How the legal environment ompacts an organization

Business, Management

The paper “ How the Legal Environment Impacts an Organization" is a sapid example of a term paper on management. The legal environment provides a healthy ground in which the organization conducts its daily routines. All employees in an organization are guided by a set of rules that are defined by the legal environment of a particular organization. Information security is also very fundamental if an organization is to succeed in its day-to-day routines. The existence of the legal environment, therefore, ensures that data is secured by setting up protocols to be followed for maximum data integrity, availability, and confidentiality. The purpose of this research paper is to enable senior managers to understand how the legal environment impacts an organization and how it ensures confidentiality, integrity, and availability of information and information system. The first component of the legal environment is policies, which are actions to adopt. They are categorized in to governmental and organizational. Government policies are rules and regulations issued by local, federal or state government and which provide a basis from which other organizations can establish local policies to enable them to safeguard information and technological instruments hence maintaining data integrity, confidentiality, and availability. On the other hand, organizational policies are rules and regulations that a given organization comes up with to guide the organization in conformity to policies, regulations, and laws. In an organization, protection of people and information should be the first priority (Robbins, 2003). As a result, rules governing the behavior of users like system administrators, security personnel and the entire management should be established.

These rules are meant to authorize people, working on information systems, keep an eye on, probe and approve how data and information circulates in the organization.

Implementation and adoption of the two policies, governmental and organizational, is very important. With such policies in place, an organization will be able to minimize and eliminate the risk involved in losing data. The organization should ensure that all employees have access to the rules and have a clear understanding of the consequences that arise by breaking a particular rule. In addition to that, workers should be exposed to an environment that will enable them to practice to apply those rule, as this will enable the employees to adhere to the rules. In addition to that, policies on information security are meant to regulate how workers handle the information resources of an organization. Many organizations nowadays give their employees ID card and login passwords and other sensitive information through which workers can have access to the organization’s premises and workstations. Without proper policies, workers may tend to misuse such information. For instance, workers who have logins to the corporate mailing system may want to access the mailing system from outside the company premises. However, with the implementation of policies to regulate this, employees will be restricted from such misconducts.

The second component of the legal environment of an organization is regulation. This entity simply deals with the documentation of how something should be done. It is good to understand that if rules and policies are set but not followed, definition and implementation of such rules is in

vain. Through regulation, the rules are enforced and employees are compelled to follow them.

Finally, the last component is the law. Employees should be aware of private and public laws of the organization. Private laws are meant to control the relationship that exists between the organization and the employee (Tolliday, 2001). On the other hand, public laws exist to govern the relationship between an organization and other governing bodies. The employees are mandated to know both the private and the public laws so that in case there has been information breach, the employee can be held liable and reproved in view of those laws.

The study has shown that several laws have been formulated to enhance information security. Some of them include the Computer Fraud and Abuse Act. This Act is meant to formalize laws meant to protect information against computer threats and other offenses. Another rule is the Federal Privacy Act that protects an organization against the misuse of personal information. Take for example an employee knowingly or unknowingly give out client's private information to another organization (Twomey & Jennings, 2002). The employee will be charged with committing a federal crime and will be prosecuted accordingly. As a result of the existence of these laws, information confidentiality, integrity and availability have been highly upheld.

As to conclusion, the purpose of rules, laws, and regulations in an

organization, is to provide a healthy working environment for the workers. Managers of an organization are advised to make organizational policies that encourage workers to work. Some rules tend to scare employees and should, therefore, be avoided. By doing so, information security will be achieved, leading to data integrity, confidentiality, and availability.