****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Matt Lorenzen

**IHP4 Task 1: Legal Analysis**

**IHP4 Task 1: Legal Analysis**

**A1. CFAA and ECPA**

*Identify and discuss a specific instance where information on a protected computer was accessed without authorization. This activity constitutes criminal activity that violates the CFAA.*

The findings within the BI Unit indicate Metasploit was installed on multiple machines and that further evidence indicates penetration and scanning activity into multiple external companies IP space.

*Identify and discuss a specific instance of unauthorized access, use, disclosure, or interception of electronic communications. This activity constitutes criminal activity that violates the ECPA.*

The BI Unit gaining access to other groups and units within TechFite without authorization. Evidence was found to support activities of privilege escalation has occurred on accounts to permit access to multiple departments within TechFite without authorization to perform such acts. Logging taking from network monitoring further confirms this evidence.

**A2. Three Laws**

*Identify and discuss a specific instance of negligence that facilitated the actual criminal activity you noted involving ECPA (you can use different laws if you like). Then elaborate on how the follow on actual criminal activity is justification of legal action.*

The BI Unit at TechFite was not enforcing “least privilege” for their department. Without least privilege enforcement members of the BI Unit were able to install software and tools that allowed for scanning of both internal and external targets. This further allowed those members of the business unit to escalate privileges within other departments.

*Identify and discuss a specific instance of negligence that facilitated the actual criminal activity you noted involving CFAA (you can use different laws if you like). Then elaborate on how the follow on actual criminal activity is justification of legal action.*

The aforementioned actions violate the CFAA section wherein “Accessing a Computer and Obtaining information” can include internal systems accessed without authorization and can carry a sentence of up to 1 to 5 years.

*Identify and discuss a specific instance of negligence that facilitated the actual criminal activity you noted involving SOX (you can use different laws if you like). Then elaborate on how the follow on actual criminal activity is justification of legal action.*

The lack of coverage on the critical issue of safeguarding sensitive and proprietary information for previous, potential, and existing clients indicates negligence. This negligent behavior attributed to the BI Unit being able to further their tactics of abusing vulnerabilities and compromising systems that were not safeguarded correctly.

*Additional clarification:* Explain how **three** laws, regulations, or legal cases apply in the justification of legal action based upon negligence described in the case study. Example: If a person responsible for locking a door forgets/fails to do so, and later that evening a thief entered that door and burglarized the building. The negligent action/inaction of the person who failed to lock the door allowed a criminal with no association to walk in after hours and commit the criminal act of theft. The negligence becomes a basis for the activity, but the actual crime committed is where legal action will be directed.

**A3. Duty of Due Care**

*Identify and discuss two (2) specific examples where you observed lack of duty of due care.*

The documentation on the internal oversight for the BI Unit utilizing “blanket summaries” that no “irregularities” were found within the internal operations is the first example of lack of duty of care. Any statements of audit for threat management should be detailed and include examples and accounts used for testing in order for the appropriate teams to perform follow up.

By not enforcing separation of duties within the BI Unit TechFite risks their brand integrity and displays a lack of duty of care. By allowing the BI Unit privileges that could allow them to abuse the customer base by creating accounts is a risk.

**A4. SOX**

*State why SOX is applicable to the company based on the type of company it is/type of business it conducts and discuss a specific SOX violation you observed in the case study.*

TechFite is a publicly traded organization on the NASDAQ, and therefore is bound by the SOX Act. I believe the largest SOX violation to be found within the case study to be the “internal compromise via covert techniques” of various “TechFite groups and units”. This is an insider threat and should have been reported to accordingly. Additionally, TechFite was unable to “prove their funds were authentic”.

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

Identify and discuss a specific criminal 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.

K

1. Carl Jaspers

2. Dummy users accounts created as per his request have been used to compromise other groups and units within the TechFite divisions. This was done without proper authorization.

3. Potential victims are Noah Stevenson from Orange Leaf Software and Ana Capperson with Union City Electronic Ventures.

Identify and discuss a second specific criminal 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.

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

1. Nadia Johnson

2. Failure to disclose as per Section 404.B Sarbane’s Oxyley, Nadia Johnson

3. Shareholders for TechFite

**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**.**

Failure to prevent criminal activity, DLP, Chinese Wall, Separation of Duties, Auditing, Account Creation, Acceptable Use. Identify 2 of these that tie to criminal activity and how they present in a case study.

**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**.**

Topics from B1a but discuss the negligence

**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. What it was, were they compliant, and why

**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.

<https://www.sarbanes-oxley-101.com/sarbanes-oxley-checklist.htm> Section 404.B