Western Governors University

Legal Issues in Information Security

C841

Ryan Burke

IHP4 Task 2: Ethics and Cyber Security

A.1. Ethical guidelines within cyber security pertain to the integrity of information based upon someone who is working or using certain information or data. Using good ethics is within the best interest of not only the employee but the employer and those that the employer provides services to. Policies and procedures should guide the person working with information security to make the right ethical decisions. To enforce good ethical behaviors and procedures among employees, effective oversight must be taken to prevent the abuse of power among staff and to ensure the integrity of the information is being used as intended and not violating any codes of conduct or policies within the organization. Applicable to this case study, to accomplish this goal and to meet the needs of the organization while using safe and appropriate measures, “Information Security Governance (ISG)” should be used as means to structure and arrange the organization to meet its goals all while ensuring the integrity of the information is kept and maintained. In conjunction we also have procedures, standards, and policies that need to be used within the organization of TechFite to ensure there is a hierarchical set of governance to ensure these duties are carried out and applied within the organization. Failing to carry about a set up standards guided by the leading principles of (ISG) can lead to potential catastrophic consequences as seen in this case study. Ethical guidance provided by the policies and procedures set in place should be able to steer the employees of TechFite in the right direction, provide training, as well as steer them in the right direction to develop a strong ethical code of conduct to make the right decisions when needed. Establishing these ethical principles should be embodied within the organization of TechFite in a manner that is clear and concise and calls its employees to take the responsible and appropriate course of action to do the right thing throughout the organization. If they are appropriately guided by strong ethics this will not only lead to better results within the organization but can prevent many potential lawsuits down the road as well as prevent employees from getting into troublesome situations as we see within this case study with Carl Jasper and multiple other employees within the BI unit.

A.2. Unethical behaviors pertaining to the case study of TechFite include those of Carl Jasper where he “regularly gives Johnson’s boss, the CISO, positive recommendations about Johnon during annual reviews and she gets ample raises.” Though this does not pertain to information security in particular, we can identify that this behavior is unethical and morally wrong in that the relationship can risk bigger wrongdoings in the coming future. Though there is no current policy within TechFite to prevent such relationships within the company, we can assume that such a relationship can put the company at risk of leaking information to put the integrity of it at risk. It is also worth noting that among the BI unit, Sarah Miller as well as other employees such as Megan Rogers and Jack Hudson were all involved in unethical practices of intelligence gathering though mining companies’ trash.

A.3. The lack of clear and concise policy that prevents wrongdoings and unethical behavior is not set in place to prevent such a thing. I would also regard the lack of oversight within the company to oversee its employees contributes to the lax of ethical behavior within the company. TechFite is clearly not enforcing such policies among its employees.

B.1. The Acceptable Use Policy could have prevented its employees from using fake accounts to “dumpster dive” on clients as it did. The use of the Workplace privacy and monitoring process could have also been issued to prevent the BI Unit from intruding on other areas within the company. Ultimately, we want to use these policies to protect the integrity of information and prevent information from falling into the wrong hands like it did with TechFite.

B.2 The key components of a Security Awareness Training and Education program (SATE) include informing the individual of the rights and responsibilities they hold in the workplace and outside. The program’s relevance to the situation could have easily been used to give awareness and shed some light on the wrongdoings the employees were conducting in, as well as give awareness to the fact that they have an obligation to protect the integrity of information within the workplace. In particular it would have stopped employees such as Sarah Miller, Megan Rogers and Jack Hudson from dumpster diving through other mining companies as this is seen as an unethical practice. The (SATE) would have given the team a driving motivation to cover critical issues regarding sensitive information belonging to clients. As stated, “no plan was evident in keeping different clients’ information segregated from each other and employing a Chinese wall methodology. " The clear and concise use of the SATE program would have given the team a chance to evaluate the potential security concerns regarding the information security of TechFite. The SATE should be an ongoing program that evaluates team members to ensure the right measures are in place to possess a safe, available, and secure system for all. Having the program easily accessible to employees through the web as well as having training program seminars could have been used to communicate the standards and procedures that TechFite employees must adhere to.

C. In regards to the practices and policies set in place for the company, they do not meet the required and sufficient standard practices for a company of this caliber. The unethical behaviors conducted by its employees and upper management do not go unnoticed and must be dealt with. In particular the behavior sought out by Carl Jasper in regards to providing raises based on his relationship with another employee is not against company policy but must be addressed. A company policy such as the “Workplace and Monitoring” Privacy must be put in place to provide a healthy and ethical working environment and to provide the oversight needed within the company to ensure best practices are being used. The “Acceptable Use Policy” could have been used in regard to the employee using accounts of other past employees to gather information on various companies through “dumpster diving.” The use of unauthorized access to these accounts as well as the illegal action taken done by this certain employee could have been prevented if the right policy was set in place. The same could be said for all the illegal and unethical practices the employees have conducted in. Better training and oversight is needed within the company and I hope it can be resolved in the forthcoming future.

Work Cited:

TechFite Case Study. Acquired: 17 August 2022