****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Matthew Lorenzen

**IHP4 Task 2: Ethics and Cybersecurity**

**IHP4 Task 2: Ethics and Cybersecurity**

**A1/A1a. Ethical Guidelines Related to Information Security**

**Example One:**

At eBay, the principal of separation of duties is heavy enforced. This is due to eBay needing to remain compliant for PCI-DSS. Each business unit with eBay is isolated from each other. This forces team to engage the appropriate people and follow the processes and governance in place to protect not only the company but the employees as well. In comparison, the business unit in the case study did not enforce separation of duties and was able to create, modify, and manipulate customer information including sales. This helps move the compliance from a “check the box” action once a year to being an “ethical guideline” where eBay employees understand separation of duties is there to protect the customers and if we act ethically, we do just that, all while improving the customer experience. As eBay customers know when they need assistance, they can “trust” what is being done and how their information is handled.

**Example Two:**

The next ethical issue I see is TechFite using a computer to do harm this goes against EC Council’s guideline of “Neither associate with malicious hackers nor engage in any malicious activities,” many organizations practice the ethical approach like that of a doctor, “Do not use a computer to harm other people.” (EC-Council Logo) This same practice is held at corporations like eBay and the FAANG companies. TechFite used their systems to compromise other machines within and external to their network for gain. This has a direct impact on multiple individuals and companies.

**A2. Unethical Practices**

**Example One:**

Carl Jasper had a conflict of interest with Yu Lee. Yu Lee had three companies registered to him in Nevada, Carl Jasper went to school at Standford University with Yu Lee. These three companies had no internet presence, however were paying for services at TechFite. This relationship should have been disclosed as both parties have now both performed actions that may be considered “a conflict of interest or otherwise damage the reputation of the employer.” (ISSA International)

**Example Two:**

Sarah Miller, was using the TechFite systems to perform scans of internal and external computers in a malicious manner. (EC-Council Logo) Sarah Miller engaged in malicious activities, this ties back to the EC Council guideline related to “associating with or engaging in malicious activities.”

**A3. Factors**

**Example One:**

Sarah Miller’s behaviors and actions as a senior analyst were inappropriate and had direct influence on Megan Rogers and Jack Hudson. With Sarah being in a position of influence, Megan and Jack felt comfortable enough to perform similar activities acting un-ethically. This ties back to the EC Council guideline related to “associating with or engaging in malicious activities.”

**Example Two:**

Carl Jaspers and Nadia Johnson – Carl Jaspers would give Nadia’s boss, the CISO positive feedback for annual reviews, where Nadia would receive increases in compensation. Nadia and Jaspers are frequently seen at social gatherings and sharing gifts. This is un-ethical as Jaspers could actions could easily be interpreted as “bribery” or “quid-pro-quo,” to entice Nadia into overlooking security events that could be related to the malicious activities.

**B1. Information Security Policies**

**Example One:**

The first policy that would have provided preventative measures within TechFite would be “Network Security Policy.” This is due to the BI unit having the ability to use Metasploit to scan machines at other companies, a good Network Security Policy would include network monitoring that would trigger an alert for malicious traffic if a Metasploit scan was kicked off from within the network. This would have significantly reduced the threat to those external companies’ intellectual property as well.

**Example Two:**

The second security policy that would have benefit TechFite would have been an “Firewall Policy.” With a properly configured “Firewall Policy” in place, those participating in scanning external companies’ traffic would have been detected by most next generation firewalls and dropped. This would have provided not only a security measure to potentially stop the malicious activity, but would also provide a layer of event detection to alert the Security Analysts to the events.

**B2. SATE Components**

**Example One:**

The first component I would choose would be the “who will participate in the training”, I feel that all employees should be required to take the SATE training. A blanket coverage to ensure all individuals within TechFite have the same base-level of training. This removes ambiguity surrounding who has been trained and who has not been.

**Example Two:**

The second component of SATE that I would choose would be the repercussions for non-compliance, like an acceptable use policy, everyone agrees to it, is expected to adhere to it, and when someone fails to do so, repercussions must be enforced. This can be seen as a fear tactic at times, however taking the time during the training to explain the “why” can clear up any ill feelings. Enforcing the baseline ensures the company and the employees are protected.

**B2a. SATE Program Communication**

The SATE program would be communicated via email, directing employees to a work-site such as Workday that can then keep track of who has and has not taken the training.

**B2b. SATE Program Justification**

**Example One:** The SATE program will help protect TechFite against allegations of “bribery” or “fraternization” by educating the employees on what is acceptable relations with co-workers. This will help mitigate against the situation between Nadia Johnson and Carl Jasper that could be perceived as fraternization.

**Example Two:** The SATE program will help train TechFite on the acceptable use policy and ensure employees are aware of what can be considered malicious activity. This will help mitigate against situations like Nadia Johnson using Metasploit to scan external systems.

**C. Ethics Issues and Mitigation Summary for Management**

Succinctly recap the ethical issues discussed in parts A and B along with your recommended mitigation for each of them. Provide a paragraph or two to complete this section.

**Example One:**  The first ethical challenge is the questionable relations between Carl Jaspers and Yu Lee. I feel this can be mitigated through a SATE program and reporting hotline.

**Example Two:** The second ethical challenge is the situation between Nadia Johnson, Megan Rogers and Jack Hudson. Educating the employees (SATE) and providing them an anonymous way to report the behavior of Nadia Johnson could have prevented further scans from being performed by Megan and Jack.

**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.

“Cybersecurity Ethics: Establishing a Code for Your SOC.” *Security Intelligence*, Koen Van Impe, 8 Jan. 2022, https://securityintelligence.com/articles/cybersecurity-ethics-establishing-a-code-of-conduct-for-soc/.

EC-Council Logo. “Code of Ethics - EC-Council.” *EC-Council Logo*, 15 Dec. 2021, [www.eccouncil.org/code-of-ethics](http://www.eccouncil.org/code-of-ethics).

ISSA International. “Code of Ethics.” *ISSA International*, 9 Feb. 2019, www.issa.org/code-of-ethics.