MPCR 5661 Categorizing, Selecting, & Prioritizing Assets to Protect

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

Module 3: Hoya Inc. Project Group 3

MPCR-5661-101

Professor Sumera Baker

October 13, 2024

Abstract

The following assets for Hoyas Inc. are to be categorized, selected, and prioritized based on various criteria. As Hoyas Inc. specializes in manufacturing, the assets included are mapped with manufacturing requirements. In addition, severity and impact levels will be addressed in the categorization, selection, and prioritization process.

Controls for the assets will be incorporated as well that align with NIST Special Publication 800-53, Center for Internet Security (CIS), and the Payment Card Industry Data Security Standard (PCI DSS) . These controls will then assist in further categorizing, selecting, and prioritizing assets for Hoyas Inc.

Categorize

- **Manufacturing Assets:** Current assets that are deemed tangible assets. Considered at a level of moderate to high, manufacturing assets will require controls such as controlled maintenance (NIST, 2020). Controlled maintenance can approve maintenance activities for manufacturing equipment, sanitize equipment, and ensuring impacted equipment continues to function properly (NIST, 2020).

  Other controls for manufacturing assets include CIS Controls such as Maintenance, Monitoring, and Analysis of Audit Logs that can be aligned for moderate to high severity levels (CIS, n.d.a). As manufacturing assets are current assets, the CIS auditing controls can ensure logs from equipment are managed appropriately as well (CIS, n.d.a).

- **Information Resources:** Current assets that provide information and knowledge management within the organization, and are considered moderate. Controls may include CIS controls such as Data Recovery Capabilities where documentation is emphasized for system backups and recovery procedures (CIS, n.d.a). Data Recovery Capabilities are primarily used for industrial control systems that will utilize information resources in Hoyas Inc. (CIS, n.d.a).
- **Outsourced Assets:** Current and legacy assets that derive from external parties to Hoyas Inc and are considered moderate to high. Controls encompass malware defenses and email and web browser protections from CIS (CIS, n.d.a). Malware defenses can ensure that any external malware intrusions can be prevented (CIS, n.d.a). Regression testing is required for anti-malware solutions and are to be configured for reducing impact of false positives (CIS, n.d.a).

  Email and web browser protections protect separate networks, ensure email clients are outbound, and maintain system segmentation (CIS, n.d.a).
- **IT Assets:** Current assets related to the organization's IT systems and are considered moderate. Controls include continuous vulnerability management that aid IT systems, mitigation, and vulnerability scanning control (CIS, n.d.a).
- **Cloud Computing Assets:** Current assets related to the organization's data with cloud service providers, and is considered moderate to high. Controls for cloud environments can utilize foundational controls from CIS and tailored controls for services including IBM Cloud or AWS (CIS, n.d.b).

- **Technical Devices:** Older assets that the organization utilizes and are considered low to moderate. NIST controls such as authenticator management controls can manage authenticators in devices (NIST, 2020).
- **Legacy Computer/Network Systems:** Older assets that have end of life software and hardware which are considered highly vulnerable to exploitation. These older assets need to be secured and updated in order to be protected against more modern threats (Quinn, Souppaya, Cook, Scarfone, 2018) Legacy networks will have to be separated from the main production network due to the older software that is running on them and the vulnerabilities they inherit.
- **Security Operations Center (SOC):**

  The focal point of security operations and network defense for Hoyas Inc (NIST, 2020). The SOC provides continuous monitoring of Hoyas Inc.'s networks and systems and are alerted when there is nefarious activity happening (NIST, 2020). This is a pivotal function of Hoyas Inc. in order to be aware of the threats that are targeting the organization on a continuous basis.
- **Sales and Management:** Current assets that pertain to sales and management operations, and are considered moderate to high. Sales and management will require controls for resolving privilege escalation, data compression, and weakened encryption (NSA, 2018).
- **Online Payment Methods:**

