya Inc. will incorporate the four NIST CSF tiers—partial, risk-informed, repeatable, and adaptive—into its risk management strategy. Currently, Hoya Inc. operates at **Tier 1** (Partial), where security awareness is limited and foundational security measures are underdeveloped. By progressing to **Tier 2** (Risk-Informed), the company will integrate formal risk management processes, though they may not yet be consistently applied. At **Tier 3** (Repeatable), Hoya Inc. will aim for executive-level approval of cybersecurity practices, ensuring that security efforts are standardized and aligned with the broader business strategy. Finally, reaching **Tier 4** (adaptive) will enable the organization to implement cutting-edge security technologies, continuously improve its cybersecurity posture, and adapt to evolving threats which enhances its overall resilience.

The incorporation of ERM will begin with the creation of a cross-functional risk committee, which includes key stakeholders from various departments—IT, finance, legal, compliance, and operations. This committee will be responsible for identifying risks specific to each department and reporting them to senior leadership. Additionally, the board of directors will play an active role in overseeing ERM as part of its corporate governance responsibilities. A board-level committee or a board representative will be involved in the ERM team to ensure alignment with organizational goals and risk tolerance. For instance, Deloitte's board has a formal risk committee that plays a key role in risk oversight, as noted by Calagna (Morgan, 2023). Similarly, Hoya Inc.'s ERM team will include a diverse mix of executives and managers from across the company to address risks from all facets of operations.

A centralized risk dashboard will be implemented to monitor risks in real time, providing visibility into how each area is managing its risks in alignment with the company's overall strategy. Additionally, regular risk assessments will be conducted to update the risk profile, ensuring that both emerging threats and new business opportunities are addressed.

References:

1. NIST. (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity Framework. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

2. Jha, S. (2024, July 4). *NIST implementation tiers explained*. Sprinto. https://sprinto.com/blog/nist-implementation-tiers/

3. Jha, S. (2024, January 24). *NIST implementation tiers 101: All you need to know.* Sprinto. https://sprinto.com/blog/nist-implementation-tiers/#:~:text=Respond:,analysis%2C%20mitigation%2C%20and%20improvements.

4. Bresnahan, E. (2019, June 11). *Nist Cybersecurity Framework (CSF) core explained*. CyberSaint Security. https://www.cybersaint.io/blog/nist-cybersecurity-framework-core-explained

5. CrowdStrike. (2023, March 23). *What is Cyber Threat Intelligence? [beginner's guide]*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

6. Stouffer, K., Zimmerman, T., Tang, C., Pease, M., Lubell, J., Cichonski, J., & McCarthy, J. (2020). *Cybersecurity framework version 1. 1 manufacturing profile* (NIST Internal or Interagency Report (NISTIR) 8183 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8183r1

7. Morgan, L. (2023, August 7). *Enterprise risk management team: Roles and responsibilities*. CIO. https://www.techtarget.com/searchcio/feature/Enterprise-risk-management-team-Roles-and-responsibilities

8. Helixstorm. (2023, July 6). *Legacy System Alert: 8 Signs It’s Time to Modernize*. https://www.helixstorm.com/blog/9-signs-its-time-to-upgrade-your-outdated-infrastructure/#:~:text=8.%20High%20Maintenance%20Costs%20If%