Legal Analysis of TechFite

A1

TechFite violated the Computer Fraud and Abuse Act (CFAA) by not enforcing the principle of least privilege or creating a separation of duties. This led to all computers in the company having full administrative rights to all data. The lack of policy failed to protect proprietary information. This is a direct violation of the CFAA that requires authorization to access this data type. The separation of duties and proper administrative control would have protected the information. The Electronic Communications Privacy Act (ECPA) was violated when a Metasploit tool was used by members of the business intelligence (BI) unit to scan the IP addresses of other internet-based companies. This scanning was done without consent, making the act illegal under the ECPA. Compliance of the ECPA protects all businesses data.

A2

The three laws that require legal action are the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Act (ECPA), and the Sarbanes-Oxley Act (SOX). The CFAA requires action because members of BI unit accessed legal, human resources, and finance departments without authorization. Regular traffic was seen of these data types being examined. The ECPA requires legal action because Sarah Miller, Megan Rogers, and Jack Hudson worked as a separate team to illegally gather information on other internet-based companies. Jack Hudson, specifically, ignored his membership to SCIP that prohibits this behavior. SOX requires legal action because Carl Jaspers appeared to be inflating the sales of TechFite by moving money through accounts registered to fake companies.

A3

Duty of due care was lacking in two instances - when proprietary information was leaked and when there was little to no documentation on internal operations. The first instance damaged the business efforts of two TechFite clients. Had a separation of duties been in place only the necessary teams would have had access to the information. This would have made it less likely someone from another unrelated department would have been able to leak the information. The other instance was the blanket summaries that no information was found. These claims could not be verified through documentation. Documentation would have made it possible to see errors or wrongdoing much more quickly as you have a baseline to track. Documentation would have also shown the company's efforts to keep up with client security.

A4

The Sarbanes-Oxley Act applies to this investigation because three ill-legitimate companies were found to be clients of TechFite. All three companies had the same registering agent, who was a friend of Carl Jaspers. The companies were reporting profits that were included in sales numbers, falsely inflating them. This violates SOX because the illegal action made them look more profitable, which is financial fraud.

B1a

Evidence on hardrives indicated recent scanning activity into IP addresses of other internet-based companies supports claims of alleged criminal activity at TechFite. This act was committed by Sarah Miller, Megan rogers, and Jack Hudson and victimized the internet-based companies they were falsely gathering information from. Sarah Miller had the most traffic in scanning other networks. A second example of alleged criminal activity would be Carl Jaspers creating fake accounts in the name of old employees to conduct intelligence gathering. This victimizes the former employees and the businesses whose information is being gathered.

B1b

There were some policies that did not stop criminal activity. The principle of least privilege was ignored as multiple accounts in the BI unit had unrestricted administration privileges. These privileges were used to create and edit financial information. TechFite also did not use the Chinese Wall method to make info only available to those who needed it. The lack of these policies did not prevent criminal activity.

B2/B2a

The lack of documentation on internal oversight supports claims of alleged negligent activity at TechFite. The BI unit was a serious offender of this. IT Security Analyst Nadia Johnson was responsible for reviewing reports for the CISO. Both the CISO and Nadia Johnson would be responsible for the negligence that victimized users or companies working with TechFite.

B2b

The BI unit at TechFite did not have any policies in place to prevent negligent activity. There was no policy or plan in place to protect clients' and their information. They ignored the standard security practice of least privilege and separation of duties. This allowed for admin controls to be used in any manner as well as anyone to see anything from any unit.

Summary

The results from the investigation of TechFite were overwhelming. The business practices that were found were negligent and criminal. There are multiple instances of unsavory actions throughout the BI unit and from Carl Jaspers. This included illegal scanning and unauthorized edits to sales figures. Adherence to laws and acts would have protected the company, its employees, and its users. The misconduct and harm brought to clients would have been minimized with proper policy and procedures. Negligence can be seen in the lack of policy implementing separation of duties and in the lack of documentation for internal operations. Separation of duties would have protected client information from those that did not need it to conduct their job duties. Proper audits and more documentation on internal operations would have alerted the CISO to wrongdoing. The failure to comply with standard cybersecurity practices should signal a change of leadership and management is needed.