IHP4 Task 1: Legal Analysis

A1. CFAA and ECPA

The Computer Fraud and Abuse Act (CFAA) is a United States federal law that governs unauthorized access and damage to protected computers. In the TechFite case study, Carl Jaspers, the head of the Applications Division, used TechFite accounts to create fake user accounts linked to the emails of ex-employees at TechFite. Reactivating these accounts allowed unauthorized users to access email communications from former employees; this is a direct violation of the CFAA. In addition, these user accounts were being used for intelligence gathering activities such as dumpster diving and trash surveillance against other companies. The unauthorized access and use of information on TechFite's computers directly violate the CFAA.

The Electronic Communication Privacy Act (ECPA) restricts the unauthorized access, disclosure, and interception of electronic communications. The TechFite case study showed evidence that some of the computers within the BI Unit were being used for penetration and intercepting company traffic using the Metasploit tool. The unauthorized interception of electronic communication is a violation of the ECPA.

A2. Three Laws

The negligence observed in the case study that led to a violation of the ECPA was due to the lack of internal auditing performed within TechFite. User accounts and activity should be constantly monitored and audited to ensure correct permissions and best practices are being followed. The failure to conduct regular audits led to the criminal activity performed by the BI Unit, which conducted unauthorized penetration and scanning activities involving the unauthorized interception of data, which are violations of the ECPA that warrant legal action to take place.

The negligence observed in the case study that led to the CFAA violation was the lack of auditing user permissions on accounts by senior staff members within the BI Unit. This negligence allowed the BI Unit to create dummy accounts to escalate privileges and perform unauthorized activities, such as gathering confidential information from the legal department, human resources (HR), and finance departments. The actions of the BI Unit to exfiltrate information without authorization compromised the integrity of TechFite's computer systems. These actions warrant legal action in direct violation of the CFAA.

The negligence observed in the case study was the violation of SOX, which aims to protect shareholders and investors from financial fraud by publicly traded companies. SOX requires these companies to maintain accurate financial records. TechFite, a publicly traded company on NASDAQ, failed to perform internal auditing of its client database. This allowed the creation of three fictitious organizations that were being used to inflate financial records. This direct violation of SOX compliance warrants legal action; this could have been avoided with proper security controls and policies in place.

A3. Duty of Due Care

In the case study, the first instance found lacking in the duty of due care was the lack of proper auditing and security controls pertaining to the company's internal operations. TechFite's failure to regularly audit user accounts and permissions led to privilege escalation, allowing users to gain unauthorized access to sensitive information from the HR department, Legal Department, and financial departments. Implementing strong security controls and policies would ensure proper user account permissions are enforced for all TechFite accounts.

The second instance of due care lacking was the failure to enforce the principle of least privilege within the information security policy at TechFite. Every workstation and computer within the BI Unit had full administrative privileges, allowing users to perform unauthorized activity and access sensitive

information. Incorporating least privilege, will ensure user accounts have the correct permissions, improving their overall security posture.

A4. SOX

The Sarbanes-Oxley Act (SOX) applies to the TechFite case study, with company TechFite failing to maintain accurate financial records. TechFite's client database included three shell companies, Bebop Software, FGH Research Group of Indiana, and Dazzling Comet Software of Florida, which were used for manipulating and inflating financial data. TechFite is a publicly traded company that has demonstrated the financial fraud being committed by TechFite. They are creating a false public image of their company's financial health, which is a violation of SOX. Enforcing security controls and the AAA (authentication, authorization, accounting) framework, along with separation of duties, would ensure no transaction can be processed by the same person, preventing fraudulent activities within TechFite.

