Humberto Gonzalez

November 17, 2024

Categorize a Company Using a Security Maturity Model

You will use the three images in the resources section below entitled "Simple Maturity Model Graphic," "CMMC Domains," and the "Maturity Rating Levels" for this task. You will want to download these items.

Here are the steps for this deliverable:

a. Create a spreadsheet similar to the "Simple Maturity Model Graphic" image. You will not need the business unit column since the rating is based on the entire company versus each business unit (typically for larger organizations). On the top row, you will list all 17 domains from the "CMMC Domains" image.

b. Using the spreadsheet and information above, and the information for SnowBe company, rate all 17 domains using the levels documented in the "Maturity Rating Levels" image. Use similar colors for the rating as the "Simple Maturity Model Graphic" image. See the deliverables section below on how to deliver the answer to this question.

c. Using 1b above, prioritize the order of all 17 domains starting from the most important domain to the last domain that would be given attention. In 100 words or more, document why you prioritized the domains in the order you did. See the deliverables section below on how to deliver the answers for this task.

Prioritization of the 17 Domains

1. System and Communications Protection (SC) - Critical to ensuring secure data exchange across systems, especially for an e-commerce platform like SnowBe.
2. System and Information Integrity (SI) - Necessary for maintaining data integrity, identifying malware, and patching vulnerabilities.
3. Incident Response (IR) - Rapid response to breaches is vital for minimizing potential damage and regulatory impact.
4. Access Control (AC) - Controls to restrict unauthorized access are essential for data and system security.
5. Risk Management (RM) - Identifying and mitigating risks ensure proactive security measures.
6. Recovery (RE) - Key to restoring operations after incidents or disasters, minimizing downtime.
7. Configuration Management (CM) - Prevents misconfigurations that could lead to vulnerabilities.
8. Identification and Authentication (IA) - Essential for verifying user identity and ensuring secure logins.
9. Audit and Accountability (AU) - Enables tracking of activities, critical for compliance and forensic investigations.

10. Awareness and Training (AT) - Educates employees to recognize and respond to threats effectively.
11. Situational Awareness (SA) - Helps monitor and analyze threats, staying ahead of potential issues.
12. Media Protection (MP) - Safeguards sensitive data stored on physical or digital media.
13. Personnel Security (PS) - Ensures that employees with access to sensitive data are vetted and monitored.
14. Physical Protection (PE) - Protects physical infrastructure from unauthorized access.
15. Asset Management (AM) - Tracks and secures organizational assets.
16. Security Assessment (CA) - Evaluates security measures for compliance and effectiveness.
17. Maintenance (MA) - Ensures systems remain operational and updated, though less critical compared to others.

The prioritizing of the 17 domains demonstrates SnowBe's reliance on secure online operations, as well as the significance of securing sensitive client data. System and Communications Protection (SC) and System and Information Integrity (SI) are key priority because they provide safe data interchange, malware detection, and the patching of critical vulnerabilities in the e-commerce platform. Incident response (IR) follows closely, as a quick breach reaction reduces damage. Access Control (AC) and Risk Management (RM) are critical for protecting against illegal access and managing vulnerabilities. Recovery (RE) enables business continuity following a disaster, while Configuration Management (CM) prevents misconfigurations. Identification and Authentication (IA) safeguards user access, while Audit and Accountability (AU) allows for activity tracking for compliance.

Awareness and Training (AT) prepares personnel to spot threats, whereas Situational Awareness (SA) assists in monitoring new risks. Media Protection (MP) protects physical or digital material, and Personnel Security (PS) assures that trusted personnel manage sensitive assets. Physical Protection (PE) defends infrastructure, while Asset Management (AM) monitors and safeguards organizational resources. Security Assessment (CA) examines current security measures, while Maintenance (MA) keeps systems working. This directive targets technical threats initially, then gradually strengthens other areas to ensure long-term security maturity.

2. You will use the CMMC spreadsheet for this task. The spreadsheet is in the resources section, under "CMMC Model and Assessment Guides."

Here are the steps for this deliverable:

a. Using the prioritized data from 1c above, select the domain names for priorities 1, 3, 5 & 7 (you should have a domain name for each number). See the deliverables section below on how to deliver the answers for this task.

1. System and Communications Protection (SC)

3. Incident Response (IR)

5. Risk Management (RM)

7. Configuration Management (CM)

b. Using the domain list from 2a and the CMMC spreadsheet, look for the matching tab and select the capability (see the capability column) with the most levels filled in. You will do this for each domain in 2a. See the deliverables section below on how to deliver the answers for this task.

1. C038- Define security requirements for systems and communications.

3. C018- Develop and implement a response to a declared incident.

5. C031- Identify and evaluate risk.

7. C014- Perform configuration and change management.

c. Document the acronym for the domain, the level number, and the practice number that matches the current state for each domain. If the current state is not defined, select the capability that is the next best step. You will do this for each domain in 2a. See the deliverables section below on how to deliver the answers for this task.

