Security threats and defenses

Technology, Information Technology

Security threats and defenses Role of information system security The term social security in the context of organization is defined as the act in which, employees of an organization are manipulated by outsiders to rely key and confidential information details regarding an organization (Hadnagy, 2011). This information is sort by ill intentioned people for purposes of hacking computer systems or committing fraud. Social engineering is the newest form of crime in organizations and involves manipulation of the mind in hidden ways (Hadnagy, 2011). The successful operation of any organization is highly dependent on the performance of its work force. It is therefore the responsibility of any success oriented organization to enlighten its employees on the underlying security threat. An ethical, well goal oriented team is always desired.

Information security is a major concern to all organizations. It ought to be part of every organization's internal controls and operations. These controls ought to be internalized in a way that the employees are made to realize that violation of security puts them at a greater risk. These services to make employees feel their loyalty is crucial to the success of the business. In addition, information security need be given priority and adopted as a distinct value in any institutional culture governing staff behavior. It is therefore necessary to review security policies by offering training forums to employees. Another way of promoting security is by way of regularly reviewing security guidelines to ensure they are relevant an in line with the expected performance.

Communication between the management and the employees ought to be health for security purposes. This aids in that employees can report underlying identified security threats before they occur. Healthy communication patterns not only boost security, but also save the company from incurring unnecessary costs arising from security compromises.

Social engineering techniques

Fraudsters have devised many forms of interfering with the security systems of organizations. For instance, there has been intensive use of ignorance of controls by employees. This occurs in organizations where employees think some process are long and bureaucratic and hence, want a quick way out of it. Ignorance is no defense as it compromises the security of an organization (Hadnagy, 2011). It also occurs where employees are not well briefed on internal controls and information security patterns of an organization. Proper security training need to be impacted on the employees to avoid embarrassment when sensitive and confidential information is leaked to third parties

Another form of social engineering is deliberate efforts to subvert controls of company information. From time to time, a company requires wholly entrust responsibilities to employees. In such a case the technical department will not be in a position to protect the company for fraudsters (Hadnagy, 2011). Therefore, it the employee cannot be trusted to maintain secrecy, he or she could trade crucial information for selfish gains. They could also get manipulated. It is of great need that employees are trustworthy with or without supervision.

The other aspect of social security engineering is in the form of conformity (Hadnagy, 2011). Conformity entails the ill-motive individual trying to convince an employee to confirm a password or log in information for him on the pretext that someone else such as the supervisor had already done it and he is merely confirming. This can be avoided by establishing proper communication channels within an organization so that such compromises are not made. A company can further discourage such security threats by installing tracking systems in which workers compromising the security of a company are detected and severe actions taken against them.

References

Hadnagy, C. (2011). Social engineering: The art of human hacking. Indianapolis, IN: Wiley.