IHP4 Task 2: Ethics and Cybersecurity

A1/A1a. Ethical Guidelines Related to Information Security

An ethical guideline related to information security used by ISC2 states: “The safety and welfare of society and the common good, duty to our principals, and duty to each other, require that we adhere, and be seen to adhere, to the highest ethical standards of behavior” (ISC2, n.d.). By adopting this guideline, TechFite can prevent breaches to their NDAs and confidential data disclosure from occurring with prospective clients. This guideline ensures that TechFite operates with the highest integrity and will take the necessary measurements to protect client information.

Another ethical guideline related to information security used by GIAC states: “Information security professionals are afforded a great deal of responsibility and trust in protecting the confidentiality, integrity, and availability of information assets for the organizations within which they work" (GIAC, n.d.). Adapting this guideline will reduce the chances of privilege escalation and ensure users have the correct account permissions.

A2. Unethical Practices

An unethical practice was observed when Nadia Johnson failed to audit accounts in TechFite’s client’s database—allowing users within the BI Unit to create fake user accounts and perform privilege escalation techniques to access confidential information from different divisions without authorization.

Another unethical practice observed was the close relationship between Nadia Johnson and Carl Jasper. Nadia failed to report irregularities in internal operations; this allowed Carl and the BI Unit to perform unauthorized penetrations and scans to intercept IP traffic of other company IP addresses and networks.

A3. Factors

A specific factor that led to lax ethical behavior in the TechFite case study was the lack of regular auditing of user accounts and permissions. This led to the BI Unit creating fake user accounts and unauthorized access to confidential information within TechFite. By incorporating a policy for auditing user accounts and permissions, these types of activities can be significantly reduced.

The second factor observed was the failure to enforce a policy involving conflicts of interest between personnel at TechFite. This would lead to a close relationship between Nadia Johnson and Carl Jasper, leading to a conflict of interest. Carl would give glowing recommendations to Nadia's CISO, and in return, Nadia disregarded auditing internal operations.

B1. Information Security Policies

A Secure Disposal policy is designed to ensure that all confidential and sensitive information is appropriately destroyed. This policy includes methods of secure paper disposal and wiping of electronic media by means of degaussing, pulping, shredding or hiring a third party for destruction services. Pertaining to the TechFite case study, this would prevent dumpster diving from insider threats and retrieving confidential information such as financial records, customer data, or proprietary intellectual property. Carl Jasper had two dummy accounts with email addresses not associated with TechFite; the correspondence exchanged in emails frequently referred to intelligence gathering activities, referencing 'dumpster diving and 'trash surveillance.' By implementing the Secure Disposal Policy, TechFite can significantly decrease threats to intellectual property. For example, this would help ensure confidential NDA (Orange Leaf LLC) information does not fall into a competitor's hands.

A Data Loss Prevention Policy (DLP) is designed to protect sensitive information from being exfiltrated or misused by unauthorized users. DLP tools is used to monitor network traffic while preventing outbound emails containing sensitive information from leaving the company. TechFite could have prevented the breach of intellectual property for potential clients such as Orange Leaf LLC and Union Electronic Ventures by creating a DLP policy to prevent sensitive data from being exfiltrated and shared with non-authorized users. DLP ensures that sensitive information is continuously monitored and protected, including compliance with regulatory requirements.

B2. SATE Components

The first component of the Security Awareness Training Education Program (SATE) would be to hire a Chief Information Security Officer (CISO) to oversee and manage the program. The CISO is responsible for the security training program development, collaboration, leadership, and oversight, ensuring it aligns with the company's security objectives, regulatory requirements, and security policies.

The SATE program's second component would be ensuring mandatory participation for all employees. This is a crucial aspect for all TechFite employees to understand the importance of data protection, privacy, and reporting security events or incidents. TechFite can ensure its employees can identify and mitigate security threats such as phishing, social engineering, and data protection through mandatory participation.

B2a. SATE Program Communication

A multi-faceted communication strategy will be used to effectively communicate the Security Awareness Training Education (SATE) to TechFite employees. This ensures that all employees are aware of the program, its importance, security objectives, and how to participate. The CISO will send a detailed email introducing the SATE program, outlining the objectives and the importance of participation. Other forms of communication are newsletters, meetings, and visual aids such as posters and digital signage. This strategy ensures that all employees are informed and understand the SATE program and their roles and responsibilities to protect and maintain information security.

B2b. SATE Program Justification

An undesirable behavior observed was the misuse of TechFite's company computers and resources. By implementing the SATE program, proper training will provide guidance to employees regarding ethics in hacking and intelligence gathering other company's systems for their personal gain. This program will ensure that employees, particularly in the BI Unit to understand the ethical and legal implications of their actions.

Another undesirable behavior observed in the case study was the data breaches that occurred within TechFite.   This SATE program will help employees understand the importance of protecting information assets from various social engineering techniques such as dumpster diving, phishing, and best practices for securing data. This will help mitigate data breaches from occurring at TechFite in the future.

C. Ethics Issues and Mitigation Summary for Management

Ethical issues observed from the TechFite case study include the failure to protect confidential data and the lack of enforcement of policies to prevent conflicts of interest among personnel. The close relationship between Carl and Nadia created a conflict of interest, allowing Carl to manipulate financial data and inflate sales figures within TechFite. The failure to enforce proper security controls led to TechFite breaching its NDA with Orange Leaf. To mitigate conflict of interest, TechFite should enforce a policy that prevents personal relationships among personnel from influencing professional decisions. Implementing a SATE program will help mitigate confidential data from being breached. The SATE program would ensure that employees understand the importance of maintaining security controls and preventing unauthorized access.

References

ISC2 Code of Ethics. Cybersecurity Certifications and Continuing Education. (n.d.).

https://www.isc2.org/ethics

GIAC Code of Ethics overview. (n.d.). https://www.giac.org/about/ethics