****

Western Governors University

**Legal Issues in Information Security**

**C841**

**Greg Westmoreland**

**IHP4 Task 1: Legal Analysis**

**IHP4 Task 1: Legal Analysis**

**A1. CFAA and ECPA**

*The Computer Fraud and Abuse Act (CFAA) of 1986 states that a criminal offense under the act is "having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information...”.* [*[1*](#One)*] In the TechFite case study, the Business Intelligence (BI) Unit used dummy user accounts to gain unauthorized access to legal, human resource (HR), and financial department files. One of these dummy accounts had to be given escalation privilege access to the forbidden files over the computer network. The CFAA was violated when the Business Intelligence Unit examined the legal, personal, and financial documents of these other departments without proper authorization. This clearly violated the privacy rights of those divisions and their employees.*

*The Electronic Communications Privacy Act (ECPA) of 1986 states that it “…protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The act applies to email, telephone conversations, and data stored electronically.* [*[2*](#Two)*] TechFite’s Applications Division head, Carl Jaspers, requested two user accounts to be created. These user accounts were assigned to two former employees. Even though the former employee statuses were inactive, these user accounts were very active. Emails sent from these user accounts were associated with parties who were not clients of TechFite. Some of the emails refer to “intelligence gathering” by means of “dumpster diving” and “trash surveillance.” This example clearly demonstrates electronic communication being made with criminal intent to intelligence-gather information against various companies. This example violates the ECPA.*

**A2. Three Laws**

*With TechFite’s lackadaisical approach to internal oversight, especially the Business Intelligence (BI) Unit, the Electronic Communications Privacy Act (ECPA) was violated. The negligence was due to the use of dummy user accounts given unrestricted access to the HR, legal, and financial department. These dummy user accounts gained access over the computer network. The ECPA was violated by these restricted data files being transferred over the computer network. These actions should have been prevented by segregating department access to sensitive electronic communications and documents. TechFite can be held legally responsible for not implementing the least privilege principle. The least privilege principle is “…designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.”* [*[3]*](#Three) *Any employee’s workstation that had access to BI Unit, would have had full, unrestricted administrative rights, meaning that employees had more privileges and access than necessary to perform their day-to-day tasks. Creating and using these dummy user accounts justifies legal action against TechFite and its leadership under the ECPA Act.*

*Carl Jaspers, the head of the Applications Division, violated the Computer Fraud and Abuse Act (CFAA) by having two user accounts created in the names of employees no longer working for the company. It was found that these user accounts were used to gain unauthorized access to the computer’s network to send emails that demonstrated intelligence-gathering against other companies. Using these accounts justifies legal action against TechFite, the Applications Division, and individuals responsible under the CFAA Act.*

*The Sarbanes–Oxley Act (SOX) of 2002 "...mandates certain practices in financial record keeping and reporting for corporations."* [*[4]*](#Four) *Upon discovery that TechFite’s Financial Unit had received payments from three companies: Bebop Software, FGH Research Group, and Dazzling Comet Software, further research determined that these three companies did not have a real internet presence. Continued investigation determined that these companies were fictitious and all of them were incorporated in Nevada by Yu Lee. Mr. Lee attended graduate school with TechFite’s Applications Division head Carl Jaspers at Stanford University. The payments to TechFite were all drawn from the same bank, Freeworkers’ Pennsylvania Bank, NA in Scranton, Pennsylvania. TechFite does not have any business relationship with the Freeworkers' Pennsylvania Bank, and the other coincidences suggest the possibility of off-the-books or illegal activities that would violate the SOX Act. Any fraudulent financial transactions or statements would allow legal action against TechFite and its leadership for violating the SOX Act.*

**A3. Duty of Due Care**

*The first example of a lack of duty of due care is negligent oversight regarding employee user accounts. TechFite's Applications Division Department head, Carl Jaspers, requested two user accounts to be created with the names of two former employees. When the system administrator created the user accounts and assigned them to inactive employees, that should have been a red flag. However, due to inadequate auditing and compliance, the request was fulfilled without question*. *This lack of compliance produced a failure to exercise duty of due care in fulfilling suspicious user account creation requests.*

*The second example of a lack of duty of due care is the lack of security handling procedures such as: auditing of employee user accounts, escalation of privileges, enforcing data loss prevention (DLP) on sensitive documents, and monitoring internal network traffic and activity. This lack of compliance produced a failure to exercise duty of due care in security monitoring coming from the Business Intelligence (BI) Unit.*

