Ethics and Cybersecurity

A1/A1a

Ethical guidelines and standards that apply to this case study are the policy of best practices and standards and the ability to refrain from activities that create a conflict of interest. TechFite was not in compliance with ISSA's policy of best practices and standards. This was evident in the lack of documentation and the overuse of administrative privileges. The lack of documentation was not in the best practice of the company. This led to oversights that put client information at risk. Administrative privileges should have required authorization at a higher level but were given to anyone with a computer in the BI unit. This led to unauthorized access of financial information. Also, Carl Jaspers would invite Nadia Johnson to social events and gave positive reviews of her work in annual reviews. This created a conflict of interest that is unethical because she was not doing her job and allowed fraudulent accounts to be made undetected.

A2

Carl Jaspers and Sarah Miller both fostered unethical practices. Carl Jaspers created three fake companies that were reporting sales profits, which inflated the sales of TechFite. This is unethical and fraudulent because it gives a false idea of company efforts to investors and stakeholders. Sarah Millers fostered an unethical work environment when she had Megan Rogers and Jack Hudson illegally gather info on other internet-based businesses. Sarah Miller and her co-workers did not have the consent of the internet companies to conduct this search.

A3

Lax ethical behavior of the BI unit can be tied directly to IT analyst Nadia Johnson and Carl Jaspers. Nadia was responsible for reporting to the CISO and failed to do so when it came to the documentation of internal operations. Nadia's shortcomings could have been overlooked because of her relationship with Jaspers. Jaspers frequently gave positive recommendations of her work in annual review, invited her to many social events, and gave her gifts. This is unethical because Jaspers oversees Nadias job, and it can and does display favoritism. Also, there was no separation of duties. This gave the BI unit access to proprietary information not needed for their job duties. Proper administrative controls would have kept it safe.

B/B1

Two information security policies that could have deterred criminal acts were the principle of least privilege and proper audits. The principle of least privilege was not used in the BI unit of TechFite. Every

computer had full administrative privileges. This made it so Carl Jaspers could create fake clients and report false sales numbers. The full visibility that each unit had into another unit is unethical. Had this policy of least privilege been in place, Jaspers would not have been able to change the sales information. Proper audits should have also been conducted. Since Nadia Johnson reported no documentation of internal operations to the CISO they never had any reason to be alerted to the wrongdoings of the BI unit. Had proper audits been conducted the escalation of privilege and the illegal gathering of info would have been noticed sooner.

B2

A key component of the SATE training programing that could be implemented at TechFite would be having a third party to oversee the activities of the company. This would prevent any conflict of interest. The third party could contact the CISO with any issues and make sure training material is sent to employees. Also, the consequences for failure to adhere to laws should be written and clearly stated. This would also give the company an alert when policies were violated. There would also be evidence to determine where issues are.

B2a

Notice of the SATE program would be given to employees through email. A virtual meeting could be held with all members to conduct the training. This way all employees would know of the changes and hear the information being provided. Attendance could be taken at the end of the meeting to ensure those that did not attend could be reprimanded and given the information in a one-on-one manner.

B2b

A relevant SATE program to mitigate undesirable behaviors would be training on acceptable use and more knowledge on intellectual property rights. Training on acceptable use would teach employees what is acceptable when using technology in TechFite's environment. This would mitigate the issues with units examining and editing information that is not relevant to their unit. Also, if employees had more knowledge on the laws and regulations of intellectual property they could better adhere to the guidelines of those policies and keep the information of the clients at TechFite safe from leaks.

Summary

Two of the main issues at TechFite are employees accessing data not relevant to their unit and lack of separation of duties. Employees with unrestricted administrative controls can change, edit, or destroy information. As mentioned in part B, Jaspers created fake accounts to influence financial information. This would have been mitigated by implementing the principle of least privilege which would have required authorization from someone above him. This would have made it harder to commit fraud and

also alerted higher-ups to wrongdoing. The lack of separation of duties allowed the Bi unit to see other units' information, as mentioned in part B. By enacting separation of duties this would not have happened. The access to financial information would have been kept confidential for those that need it for their job duties.