Quinton Green

Legal Issues in Information Security

Task 2: Ethics in Cybersecurity

**A.  Address ethical issues for cybersecurity by doing the following:**

**1.  Discuss the ethical guidelines or standards relating to information security that should apply to the case study.**

Some ethical guideline standards for information security that apply to this case study are monitoring of employees, protect privacy, and not collect data illegally. If there were policies and procedures set in place to monitor employees and protect privacy of potential clients no data would have been collected illegally by the analyst team, the information gathered from the potential client questionnaire would have been protected and not compromised and the employees conducting the criminal activity would have been discovered sooner.

1. **Justify your reasoning.**

The reasoning for these standards is TechFite needs corporate responsibility. There are laws in place TechFite employees violated with Union City Electronic Ventures and OrangeLeaf’s intellectual property due to TechFite’s lack of security safeguards and policies which allowed employees to misuse information and participate in unethical activity

2**.  Identify the behaviors, or omission of behaviors, of the people who fostered the unethical practices.**

The behaviors of IT Security Analyst Nadia Johnson fostered unethical practices because she would be more inclined to follow anything Carl Jaspers suggests because he provides perks and incentives for her. It was reported he regularly gives here positive reviews which increase her pay. There is a conflict of interest here which would promote unethical behavior in order to get a higher salary. This incentive could be the factor that made her lax in auditing the client list database where several fake accounts were found. Her responsibility to analyze IT security is compromised because those fake accounts were needed by Carl for financial gain and he in turn rewards her with raises.  Yu Lee who went to graduate school with Carl Jaspers is linked to alleged fake companies who are clients of TechFite that are helping to boost sales figures for the financial unit. This unethical behavior would make TechFite appear more lucrative and appealing to new potential clients because it gives the illusion of success in the industry. Sarah Miller the senior analyst not only was scanning other companies’ networks but directed Analysts Megan Rogers and Jack Hudson to do so as well. Jack Hudson clearly was aware of the unethical practices because the report found that he was a member of the Strategic and Competitive Intelligence Professionals (SCIP), which has a very strong code of ethics. Carl Jaspers fostered unethical practices of requesting creation of accounts using ex- employee information and appears to be the ringleader of the whole operation.  All the employees listed omitted corporate responsibility and ethical standards

**3.  Discuss what factors at TechFite led to lax ethical behavior.**

There are several factors that led to lax ethical behavior. The lack of (SATE) security awareness training and education left employees open and unaccountable. The lack of Acceptable Use Policy and Employee Workplace Monitoring allowed employees to engage in undesirable behavior by being unmonitored. The principles of least privilege and separation of duties were not enforced because all employees had administrative privileges and were able to see all information of every department. There were no safeguards in place to protect the intellectual property of potential new clients. There was a lack of corporate responsibility and internal control monitoring. TechFite lacks a board of directors as well which would hold executive management accountable.

The personal relationship between IT Security Analyst Nadia Johnson and Carl Jaspers along with Yu Lee’s personal ties to Carl Jasper played a role in lax ethical behavior. Also, Carl Jaspers’ misuse of authority and no security governance system in the company to enforce a checks and balances system for executives. The fact that former employees accounts were still active after years of not working there was a vulnerability that was taken advantage of. There was a lack of accountability. There are no strong compliance policies set under SOX standards to audit and monitor internal controls, code of ethics and corporate responsibility, no policy for employee relations, and no security policy set to prevent information security abuse.  

**B.  Describe ways to mitigate problems and build security awareness by doing the following:**

**1.  Describe two information security policies that may have prevented or reduced the criminal activity, deterred the negligent acts, and decreased the threats to intellectual property.**

Two information security policies that may have prevented or reduced criminal activity are the Acceptable Use Policy and Workplace Privacy and Monitoring Policy. The Acceptable Use Policy states that employees must not tamper with IT resources or data on those resources. Employees should not access any data they do not have a business reason to see. No personal use of organizational IT resources is allowed. Do not use IT resources to circumvent security measures. IT resources may be monitored to ensure employee compliance – This policy will deter activity by making employees aware there are consequences for misuse. The [Workplace Privacy and Monitoring Policies-](https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/reader.action?docID=6380267&ppg=392#ppg=566)assess employee productivity, monitors operational use of IT resources, monitors policy compliance, monitors the use of the organization’s intellectual property, investigates allegations of wrongdoing, and manages risk and protecting against legal liability. These policies would help IT security to discover any malicious activity taking place and mitigate it. If the employees were monitored, then intellectual property of Union City Electronic Ventures and OrangeLeaf would have never been compromised and be able to be sent to their competitors

**2.  Describe the key components of a Security Awareness Training and Education (SATE) program that could be implemented at TechFite.**

The key components of the SATE program are education, engagement, effectiveness. Employees need to be educated about the threats, risks, and consequences for breaches in information security and held accountable. Engagement is important and needs to be accepted and implemented from the executive down the company hierarchy. If the people at the head of the company don’t engage and value security awareness training, you can’t expect the rest of the employees to value it. Effectiveness is important because strict policies and procedures need to be set in place and conveyed to staff to gain the understanding of the severity information security.

**a.  Explain how the SATE program will be communicated to TechFite employees.**

The SATE program will be communicated to TechFite employees through training. The training will consist of mandatory video module courses upon hire for new employees or scheduled training for existing employees and periodic refresher courses throughout the duration of employment. All material will be updated to reflect new threats as well and educate about known threats.

**b.  Justify the SATE program’s relevance to mitigating the undesirable behaviors at TechFite.**

The SATE program is relevant to mitigating undesirable behaviors because many people are not aware how the human component contributes to information security threats. SATE will educate employees as well as inform the various types of security threats, abuse, and consequences professionally and legally to engaging in undesirable behavior.

**C.  Prepare a summary directed to senior management (*suggested length of 1–2 paragraphs*) that states TechFite’s ethical issues from Part A and the related mitigation strategies from Part B.**

To the Senior Management of TechFite,

It has been found that TechFite has ethical issues. These issues involve monitoring employee activity, collecting data illegally and misuse of intellectual property, and privacy protection. Several employees were found through an audit process to have allegedly participated in unethical and illegal behaviors which led to intellectual property of former potential clients Union City Electronic Ventures, OrangeLeaf to be compromised and sent to their competitors due to the lax ethical behavior. For the sake of the company and its future business operations and endeavors to solidify new clientele I recommend implementing a mitigation plan. This plan will consist of implementing an Acceptable Use Policy, Workplace Privacy and Monitoring Policy which will monitor and detect misuse of business IT information by TechFite employees, a (SATE) Security Awareness Training and Education program, setting a principle of least privilege to only give employees access and user rights according to there job position and duties and setting up information security governance according to the Sarbanes-Oxley (SOX) Act.

References:

1) Grama, Joanna Lyn. *Legal and Privacy Issues in Information Security*, Jones & Bartlett Learning, LLC, 2020.*ProQuest Ebook Central*, http://ebookcentral.proquest.com/lib/westerngovernors-ebooks/detail.action?docID=6380267.

2) [Security Awareness Training and Education (SATE) Archives - PeopleSec™-](https://peoplesec.org/category/security-awareness-training-and-education-sate/#:~:text=Security%20Awareness%20Training%20%26%20Education%20Program%2C%20Crucial%20Elements,Insight.%20...%206%20Measure%20Everything.%20...%207%20Customize) https://peoplesec.org/category/security-awareness-training-and-education-sate/