  This is considered a high level asset as it processes customer transactions and handles data such as credit card information. Controls for this system need to ensure that there is a minimized chance for data leaks of customer data. Hoyas Inc. needs to be PCI DSS compliant as they deal with credit card data. All entities that are handling this type of information need to be PCI DSS compliant (PCI Security Standards Council, 2018)

- **Enterprise Goals:** Current assets that are directly tied to the mission of the organization, and are considered high. Enterprise goals will require controls to prevent lateral movement, account enumeration, and information gathering (NSA, 2018).
- **Behavioral Analytics for Threat Detection**:

  Add a control for behavioral analytics to monitor operational systems and detect deviations from normal behavior. This can identify insider threats or potential cyber intrusions targeting the manufacturing environment by recognizing unusual patterns in system activity (Nist, 2020).
- **Network Segmentation for Manufacturing and Legacy Systems:**

  Implement network segmentation to isolate manufacturing systems, especially older or legacy systems, from the main IT infrastructure. This minimizes the risk of lateral movement by attackers from less secure to more critical systems (NIST, 2020; NIST, 2015).
- **SIEM Integration for Real-time Monitoring:**

  Include the use of Security Information and Event Management (SIEM) systems for aggregating and analyzing logs from manufacturing assets. SIEM can provide real-time monitoring, detect suspicious activities, and alert the security team to any potential threats (NIST, 2020; NIST, 2011).

Select

- **Manufacturing Assets:** Manufacturing assets are selected due to Hoyas Inc. focusing on manufacturing. As manufacturing assets involve equipment and machinery for Hoyas Inc. operations, they are critical assets for maintaining product development and consistency.
- **Monetary Assets:** Monetary assets are chosen due to their critical nature involving currency. As monetary assets are a liability for the organization and can impact how the organization functions, these assets are selected.
- **IT Assets:** IT assets are selected as they pertain to hardware, software, and information management within the organization (Atlassian, n.d.). As IT assets are mission-critical and aid in understanding total cost of ownership, these assets are chosen (Atlassian, n.d.).
- **Risk Management Framework:** Assets in the risk management framework are selected due to how the risk management framework is outdated. The assets in the risk management framework may be deprecated as well, and may require upgrading to reduce vulnerabilities.

Prioritize

- **Risk Management Framework:**

The risk management framework is to be prioritized first as it requires updating. The NIST Cybersecurity Framework (CSF) will be incorporated into Hoyas Inc.'s business operations to strengthen the overall IT infrastructure and reduce current vulnerabilities stemming from the outdated Risk Management Framework (RMF), which was last updated in 2019. We believe integrating the NIST Cybersecurity Framework (CSF) into Hoyas Inc.'s RMF will provide a more adaptable, proactive approach to identifying and mitigating cybersecurity risks. The NIST

CSF's five key functions—Identify, Protect, Detect, Respond, and Recover—should be embedded in the RMF to ensure continuous improvement and resilience (NIST, 2020).

Incorporation of NIST CSF:

- **Identify:** Prioritize risk identification for key assets (manufacturing, IT systems, cloud services, legacy systems) based on their criticality to the business. Establish an asset inventory as a baseline for all risk management activities.
- **Protect:** Implement proactive protections (e.g., encryption, network segmentation) for sensitive assets, especially those supporting government contracts and payment systems.
- **Detect:** Strengthen detection capabilities through real-time monitoring (SIEM systems) and behavioral analytics to identify threats quickly.
- **Respond:** Develop tailored incident response plans for different asset categories, including manufacturing systems, IT environments, and cloud assets.
- **Recover:** Include disaster recovery and business continuity planning for critical operations, ensuring minimal downtime and financial losses during a cyber incident.
- **Manufacturing Assets:** Manufacturing assets are prioritized as the organization's operations are in manufacturing. Assets may include equipment, processes, and frameworks that handle operations in this domain.
- **Monetary Assets:**

Monetary Assets such as the online payment system that Hoyas Inc. utilizes is a top priority in terms of compliance and protecting the confidentiality, integrity and availability of the data. As mentioned previously, since Hoyas Inc. uses credit card payment systems for their online transitions, they have to be PCI DSS compliant which comes with its own set of controls to ensure those layers of protection are there for customer's financial data (PCI Security Standards Council, 2018). Requirements and controls to be PCI DSS compliant include, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, etc… (PCI Security Standards Council, 2018).

