****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

[**Brian Pham**]

**IHP4 Task 1: Legal Analysis**

**IHP4 Task 1: Legal Analysis**

**A1. CFAA and ECPA**

The Business Unit, through its fake user accounts created at the request of Carl Jasper and privilege escalation, gained access to other departments within TechFite without proper authorization. The departments included the legal, human resources, and finance departments which gave the BI unauthorized access to financial records and documents, potentially exposing sensitive data. This violation of the CFAA is further evidenced by the network logs, which showed a regular pattern of traffic between the BI unit and these departments, confirming their unauthorized involvement.

TechFite has clearly violated the ECPA. Carl Jasper requested user accounts be created in the name of former employees and emails that were linked to the fake accounts, were involved in communication between entities who were not TechFite's clients. The content of these emails referred to suspicious activities like 'dumpster diving' and 'trash surveillance.' By using and disclosing electronic communications in this unauthorized manner, TechFite has breached the ECPA.

**A2. Three Laws**

Negligence involving the ECPA:

The lack of oversight on the creation and usage of user accounts stands out as negligence in TechFite's case. The creation of accounts for non-existent employees at the request of Carl Jasper was allowed without anyone raising a cause for concern. These accounts facilitated the unauthorized sending of emails related to illicit activities like 'dumpster diving' and 'trash surveillance,' which are also violations of the ECPA. The ECPA was enacted to protect electronic communications from unauthorized use and disclosure, hence TechFite should be subject to legal action.

Negligence involving the Sarbanes-Oxley Act (SOX):

This law was created to regulate the conduct of public businesses and their auditing processes. TechFite was negligent in this aspect, as evidenced by the potential inflation of their sales figures through the inclusion of faux companies like Bebop Software, FGH Research Group, and Dazzling Comet Software. All these firms were registered to the same agent, and payments were made from the same bank. This suspicion of financial irregularity implies a violation of the SOX, thereby justifying legal action.

Negligence involving the Gramm-Leach-Bliley Act (GLBA):

GLBA requires firms to explain their information-sharing practices to customers and safeguard sensitive data. In TechFite's case, they've neglected their duty to protect the proprietary information of their clients. Evidence lies in the disclosure of technical information about Orange Leaf's products and those of Union City Electronic Ventures to competitors. This failure to protect clients' confidential data could be seen as a violation of GLBA, which could potentially lead to legal action.

**A3. Duty of Due Care**

TechFite's duty of due care should have been the regular monitoring and auditing of user account activity. This oversight was notably absent, allowing Carl Jasper to request the creation of user accounts for non-existent employees. These accounts were then later used for unauthorized activities. This negligence led to violations of the ECPA, a potential breach of confidential information, and a potential breach of internal security measures. TechFite failed by not putting checks and balances in place to ensure the appropriate use of user accounts.

TechFite also demonstrated a lack of due care in maintaining appropriate internal controls on its financial reporting. This is evidenced by the spoofing of companies like Bebop Software, FGH Research Group, and Dazzling Comet Software. Payments from these companies, which were suspiciously all registered to the same agent and all paid from the same bank, were included in TechFite's sales figures. This could be seen as a potential inflation of sales figures, which is a red flag for financial reporting. This negligence could lead to violations of the Sarbanes-Oxley Act and have serious consequences for TechFite, including legal action and loss of trust from shareholders and the public. TechFite failed in its duty of due care by not ensuring robust internal controls and oversight on its financial reporting.

**A4. SOX**

TechFite, being a publicly traded company listed on NASDAQ, is obligated to comply with the Sarbanes-Oxley Act (SOX).

SOX mandates that companies establish and maintain an internal control structure and procedures for financial reporting. In TechFite’s case, we observe suspicious financial activity with respect to three companies. These companies, registered to the same agent, had no real internet presence, and all paid for services at TechFite with checks drawn from the same bank. This raises the question of whether these firms were simply conduits for inflating TechFite’s sales figures, a clear violation of SOX’s provisions against fraudulent financial reporting.

