Western Governor's University

Legal Issues in Information Security

C841

Kern Grant

IHP4 Task 1: Legal Analysis

IHP4 Task 1: Legal Analysis

A1. CFAA and ECPA

Under the Computer Fraud and Abuse Act (CFAA), TechFIte and its victims qualify as a protected computer because its network connects to the internet. However, some of TechFite employees violate the CFAA. Carl Jasper, TechFite Head of the Applications division, requested the creation of two user accounts assigned to former employees. The mentioned accounts are still active and regularly used. Some activities include email communication to non-clients referencing illegal data-gathering activities to various companies. The victims of such actions are TechFite, and the various targeted companies used to gather intelligence. Past employees should not be assigned to active user accounts; illicit intelligence-gather activities are criminal. Jasper's actions suggest an intent to defraud and abuse power, violating the Computer Fraud and Abuse Act.

Techfite employees performed criminal activities identified by the Electronic Communications Privacy Act (ECPA). TechFite's Business Intelligence unit employees, Sarah Miller, Megan Rogers, and Jack Hudson, all participate in the unauthorized access to other companies' electronic communications. They used a Metasploit tool to penetrate and scan activities of IP addresses for other companies' networks. Additionally, Mr. Hudson was involved in illegally gathering data intelligence. The unauthorized access and the interception of communications from the companies' networks is a criminal act and violates the Electronic Communications Privacy Act.

A2. Three Laws

The Computers Fraud and Abuse Act (CFAA), Electronic Communication Privacy Act, and Sarbanes-Oxley Act are laws that TechFite violated, justifying legal actions based on their negligence.

Carl Jasper's the Head of Applications Division negligent actions is a violation of the Computer Fraud and Abuse Act (CFAA). He requested the creation of user accounts to be assigned to former employees. The accounts email communication reference illegal intelligence-gathering activities. Jaspers' actions illustrate intent to defraud and abuse power, violating the CFAA.

The Electronics Communications Privacy Act (EPCA) aims to protect electronic communications. The negligent activity of TechFite BI unit employees violated that act. Senior Analyst Sarah Miller and her staff, Megan Rogers and Jack Hudson, intentionally intercepted private communications from their employer and other companies. They used a Metasploit tool to penetrate and scan the IP address of several external companies. Mr. Hudson, 1/3 of the BI unit, was also involved with illegal data intelligence gathering. In addition, the BI unit accessed and examined other TechFite departments' sensitive data from dummy accounts by escalating privilege. The employee's actions were unauthorized, which can cause damage to their employer and other targeted companies. Therefore, such negligent activities justify legal actions.

Sarbanes-Oxley Act (SOX) aims to protect investors from financial fraud. TechFite negligent business practices and activities violate the SOX act. Suspicious business activities suggest they are misleading investors; by using shell companies

to help boost their sales and financial performance. The three companies in reference have no online presence as an internet business. They are all incorporated by Yu Lee, who attended grad school with Carl Jasper, and all make payments to TechFite from the same bank. Another issue that violates SOX is TechFite's poor auditing practices. Their company network must be secure to store financial data. However, based on poor auditing practices TechFite lacks internal network documentation; the auditor also manages IT security. Lastly, the re-occurring negligent activities and practices show that TechFite information systems are not sufficiently secure, violating the SOX act.

A3. Duty of Due Care

TechFite case study had two instances in which Duty of care was lacking. Two TechFite case study instances in which Duty of care was lacking involve Nadia Johnson, IT Security Analyst, and Carl Jasper, Head of the Application Division.

Nadia Johnson lacked Duty of care as an employee and leader of TechFite. Her job as the IT security Analyst is to manage and secure TechFite network. She reviewed the network audit reports for her boss. The report summary indicates no abnormalities, yet it lacked auditing notes of users' accounts, escalation of privilege, monitoring network traffic, and coverage for safeguarding sensitive information, to name a few. Nadia was aware of the lack of security procedures and bad practices. TechFite network was not secure, therefore, at risk. In such circumstances, Nadia Johnson was responsible for doing her job by investigating to improve these issues. However, that did not occur.

Therefore, the employee's Illicit activities within the TechFite network are a credit to Nadia Johnson lack of care.

