CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #3 - Option A

Team: Project Team 11
Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the four options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
Your text provides an overview of the Payment Card Industry Data Security Standard (PCI DSS) v. 3.0 but the latest standard is version 3.2.1 (May 2018). Review the attached Quick Reference Guide for v. 3.2.1 – the latest available (retrieved from https://www.pcisecuritystandards.org/). There are still six overall goals and twelve requirements but version 3.2 expands on most of these areas. As you review the mini-case below, make note of relevant specific requirements such as 1.2, 1.3, etc.

Meager Media is a small- to medium-sized business that is involved in the sale of used books, CDs/DVDs, and computer games. Meager Media has stores in several cities across the U.S. and is planning to bring its inventory online. The company will need to support a credit card transaction processing and e-commerce Web site.

Write a summary report detailing what Meager Media must do when setting up its Web site to maintain compliance with PCI DSS as it transitions from a pure brick and mortar store to having an online presence. Focus on requirements that will be *new or different* because of the new e-commerce Web site. *(25 points)*

Answer:
The following text was located in a table taken from this document PCI DSS Quick Reference Guide :

Build and Maintain a Secure Network and Systems
1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

Merger Media is a brick and mortar store that sells used books, CDs/DVDs, and computer games. They want to move their business to an online platform. We know that their site will be targeted by hackers, because they only need cardholder's information to access their bank account. Merger Media needs to follow these six goals and twelve requirements to effectively serve their customers from an online platform. Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1 is the latest version available to the public.

Merger Media must Build and maintain a secure network and system. Two requirements can make this goal possible:

- Install and maintain a firewall configuration to protect cardholder data
    - The firewall will protect the cardholder's information from being accessed from outside sites by monitoring traffic that travels inside and outside of the website. Traffic that comes from untrusted networks will be denied access (1.2)
    - To summarize the firewall being implemented will protect cardholder's information and company information.
- Do not use vendor-supplied defaults for system passwords and other security parameters
    - The password from vendor-suppliers will be given to company with default passwords in place follow requirement 2.3 "Using strong cryptography, encrypt all non-console administrative access", when creating a new password
    - Strong passwords will protect Merger Media's new site from Hackers with ill intent.

Merger Media must Protect cardholders Data. Two requirements can make this goal possible:

- Protect stored cardholder data
    - Cardholder data should not be stored unless it is absolutely necessary.
    - Requirement 3.1 and 3.2 state that the amount of cardholder data must be limited, that sensitive data must not be stored for confidentiality purposes.
- Encrypt transmission of cardholder data across open, public networks
    - "Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong

encryption for authentication and transmission." Requirement 4.1 stresses the importance of encryption on data when cardholders are accessing the site from a public network.

Merger Media must Maintain a Vulnerability Management Program. Two requirements can make this goal possible:

- Protect all systems against malware and regularly update antivirus software or programs
    - Requirement 5.1 suggests to deploy antivirus software and requirement 5.2 stresses the importance of keeping the software updated.
    - "Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties." Requirement 5.4 is in place to remind the company to be aware of the procedures set in place if a security breach happens.
    - Vulnerability management plans are set in place for the security of the company. Company personnel must be aware, because if they aren't company and cardholder data may be lost or stolen.
- Develop and maintain secure systems and applications
    - This requirement can be summarized as assessing assets potential risk (6.1) and implementing the software that can protect these assets internally and externally (6.2 & 6.3).
    - security system software will further protect company and cardholder data.

Merger Media must Implement Strong Access Control Measures. Three requirements can make this goal possible:

- Restrict access to cardholder data by business need to know
    - "To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities." The data should only be accessed by those who need access to it, and those who don't will be denied. (7.1)
    - "Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed." Requirement 7.2 suggests the implementation of controls that will restrict access of everyone unless they are of the specified few that need access.
- Identify and authenticate access to system components
    - To summarize, everyone that has access to the system, be it company personnel or cardholders, must be able to login to identify themselves.
    - This method makes it easier for the system to accept or reject requested access based on the user's credentials.
- Restrict physical access to cardholder data
    - " "Onsite personnel" are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration – usually up to one day. "Media" is all paper and electronic media containing cardholder data." These people need to be able to access the site, but they should not be able to access cardholder's data.

Merger Media must Regularly Monitor and Test Networks. Two requirements can make this goal possible:

- Track and monitor all access to network resources and cardholder data
    - Requirements 10.1 -10.5 deal with the implementation of audits that will be performed on the system.
    - A log should be created to monitor who accesses network resources. This log will be periodically reviewed.
- Regularly test security systems and processes
    - Security systems must be periodically tested, and procedures must be set in place for the tests that are going to be run.
    - Each system is vulnerable to potential attacks. The job of vulnerability tests is to identify the vulnerability and decide whether to accept the risk or to put more security measures in place for the benefit of the system.

Finally, Merger Media must Regularly Monitor and Test Networks. One requirements can make this goal possible:

- Maintain a policy that addresses information security for all personnel
    - A security policy must be created for addressing all security issues. Once a formal policy is created dealing with security issues will be easily resolved, because a detailed plan is put in place.
    - Meager Media should get compliance of Cyber Maturity Model Compliance (C.M.M.C), ISO 27001 and GDPR, to get enhanced security services.

Work Cited

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. (n.d.). Retrieved June 17, 2020, from https://www.pcisecuritystandards.org/