****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Ali Gautreaux

**IHP4 Task 1: Legal Analysis**

**IHP4 Task 1: Legal Analysis**

**A1. CFAA and ECPA**

CFFA- Computer Fraud and Abuse Act: This act prohibits intentionally accessing computer without authorization.

The Applications Division Business intelligence (BI) Unit had the ability to create dummy user accounts that had full administrative rights on the computers, that allowed them to gain be able gain unauthorized access to departments that hold sensitive information shouldn’t be handled by untrained personnel.

ECPA- Electronic Communications Privacy Act: This act protects any form of Electronic Communications that have being made, being sent, or being stored on a computer.

Recreating accounts using past users who not worked for the company in over a year, user who are not original individuals to gain access past electronic communications through email and their past locations and used for future potential malicious activities.

**A2. Three Laws**

CFFA:

The Principle of Least Privilege (PoLP) was not being upheld properly. The dummy accounts that were created by the BI Unit that had full admin rights, where able to use their escalated privileges to gain access to the Human Resources (HR), Financial and Legal departments, which they did not have authorization to be accessing.

ECPA:

The security police of Auditing User Account Management were not being enforced.

Carl Jaspers requested to create two accounts using past employee who have not worked company in over a year, with these past employees being tied to these accounts their previous emails and location can be accessed by one using the new accounts. These accounts are noted to be in constant communication with non-client parties of TechFite along with potential preform Social Engineering tactics against various companies.

SOX:

There is no evidence of TechFite every having independent of their financial statements and records. The IT Security Analyst Nadia Johnson had never performed her own audit on TechFite financial statements and records, she also never had outside auditing party come look over everything as well.

**A3. Duty of Due Care**

Carl Jasper did not uphold the nondisclosure agreement (NDA) with Orange Leaf that was executed by Applications Division. It was required as part of the pre-consulting process that questionnaire that included technical information about how Orange Leaf’s products work, these questions were answered by Orange Leaf’s CEO, Chief Technology Officer, along with their Lead Software Engineer. When Orange Leaf deiced to not go with Applications Division, it was noted by Noah Stevenson that several months later that one of there competitors was lunching products very similar to their own, that they divulged in confidence during the pre-consultation.

IT Security Analyst Nadia Johnson of TechFite’s Applications Division reviewed the reports form the Chief Information Security Officer (CISO), that showed they organization performed proper steps for protecting the network form external threats. When it came to reviewing possible internal threats for company there was a blanket summaries that there are no i

**A4. SOX**

TechFite did not comply with SOX requirements when it comes to properly reporting finances, there are three shell companies that were found within audit of client’s data base list, by investigators.

The three companies appeared as legitimate companies, but they had no internet presence unlike the other companies who are apart of the client list. The three companies are also registered under Yu Lee, a follow alumnus of Carl Jaspers.

When all three of companies that are owned by Yu Lee, it was founded that they pay for services at TechFite with checks being drawn from the same bank which is Freeworkers’ Pennsylvania Bank.

These three companies appear being used to move money into TechFite’s sales figures for division help boost their high sales to drawn in new investors. It was also noted that TechFite’s does not do any business with Freeworkers bank there where not accounts to be found which allowing for off the book method payments to being made elsewhere.

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

Preforming unauthorized system penetration, it was founded that Metasploit common tool used for penetration testing was found on BI Unit computers, which the hard driver showed that recently penetration and scanning activities had been taking place. BI Unit is made up of the Senior Analysts Sarah Miller along with Analysts Megan Rogers and Jack Hudson. Sarah Miller was noted to have the most traffic in scanning other companies’ networks. There where several internet-based companies who affected by this attack.

Creating False sales figures,

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

State and describe a specific cybersecurity policy (by name i.e. *Password Lockout Policy*”) and accompanying procedure that could have helped prevent a specific instance of criminal activity you observed.

State and describe a second specific cybersecurity policy (by name i.e. *Password Lockout Policy*”) and accompanying procedure that could have helped prevent a second specific instance of criminal activity you observed**.**

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

Identify and discuss a specific negligent act you observed in the case study. Be sure to include (1) what the activity was, (2) what specific actor (person/group/entity) committed the activity, and (3) what specific person/group/entity was the victim of the activity.

Identify and discuss a second specific negligent act you observed in the case study. Be sure to include (1) what the act was, (2) what specific actor (person/group/entity) committed the act, and (3) what specific person/group/entity was the victim of the activity.

The actor, activity, and victims for your first example need to be different from those in your second example.

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

State and describe a specific cybersecurity policy (by name i.e. *Password Lockout Policy*”) and accompanying procedure that could have helped prevent a specific instance of negligent activity you observed.

State and describe a second specific cybersecurity policy (by name i.e. *Password Lockout Policy*”) and accompanying procedure that could have helped prevent a second specific instance of negligent activity you observed**.**

**C. Legal Compliance Summary for Management**

Succinctly recap the compliance status (actually state “compliant” or “not compliant”) of each law discussed in parts A and B above. Discuss contributing factors for each law. Provide a paragraph or two to complete this section.

**References**

Annotate sources of any quoted, paraphrases or summarized content used. Delete this slide prior to submission if you have none to include. Delete the reference page/section if you do not have quoted, paraphrased, or summarized content.