TechFite and Carl Jasper, Head of the Application Division, for lacking care of Duty. He has a pattern of mishandling information. He requested the creation of two user accounts assigned to former TechFite employees. The accounts were involved with illegal intelligence-gathering activities. In addition, he was directly involved with TechFite's lousy business practices, as reported by past business prospects who reported similar experiences with TechFite. During their pre-consultation, Carl Jasper made them sign non-disclosure agreements and complete a questionnaire that contained valuable product information. After denying TechFite services, each company discovered that their competitor had launched a similar product. The referenced competitor is also a client of TechFite. Jaspers's actions suggest a lack of managing sensitive data of his department, abuse of power, or being directly involved in criminal activities. Therefore, he lacked the Duty of care to prevent such actions.

A4. SOX

The SOX act applies to this case study because TechFite is a publicly traded company on Nasdaq involved in questionable financial-related activities that can deceive investors. For example, three suspicious clients have no online presence as internet businesses; they all pay TechFite from the same bank. In addition, Yu Lee, who attended grad school with Carl Jasper, incorporated all three companies. The activities suggest the companies may be a front for making service payments to improve TechFite sales and financial statements. The SOX act also includes IT

and internal controls audits because financial data is stored on a company network and should be secured. However, TechFite audits and activities show a lack of safeguarding sensitive information. For example, one event includes the BI unit accessing and examining financial and executive documents through dummy user accounts and privilege escalation. These events illustrate illicit financial-related activities, which suggest TechFite's data can be misleading and unsecured. Therefore, TechFite violates the SOX act.

B1/B1a. Criminal Evidence, Activity, Actors and Victims

TechFite BI unit and Carl Jasper performed criminal activities, which made them bad actors. Their victims include the various companies they targeted and their employers. In addition, illegal actions can harm the intelligence gathering target companies and their employer's brand.

Tech Fite BI unit team led by senior analyst Sarah Miller were bad actors that performed criminal activities. According to the investigator's findings, evidence indicates Sarah Miller, Megan Rogers, and Jack Hudson are actively performing unauthorized penetration and scanning activity into IP addresses for other companies. Their victims were several unknown internet-based companies. They were using a Metasploit tool to penetrate and scan the IP addresses of several external companies. Mr. Hudson, 1/3 of the BI unit, was also involved with illegal data intelligence gathering. The entire BI unit, collectively and individually, is a bad actor that intentionally victimized various targeted companies with their illegal network activities.

Carl Jasper, TechFite head of the applications division, is a bad actor who performed criminal activities against his employer and unknown targeted companies. First, he requested the creation of two user accounts to be assigned by employees that no longer work for TechFIte. The account's email communication indicates illegal intelligence-gathering activities with non-TechFite clients. The Victims of her activities are her employer TechFite, due to his part in the illicit creation and use of a user account with illegal intent. The second Victims are the various companies the data gathering act targeted. Carl Jasper's actions make him a bad actor.

B1b. Cybersecurity Policies & Procedures for Criminal Activity

Account creation/termination and auditing are two cybersecurity policies TechFite needs to improve. Correctly enforcing policy procedures could prevent or mitigate the actions that led to TechFite's employee's criminal activities.

The account creation/termination policy monitors approve account creation and close accounts as necessary. However, due to the lack of sufficient procedure enforcement, TechFite employees misused actions led to criminal activities. For example, Carl Jasper, TechFite head of the application division, requested the creation of two user accounts assigned to former employees. As a result, the accounts were a part of illegal intelligence-gathering activities. Also, Sarah Miller, senior IT analyst, and the BI unit accessed sensitive information from other departments with dummy accounts be the means of privilege escalation. The Account Creation/ Termination policy failed because it did not deny creating a user account assigned to a former employee or unaware of user dummy

accounts. If this policy were enforced correctly by TechFite employees, it would prevent or terminate such accounts. Also, possibly denying criminal activities.

The auditing policy and procedures help ensure that proper cybersecurity measures are in place. A sufficient audit procedure highlights the network vulnerabilities that need repair. However, TechFite failed to perform a proper system audit, which led to recurring criminal activities. For example, the IT auditing summary reported no internal operations abnormalities. However, it lacks notes on auditing users' accounts, surveilling internal network traffic and activity, or checking for the escalation of privilege; it also lacks a plan for proper controls to secure sensitive data. Some criminal actions include illegal intelligence gathering under accounts created and assigned to former employees, penetrating and scanning external companies' IP addresses, and escalating privileges on dummy accounts to gain access to sensitive data. In addition, the leaking and unauthorized accessing of data. The proper procedure and enforcement of The Auditing Policy might mitigate or prevent these activities' reoccurrence.

