Western Governors University

Legal Issues in information Security

C841

Ryan Burke

IHP4 Taks 1: Legal Analysis

A1. The company TechfFite violated both acts as the company enabled its employees to violate terms under the Computer Fraud and Abuse Act (CFAA) and Electronic Communication Privacy Act (ECPA). The company enabled the use of fake or Dummy accounts within the use of their internal system to access sensitive information and they allowed the Business Intelligence Unit (BI) to gather public available information of other companies to within the internet sector “to benefit the division’s marketing of its services to aid clients,” according to the TechFite Case Study. This failure to issue the least privileged principle is where the (BI) Unit was able to access other information within departments like Human Resources and Finance within the TechFite system.

A2. TechFite violated the Computer Fraud and Abuse Act (CFAA), in that they enabled employees to allow dummy or fake accounts to intrude and gain information on other departments within the TechFite ecosystem. TechFite was also in violation of the Oxely Act (SOX). The lack of accurate and concise financial statements given by the company shows that TechFite is indeed moving money to change the numbers of their financial statements, which is a clear violation of (SOX) policy. TechFite is also in clear violation of the Electronic Communication Privacy Act (ECPA), in that employees of the company were able to intrude devices belonging to several internet-based companies using a system penetration tool to gather IP addresses.

A3. Instances where duty of due care was lacking was the use of social media posts and text documenting social events hosted by a particular employee of the company, and the lack of due diligence to delete an account belonging to a past employee that has not worked for TechFite for over a year was clearly at fault.

A.4 . The Sarbanes-Oxely Act (SOX) applies to the case in that it requires public companies to have in place internal procedures and methods for ensuring accurate financial statements. In this case we note that TechFrite receives checks from three companies drawn from the same bank. This gives reason to believe that TechFrite is using fake clients to move money into TechFrites sales figures thus giving us a false representation of the financial situation. This is clearly in violation of (SOX) as companies are required by law to have accurate and concise financial statements at all times.

# B.1. A The Business Intelligence Unit (BI), committed alleged criminal activity in that they used a system penetration tool to scan IP addresses for “several internet-based companies.” This would clearly be a breach of law of 38 CFR 75.113 according to the California Penal Code. As well as breaching other systems to gain information the BI unit was involved in creating dummy accounts to intrude other parts of the TechFite corporation, allowing the unit to gain valuable information such as financial and executive documents.

B.2.B With the lack of oversight and access of least privilege, the Business Intelligence Unit (BI) was able to take advantage of the situation and gain access to vital information within the TechFite ecosystem and other internet-based companies. The policies and procedures of TechFite did not seek to enforce existing policies nor did they seek to keep the employees and executives informed on good ethical practices and procedures to avoid illegal doings throughout the company.

B.2.A The act of negligence is as follows. Upon the request of Carl Jaspers employees were assigned two accounts. Though these employees' accounts have not been used for over a year they are still being used to dumpster dive into and conduct trash surveillance. The lack of due diligence as a manager to not delete these accounts is alarming. The victims in this case are those that are being surveyed in their trash being spied on by the company. One could also say that employees such as Sarah Miller, Megan Rogers and Jack Hudson are also acting in negligence, knowingly gathering intelligence through mining companies’ trash.

B.2.B Again the lack of training and oversight from the higherups could have instilled good moral ethics within the team to act in a manner that is most appropriate. Good moral practices, procedures and policies need to be clearly instilled and engrained within the company to follow. It should act as a baseline and guide the employees of the company to make good decsions and follow the rules. Having the proper measures in place to make sure these policies and procedures are followed is also just as important.

C. TechFite has not acted in the best interests of the company nor its clients in the way it conducts itself daily. The illegal doings of employees and lack of oversight to maintain a healthy and ethical working environment is not up to standard and must be addressed immediately to avoid further complications in the near future. Poor practices among the employees as well as a lack of guiding principles and polices to ensure an effective and ethical workplace is needed or must be reinforced to ensure good practices within the company and its executives. To maintain a strong code of ethics all departments within the system must be investigated further to ensure operations are at play in a safe and cohesive manner and that TechFite is not at risk of being put under criminal charges or lawsuits.

Work Cited

*Code section*. Law section. (n.d.). Retrieved August 17, 2022, from <https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.29>

TechFite Case Study. Retrieved August 17, 2022.