Quinton Green

Legal Issues in Information Security

Task 1- Legal Analysis

**A.  Demonstrate your knowledge of application of the law by doing the following:**

**1.  Explain how the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act *each* specifically relate to the criminal activity described in the case study.**

The Computer Fraud and Abuse act relates to the criminal activity in this case study because the BI Unit employees, Sarah Miller, the senior analyst along with Analysts Megan Rogers and Jack Hudson who take direction from Miller were scanning other companies' networks via a Metasploit tool. Jack Hudson coordinated efforts by third parties to gather intelligence through surveilling and through mining companies’ trash or which is “dumpster diving” and “trash surveillance” attacks which are all crimes against protected computers by accessing information unauthorized

The Electronic Communications Privacy Act relates to the criminal activity because a Metasploit tool was used in penetration and scanning activity into IP addresses for several Internet-based companies and placed on a TechFite hard drive. Analyst Jack Hudson was allegedly “dumpster diving” and doing “trash surveillance” of other companies. ECPA makes it unlawful to intentionally access a facility in which electronic communication services are provided and obtain, alter, or prevent unauthorized access to a wire or electronic communication while it is in electronic storage in such system

**2.  Explain how three laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study.**

1) The OMB breach notification policy justifies legal action upon negligence for the former employees whose accounts were still active and being used. TechFite was negligent because those accounts should have been terminated upon the employees leaving the company. Their PII was compromised without them knowing.

2) Computer Trespass and Intrusion applies to this case because TechFite employees had a Metasploit device set up to scan and penetrate other companies' network and IP addresses

3) Data retention and destruction- lack of proper destruction of data allowed TechFite employees to “dumpster dive” and do “trash surveillance”.

**3.**  **Discuss two instances in which duty of due care was lacking.**

A duty of due care is a person’s obligation to avoid acts or omissions that can harm others. The level of duty that one person owes to another is based on the reasonable person standard, a legal concept used to describe how an ordinary person would think and act. Carl Jaspers lacked duty of care regarding agent Yu Lee by requesting him to create fake accounts to commit financial fraud information for the finance department. Also, Carl Jaspers lacked duty of care to the former employees whose account information was used to in relation to send emails. Senior Analyst Sarah Miller lacked duty of care regarding her analysts Megan Rogers and Jack Hudson

**4.  Describe how the Sarbanes-Oxley Act (SOX) applies to the case study.**

  The main goal of SOX was to protect shareholders and investors from financial fraud. The report found that three clients of TechFite may not be actual, real clients but may simply be conduits for moving money into TechFite’s sales figures for the division which violates SOX. SOX requires the executive management of a company to certify that there are controls in place to protect the accuracy of company information and Carl Jaspers requested two fraudulent accounts to be created using former employees’ information which violates SOX. Under SOX, Corporate Fraud and Accountability (Title XI)- Establishes criminal liability for certain types of fraud committed by corporate officers, the report found that fake companies all had ties to the same bank in another state that are supposed to be clients of TechFite.

**B.  Discuss legal theories by doing the following:**

**1.  Explain how evidence in the case study supports claims of alleged criminal activity in TechFite.**

**a.  Identify who committed the alleged criminal acts and who were the victims.**

The people who committed the alleged criminal acts are Carl Jaspers, IT Security Analyst Nadia Johnson, Agent Yu Lee, the senior analyst Sarah Miller, and Analysts Megan Rogers and Jack Hudson who take direction from Sarah Miller

The victims are Union City Electronic Ventures, OrangeLeaf, and the former employees whose email accounts were in use. The PII was breached, and they don’t even work for the company, but it appears like they currently are and would be blamed for the misuse

b.  **Explain how existing cybersecurity policies and procedures failed to prevent the alleged criminal activity**.

The following cybersecurity policies and procedures failed to prevent the alleged criminal activity. All employees had administrative privileges. The principal of least privilege should be applied to only allow employees to have access to perform duties related to their job. All TechFite employees at the time of hire sign a release permitting company surveillance of any electronic communications using TechFite equipment but there were no Workplace monitoring taking place. The organization had performed a credible job of protecting the division’s network against external threats. Vulnerability scanning, penetration testing, and UTM (unified threat management) were all in place but there were no internal monitoring controls set up.

**2.  Explain how evidence in the case study supports claims of alleged acts of negligence in TechFite.**

**a.  Identify who was negligent and who were the victims.**

The negligent people were IT Security Analyst Nadia Johnson. Carl Jaspers, and Sarah Miller

The victims were Union City Electronic Ventures, OrangeLeaf, the former employees whose email account were still being used, Analysts Megan Rogers and Jack Hudson who take direction from Miller.

**b.  Explain how existing cybersecurity policies and procedures failed to prevent the negligent practices.**

There were no checks and balances system set up to monitor employee activities. A Workplace Privacy and Monitoring policy would mitigate negligence. The fact that IT Security Analyst Nadia Miller was negligent in verifying the client database. There was no board of directors, or any auditing systems set up to catch things like the Metasploit device.

**C.  Prepare a summary (*suggested length of 1–2 paragraphs*) directed to senior management that states the status of TechFite’s legal compliance.**

To the TechFite Senior Management,

This is to inform you of the state of TechFite’s legal compliance. I must report to you that TechFite is not aligned within legal compliance standards. After the company was audited for Information security governance it was found that behaviors are being engaged that go against the Sarbanes-Oxley Act (SOX). Department segmentation and the Principal of Least Privilege need to be instituted. Also, policies need to be updated in accordance with the Computer Fraud and Abuse Act and the Electronics Communication Privacy Act to combat employee negligence. Other discovers found Computer Trespass and Intrusion acts, OMB breach notification violations and Data Retention and Destruction violations. Legal Compliance is pertinent to business practices and being aligned with the law is factor that must be taken seriously for this purpose. I implore you institute changes to realign TechFite in compliance standards.

**REFERENCES**

1) Grama, Joanna Lyn. *Legal and Privacy Issues in Information Security*, Jones & Bartlett Learning, LLC, 2020.*ProQuest Ebook Central*, http://ebookcentral.proquest.com/lib/westerngovernors-ebooks/detail.action?docID=6380267. 

2) [Electronic Communications Privacy Act (ECPA) – EPIC – Electronic Privacy Information Center](https://epic.org/ecpa/) - http://epic.org/ecpa/