Information security: law and policy

Technology, Information Technology

The paper " Information Security: Law and Policy" is a worthy example of a term paper on information technology. Legal policies are detrimental for any organization to comply with before it sets up or it implements any new system in place. Information security is critical and necessary within any organization. This is because, organization information is a critical asset in that it needs to be accurate, relevant, timely and should be properly protected from any unauthorized access to it. The organization should demonstrate a commitment to ensure that its system adheres to legal policies and guidelines as set out by the organization and the government. The aim of the document is to highlight the legal environment such as laws, regulations and policies and its impact upon how an organization puts measures to achieve information and information systems confidentiality, integrity and availability. Information security in an organization involves ensuring that only people with rights to read, change, broadcast and use it have access to it. Different organizations have their own policies which guide the implementation of any new system. Policies in an organization need employees to comply with them. Policies describe the rules and procedures for organization employ to comply with (Kiefer, Wu, Wilson & Sabett 2004). The need for information security is to primarily protect information from any unauthorized party. Several threats can pose to make information insecure. There is a need to ensure information is secure while ensuring that the policies and legal guidelines of the organization and the surrounding environment are adhered with (Kiefer, Wu, Wilson & Sabett 2004). Government and organizational policies dictate the implementation of an information security system. The government policies are determined and

issued to organizations depending on the type or kind of governing environment within the organization's operation. The government can be federal, state, local or tribal. The on the type of the business industry, the government policies act as a framework for organizations' administration or management to comply with in order to secure information and information systems (Straub, Goodman & Baskerville 2008). The need for government policies is to control and regulate the relevant market in order to avoid conflicts which might arise among the industry players. The government policies give a procedure and guidelines for organizational governments to follow when implementing information security systems.

Organization policies are devised by the organization as a guideline when implementing a new system. The policies are devised to ensure that laws, regulations, and policies are complied to. The policies provide a framework for relevant restrictions and privileges for the use of information for every employee. The organization policies strive to ensure that people and information are protected (Straub, Goodman & Baskerville 2008). This is normally accomplished by setting the rules for access to information for each and every employee use of information (Straub, Goodman & Baskerville 2008). Organizational policies assist the organization in complying with governmental policies in order to avoid violation of the latter's policies. The policies include the rules which control the actions of information users and management. The policies include authorization privileges for use of information, need for probe, monitoring, and investigation on the use of information. The policies also include information infringement consequences, the information security baseline position by the

organization. The policies restrict users from accessing what they are not supposed to in order to reduce risk and tampering of information (Straub, Goodman & Baskerville 2008).

Organizations need information security policies in order to eradicate or minimize any looming risks associated with the use of information. The eminent risks can be unauthorized access to organization information either internally or externally. The policies set the laws required before the use of any information or implementation of an information security system (Kiefer, Wu, Wilson & Sabett 2004). The policies ensure every information user has a responsibility for the use of information and the consequences in case of any violation of laws. The policies also regulate the use of information among the industry organization as set out by the government. Any organization which needs to set up a new information security systems need to comply with the government policies to avoid industry crisis or conflicts. The organization policies ensure that information users comply fully with the use of organizational information policies.

The side of regulations should also be considered in an organization when implementing an information security system. According to Stamp, regulations are rules, laws or orders determining how the action has to be taken or done. In information security, regulation involves coming up or devising enforcement security control mechanisms aimed at minimizing or reducing risks associated with the use of information. The organization management comes up with the regulations to be adhered to by every user of information. This is aimed at ensuring that information security is adequately achieved. The regulation gives a guideline to users on what is to

be accessed and not (Stamp 2009).

The laws are part of mechanisms to be followed by organizations when it comes to information security. According to Gifford, laws are made by governing bodies to give a guideline on how to govern behavior (Gifford 2009). Organizational laws control the behavior of information users in order to maintain and safeguard information security. Laws seek to protect the privacy of information users and also between organizational users and the organization. Also, laws are involved between the organizational and the government. They ensure that proper use of information and information security practices are complied to. Every information user should be aware of the laws before the use of information.

In the understanding of fair practices, the government seeks to regulate information security practices. Policies, regulations, and laws are detrimental when devising a new system within an organization environment. The three aspects are part of the necessary requirements which ensure that information security procedures are followed accordingly to ensure information is not tampered to. They also aim at eliminating any disagreement or violations which might be associated with the use of information. The legal environment will be conducive including the business environment if the three aspects are followed to in order to avoid any misunderstanding among the involved parties.