****

Western Governors University

**Legal Issues in Information Security**

**C841**

Greg Westmoreland

**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) has an organized list of ethical guidelines for its members and certificate holders. One of those guidelines states that a company should “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.” [[1]](#One) This ethical guideline is highly applicable to the activity in the case study, where it was observed with the mishandling of sensitive and proprietary information belonging to existing, potential, and previous clients.

The Applications Division did not implement proper restrictions to protect sensitive information. The Business Intelligence (BI) Unit, along with the Sales and Marketing Unit, had access to each other’s data when their data should have been separated with the Least Privilege Principle. Had TechFite implemented ISACA’s ethical guideline of maintaining privacy and confidentiality, the sensitive information would not have been accessible. Applying this ISACA’s ethical guideline can lower the risk of leaking sensitive and proprietary information to competitors or unauthorized personnel.

The International Information System Security Certification Consortium (ISC)2 has a “Code of Ethics Canons.” The second point states that one should “Act honorably, honestly, justly, responsibly, and legally.” [[2]](#Two) This ethical guideline applies to this case study based on the activity of Sarah Miller, a senior analyst for TechFite. Sarah participated in dishonorable, dishonest, unjust, irresponsible, and illegal activities. Sarah and two of her subordinates were attempting to intelligence-gather information on various companies by using “dumpster diving” and “trash surveillance.” These activities violate the (ISC)2’s ethical guideline and could be considered illegal with unauthorized access to private information regarding these companies. Had TechFite implemented (ISC)2’s ethical guideline of “act honorably, honestly, justly, responsibility, and legally,” it would have produced an environment of integrity, virtue, and principle within the company. After applying (ISC)2’s ethical guideline, TechFite would avoid ethical and legal issues regarding access to unauthorized information.

**A2. Unethical Practices**

One specific behavior observed was the absence of oversight along with the practice of access control regarding the Business Intelligence (BI) Unit. Nadia Johnson, an IT Security Analyst with TechFite, demonstrated this behavior. Nadia’s responsibility included providing a security report to the Chief Information Security Officer (CISO) with detailed security threats against the company. Nadia reported external security threats against the company’s network; however, she neglected to report any security threats that occurred internally. This omission did not capture internal security breaches within TechFite, specifically the unauthorized access by the Business Intelligence (BI) Unit.

A secondary specific behavior observed was the creation of two user accounts at the request of Carl Jaspers, head of the Applications Division of TechFite. Carl requested these accounts be assigned to former employees that had not been employed in over a year. Having policy and procedures for user accounts would have alerted the System Administrator that the accounts were assigned to inactive employees. Carl was able to utilize these user accounts to conduct unethical and unauthorized activity over the computer network. His actions with these user accounts would not have been traceable back to his account. Establishing clear policies and procedures for user accounts would have prevented this activity.

**A3. Factors**

A specific factor observed in the case study that contributed to lax ethical behavior was the absence of a Compliance Division. This department would have overseen rules and regulations governing all departments, including the Applications Division’s Business Intelligence (BI) Unit. By establishing a Compliance Division, several security rules could be followed that would have prevented unauthorized access by the Business Intelligence (BI) Unit. The Compliance Division would establish regularly scheduled and spontaneous audits of user accounts and access privileges. The Compliance Division would document policies of segregated duties based on job roles. They would require all employees to participate in mandatory training to discuss ethical behavior and avoid unethical practices.

A secondary specific factor observed in the case study that contributed to lax ethical behavior was the missing employee policy regarding social relationships between IT security staff and the individuals they audit. IT Senior Security Analyst, Nadia Johnson, had a relationship with the head of the Applications Division, Carl Jaspers. Their relationship outside TechFite should have been prohibited due to the working relationship of their positions at TechFite. Nadia performs regular security audits of Carl’s department. Carl posted several social media posts with photos and text documenting Nadia attending events he hosted. A recent post even showed a birthday gift given to Nadia by Carl. Carl provided positive recommendations to the CISO regarding Nadia during her annual reviews, leading to several pay raises. These recommendations and gifts should be seen as suspicious and a conflict of interest. Nadia did not report any unethical behavior by Carl or his department because of their relationship. TechFite must establish a well-defined policy regarding social relationships between IT Security Staff and the individuals they conduct security audits on.

