3.5 – ASSIGNMENT: CATEGORIZE A COMPANY USING A SECURITY MATURITY MODEL

Joan V. Rodriguez Collazo
CYB359-O Section 01
Term C202302

SNOWBE ONLINE CASE STUDY UPDATE

Karen asked Brad about the next best steps to increase SnowBe's technical maturity without any financial commitment. Brad requested to start with an initial review of the IT environment. He decided to use the Simple Maturity Model Assessment Tool to quickly get an idea of security gaps, to gather the next best steps for SnowBe's technical maturity direction, and to be able to quote the work.

DELIVERABLE INSTRUCTIONS

Please answer each question separately. Elaborate on your answers to demonstrate your depth of knowledge for this week's topics. You will have to make strategic and tactical decisions to ensure that SnowBe is headed towards better technical and security maturity. You will be Brad for the below tasks.

DELIVERABLE 1

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.

Domain Name	AC Access Control	AM Asset Management	AU Audit & Accountability	AT Awareness & Training	CM Configuration Management	IA Identification & Authentication	IR Incident Response	MA Maintenance	MP Media Protection	PS Personnel Security	PE Physical Protection	RE Recovery	RM Risk Management	CA Security Assessment	SA Situational Awareness	SC System & Communications Protection	SI System & Information Integrity
Maturity Rating																	

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.

Key:

Level 1	IT Processes are unorganized and may be unstructured. Success is likely to depend on individual efforts and is NOT considered to be repeatable or scalable.
Level 2	IT efforts are at a repeatable level. Basic project management techniques are established, and successes can be repeated.
Level 3	IT efforts have greater attention to documentation, standardization & maintenance.
Level 4	Monitors & controls its own IT processes through data colelction and analysis.
Level 5	Optimizing level where IT processes are constantly being improved through monitoring feedback from existing processes and introducing new processes.

Domain Name	AC Access Control	AM Asset Management	AU Audit & Accountability	AT Awareness & Training	CM Configuration Management	IA Identification & Authentication	IR Incident Response	MA Maintenance	MP Media Protection	PS Personnel Security	PE Physical Protection	RE Recovery	RM Risk Management	CA Security Assessment	SA Situational Awareness	SC System & Communications Protection	SI System & Information Integrity
Maturity Rating	1	2	1	1	2	1	3	3	2	1	2	3	2	2	3	2	1

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.

1. Access Control
2. Identification and Authentication
3. Media Protection
4. Personnel Security
5. Physical Protection
6. System Communications Protection
7. System & Information Integrity
8. Incident Response
9. Recovery
10. Awareness & Training
11. Security Assessment
12. Situational Awareness
13. Risk Management
14. Asset Management
15. Configuration Management
16. Maintenance
17. Audit & Accountability

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.

I prioritized the domains in this order because the first half of the list contains the building blocks necessary for cybersecurity. I put access control at the very top of the list because one of the most important and simplest things an organization can do is limit access to information by user type to ensure that only people who need it can see it. This ties into Identification and Authentication because now that access is only granted to specific users, we need to ensure they are whom they say they are. Next, we must protect media and limit physical access to information systems to only authorized individuals. The next thing on my list of priorities is to control internal and external communications, so that information and data travel safely. The integrity piece is crucial because we need to be able to identify any flaws or threats quickly. We move on to incident response and recovery.

The second half of my list focuses on awareness, training, assessments, risk, asset, configuration management, maintenance, and audit and accountability. I listed these all toward the back end because they are ongoing processes that are constantly evolving.

DELIVERABLE 2

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 – Access Control
3 – Media Protection
5 – Physical Protection
7 – System & Information Integrity

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 – Access Control: C002 – Control Internal System Access
3 – Media Protection: C023 – Protect and control media
5 – Physical Protection: C028 – Limit Physical Access
7 – System & Information Integrity: C042 - Perform Network and System Monitoring

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.

Priority Number	1	3	5	7
Domain Name	Access Control	Media Protection	Physical Protection	System & Information Integrity
Acronym	AC	MP	PE	SI
Level Number	Level 2 (L2)	Level 2 (L2)	Level 1 (L1)	Level 2 (L2)
Practice Number	AC.2.007	MP.2.120	PE.1.131	SI.2.216

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.

I decided to base my next best steps on the background of the case study. Brad was recently hired to implement a few different items. That list contained things such as ensuring that all users had access only to the data needed to do their jobs. For this reason, I selected AC.2.007 for Access Control, related to the principle of least privilege. The process was already documented, so the next logical best step is to ensure that all users are treated the same and that the principle of least privilege is applied to every user. I selected MP.2.120 for Media Protection because it is related to that same type of thing, limiting access to authorized users. Once that is handled, the next logical step for me would be to control and, in some cases, prohibit the use of portable or removable devices. For physical protection, I selected PE.1.131, and the next step I would implement is only to allow authorized users to enter secure areas or escort them. Physical access should always be logged. Lastly, for System and Information Integrity, I chose SI.2.216, and the next step to monitoring the system traffic would be to protect access entry and exit points from spam.

DELIVERABLE 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).

  As I prioritized my list, I thought about not only SnowBe but also how this could positively impact any organization. The most important thing I learned is that many of these functions are the foundation for others. Identifying where you are now and where you want to be is critical in establishing a plan for cybersecurity success. Protecting each part, system, and component is critical for the big cybersecurity picture, and CMMS helps establish a pathway for continuous improvements for an organization like SnowBe. The end goal for SnowBe and for all organizations looking to obtain a CMMC certification is maximizing cybersecurity resilience.

REFERENCES

- **CMMC_ModelMain_V1.02_20200318.pdf**
- **CMMC_AG_Lvl1_20201208_editable.pdf**
- **CMMC_AG_Lvl3_20201208_editable.pdf**
- **CMMC_Model_V1.02_20200318.xlsx**
- **CMMCv1.0AssessmentTool(2020.02Public).xlsx**
- **Index assistant guide for CMMC practices**
- **US-CERT – Threat Intelligence**