

Western Governor’s University

**Legal Issues in Information Security**

**C841**

Ikeolu Ajiboye

**IHP4 Task 2: Ethics and Cybersecurity**

**IHP4 Task 2: Ethics and Cybersecurity**

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

One of (ISC)²s’ ethical guidelines is to “Act honorably, honestly, justly, responsibly, and legally” (ISC2, 2023). This guideline would apply to the BI Unit employees who gained unauthorized access to sensitive information of other departments within TechFite, which violates that guideline. If TechFite had employed this guideline it might have deterred the bad actors from accessing that data.

Another guideline is from ISACA, and it reads: “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, 2023). This guideline applies to the activity of the Security Analyst Nadia Johnson because she used confidential data for unauthorized purposes. If TechFite used this guideline Nadia would have had the obligation to protect the data and refrain from sharing it to unauthorized parties.

**A2. Unethical Practices**

The head of the Applications Divisions, Carl Jaspers’ failed to ensure oversight and confidentiality within the Business Intelligence Unit. This let Sarah Miller, Megan Rogers, and Jack Hudson access sensitive information from other departments within TechFite.

Another example is from Security analyst Nadia Johnson. Her social media posts show she has some sort of relationship with Carl Jaspers and the background check also shows the bias and favoritism she receives from him. This might’ve led her to contribute to the unethical activities related to the Business Intelligence Unit.

**A3. Factors**

One factor that led to the lax behavior it TechFite was them not implementing the principle of least privilege. This let Business Intelligence Unit employees have unauthorized access to sensitive information including access to other departments within TechFite. Which then ultimately led to unauthorized data sharing.

An additional factor that led to lax behavior was the lack of a social relationship policy between employees. This led to Nadia Johnson having a relationship with Carl Jaspers in which he showed Bias and Favorable treatment towards her.

**B1. Information Security Policies**

A data loss prevention policy (DLP) could’ve prevented Business Intelligence Unit employees from sharing and stealing data they weren’t authorized to have access to. “DLP software controls and monitors sensitive data while in use, in motion, and at rest” ("Data loss prevention software", 2023) . The policy would’ve flagged unauthorized access and deterred employees from sharing sensitive data. It also would’ve protected TechFites’s intellectual property and client information.

Another policy that may have prevented criminal activity is an access control policy. By restricting users account access to their job roles and ensuring proper authorization, the policy would’ve reduced the risk of a data breach and intellectual property theft. It also would’ve prevented the creation of dummy user accounts which had access to sensitive data within other departments in Techfite, in turn that would protect TechFites intellectual assets.

**B2. SATE Components**

I would recommend TechFite to hire an Information Security Officer to manage their SATE program. An Information security Officer would ensure that the programs main points and objective are communicated effectively. They would also play a vital role in identifying future risks and vulnerabilities.

TechFite should also require all employees to participate in the SATE program. This benefits TechFite by educating their employees of security while also preventing them from claiming ignorance.

**B2a. SATE Program Communication**

TechFite should Inform their employees of the SATE program by using a company-wide email sent by an executive. This ensures that employees have easy access to the message, and it ensures they receive the information simultaneously.

**B2b. SATE Program Justification**

One behavior the TechFite Sate program should address is unauthorized intelligence-gathering, like how the BI Unit employees were scanning other companies’ networks. To address it, the SATE program should have training on ethical conduct, proper authorization, and the possible legal consequences of such actions.

Another behavior that should be addressed was the unauthorized data access from the BI Unit, they had accessed information from other departments within TechFite without proper authorization. To address it, the SATE program should include training on the Access Control Policy and the principle of least privilege. This would ensure employees only have access to data they need and enhance security overall.

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

TechFite has faced several ethical issues in its company. Firstly, BI Unit employees were engaged in unauthorized intelligence-gathering activity and accessed sensitive data from other departments within TechFite. To mitigate this, the proposed SATE program should have training on ethical conduct, legal consequences, and proper authorization procedures. Also, there were clear signs of favoritism and bias between Nadia Johnson and Carl Jasper. This could be mitigated by including fair treatment and unbiased behavior training in the SATE program, also a social relationship policy. Additionally, TechFite policies lacked the principle of least privilege leading to employees accessing unauthorized sensitive data and sharing that said data. This could be fixed by implementing an Access Control Policy. Furthermore, the unauthorized data sharing and access could be mitigated by including a Data Loss Prevention Policy. This would monitor and data and reduce the risk of data breaches. Then lastly the lack of and Information Security Officer resulted in lacking oversight, appointing one would ensure best security practices and effective implementation of the SATE program. With these proposed mitigation measures along with the SATE program, TechFite can foster a culture of security awareness, protect sensitive information, and prevent unethical behavior.

**References**

ISC2 (2023). (ISC)² Code Of Ethics. Retrieved July 30, 2023, from https://www.isc2.org/Ethics

ISACA (2023). Code of Professional Ethics. Retrieved July 30, 2023, from <https://www.isaca.org/credentialing/code-of-professional-ethics>

Data loss prevention software. (2023, February 7). In Wikipedia. https://en.wikipedia.org/wiki/Data\_loss\_prevention\_software