**A4. SOX**

*TechFite is a moderately sized company of 1000 employees and is publicly traded on the NASDAQ stock market. The company’s core business involves consulting with and advising internet organizations on promoting and monetizing their online business ventures. Since TechFite is publicly traded, the Sarbanes–Oxley Act (SOX) regulations apply to TechFite. The case study indicated that TechFite accepted payments from suspicious companies (Bebop Software, FGH Research Group, and Dazzling Comet Software). These companies have no real internet presence and were incorporated in Nevada. Their services were paid with checks drawn from Freeworkers' Pennsylvania Bank, with which TechFite had no established business relationship. Section 302 of the SOX Act states that “…the CEO and CFO are directly responsible for the accuracy, documentation, and submission of all financial reports as well as the internal control structure to the SEC.”* [*[5]*](#Five) *The lack of verifying the legitimacy of these three companies and accepting payments from a bank that your company does not have a relationship with, raises doubts from internal control and accurate financial reporting perspectives. These financial discoveries would violate the SOX Act and bring legal justification against TechFite and its leadership.*

**B1/B1a. Criminal Evidence, Activity, Actors, and Victims**

*One example of a specific criminal activity observed in the case study was the unauthorized use and access of files outside the Business Intelligence (BI) Unit using dummy user accounts*. *The offending actor was the BI Unit within the Applications Division of TechFite. The victim of the criminal act was the legal, human resources (HR), and finance departments within TechFite. Their departmental documents were accessed, and this may have lead to the exposure of confidential and sensitive information. This breach of conduct could have legal implications should this information be made public against TechFite and its leadership.*

*A second example of a specific criminal activity observed in the case study was the use of a Metasploit tool on several machines for penetration testing and IP address scanning*. *Hard drive evidence confirmed penetration testing and IP address scanning against several internet-based companies. The offending actors were Sarah Miller, a senior analyst, and two of her subordinates, Megan Rogers and Jack Hudson, junior analysts from the Business Intelligence (BI) Unit within the Applications Division of TechFite. These Internet-based companies were victimized by penetration attempts and IP address scans against their networks without consent. Unauthorized penetration testing and network scans can be considered a criminal act and have legal implications against TechFite and its leadership.*

**B1b. Cybersecurity Policies & Procedures for Criminal Activity**

*One specific cybersecurity policy that could have been implemented is “Data Access Control.” Data Access Control is when “you restrict access based on a set of policies. By implementing robust policies for your data access, you’re helping keep personally identifiable information (PII), intellectual property, and other confidential information from getting into the wrong hands, whether internally or externally.”* [*[6]*](#Six) *TechFite could have implemented this policy with several steps: (1) User Account Creation – only created for active and current employees, (2) Access Rights – given specific job responsibility and roles with that position based on least privilege, (3) Regular Access Review and Audit – quarterly review of active employees’ rights, roles, and access based on least privilege, and (4) Former Employees – access restrictions revoked, and employment status set to inactive. Implementing a “Data Access Control” policy would have prevented unauthorized access for fictitious user accounts assigned to former employees.*

*A second specific cybersecurity policy that could have been implemented is “Data Classification”****.*** *Data Classification is "...a comprehensive plan used to categorize a company’s stored information based on its sensitivity level, ensuring proper handling and lowering organizational risk. A data classification policy identifies and helps protect sensitive/confidential data with a framework of rules, processes, and procedures...".* [*[7]*](#Seven) *This cybersecurity policy would help establish company guidelines for the classification and proper handling of data based on the data's sensitivity and criticality. Written policies and procedures would have set a standard for being able to identify, categorize, and apply proper security controls to protect the data throughout its lifecycle. The implementation of a Data Classification policy would have prevented unauthorized access for fictitious user accounts assigned to former employees.*

**B2/B2a. Evidence of Negligent Activity, Actors and Victims**

*One example of a specific negligent act observed from the case study was the apparent lack of segregation of duties and access control. This gross negligent act failed to enforce separation of duties and access control for the Business Intelligence (BI) unit and the marketing/sales unit associated with it. The actor can be identified as any employee with full administrative rights with the BI Unit on their workstation. That employee would have been able to create customers (clients), report sales, and post financial transactions onto the system. The victims could be identified as the clients of TechFite having their confidential information compromised and potentially being leaked to the public.*

*A second example of a specific negligent act observed from the case study was the apparent lack of oversight and protection. This gross negligent act was failing to provide oversight and safeguards to sensitive information that belonged to TechFite’s clients. The actor was the leader of the Applications Division. This individual was responsible for the department’s operational and security policies. The victims were TechFite’s existing, previous, and potential clients, having their trust in TechFite’s integrity and safeguarding so easily compromised.*

