Tyreon Love

Cybersecurity Fundamentals

4/7/2023

Research Project

I have reviewed the comprehensive report on the company's cybersecurity posture. The assessment found that the company lacked basic security policies, failed to comply with information privacy laws and regulations, and had no standard procedure for accepting payments in accordance with the Payment Card Industry Data Security Standard (PCI DSS). Also, the assessment revealed that the organization lacked a risk register to monitor, track and calculate risks associated with assets.In response to these findings, this paper proposes security improvements for Altamaha Tech to enhance its cybersecurity health..This report recommends the implementation of policies, procedures, and strategies to address the identified security issues. These policies and procedures include the development of an Acceptable Use Policy (AUP), Mobile Device Management (MDM) policy, Personally Identifiable Information (PII) policy, and a comprehensive PCI DSS guideline. This paper will also propose the implementation of a backup strategy, continuous security monitoring policies, training and continuing education policies, and a continuity of operations plan. To determine threats and vulnerabilities, Altamaha Tech should conduct a comprehensive risk assessment. This assessment should identify and evaluate the assets, threats, vulnerabilities, and potential impacts of risks to the company's information systems. The company should utilize a combination of assessment techniques such as vulnerability scanning, penetration testing, and risk analysis.

Physical security threats and vulnerabilities refer to threats that are external to an organization's information systems. These threats may include natural disasters, unauthorized

access to facilities, theft, and damage to equipment. Altamaha Tech should implement physical security controls such as access controls, surveillance cameras, and secure storage for sensitive data.

Technical security threats and vulnerabilities are a significant concern for any organization that stores, processes, or transmits sensitive data. These types of threats are often internal and can originate from employees, contractors, or other individuals with access to the company's information systems. The consequences of a technical security breach can be severe, including data theft, financial loss, and damage to the company's reputation To mitigate technical security threats and vulnerabilities, Altamaha Tech should implement logical security controls. These controls are designed to protect the company's information systems from unauthorized access, manipulation, or destruction. Some common logical security controls include firewalls, intrusion detection and prevention systems (IDPS), and security information and event management (SIEM) systems.

Altamaha Tech should develop a comprehensive AUP that outlines the acceptable use of company devices, internet usage, and data security policies. The AUP should clearly define the acceptable use of company-owned devices, such as laptops, desktops, and mobile phones. It should specify that the devices are the property of the company and should be used only for work-related purposes. The policy should also include guidelines for the appropriate use of personal devices when accessing company information systems The AUP should also provide clear guidelines for internet usage. It should outline which websites and online activities are acceptable and which are not. The policy should prohibit employees from accessing inappropriate content, downloading unapproved software or applications, and engaging in any activities that may pose a risk to the security of the company's information systems.

Altamaha Tech should prioritize the development and enforcement of a comprehensive Mobile Device Management (MDM) policy to protect sensitive information and prevent security breaches. An MDM policy outlines the rules and guidelines for the use and management of mobile devices within the organization. The policy should include guidelines for acceptable device usage, secure data transmission and storage, and regular updates and maintenance.An effective MDM policy should require employees to use strong passwords or passcodes, encrypt data on the device, and enable remote wiping capabilities. This will help prevent unauthorized access to company data in the event of a lost or stolen device. Furthermore, the policy should establish protocols for employees to report lost or stolen devices immediately to the IT department. The IT department can then take action to remotely wipe the device and minimize the risk of data loss . Another important component of an MDM policy is the requirement to keep devices up-to-date with the latest software and security patches. This can prevent security vulnerabilities that can be exploited by hackers. The policy should establish a clear process for regularly updating devices and require employees to comply with these updates.

Personally Identifiable Information (PII) refers to any information that can be used to identify an individual. This includes data such as name, address, social security number, and date of birth. It is essential for Altamaha Tech to develop a comprehensive PII policy that outlines the proper handling, storage, and disposal of PII data. The policy should include guidelines for how to obtain and use PII data, who has access to it, and how it should be secured. To ensure the protection of PII data, Altamaha Tech should establish data classification guidelines that determine the sensitivity and value of different types of data. This will help determine the level of protection required for each type of data. The PII policy should also address the proper disposal of PII data, including procedures for securely erasing or destroying data when it is no

longer needed. The policy should also include guidelines for reporting data breaches, notifying affected individuals, and implementing corrective actions. Employee training and awareness programs should also be developed to ensure that all employees understand the importance of protecting PII data and the policies and procedures in place to do so. Regular reviews and updates to the policy should be conducted to ensure that it remains relevant and effective in protecting PII data.. This policy should comply with United States and international laws and regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act

