****

Western Governor’s University

**Legal Issues in Information Security**

**C841**

[**Brian Pham**]

**IHP4 Task 2: Ethics and Cybersecurity**

**IHP4 Task 2: Ethics and Cybersecurity**

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

The guideline from (ISSA): "Provide diligent and competent service to principles." states the need for information security professionals to be diligent and competent in their work. In the context of the TechFite case study, this guideline could have helped prevent the unauthorized access and sharing of sensitive information if it was adopted. For instance, if the Business Intelligence unit had been more diligent and competent, they wouldn't have created fake accounts to gain unauthorized access.

The guideline from ISC2: "Protect society, the common good, necessary public trust and confidence, and the infrastructure." emphasizes the responsibility of information security professionals to protect not just the assets of their organization but also maintain public trust and confidence. In the TechFite case study, the unauthorized sharing of proprietary information and communication with non-clients not only put the company at risk but also damaged its reputation and trust with its clients. If this guideline was adopted and followed by the employees at TechFite, such activities that comprise public trust would have been avoided.

**A2. Unethical Practices**

Carl Jasper, a manager at TechFite, specifically requested the creation of user accounts in the names of former employees. This behavior fostered unethical practices, as it directly facilitated unauthorized access to protected information and potentially sensitive communication with entities outside the organization.

The IT department at TechFite showed a significant omission of behavior by failing to enforce the company's Access Control Policy effectively. The lack of diligence enabled the BI unit to gain unauthorized access to information from other departments, potentially leading to data breaches and violation of legal regulations

**A3. Factors**

The company's culture itself appears to have contributed to the unethical behavior. The acceptance of practices such as creating fake user accounts, not adhering to segregation of duties, and ignoring the need for strict enforcement of cybersecurity policies, suggests a culture of complacency or indifference towards ethical conduct. When the organizational culture itself does not prioritize ethical behavior, employees are more likely to engage in unethical activities.

To tie into the response above TechFite could have lacked adequate training programs focused on the importance of ethical conduct and cybersecurity. This meant employees were not fully aware of the implications of their actions. Without this awareness, the employees may not have fully understood the potential legal and ethical ramifications of their actions, which lead to unethical behavior such as unauthorized access to sensitive information.

**B1. Information Security Policies**

TechFite would greatly benefit from a proper Access Control Policy. This policy would dictate who has access to what information and systems within the organization. It would define the roles and responsibilities of each user with least privilege in mind. If properly implemented and enforced, would have prevented the BI unit's unauthorized access to sensitive data, thus mitigating the criminal activity and protecting intellectual property.

Moreover, the Access Control Policy would reduce negligence by emphasizing the importance of access controls and educating employees about the risks of unauthorized access. The policy would foster a security-focused culture, where employees are aware of their roles in protecting company data and intellectual property.

An information sharing policy would explicitly outline the dos and don'ts of data sharing within and outside the organization. This policy should detail who can share data, what data can be shared, how it can be shared, and with whom. Had TechFite implemented and enforced an effective information sharing policy, the incident of sharing proprietary data with competitors could have been avoided. Employees would be aware of the potential legal and reputational consequences of such actions, and any attempts to do so could be promptly identified and stopped.

**B2. SATE Components**

Establishing who will oversee and manage the SATE program. It is vital to have a dedicated team or individual, to oversee the program. This role involves developing the program's framework, content, and methodology. They would also be responsible for measuring the program's effectiveness, performing regular updates to the program. This component ensures there's ownership and accountability for the SATE program, leading to a more effective implementation.

Participation component: Defining who will be required to participate. All employees, contractors, and third parties with access to TechFite's system should be required to participate in the SATE program. This is because cybersecurity awareness is everyone's responsibility, and even one weak link can compromise the entire system.

**B2a. SATE Program Communication**

Email Announcement: The initial announcement about the introduction of the SATE program could be done via an official email sent to all employees and third parties. This email should come from a top executive, preferably the CEO or CISO, to underline the importance of the program. The email should contain information about what the SATE program is, why it's being implemented, who it applies to, and what the expectations are from each employee.

Intranet Postings and Newsletter Updates: For ongoing communication, updates and reminders about the program could be posted on the company intranet or shared via a company newsletter. This can include updates on the program, tips for staying secure, and any changes to the program.

Meetings: Meetings, either physical or virtual, can be utilized to discuss the SATE program. These meetings can provide a space for employees to ask questions, voice concerns, and gain a deeper understanding of the program. Representatives from the management team or the program's overseer can present updates on the program's progress and any future plans.

**B2b. SATE Program Justification**

As identified in the case study, one of the major issues was the unauthorized access and privilege escalation by the BI unit. They were able to gain access to other departments which potentially exposed sensitive data.

To mitigate this behavior, the SATE program would include training on the principles of 'Least Privilege'. Employees will be educated about the importance of these principles, why they are necessary for maintaining a secure environment, and the consequences of bypassing these controls. Periodic audits and scenario-based training would be conducted to ensure employees understand and adhere to these principles. This approach would significantly enhance TechFite's data security.

The case study also highlighted the sharing of proprietary information with TechFite's competitors. This behavior not only breaches trust but also puts potential client's intellectual property at risk.

To counter this behavior, the SATE program would implement specific training on data handling and the ethical use of information. Employees would be trained on how to properly handle sensitive information, understanding the different data classifications, and the repercussions of mishandling proprietary data. They would also be educated about the company's policies and the legal implications of unethical information sharing. This aspect of the SATE program would encourage ethical behavior, protect client's intellectual property, and foster a culture of trust and responsibility.

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

In the case study, it was observed that the BI unit was able to gain unauthorized access to departments such as legal, human resources, and finance, posing a significant risk to data security. To mitigate this issue, a Security Awareness Training and Education (SATE) program has been proposed. This program will focus on educating employees about the principles of 'Least Privilege' and 'Need to Know,' helping them understand their importance, necessity, and the consequences of bypassing these controls. Regular audits and scenario-based training will further strengthen the adherence to these principles, effectively reducing the risk of unauthorized access.

Another ethical challenge is the sharing of proprietary information with competitors, which not only breaches trust but also puts TechFite's client’s intellectual property at significant risk. The SATE program will include specific training modules on data handling and the ethical use of information. The training will provide employees how to properly handle sensitive information, different data classifications, and the repercussions of mishandling proprietary data. It will also emphasize the company's policies and the consequences of unethical information sharing.