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

1. The first criminal act is the unauthorized access to protected computer systems. The perpetrator here is the Business Intelligence (BI) Unit of TechFite, specifically Sarah Miller, Megan Rogers, and Jack Hudson. These individuals used dummy user accounts to escalate privileges and gain unauthorized access to other departments within TechFite. The victims in this situation are the legal, human resources (HR), and finance departments of TechFite, as their confidential data and documents were potentially exposed and compromised.

2. A separate criminal act observed in the case study involves potential violation of non-disclosure agreements (NDAs) and misuse of proprietary information. In this instance, the perpetrator is the Applications Division of TechFite, specifically Carl Jaspers, the head of the division. According to the report, Jaspers secured NDAs with Orange Leaf Software LLC and Union City Electronic Ventures before they disclosed technical details about their products. After deciding not to hire TechFite, both companies found out later that a competitor was launching products eerily similar to their own, indicating a potential leak of their proprietary information. In this case, the victims are Orange Leaf Software LLC and Union City Electronic Ventures.

**B1b. Cybersecurity Policies & Procedures for Criminal Activity**

The Access Control Policy, if enforced properly, could have prevented unauthorized access to protected computer systems within TechFite. This policy would outline who has access to which data and systems, and under what circumstances. It should enforce the principles of least privilege and separation of duties, ensuring that employees only have access to the data and systems they need to perform their jobs**.** The procedure would involve regular audits of user accounts to ensure compliance. Any accounts associated with employees no longer with the company should be deactivated, and usage logs would be regularly reviewed to detect any suspicious activity.

An Information Handling and Classification Policy could have prevented the potential violation of (NDAs) and misuse of proprietary information. This policy would outline how different types of information should be handled, stored, and shared. It would include requirements for protecting sensitive and proprietary information and ensuring that such information is only shared with authorized individuals.Regular audits of information handling would be conducted to ensure compliance with the policy. Specific measures for securely storing and separating clients’ information would be in place to prevent proprietary information from reaching competitors.

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

Neglect in safeguarding client’s proprietary information. The actor in this negligent act is TechFite’s Applications Division, particularly Carl Jaspers. The victims in this scenario are Orange Leaf Software LLC and Union City Electronic Ventures. Both companies provided TechFite with proprietary technical information as part of the preconsulting process and later found out that competitors were launching similar products.

Negligence in internal oversight and auditing. The actor here is TechFite’s IT Security Analyst, Nadia Johnson, and her superior, (CISO). They neglected to thoroughly audit internal operations, particularly in terms of user account audits, checking for escalation of privilege, and enforcing data loss prevention. The victims in this scenario are the entirety of TechFite. The negligence of the IT security team led to security breaches and a loss of trust from potential and current clients.

**B2b. Cybersecurity Policies & procedures for Negligent Activity**

TechFite likely had some form of an Access Control Policy in place. However, the enforcement of this policy was inadequate, as evidenced by the unauthorized access gained by the Business Intelligence unit. This could be due to the lack of regular audits, failure to keep the policy up-to-date with the organization’s evolving needs, or lack of effective training and awareness programs to ensure employees understand and adhere to the policy..

DLP policy, TechFite failed to prevent the unauthorized sharing of proprietary information. This could be due to a lack of sophisticated DLP tools, failure to keep the policy and tools updated to meet changing data landscapes, or inadequate training of employees regarding the importance of data security.

**C. Legal Compliance Summary for Management**

Computer Fraud and Abuse Act (CFAA): TechFite is not compliant. This is mainly due to the creation and use of fake user accounts to access sensitive information from other departments without proper authorization. Also, evidence of privilege escalation facilitated by Carl Jasper was identified, violating the regulations under CFAA.

Electronic Communications Privacy Act (ECPA): TechFite is not compliant. The unauthorized use and disclosure of electronic communications were facilitated through fake user accounts. Specifically, the company intercepted and disclosed emails without the consent of the parties involved, a clear violation of ECPA.