If there were customer data leaks or a PCI DSS audit discovers that controls and protections were not implemented and Hoyas Inc. was noncompliant, then major fines could be served to the organization (varying from $5,000 to $100,000, depending on the state of noncompliance and if there was a data breach) (IXOPAY, 2024). Other damages to Hoyas Inc. could be damaged reputation for having customers' data leaked, revenue losses, and the inability to process credit cards as a payment method (IXOPAY, 2024). With this, it is a top priority for Hoyas Inc. to ensure that proper controls and protections are set in place with regards to protecting their financial systems from exploitation and more importantly protecting customer data such as credit card information.

- **IT Assets:**

IT Assets are a core function of Hoyas Inc.'s operations. They are a high level of priority for the organization to protect against threats and exploits. Based off of NIST SP 800-53, Incident Handling control IR-4, it is imperative that Hoya's Inc maintains their security operation center to be able to proactively and reactively respond to threats and ongoing incidents that might occur on the organization's IT assets and networks (NIST, 2020). A top priority for Hoya Inc. is to secure and update their legacy system inventory. Legacy systems inherently come with copious amounts of vulnerabilities due to the systems running outdated hardware and software that is no longer supported by the vendor (McCarty, n.d.). Other issues with legacy systems that come up are the inability to communicate with newer technologies. As newer technologies developed and were implemented, the older systems were never designed to integrate with newer models hence why they stay in their own enclave (McCarty, n.d.).

All systems rely on IT systems for continuous operations, that goes for monetary systems and manufacturing systems. Both rely on the availability of IT systems to be up and running without any outages and if there are then having a contingency plan in place to ensure mission essential functions are not disrupted (NIST, 2020). Contingency controls from NIST SP 800-53 (CP-2) lays out the need for an organization to be able to have recovery and continuity objectives mapped out in case there is an incident where high level impact IT assets are affected (NIST, 2020). Members of Hoyas Inc. need to be aware of the contingency plans if something goes wrong and who is responsible for what in terms of ensuring those critical IT assets are still operational (NIST, 2020).

References

Atlassian. (n.d.). *ITAM: The ultimate guide to IT asset management*. Atlassian. Retrieved October 11, 2024, from https://www.atlassian.com/itsm/it-asset-management

CIS. (n.d.). *Cis controls^{TM} implementation guide for industrial control systems*. CIS. Retrieved October 8, 2024, from https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

CIS. (n.d.). *Blog | foundational cloud security with cis benchmarks*. CIS. Retrieved October 9, 2024, from https://www.cisecurity.org/blog/foundational-cloud-security-with-cis-benchmarks/

NIST. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

NSA. (2018). *NSA/CSS technical cyber threat framework v2*. NSA. https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf

Quinn, S., Souppaya, M., Cook, M., & Scarfone, K. (2018, February). NIST Special Publication 800-70 Revision 4: National Checklist Program for IT Products – Guidelines for Checklist Users and Developers. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

PCI Security Standards Council. (2018b, July). PCI DSS Quick Reference Guide. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

McCarty, D. (n.d.). *What are the biggest problems with legacy software?*. Gavant Software. https://www.gavant.com/library/what-are-the-biggest-problems-with-legacy-software

IXOPAY. (2024, July 1). 5 consequences of PCI Non-Compliance. https://www.ixopay.com/en/news/5-consequences-of-pci-noncompliance

Security and privacy controls for information systems and organizations. (2020d). https://doi.org/10.6028/nist.sp.800-53r5

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2015). *Guide to Industrial Control Systems (ICS) Security*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

JOINT TASK FORCE, Ross, W. L., Jr., & Copan, W. (2020). *NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for information systems and organizations*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf