Western Governor’s University

Legal Issues in Information Security

C841

Kern Grant

IHP4 Task 2: Ethics and Cybersecurity

IHP4 Task 2: Ethics and Cybersecurity

A1/A1a. Ethical Guidelines Related to Information Security

The Information Systems Audit and Control Association (ISACA) is an organization that governs Information systems. They provide members with a framework to comply with industry standards. One of their ethical guideline related to information security states, “Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties" (ISACA Code Of Ethics, n.d.). It relates to the TechFite data leaking incident. Carl Jasper TechFite Applications Division had two companies reporting similar experiences that led to their product propriety information leak. Orange Leaf Software LLC and Union City Electronic Ventures were the prospective companies considering working with TechFite. During their pre-consulting process, they completed Non-Disclosure Agreement executed by Jasper and questionnaires that contained valuable product information. After they denied TechFite services, months later, each company discovered that their competitor had launched a similar product. The mentioned competitors were TechFite clients. The similarity of the chain of events suggests TechFite and Carl Jasper did not comply with the mentioned ISACA ethical guideline. If TechFite had used the ISACA ethical guideline, their compliance framework would of better maintained the privacy and confidentiality of the companies, therfore preventing the adverse news reports as a company with bad practices.

The EC-Council organization aims to mitigate cyber-attacks by providing Information security training & programs. An ethical EC-Council guideline related to information security states, "Ensure all penetration testing activities are authorized and within legal limits. Not to take part in any black hat activities or be associated with any black Hat community that serves to endanger networks" (EC-Council Code of Ethics, n.d.). It relates to the criminal activities performed by the TechFite BI unit. The team used a Metasploit tool to penetrate and scan the IP addresses of several internet-based companies. Their actions were unauthorized as they accessed other companies' networks with criminal intent. Therefore, they would not comply with the Ec-council ethical guideline. If TechFite used and enforced the EC-Council guide, it would prevent these criminal actions by the BI unit.

The guidance and awareness of the ISACA and EC-Council standards could have prevented illegal activities by TechFite employees. The guideline framework provides compliance rules and regulations employees should follow, also the company and employees are accountable for their actions to be compliant.

A2. Unethical Practices

Nadia Johnson's behavior lacked duty of care, which led to unethical business practices by her and others. As IT Security Analyst, Nadia reviewed the TechFite network audit for her boss. The report summary suggests no internal abnormalities. However, the report lacked notes for safeguarding sensitive information and checking or monitoring the separation of duty, user account, and escalation privilege. It proved TechFite network security was poorly managed and vulnerable. Nadia did not attempt to correct or enforce security protocols. Her behavior fostered unethical practices within TechFite, making it easier for employees to mishandle or illegally access sensitive information.

Carl's Jasper, the head of the Tech Fite application division, abused his power by creating a dummy account. He requested that two user accounts be created and assigned to a former employee. As a result, the accounts are being used for illegal intelligence-gathering activities. A user account request and creation of this nature and all the activities fostered are unethical. Furthermore, it suggests that Jasper's authority manipulated the account creator to follow his unethical request for unauthorized intelligence activities.

A3. Factors

A lack of Duty of Care and Abuse of power are the factors that led to the lax ethical behavior within TechFite. Carl Jasper and Nadia Johnson are the individuals that set this tone for the employees. Their behaviors and position influence the company culture.

Carl Jasper is the head of the TechFite Application Division. Unfortunately, as the leader, he has patterns of abusing his power. For example, he requested that two user accounts be assigned to former employees, which were used for illegal data-gathering activities. The nature of the user account request and creation is unethical. It suggests that Jasper's authority manipulated the account creator to follow. In addition, his history with Yu Lee, and the evidence suggest shell companies are used to boost TechFite Sales to mislead investors. Jasper's work position and history with Yu Lee, who incorporated the three suspicious clients, make him a part of the deception because he benefits from increased sales and the appeal of the Application division. Jasper's unethical behavior is being used to benefit his work, yet it also influences his department staff. For example, Sarah Miller, the senior analyst and leader of the BI unit, directed her team to illegally penetrate and scan the Ip address of other companies for information. The BI unit also accesses sensitive information about the TechFite finance department via a dummy account. The abuse of power Carl Jasper illustrated is the same as Sarah Miller did to her team and the entire BI unit using their skill sets and software to access other companies' sensitive information illegally.