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

In the TechFite case study, Carl Jasper, head of the Applications Division, and Nadia Johnson, IT Security Analyst of TechFite's Application Division, collaborated in a quid pro quo exchange. Nadia neglected to audit TechFite's client database, allowing Carl to form three shell companies, Bebop Software of Alberta, FGH Research Group of Indiana, and Dazzling Comet Software of Florida, to inflate sales figures for their division. This created a false public perception of TechFite's financial health, with the victims being the shareholders, investors, and TechFite. Inflating sales figures to deceive shareholders violates SOX and is against the law. These actions tarnished TechFite's public image and lost the trust of its shareholders and investors.

The criminal activity and evidence were discovered within TechFite's BI Unit's computers. Network monitoring logs discovered regular IP traffic between the BI Unit and other divisions with

TechFite. The BI Unit created and used dummy accounts to escalate their privileges for unauthorized access to financial and executive documents from the legal, human resources, and financial departments. Unauthorized access to confidential information without consent is a criminal act and a direct violation of the CFAA, warranting legal action.

B1b. Cybersecurity policies and procedures (Criminal Activity Prevention)

TechFite should implement a Separation of Duties policy involving internal controls designed to prevent fraud and errors. Separation of duties is accomplished by dividing critical tasks to ensure that no single individual has complete control over a transaction or process. For example, in the finance department, one individual approves a purchase while a different individual processes the payment. This policy would help benefit TechFite's financial accounting systems, ensuring compliance with SOX by reducing the damage that can be done by one person. The separation of duties policy is a crucial policy used in accounting to ensure that no single individual can perform more than one critical task.

TechFite should implement the principle of least privilege in their Cybersecurity policy, involving a systematic review of user account permissions to ensure compliance and proper account usage. The principle of least privilege ensures they have a minimum level of access and permissions to perform their job duties. Pertaining to this case study, the BI Unit would not have unauthorized access to confidential client information without consent from different divisions within TechFite. Enforcing this policy would help prevent data breaches and ensure compliance with the CFAA.

B2/B2a. Evidence of Negligent Activity, Actors, and Victims

In the TechFite case study, Carl Jasper (head of the Applications Division) was negligent in protecting a signed NDA between TechFite and Orange Leaf LLC. The lack of proper security controls led

to Orange Leaf's proprietary intellectual property being leaked to its competitors. As a part of the consulting process, Orange Leaf completed a questionnaire that provided technical information about their products. Months later, Orange Leaf discovered a competitor was releasing products very similar to theirs. Carl's negligence in protecting confidential information resulted from poor security controls and best practices.

Another act of negligence was performed by Nadia Johnson, IT Security Analyst of TechFite's Application Division, breaking the shareholder's trust in the company. Nadia failed to perform internal audits on client accounts in the BI Unit, leading to the creation of shell companies used to inflate sales figures at TechFite. This oversight damaged TechFite's public image and reputation, causing a loss of trust with the public and their shareholders and possible SOX compliance fines. This negligence can be significantly reduced by adapting security policies and security controls that will meet compliance and regulation standards.

B2b. Cybersecurity policies and procedures (Negligence Prevention)

In the TechFite case study, the failure to enforce the separation of duties policy led to SOX compliance violations, losing shareholders' trust and tarnishing TechFite's reputation. Enforcing separation of duties ensures no single person can perform multiple critical tasks, preventing Carl Jasper, head of the Applications Division, from creating multiple user accounts and using them to perform transactions, resulting in inflated sales figures.

Enforcing the principle of least privilege in TechFite's Cybersecurity policy would greatly reduce the chances of privilege escalation and data breaches. The principle of least privilege ensures users have the minimum level of user permissions and access to perform their job duties at TechFite. By enforcing this policy, users in the BI Unit will not be able to escalate their user permissions and access confidential

information across different divisions at TechFite. This would help TechFite protect confidential information and comply with the CFAA.

C. Legal Compliance Summary

TechFite is currently in violation of the CFAA and SOX. They are not compliant with the CFAA due to the failure to implement proper internal security controls to protect access to confidential client data among different divisions. Additionally, the failure to implement separation of duties has resulted in inflated sales figures, creating a false perception of their financial health and resulting in a SOX violation.