****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Matt Lorenzen

**IHP4 Task 1: Legal Analysis**

**Task 1**

**A1.**

CFAA specific example

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.

ECPA specific example

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.**

List the 3 specific laws you will discuss and the specific activity that justifies legal action

Law 1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Negligent Activity
  + 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.
* Criminal Activity
  + This further allowed those members of the business unit to escalate privileges within other departments. This allowed for compromise of systems protected under the CFAA

Law 2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Negligent Activity
  + 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.
* Criminal Activity
  + Violation of the CFAA

Law 3 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Negligent Activity
  + 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.
* Criminal Activity
  + Violation of Sarbanes Oxley

**A3.**

Duty of care example 1

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.

Duty of care example 2

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 application example

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.**

List the criminal activity that occurred; the actor that committed the activity; and the victim of the activity

Example 1

* Activity: 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
* Actor(s): Carl Jaspers
* Victim (s): Potential victims are Noah Stevens from Orange Leaf Software and Ana Capperson with Union City Electronic Ventures

Example 2

* Activity: Failure to disclose as per Section of 404.B Sarbanes Oxley
* Actor(s): Nadia Johnson
* Victim(s): Shareholders of TechFite, as non-disclosure can significantly impact financials for a corporation

**B1b.**

List two specific cybersecurity policies and accompanying recommended procedures and what activity they will address

Policy 1

* Procedure: Failure to prevent criminal activity, DLP, Chinese Wall, Separation of Duties, Auditing, Account Creation.
* Criminal activity: Failure to comply with Section 404 Sarbanes Oxley. Maintaining a management assessment of internal controls.

Policy 2

* Procedure: Section 509 Sarbanes Oxley – Real Time Disclosure, this requires an organization to quickly communicate material changes related to its financial state, with data included to the public.
* Criminal activity addressed: TechFite leadership is unable to speak to the sales figures from the sales division, there may be funds that are being included to a bank that is “off-the -books”.

**B2/B2a.**

List two specific individuals/groups that acted negligently and who the victims of that activity were

Negligent actor 1: Sarah Miller

* Activity: Scanning other companies’ networks
* Victim 1: TechFite customers, such as Noah Stevenson from Orange Leaf Software LLC.

Negligent actor 2: Megan Rogers

* Activity: Similarly scanning both external and internal network devices to further financial gains.
* Victim 2: Customers of TechFite, such as Ana Capperson from Union City Electronic Ventures.

**B2b.**

List two specific cybersecurity policies and accompanying recommended procedures and what activity they will address

Policy 1

* Procedure: Least Privilege – limiting access employees have to prevent insider threats and inappropriate of computers.
* Negligent activity addressed: This addresses the ability of the BI Unit having permissions to scan internal and external computers. With “Least Privilege” in place, the BI Unit would not have access to install Metasploit. (ArcSight, “The Intersection of Sarbanes-Oxley and Insider Threats”)

Policy 2

* Procedure: Separation of Duty
* Negligent activity addressed: Members of the BI Unit were able to create customers/clients for TechFite, then report sales and post sales on the system. This should not be handled by the same person, but instead should be handled by three separate employees/divisions of TechFite. (ArcSight, “The Intersection of Sarbanes-Oxley and Insider Threats”)

C. Summarize compliance status of the laws discussed in parts A & B.

In summary of the TechFite case study, it has been determined that TechFite was in violation of Section 404 and 409 of the Sarbanes Oxley Act. The company failed to disclose and insider threat, through negligence and in-action TechFite employees have been allowed to execute and act with malice for financial gain.

References

“The Intersection of Sarbanes-Oxley and Insider Threats.” *Computerworld*, 16 Mar. 2006, www.computerworld.com/article/2562262/the-intersection-of-sarbanes-oxley-and-insider-threats.html.

*Sarbanes-Oxley Compliance Checklist*. www.sarbanes-oxley-101.com/sarbanes-oxley-checklist.htm. Accessed 5 Nov. 2022.

(☑ Sarbanes-Oxley Compliance Checklist)