**B1. Information Security Policies**

A specific information security policy that could have been utilized in the case study is the "Data Encryption Policy." “This policy defines organizational requirements for the use of cryptographic controls, as well as the requirements for cryptographic keys, in order to protect the confidentiality, integrity, authenticity, and nonrepudiation of information.” [[3]](#Three) These guidelines would formalize encryption methods to protect sensitive information stored, transmitted, or used at TechFite. The proper use of data encryption would have prevented the Business Intelligence (BI) Unit from being able to decipher the intellectual property of TechFite’s client applications. With the “Data Encryption Policy” being used, the intellectual property would be unattainable from unauthorized users within the company. This policy would protect data and mitigate insider threats, even if malicious users are internal. If a user could access the data, they would not be able to decipher the text to view it. By implementing industry standards and using the latest encryption protocols, unauthorized access, network interception, and data breaches would be avoided.

A secondary specific information security policy that could have been utilized in this case study could be the "Access Control Policy." “Access control policy refers to a data security technique that prevents unauthorized physical or remote access to company data. This technique aims to minimize the security risks to the physical and logical systems of an organization.” [[4]](#Four) The Applications Division information system and data would not have been vulnerable had TechFite used an “Access Control Policy.” The unauthorized access of intellectual property could be construed as criminal behavior. A vigorous “Access Control Policy” would have greatly reduced and mitigated internal threats to intellectual property. Enforcing the segregation of duties based on employee roles, using the principle of least privilege, conducting regularly scheduled review audits, monitoring and alerting when forbidden access attempts are made, and mandatory employee training about ethical behavior are all actions that would have prevented these activities documented in the case study.

**B2. SATE Components**

“Security Awareness Training and Education (SATE) is essential for businesses to keep up with the dynamic nature of current cybersecurity threats. Experts need to be aware of both external and internal risks to the company’s security.” [[5]](#Five) TechFite’s component of a comprehensive SATE program will be who is required to receive the training. TechFite will require all employees to participate in the SATE program. The SATE would be made available for all existing employees during their annual education and instructional training in January. For new employees, the SATE program would be required during their orientation period and then be repeated every January as part of their annual training. The theme of the SATE would be "Cybersecurity Awareness is Everyone’s Job!" The training would consist of an online program with slides, video scenarios, audio examples, and a test of the covered material. Adopting a security awareness training program would help cultivate a more vigilant workforce that actively contributes to the organization's cybersecurity defense.

A second component of TechFite’s SATE program will be who will deliver the training. An IT Security Team will provide the security training. This team will comprise employees from several departments, including the Applications Division, Human Resources, Legal, Security Analysts, and Compliance. The training will be placed on the internal network with readable slides, videos dealing with cybersecurity scenarios, audio testimonies of employees on how to fight cybersecurity threats, and a comprehensive exam on the material covered.

**B2a. SATE Program Communication**

Employees at TechFite will be informed of the company's new SATE program by an email announcement from the Chief Executive Officer (CEO). This email will focus on the company's commitment to fighting cybersecurity externally and internally. This email will discuss where the employee can access the training on the internal network and the completion deadline. This email will be sent to all existing employees. Any new hires that receive a welcome packet as part of their orientation will also receive a copy of this letter describing the SATE program.

In addition to the email, a dedicated web page on the employee portal will use a highlighted section about the new SATE program. The link to the SATE page will feature a video message from the Chief Information Security Officer (CISO) discussing the new training program. His announcement will describe how the SATE program will become part of everyone’s training every January. Department managers will schedule one-on-one meetings with their subordinates. These meetings will remind the employees about the SATE program. The managers will point the employees to the CEO's email and the CISO's video message.

