ISEC 675: Information Systems Auditing

Summer Term 2023

Eric Webb

Professor Ling Wang

Assignment 1: Written Essays

Written Essay 1-1:

One of the most infamous corporate scandals in American history was the Enron fraud case. During the turn of the century Enron had grown to be considered one of the world's leading energy companies, but Enron collapsed due to the company's financial prowess being a façade. It was later revealed that the company engaged in various fraudulent accounting practices by the executive's hiding debt and inflating profits. The outcome of the collapse of Enron was the adoption of the Sarbanes-Oxley (SOX) compliance laws along with other acts and reforms to prevent corporate fraud and protect investors.

Enron's fraud contained many techniques including accounting manipulations, false financial reporting, and insider trading. To give the illusion of profitability, Enron executives manipulated earnings reports and used special purpose entities that were off the balance sheets to conceal debt. Executives were also caught performing insider trading by selling shares of stock before the company's true financial situation became known. Because of these fraudulent practices Enron went bankrupt which led to the loss of billions of dollars for investors and stakeholders.

The failure of Enron led congress to pass the Sarbanes-Oxley Act in 2002. The laws composed within SOX require publicly traded companies to establish and maintain internal controls over finances and require more accurate and transparent financial statements. Another result of the SOX Act was the creation of the Public Company Accounting Oversight Board (PCAOB) to help regulate public accounting firms and auditors. The PCAOB helped provision laws that increased penalties for corporate fraud and raised the requirements on executives to certify the accuracy of their financial statements.

The scandal that was Enron also led to the passage of other financial compliance laws in the United States. The Dodd-Frank Wall Street Reform and the Consumer Protection Act were both passed in 2010 to prevent other financial crises and required financial institutions to be more transparent in their finances and forced companies to establish stronger risk management protocols. These laws also helped form the Consumer Fraud Protection Bureau to protect consumers from financial fraud and abuse.

In conclusion, the fraud performed by Enron had a major impact on corporate governance and compliance within the United States. The Sarbanes-Oxley Act was passed because of so, to prevent corporate fraud, protect investors, and established new standards for financial accountability and reporting. The Enron fraud also influenced the development of the Public Company Accounting Oversight Board, Dodd-Frank Wall Street Reform, and the Consumer Protection Act. Overall, the Enron fraud served as a reminder of the importance of transparency and accountability in corporate governance and proved the need for strong regulatory oversight.

Written Essay 1-3:

When it comes to government networks and business units, having a strong security posture is crucial. It is important that government officials adhere to the minimum baseline requirements and the hardening guidelines established. These guidelines provide a framework for establishing a secure network posture for the government to maintain the confidentiality, integrity, and availability (CIA) triad, while also reducing the risk of cyber threats. The minimum requirements that the government should adhere to are as follows:

1. Network Segmentation: To separate systems and data from less critical ones using techniques such as Virtual Local Area Networks (VLAN's).
2. Access Control: Employ the principle of least privilege, to ensure that users have only need to know access.
3. Encryption: Encrypt data in motion and a rest.
4. Endpoint Protection: Protect the network from the brunt of the open internet such as firewalls to block IP addresses and port numbers while also using load balancers to handle allowed incoming traffic.
5. Intrusion Detection and Prevention Systems (IDS/IPS): To detect and prevent breaches from allowed traffic.
6. Data Backup and Recovery: Implement a backup and recovery strategy and verify the backup restoration process works.
7. Patch Management: Establish a process for security updates and patches while prioritizing vulnerabilities based on severity.
8. Security Awareness Training: Educate employees about common cyber-attacks.
9. Incident Response Plan: Outline the steps on how to proceed in case of a security incident.
10. Security Monitoring and Logging: Implement monitoring and logging to track system and network activities. Centralizing logs can be done with a Security Information and Event Management (SIEM) system.
11. Vulnerability Management: Establish a program to scan for known vulnerabilities and prioritize and fix vulnerabilities based on risk.
12. Security Assessments and Audits: Conduct assessments and audits to identify vulnerabilities and review compliance.

13. Physical Security: Implement physical security controls such as guards, restricted access to rooms, and Closed-circuit Television (CCTV).

The Department of Defense (DoD) oversees these initiatives with many sub-agencies under its domain. These agencies include the Defense Information Systems Agency (DISA), National Security Agency (NSA), Defense Counterintelligence and Security Agency (DCSA), United States Cyber Command (USCYBERCOM), along with a myriad of other agencies including all the US military branches.

Two examples of auditing frameworks and hardening guidelines used by the Department of Defense (DoD) are the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

The DISA's STIGs are a collection of documents that provide guidelines for hardening and securing government computer systems and networks. The STIG's outline the minimum barebones requirements for the secure deployment of such systems. Requirements include security concepts such as access control, auditing, logging, configuration management, network security, and vulnerability management. The STIGs produced by the DISA are available for many products such as operating systems, databases, and web applications. The guidelines are updated frequently from the DISA and align with the latest security standards. Often government contracts will have to submit their work to be audited by the guidelines in the STIGs.

Another hardening guideline used within the DoD is (NIST) Special Publication (SP) 800-171. The NIST SP 800-171 provides guidelines for protecting the confidentiality of Controlled Unclassified Information (CUI) in nonfederal information systems and organizations and provides a framework of control over a domain of 14 categories that include access control, awareness and training, configuration management, incident response, and network security.

Compliance with the NIST SP 800-171 is mandatory for all non-federal organizations that handle, store, process, or transmit CUI and helps deter risk when handling important government documentation.

To conclude, the DoD provides and uses a various amount of auditing frameworks and hardening guidelines that provide a framework for securing government networks and business units. The DISA’s STIGs and the NIST’s SP 800-171 are two examples of frameworks and guidelines that are available for securing DoD systems and networks. It is essential to adhere to these guidelines to ensure that DoD networks and systems are secure and safeguarded against cyber-attacks.

References:

Defense Information Systems Agency. (n.d.). Home. Retrieved from https://www.disa.mil/

Defense Counterintelligence and Security Agency. (n.d.). Home. Retrieved from https://www.dcsa.mil/

Department of Defense. (n.d.). Home. Retrieved from https://www.defense.gov/

National Security Agency. (n.d.). Home. Retrieved from https://www.nsa.gov/

Securities and Exchange Commission. (2009). Study on the Implementation of Section 404 of the Sarbanes-Oxley Act of 2002. Retrieved from https://www.sec.gov/news/studies/2009/sox-404_study.pdf

U.S. Securities and Exchange Commission. (2009). Study and Recommendations on Section 404(b) of the Sarbanes-Oxley Act of 2002 for Issuers with Public Float between $75 and $250 Million. Retrieved from https://www.sec.gov/news/studies/2009/sox-404_study.pdf

United States Department of Defense. (n.d.). Security Technical Implementation Guides (STIGs). Retrieved from https://public.cyber.mil/stigs/