****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Ikeolu Ajiboye

**IHP4 Task 1: Legal Analysis**

**IHP4 Task 1: Legal Analysis**

**A1. CFAA and ECPA**

The CFAA correlates to the case because of the Applications Division of TechFites’ behavior. Specifically, because the Business Intelligence unit had unauthorized access to the HR, Finance, and legal divisions information; specifically, from their dummy accounts with escalated privileges which gave them access to sensitive information.

The ECPA correlates to the case because the Business Intelligence units’ email scanning and IP penetration of online based companies. Their actions violate the ECPA because they intercepted communications with no authorization.

**A2. Three Laws**

The TechFite Applications Division violated the CFAA by exploiting private information from potential clients. They accessed sensitive data with no proper authorization, which led to negative consequences for these clients while it benefited their competitors. This violation opens Techfite to legal action.

The Business Intelligence Unit used a system penetration tool called Metasploit to penetrate and scan the IP addresses of several Internet-based companies, which raises concerns about ECPA violations. Companies that were affected by the unauthorized surveillance have grounds to bring up legal action because their rights were violated.

TechFite's ill-success to protect sensitive client data and the potential mishandling of financial data points to negligence that could lead to a violation of SOX. This also is a violation that opens Techfite to legal action.

**A3. Duty of Due Care**

TechFite's Business Intelligence Unit lacked the proper oversight to protect sensitive information, which led to unauthorized access of client data. That led to competitors gaining access to protected information, causing potential harm to TechFite's reputation, and possibly leading to legal action from affected clients.

TechFite's failure to separate duties allowed unauthorized parties to access to sensitive departments. Which led to financial fraud, data breaches, and potential legal consequences TechFite and the employees that were involved.

**A4. SOX**

SOX applies to the case study due to the fraudulent activities from the companies Bebop Software, FGH Research Group, and Dazzling Comet Software. These companies were used as channels to manipulate sales figures for the division, which ultimately led to fraudulent financial reports, a violation of SOX regulations.

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

In the case study, one example of criminal activity was from the Business Intelligence Unit. They used sensitive client information that they were unauthorized to access. Specific culprits are Sarah Miller, Megan Rogers, and Jack Hudson. There are two victims of this criminal act, which are Orange Leaf, and Union City Electronic Ventures, because their confidential information was exploited and ended up being used by competitors.

Another example of criminal activity observed in the case study was the creation and use of dummy user accounts by the head of the Applications Division, Carl Jaspers; he also had unauthorized access to sensitive information. The victim of this is TechFite, as the unauthorized access allowed Jaspers to obtain sensitive information from different departments within Techfite, including the finance, human resources, and legal department.

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

The Applications Division's Business Intelligence Unit lacked proper internal oversight, they didn’t audit user accounts, their privileges, and data loss prevention on sensitive documents, which ultimately allowed unauthorized access and potential data breaches.

Also, without the use of the principle of least privilege, all workstations and computers in the Business Intelligence Unit had full administrative rights, which let employees gain access sensitive information without the proper authorization.

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

In the case study, one example of negligence was from the Business Intelligence Unit. They used sensitive client information that they were unauthorized to access. The actors were Sarah Miller, Megan Rogers, and Jack Hudson. The two victims of their negligence are Orange Leaf, and Union City Electronic Ventures, because their confidential information was exploited and ended up being used by competitors.

Another example of negligence observed in the case study was the creation and use of dummy user accounts by the head of the Applications Division, Carl Jaspers; he also had unauthorized access to sensitive information. The victim of this negligence is TechFite, as the unauthorized access allowed Jaspers to obtain sensitive information from different departments within Techfite, including the finance, human resources, and legal department.

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

If the Applications Division's Business Intelligence Unit had proper internal oversight, audited user accounts and privileges, and implemented data loss prevention on sensitive documents, they wouldn’t have allowed unauthorized access to cause potential data breaches.

Also, if they used the principle of least privilege, all workstations and computers in the Business Intelligence Unit would not have had full administrative rights, which in turn would not let employees gain access sensitive information without the proper authorization.

**C. Legal Compliance Summary for Management**

TechFite was non-compliant with the CFAA, the ECPA, and SOX. They violated the CFAA by exploiting private information from potential clients. They violated the ECPA by penetrating and scanning the IP addresses of several Internet-based companies. They also violated SOX by mishandling financial data. Senior management can address these issues by implementing proper cybersecurity procedures and taking corrective actions to ensure proper legal compliance and prevent further incidents.