Nadia Johnson's lack of duty of care led to TechFite's lax ethical behavior. Her position as TechFite security analyst is to manage their security network. However, the techfite network is unsecured and vulnerable, evident by audit reports and employees' illicit activities. Nadia reviewed the audit reports for her boss; the summary reports no system abnormalities. However, it lacks critical internal network notes, such as safeguarding sensitive information and checks or monitoring user accounts, separation of duty, and escalation privilege. The lack of safeguarding sensitive information led to prospective clients' proprietary data leaks and their competitors launching similar products. Because of it, TechFite received negative news coverage. In addition, Carl Jasper and the BI unit actively use dummy accounts within the internal network to gain sensitive information; the workstation has full admin rights, and users perform unauthorized activities within and outside the TechFite network. The unethical behaviors are re-occurring because of the lack of security enforcement and accountability. The enforcement of security protocols provides an awareness of the consequences, therfore making employees second-guess their actions. The lax ethical behaviors result from Nadia Johnson's lacking duty of care for her job.

B1. Information Security Policies

Two Cybersecurity policies that may of helped TechFite prevented or reduced criminal activity and deterred negligent acts are the Account Creation / Termination Policy & Auditing Policy. Additionally, the enforcement of these policies can decrease threats to intellectual property.

Enacting the account creation/termination policy could protect sensitive data from being accessed. Two instances in case FIte include the negligent activities by Carl Jasper and The BI unit that threatened intellectual data. Carl Jasper requested two user accounts assigned to former employees. As a result, illegal data-gathering activities are performed using the account. The BI unit used dummy accounts to access sensitive information from other departments within TechFte. The pattern and reoccurrence of these activities started from an account. The Account Creation/Termination policy would have prevented or mitigated these negligent activities by denying the account creation, like Carl Jasper's case, or removing the reoccurrence of dummy account use like the BI unit and Jaspers scenario. The policy enforced decreases the threats to intellectual property via dummy accounts. And prevent the activities employees perform on the accounts.

The auditing policy and procedures help ensure proper cybersecurity measures are in place. A sufficient audit procedure highlights the network vulnerabilities that need repair. However, TechFite failed to perform a proper system audit, which led to recurring criminal activities. Enforcing the Auditing policy means all network systems and protocols are reviewed and summarized with documents. However, the TechFite audit report lacks plans or details for safeguarding sensitive data and other critical security policies. That issue led to potential clients Orange Leaf Software LLC and Union City Electronic Ventures, intellectual property leak. Sufficient Auditing could have prevented the leaks or reduced the reoccurrence, reducing the threats to intellectual property. Also, employees know they are being monitored and are more likely mindful of their actions which prevent or mitigate criminal activities.

B2. SATE Components

Two Security Awareness Training and Education (SATE) programs TechFite can implement are who will be required to participate (take/receive training) and what the repercussions of non-compliance are.

Everyone accessing TechFite internal network must take the Security Awareness Training and Education program. That includes all employees, vendors, stakeholders, etc. The extent of training and education varies depending on individual access level or department. However, everyone who uses the network should be educated and trained. Increasing users' awareness makes it more likely that they identify, mitigate or report suspicious activities that are harmful to network security. In addition, it creates a culture of people trained, educated, and mindful of TechFite security.

The second key component of SATE will be the repercussions for non-compliance. TechFite should enforce this as a policy to hold everyone accountable. Non-compliant users will have specific warnings to comply or receive consequences such as suspension or termination for violating company policy. The network's security affects everyone; therefore, it should be unforced for compliance purposes.