**B2b. SATE Program Justification**

The specific undesirable behavior was the creation of user accounts being used for unauthorized intelligence gathering by the Applications Division department head. The two user accounts were assigned to former employees. They were used for intelligence-gathering activities about other companies. With the development of the SATE program, the Internal IT Security Team will create a training module that will discuss unethical conduct and the consequences caused by such behavior. This module would be called "See Something, Say Something." If the System Administrator had completed the SATE training before receiving the request, they would have ignored the request to create the user accounts assigned to former employees. These actions would have benefited TechFite and notified Compliance about the unethical request made by the head of the Applications Division.

The secondary specific undesirable behavior was the lack of access control for the Business Intelligence (BI) Unit. The principle of least privilege and separation of duties should have been followed. The new SATE program that TechFite will implement will contain a training module called "Do I Have Access?". This training module will include the importance of access control and data privacy. Access control will be based on the employee’s role and what resources they need access to for completing their day-to-day responsibilities. This training module’s emphasis on data privacy will be a focus point. It will discuss what will happen should that data become compromised. If the Security Analyst had been properly trained with the SATE program, an internal audit would have revealed that the Business Intelligence (BI) Unit had access to data it should not have had. The Security Analyst would have notified Compliance about the access breach, and actions would have been taken to mitigate the violation quickly.

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

A recap of the ethical issues will be discussed in four parts. The first is the unauthorized intelligence gathering against other companies using two user accounts assigned to former employees. This could have been mitigated with the "See Something, Say Something" training module from the SATE program that TechFite will implement. This training will include handling unethical requests and reporting behavior to the Compliance Division.

The second area discussed is the careless approach to access control by the Business Intelligence (BI) Unit. The Business Intelligence (BI) Unit was allowed unauthorized access to other departments. This could have been mitigated with the "Do I Have Access?" training module from the SATE program that TechFite will implement. This training will include how employees will be subject to limited access control, role-based access, data privacy handling, and how they are to report violations of this policy.

The third area discussed is the lack of data encryption. When data is not encrypted, it is a tempting target for any end user, even the curious one. Malicious users can gain access to sensitive data and leak that data outside the company. The unauthorized access could have been mitigated with the "Not for Prying Eyes" training module from the SATE program that TechFite will implement. This training will include the importance of data encryption when data is at rest, when data is in transit, and how to handle incidents when data has been compromised.

The fourth area discussed is the conflict of interest between the IT Security Analyst, Nadia Johnson, and the department head of the Applications Division, Carl Jaspers. Nadia's omissive security report was biased based on the benefits she receives from her relationship with Carl. Carl was able to make an unethical request, and Nadia overlooked that request. This could have been mitigated with the "Employee Fraternization" training module from the SATE program that TechFite will implement. This training will include the policy on social relationships between IT Security Staff and the individuals they audit in their reports. TechFite might consider a third-party, independent oversite company, to ensure that impartiality is insured when doing the social relationship checks.

**References**

1. “Code of Professional Ethics” <https://www.isaca.org/credentialing/code-of-professional-ethics#:~:text=Members%20and%20ISACA%20certification%20holders%20shall%3A&text=Maintain%20the%20privacy%20and%20confidentiality,or%20released%20to%20inappropriate%20parties> Retrieved July 16, 2023.

2. “(ISC)² Code Of Ethics” [https://www.isc2.org/Ethics#](https://www.isc2.org/Ethics) Retrieved July 16, 2023.

3. “Encryption Policy” <https://userflow.com/policies/security/encryption#:~:text=This%20policy%20defines%20organizational%20requirements,authenticity%2C%20and%20nonrepudiation%20of%20information> October 20, 2021.

4. “What Makes a Good Access Control Policy?” <https://www.beyondidentity.com/blog/what-makes-good-access-control-policy#:~:text=Access%20control%20policy%20refers%20to,logical%20systems%20of%20an%20organization> August 24, 2021.

5. “Security Awareness Training: What It Is and Why You Need It” <https://marinerinnovations.com/security-awareness-training-what-it-is-and-why-you-need-it/#:~:text=Security%20Awareness%20Training%20and%20Education,risks%20to%20the%20company's%20security> January 17, 2023.