B2/B2a Evidence of Negligent Activity, Actors and Victims

&

B2b. Cybersecurity Policies & procedures for Negligent Activity

Carl Jasper and Nadia Johnson TechFite acted negligently. Carl Jasper is the head of the Applications Division, and Nadia Johnson is the IT Security Analyst of TechFite.

Carl Jasper acted negligently with potential clients' proprietary product information. The victims of his actions are Orange Leaf Software LLC and Union City Electronic Ventures. They both experienced similar experiences with

TechFite. During their pre-consulting process, they completed Non-Disclosure Agreement executed by Jasper and questionnaires for TechFite. The questionnaire contained product information that was of value to competitors. A few months after denying TechFite services, their competitor launched similar products. In addition, the identified competitors were also existing clients of TechFite. The pattern suggests a leak of data. Carl Jasper's position as the head of the App Division, who initially interacted and executed the NDA with the potential client, is the negligent actor of the leak. The Chinese wall Method Policy might prevent data leaks because it aims to protect sensitive information within different parts of an organization. The procedure of this policy will separate the access of information of employees who deal with potential clients and existing clients, safeguarding clients' sensitive information. Carl Jasper and TechFite should implement this policy to prevent data leaks.

Nadia Johnson's job performance and lack of duty of care for TechFite's internal IT system make her a negligent actor. Johnson's job as the IT security analyst is to maintain the security of the company network. Nevertheless, she reviewed the system network audit for her boss, the chief information security officer (CISO). The internal network reports suggested no abnormalities. However, the report summary lacked critical documentation. Some information includes reviews on user accounts, network surveillance, escalation privilege, and plans for safeguarding sensitive information. TechFite internal network was not secured because they did not enforce or use the necessary cybersecurity policies. Nadia was aware of this information yet did not act on making corrections. As a result, it led to criminal employee activities, including illegally gathering intelligence data from various companies, creating dummy accounts, using escalating privileges to access other departments' sensitive data, and leaking other companies' sensitive data. The various data-gathering targeted companies, Orange Leaf Software LLC, Union

City Electronic Ventures, and TechFite departments, are the illegal activities' victims. The Separation of Duty Policy can address Nadia's negligent actions and possibly prevent the reoccurring illegal actions by TechFite employees. Enforcing this policy ensures that someone other than Nadia reviews the network she manages.

C. Legal Compliance Summary for Management

The inadequate information systems management for the Application Division at TechFite led to reoccurring employee actions that violated a few laws. Thus, TechFite was not compliant with the Computer Fraud and Abuse Act (CFAA), The Electronic Communications Privacy Act (ECPA), and The Sox Act (SOX). Lack of unenforced security controls of TechFite made their network vulnerable to breaches, abuse, and non-compliance. Some employees that lack duty of care are Carl Jasper, Nadia Johnson, and the entire BI unit. Their influence and illicit actions make them bad actors.

Carl Jasper's actions violate the Computer Fraud and Abuse Act (CFAA). He requested the creation of user accounts to be assigned to former employees. Account's email communication reference illegal intelligence-gathering activities. Jaspers' actions illustrate intent to defraud and abuse power, violating the CFAA.

TechFite Business Intelligence unit performed unauthorized access and interception of communications from other companies' networks by using a Metasploit tool to penetrate and scan activities of IP addresses. Mr. Hudson, 1/3 of the BI unit, was involved in illegally gathering data intelligence. The unauthorized access and interceptions of other companies' networks make TechFite not compliant with the ECPA.

Sarbanes-Oxley Act (SOX) aims to protect investors from financial fraud. However, based on the illicit activities of the TechFite Applications Division, they are not compliant with SOX. A part of SOX compliance is annual audits that include the organization's financials and the Information systems for the data it stores. The actions indicate possible misleading investors, insufficient internal auditing, and a lack of internal network security management. TechFite has three clients that draw suspicion. First, Yu Lee, who attended grad school with Carl Jasper, incorporated all three companies; they have no online presence as an internet business, and all make payments to TechFite from the same bank. The suspicious activities suggest that all three clients are shell companies. Which TechFite receives service payments to boost its sales and financial statement, therefore appealing to yet misleading investors. TechFite has poor auditing practices. It includes a lack of internal network documentation; the auditor also manages IT security. Lastly, TechFite has un-enforced or missing network safeguard controls, monitoring, and cybersecurity policies, which cause reoccurring illegal activities from their employees, leaving information systems at risk. Nadia Johnson, Tech Fite IT security analyst, was aware of TechFite vulnerabilities yet did not take action to correct them. Therefore, her negligent actions led to criminal activities. The activities and bad practices make TechFite not compliant with the SOX act.