B2a. SATE Program Communication

The mandatory compliances of the Security Awareness Training and Education (SATE) program will be communicated electronically, verbally, and visually through the TechFite organization. By sending emails to all internal network users, C-suite directly expressing to department heads to share with staff, and lastly by posters and flyers at TechFite physical locations and application database.

B2b. SATE Program Justification

The relevance of the Security Awareness Training and Education (SATE) program can help TechFite mitigate undesirable behaviors by creating an organizational culture of accountable security collaboration. Two undesirable behaviors are power abuse and a lack of duty of care. Carl Jasper, the head of TechFite Application division, abuses his power by requesting to create two user accounts assigned to former employees. In addition, Nadia Johnson lacks Duty Of Care as a TechFites security analyst. She is responsible for managing the security of the Techfite network; however, their internal system is unsecured and vulnerable. Because of that, employees are actively performing criminal activities.

Implementing Security Awareness Training and Education (SATE) programs means you care for the security of the system network. Because security affects everyone involved, they should all be in accord with the SATE program. The enforcement of SATE program allows the security collaboration and accountability of everyone exchanging information. Users accessing TechFite's internal network are educated and trained on network security. As a result, users will be mindful of suspicious or illicit activities and accountable for their actions or lack of towards TechFite security. For example, it will prevent Carl Jasper's undesirable behavior. The account creator would deny his request to assign a former employee to the user account because he would have been aware of the illicit actions and be held accountable. The SATE program will also prevent Nadia Johnsons' undesirable behavior. Because she was not ensuring the security of the TechFite network, she will be non-compliant. Therefore according to the SATE component, she will have repercussions for her actions.

C. Ethics Issues and Mitigation Summary for Management

The ethical challenges from the case study include Duty of Care and Abuse of power. A lack of Duty of Care is one unethical behavior illustrated. For example, Carl Jasper and prospective clients' proprietary information leaked. Jasper and the BI unit use a dummy account for illegal intelligence-gathering activities. Also, IT security analyst Nadia Johnson's poor management of the TechFite internal network made it unsecured and vulnerable. Other unethical behavior includes the BI unit and Carl Jasper's abuse of power. The BI network, led by Sarah Miller, performed unauthorized penetration and scanning of other companies' IP addresses for data intelligence gathering. The senior analyst Sarah abused her power by directing her team's criminal activities. The other unit members did the same, using their skills and a Metasploit tool for illegal intent. In addition, Carl Jasper abuses his power by requesting user account creation and assignment to former TechFite employees. Being the Applications Division Head, he knows his request is illicit, and his position of authority suggests he knows the account creator will complete his request.

The mentioned challenges can be mitigated by implementing the Account Creation / Termination and Auditing Policy and adding the Security Awareness Training and Education (SATE) to educate and train all internal network users. Furthermore, the Account Creation / Termination policy monitors approve, and close user accounts as necessary. Which prevents or mitigates the incident of dummy accounts used for illegal data gathering activities. The Auditing Policy ensures sufficient monitoring and report summaries of the Techfite network. The aim is to get feedback on the network to correct, repair or implement new policies or systems to maintain network safety. If Techfite uses this policy correctly, it will prevent or mitigate the vulnerability of its system and all the employee's negligent activities. In addition, The SATE program provides all internal employees with education and training to keep the TechFite system safe. The collective effort strengthens their network security. The SATE program also prevents or mitigates individuals from participating in unethical activities because there will be repercussions for their activities.

References

1. Information Systems Audit and Control Association (ISACA) Code of Professional Ethics. n.d. Retrieved from **https://www.isaca.org/credentialing/code-of-professional-ethics**

2. The EC-Council organization Code Of Ethics. n.d. Retrieved from **https://www.eccouncil.org/code-of-ethics/**