CIS 481 – Intro to Information Security

CLASS EXERCISE # 3 – Option A

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 – 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 pts.)

Meager Media will have to comply with PCI DSS standards when implementing credit card payment options. The six goals of PCI will apply to Meager Media; Build and Maintain a Secure Network, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks, and Maintain an Information Security Policy.

1. For building and maintaining a secure network, Meager Media will need to establish and implement a firewall. Included in this, is firewall and router configurations to restrict connections between untrusted networks and system components in the card holder data environment. They will also need to prohibit direct public access between the internet and any system component in the cardholder data environment. Finally, they will need to install personal firewall software or equivalent functionality on any portable computing devices that connect to the internet when outside the network.
2. For protecting cardholder data, storage must be kept to a minimum by implementing data retention and disposal policies. Storage of sensitive authentication data is prohibited, even if it is encrypted. The PAN must be masked, first six or last four digits can be displayed. Along with this, PAN should be rendered unreadable anywhere it is stored. Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse. Use Strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks. Finally, they must ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.
3. When maintaining vulnerability management program, Meager Media must deploy anti-virus software on all systems commonly affected by malicious software. They must ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. They need to ensure that all anti-virus mechanisms are kept current, perform periodic scans, and generate audit logs which are retained. Meager

Media will need to establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities. They will need to ensure that all system components and software are protected from known vulnerabilities. Following change control processes and procedures for all system components is critical. Finally, they will need to ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

4. When it comes to Implementing Strong Access Control Measures, Meager Media must limit access to system components and cardholder data to only individuals who require access to that information for their job. They will need to ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. They must also define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components. There needs to be a unique ID associated with each customer. Generic IDs and shared user IDs are strictly prohibited. Only database administrators are allowed to access cardholder data. Included within the access controls are physical controls. Meager Media will need to use appropriate facility entry controls. Develop procedures to easily distinguish between onsite personnel and visitors. Going along with this, they will need to implement procedures to identify and authorize visitors. All media and data storage need to be physically protected and monitored at all times. Finally, all of this information needs to be documented, in use, and known to all affected parties.
5. Monitoring and testing networks will include implementing audit trails to link all access to system components to each individual user. Certain entries must be tracked in the audit trails, these include:
    - User identification
    - Type of event
    - Date and time
    - Success or failure indication
    - Origination of event
    - Identity or name of affected data, system component, or resource

   These logs need to be secured so that they cannot be altered. The logs should also be reviewed for anomalies and suspicious activity. For testing purposes, processes need to be implemented to test for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Scans need to be run on internal and external networks to look for vulnerabilities in the networks. Finally, intrusion detection needs to be in place to detect or prevent intrusions to the network.
6. Finally, for maintaining an information security policy, Meager Media will need to establish, publish, maintain, and disseminate a security policy. They will also need to implement a risk-assessment process that is performed at least annually, identifies critical assets, and results in formal, documented analysis of risk. Meager Media will need to develop usage policies for critical technologies and define proper use of these technologies. Also, security policy about information needs to be clearly defined for all personnel. Individuals need to be assigned information security management. Finally, an implementation of an incident response plan is vital.

As can be seen, Meager Media will need to implement a variety of means to secure the information of their card payment holder.

Source: information used here comes from PCI security standards.