A comprehensive guideline should be developed to ensure that the company is in compliance with the PCI DSS standards., Altamaha Tech should ensure that cardholder data is stored securely by implementing access controls, such as limiting access to authorized personnel only, encrypting sensitive data, and storing cardholder data separately from other data. The company should also ensure that physical access to cardholder data is restricted and that security cameras are in place to monitor access to areas where cardholder data is stored. Encryption is also an important aspect of PCI DSS compliance. Altamaha Tech should implement encryption for all cardholder data, both in transit and at res this includes implementing secure transmission methods for online transactions, such as Secure Sockets Layer (SSL), and encrypting stored cardholder data using industry-standard encryption algorithms.

Altamaha Tech must establish a comprehensive backup plan that covers all critical data, including important company documents, employee data, and financial records. The backup plan should include regular backups of data, ensuring that data is backed up at frequent intervals, such as daily, weekly, or monthly, depending on the data's criticality. Regular backups will help ensure that if data is lost, corrupted, or otherwise compromised, the organization can quickly recover

from the incident and restore data to its previous state Testing of backup systems is vital to ensuring that backups are functioning correctly and can be restored when needed. Regular testing should be performed to ensure that backups can be quickly restored in the event of an incident. Organizations should also periodically review their backup strategy to ensure that it remains relevant and up-to-date with current best practices and technology. It is essential to note that backup plans are only effective if they are strictly enforced and followed by employees. Employees should be trained on the backup plan, their role in the process, and any security measures in place to protect backups. Any changes to the backup plan should be communicated to employees to ensure that they understand the new protocols and can implement them correctly.

Continuous security monitoring involves regular checks and tests of the organization's security measures. Policies and procedures for continuous security monitoring should outline the frequency and type of tests to be performed. They should also define the roles and responsibilities of the organization's cybersecurity team. All employees should receive regular cybersecurity awareness training that covers topics such as phishing attacks, password security, and mobile device security. New employees should receive cybersecurity training as part of their onboarding process. Ongoing training and continuing education programs should be implemented to ensure that employees stay up-to-date on the latest security threats and best practices.

To ensure business continuity during a disaster, Altamaha Tech should develop a comprehensive Continuity of Operations Plan (COOP). This plan should outline procedures and protocols for maintaining key systems and operations during a disaster, and ensuring that critical business functions can continue. The COOP should include measures such as regular data

backups, emergency power supply, alternate communication channels, and remote access capabilities. It should also establish a clear chain of command and define roles and responsibilities for key personnel during a disaster. Regular testing and updating of the COOP should also be conducted to ensure its effectiveness and relevance. This will help to minimize the impact of any potential disasters and ensure that the organization can quickly recover and resume normal operations.

In conclusion, the assessment of Altamaha Tech's cybersecurity posture revealed several significant issues that need to be addressed. This paper proposed several policies, procedures, and strategies that the company can implement to enhance its cybersecurity health. The implementation of these policies and procedures should mitigate the identified security threats and vulnerabilities, safeguard sensitive data, and prevent security breaches.

Works Cited:

Center for Internet Security. "Information Security Policy." Center for Internet Security, 2021, www.cisecurity.org/controls/information-security-policies/.

Chen, Hsinchun. "Security Threats to Mobile Devices." International Journal of Electronic Commerce Studies, vol. 6, no. 3, 2015, pp. 211-222.

Leak, Stephen. "What is PCI DSS Compliance? Requirements, Checklist, & More." Digital Guardian, 15 Dec. 2020, digitalguardian.com/blog/what-pci-dss-compliance-requirements-checklist-more.

National Institute of Standards and Technology. "Guide for Conducting Risk Assessments." National Institute of Standards and Technology, 2012, doi.org/10.6028/NIST.SP.800-30r1.

Data Breach Today. "What is PII (Personally Identifiable Information)?" Data Breach Today, 12 Apr. 2021, databreachtoday.com/what-is-pii-personally-identifiable-information-a-10398.

National Cyber Security Alliance. "Top Tips for Strong Mobile Device Security." Stay Safe Online, 2021, www.staysafeonline.org/resource/top-tips-for-strong-mobile-device-security/.

Bayuk, Jennifer L. "Mobile Device Management Policies: Best Practices and Future Directions." IEEE Security & Privacy, vol. 10, no. 2, 2012, pp. 40-49, doi:10.1109/MSP.2012.31.