1. SC- Level 3

Practice number

SC.3.177- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

SC.3.180- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

SC.3.181- Separate user functionality from system management functionality.

SC.3.182- Prevent unauthorized and unintended information transfer via shared system resources.

SC.3.183- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

SC.3.184- Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

SC.3.185- Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

SC.3.186- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

SC.3.187- Establish and manage cryptographic keys for cryptography employed in organizational systems.

SC.3.188- Control and monitor the use of mobile code.

SC.3.189- Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

SC.3.190- Protect the authenticity of communications sessions.

SC.3.191- Protect the confidentiality of CUI at rest.

3. IR- Level 1

Practice number

IR.2.096- Develop and implement responses to declared incidents according to pre-defined procedures.

5. RM- Level 3

Practice number

RM.3.144- Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

7. CM- Level 2

Practice number

CM.2.064- Establish and enforce security configuration settings for information technology products employed in organizational systems.

CM.2.065- Track, review, approve, or disapprove, and log changes to organizational systems.

CM.2.066- Analyze the security impact of changes prior to implementation.

d. Using the information from 2c, describe in 100 words or more what you would do as the next best step to meet the documented practice item. You will do this for each domain in 2a. See the deliverables section below on how to deliver the answers for this task.

To address the 13 practices for SC, the first step is to use FIPS-validated cryptographic techniques like TLS 1.2/1.3 to secure CUI during transmission (SC.3.177). Establishing solid architectural designs and engineering concepts is crucial for ensuring effective information security across systems (SC3.180). User functionality must be separated from administrative activities using role-based access controls (SC.3.181), while access control lists (ACLs) and resource isolation can avoid inadvertent information transfers (SC.3.182). A deny-all, permit-by-exception policy should be applied to network traffic through properly configured firewalls and routers (SC.3.183), and split tunneling should be turned off on distant devices (SC.3.184).

Protecting data in transit and at rest (SC.3.185 and SC.3.191) with strong encryption, such as AES-256, is critical. In order to comply with SC.3.186, idle network sessions should be

terminated automatically. Cryptographic key management (SC.3.187) requires safe systems for generation, storage, and rotation. Endpoint tools should be used to monitor and limit mobile code (SC.3.188), and secure VoIP protocols should be utilized for communication (SC.3.189). Finally, the communication authenticity and mutual authentication protocols (SC.3.190) should be implemented to prevent session spoofing. These activities will fully fulfill the security requirements for System and Communications Protection at Level 3.

To meet IR practice requirement I will create a detailed incident response strategy that complies with IR.2.096. Outline the particular methods for identifying, documenting, and responding to security incidents. Train employees on issue handling and escalation procedures. Establish communication channels for event reporting and adhere to post-incident procedures, such as root cause analysis and lessons learned. Logging and monitoring tools can help in early threat detection.

To achieve RM.3.144 in the RM domain, I will undertake a rigorous risk assessment of SnowBe's AWS-hosted systems and on-premises servers. Define risk categories and criteria for measurement. Engage stakeholders in identifying high-priority issues and developing risk mitigation solutions. Document the outcomes in a centralized repository, and update assessments on a regular basis. I will utilize tools that can aid with the process.

For CM I will Implement baseline configurations for all systems as described in CM.2.064 to ensure consistency across IT assets. Use configuration management tools to ensure compliance. For CM.2.065, use version control systems to manage and document all system changes, and keep audit trail logs. Before implementing modifications to production systems, evaluate the security implications (CM.2.066) by emulating configurations in test environments. Conduct regular reviews to detect and rectify discrepancies.

I should be able to utilize the tool RMM for the SC and CM domains particularly, due to its ability to monitor, enforce, and report on system configurations and compliance.

3. Describe in 100 words or more the most important item you learned while working on the CMMC task for this week (item 2 above).

The most important lesson I learnt while working on the CMMC task was the need of prioritizing and adjusting security controls to an organization's unique needs and maturity level. By examining domains such as System and Communications Protection (SC), Incident Response (IR), Risk Management (RM), and Configuration Management (CM), I gained insight into how each practice contributes to overall security. Additionally, I learned how to use the CMMC framework and its rating levels to assess and determine SnowBe's maturity levels based on their current state. The assignment emphasized the importance of mapping practices to maturity levels and identifying gaps, allowing for strategic planning to address both current dangers and long-term goals.

In conclusion, picking and prioritizing domains can be a difficult undertaking because it entails balancing the urgency of obvious gaps with the relevance of core improvements. This approach taught me the value of using organized frameworks such as CMMC to make educated judgments and accurately assess an organization's security postures.