**B2b. Cybersecurity Policies & Procedures for Negligent Activity**

*One specific example of a cybersecurity policy that could have been implemented is the Acceptance Use Policy (AUP). An Acceptance Use Policy is “…a document stipulating constraints and practices that a user must agree to for access to a corporate network, the internet, or other resources.”* [*[8]*](#Eight) *“From an information technology (IT) perspective, an AUP states what a user can and cannot do when using computers and computing resources.”* [*[8]*](#Eight) *With this AUP document, it would also be able to provide guidelines for reporting and responding to security incidents with violations of TechFite’s AUP. Through mandatory employee training, these incidents could have been flagged and triaged for TechFite’s Compliance Division to work through. The Compliance Division would then have been able to respond appropriately with immediate actions to mitigate the incident. Following the breach of the AUP, the Compliance Division would have been able to recommend necessary disciplinary actions against those who violated TechFite’s AUP.*

*A secondary specific example of a cybersecurity policy that could have been implemented is the Data Loss Prevention (DLP) policy. “Data loss prevention policy is a definition of how an enterprise can use, store, and transmit data. These policies enforce the protection and preservation of data in your cloud****.”*** [*[9]*](#Nine) *This policy would be able to establish detailed instructions on how TechFite’s employees would handle sensitive data, transfer sensitive data, and store sensitive data. Some guidelines that would be part of the DLP policy would be data classification, encryption methods, secure file transfer, monitoring with regular audits of employee’s activities, and proper destruction of the data at the end of its lifecycle.*

**C. Legal Compliance Summary for Management**

*Regarding the first law, Computer Fraud and Abuse Act (CFAA), TechFite’s status would be found to be in non-compliance. One example would be unauthorized access that violated the CFAA, which prohibits accessing a protected system without proper authorization. A second example would be the escalation of privilege, where Carl Jaspers requested and received two user accounts with privileges given to employees that had left the company a year ago. These user accounts were used to access sensitive computer systems without adequate authorization, which is a violation of the CFAA Act.*

*Regarding the second law, Electronic Communications Privacy Act (ECPA), TechFite’s status would be found to be in non-compliance. One example would be the intercepting of electronic communication where dummy user accounts gained unauthorized access to other divisions within the company. THE ECPA was violated when the communication took place over the computer network without proper consent being given to these user accounts.*

*A secondary example would be no oversight committee or compliance division overseeing all activities within the company. Specifically, the Business Intelligence (BI) Unit used the computer network to gain access to sensitive files without proper consent being given.*

*Regarding the third law, Sarbanes–Oxley Act (SOX), TechFite’s status would be found to be in non-compliance. One example would be the lack of financial transparency by the CEO and CFO of TechFite. The company took payments from three companies, Bebop Software of Alberta, FGH Research Group of Indiana, and Dazzling Comet Software of Florida, which had no real presence on the internet. After further research, it was discovered that these companies were all incorporated in the state of Nevada by a previous college mate of Carl Jaspers, the head of the Applications Division. The payments from these companies were all drawn from the same bank that TechFite had no obvious relationship with, past or present. With the lack of reporting, these financial transactions violate the SOX Act.*

*A second example would be fraudulent financial reporting with the Business Intelligence (BI) Unit having authorized access to the financial documents. The documentation could have been manipulated and adjusted in a way that would have misrepresented TechFite’s financial position. The provision of misleading and bogus financial reports violates the SOX Act.*

**References**

1. “Computer Fraud and Abuse Act” <https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act> June 17, 2023.

2. “Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523” <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically> Accessed July 9, 2023.

3. “Least privilege” <https://csrc.nist.gov/glossary/term/least_privilege#:~:text=Definition(s)%3A,needs%20to%20perform%20its%20function> Accessed July 9, 2023.

4. “Sarbanes–Oxley Act” <https://en.wikipedia.org/wiki/Sarbanes–Oxley_Act> July 8, 2023.

5. "SOX Section 302: Corporate Responsibility for Financial Reports" <https://www.sarbanes-oxley-101.com/SOX-302.htm> July 9, 2023.

6. “What is Data Access Control?” <https://www.sailpoint.com/identity-library/what-is-data-access-control/> July 21, 2021.

7. "Data Classification Policy: Definition, Examples, & Free Template" <https://hyperproof.io/resource/data-classification-policy/#:~:text=A%20data%20classification%20policy%20is,handling%20and%20lowering%20organizational%20risk> November 2020.

8. “Acceptable Use Policy (AUP)” <https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP#:~:text=An%20acceptable%20use%20policy%20(AUP)%20is%20a%20document%20stipulating%20constraints,being%20granted%20a%20network%20ID> June 2022.

9. “9 Steps to Create a Data Loss Prevention (DLP) Policy” <https://sonraisecurity.com/blog/data-loss-prevention-policy/> August 18, 2022.