Assignment 3.5
Categorize a Company Using a Security Maturity Model

Donald Doss
Gabriel Hernandez
Michael Kohronas
Xavier Rivera Maysonet

Michael Vazquez

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.

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

Risk management is the least focused domain for SnowBe so it was best to put it as highest priority on the list. Situational Awareness is also lacking as they were laid back at the start and never implemented more unique features for security. Configuration management is poor as there were many servers, desktops, and laptops without restrictions. Incident response is lacking with no plan as to respond in the event of an attack happening. Access controls are not all there, allowing users to have access to documents they should not have. Personnel security is limited and SnowBe showed that it had no way of determining valid employees. Physical protection at SnowBe seems to be missing, bringing it high in priority as well. Awareness and training were not completely minimal but required further enhancements considering the number of employees at the business and the number of systems running in the building that require attention. Maintenance was an issue but was resolved to an extent, so it was able to be less of a priority due to implementing firewall and active directories. Security assessments were handled because of Karen being assigned to work with it. Systems and communication protection were improved through active directory, firewall, antivirus software, and backups for the servers, also making it a low priority. System and information integrity were improved through RMM. Media protection was displayed through SnowBes RMM as well as their active directory keeping confidential data secure and monitored. Audit and accountability were shown through SnowBe’s initiative to get assistance for their systems, so no priority is needed on that. Identification and Authentication were improved with the addition of Active directory and no longer need high priority. Finally, recovery was well implemented enough to where SnowBe can bring back server software through their backups for all desktops, laptops, and servers so that also was at minimal priority.

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).

1.Risk Management

3.Configuration Management

5.Access Control

7.Physical Protection

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.

Risk Management (RM)

Level - 2

Practice numbers

RM.2.141

RM.2.142

RM.2.143

Configuration Management (CM)

Level - 2

Practice numbers

CM.2.061

CM.2.062

CM.2.063

CM.2.064

CM.2.065

CM.2.066

Access Control (AC)

Level - 1

Practice numbers

AC.1.001

AC.1.002

AC.1.003

AC.1.004

Physical Protection (PE)

Level - 1

Practice numbers

PE.1.131

PE.1.132

PE.1.133

PE.1.134

d. Using the information, describe in 100 words or more what you would do as the next best step to meet the documented practice item.

For risk management, to meet the next steps of the practice SnowBe needs to assess risk from their current systems. This means looking at desktops, laptops, servers, users, assets and anything else that could be a risk to the company. Mitigation plans should be implemented to lessen the chances of potential breaches within SnowBe that may come from physical locations (i.e. server rooms) or through the network. SnowBe should also consider managing non-vendor supported products and restrict them to mitigate potential vulnerabilities as those cannot always be trusted. Improving and pushing updates to software and applications as well as utilizing firewalls and anti-virus software would also allow SnowBe to reach the next level and prevent future risks from appearing.

For configuration management, since SnowBe seems to lack physical restrictions for their systems they should consider documenting and approving physical and logical access restrictions towards those systems. This is to better manage what can be done with them when updates or hardware changes are needed and who is approved to do so by the higher ups in the company. Restricting and preventing the use of nonessential programs, functions, ports, protocols and services are also something that can be done to improve configuration management and help SnowBe manage their devices. Tracking changes made to SnowBes system and analyzing their impact before implementing would also help SnowBe ensure changes are beneficial and security is tight leaving no room for vulnerabilities when additional security changes are implemented.

For access control, it would be best to start limiting the use of portable storage devices on external systems like laptops and desktops and employ the principle of least privilege. This will ensure users within the company only are able to access SnowBe site data and no other outside users are able to have access. Limiting unsuccessful logon attempts can deter brute force attacks and protect all devices under SnowBes network including off site servers. The use of session locking when users are inactive will prevent the access and viewing of data through pattern hiding displays ensuring employees that should not have access see anything they shouldn’t or if there is a potential breach in the system the user will have to log in again in order to have access to the device again.

For physical protection, the next best steps are a bit simpler but can have a more complicated approach to how these things can be implemented. SnowBe should invest in physical security for their physical buildings housing servers as well as housing other important technology laptops, desktops, network, ATMs, etc. This means establishing cameras in specific parts of the building, bringing in security personnel for the building, and maybe even keycards that allow employees into specific areas of the building but only if they have the required keycards. Other methods like locking devices or servers' rooms can also prevent unauthorized access but will be closely monitored when IT personnel are making changes with these devices to ensure no one else has access to them when they are exposed throughout the day.