Overview of security issues in it essay

Business, Strategy

The issue of security is a very important matter to individuals and organizations who and that have set up computer systems or networks for particular and beneficial reasons or purposes. Apparently, for IT and other types of network systems, not only virtual but also physical security is significant to ensure that data and information are well-guarded for the individual or organization’s benefit. Boran, 1999) For this reason, individuals and most especially organizations are focused on implementing various security measures in order to prevent security breaches or to lessen their effects or impacts to the IT or network system once they happen.

For instance, organizations would resort to prevention measures, deterrence or admonition. These three processes contribute to IT or network system security because of their unique purposes – prevention constitutes the implementation of various security measures that will make it difficult for external parties to breach the system, deterrence refers to masking the value and vulnerability of the system by transforming its external structure to become insignificant and unattractive, and admonition pertains to warnings or cautions presented to individuals working for the organization in order for them to avoid committing actions that might jeopardize the security of the IT or network system. Miller, N. D.) The remainder of this text will be billed to present information about admonition, looking into its definition and purpose. In addition, its significance and efficiency in resolving security issues will also be analyzed. Although admonition works better if coupled with deterrence (Miller, N. D.

), admonition alone contributes to the security of IT and network systems. A simple example of admonition is the presence of pop-up signs or windows

that display warnings to IT or network system users prior to their issuance or implementation of commands or protocols. For instance Microsoft Windows applications formulated by Bill Gates are designed with the technology of providing warning or cautionary advices to end users that will tell them the dangers or risks of going through various commands or protocols within the computer system or network. Pop-up boxes or windows contain a variety of information that allow end users to be guided on how to handle risky situations, such as the presentation of various choices that the end user might opt to take in order to prevent breaches and violations to security and security measures. Seifert, Welch, & Komisarczuk, 2006) The usefulness of admonition is evident on how it may be used as a means of preventing the possible threats and risks that come with breaches and violations to IT or network systems and security measures. In addition, IT security strategies should not only focus on the common or obvious problems related to breaches or violations, but also focus on how information within the IT system is restricted or controlled in order to prevent the occurrence of undesirable IT transfers, storage, interpretations, etc.

hat will pose threats and risks to the organization. This is supported by a factual example that looks into the need for admonition systems whenever information is supposed to be shared. For instance, confidential files sent through the IT network or systems are supposed to be kept private by the recipients. Part of admonition IT security strategies are to inform people whenever there are actions, commands, or protocols being made that might leak the confidential information to third parties. Another admonition IT security strategy is to communicate it directly to the recipient as in one-on-

one conversations. (“ Admonition Systems,” 2008) The results or outcomes of admonition is to establish influence and authority over individuals within the organization in order for them to limit or control the sharing or transfer of information whenever it is labeled restricted or confidential. With this in mind, admonition fits the overall security strategy needed by organizations by focusing on two specific parts of the system – the virtual and physical security dimensions of the IT network or system. In addition, if other strategies are present to prevent the onset of IT security breaches or violations and to alter the physical or external dimensions of the IT network or system in order to deceive external parties, admonition focuses on other aspects of IT security strategies.

It completes what other security strategies lack, or rather provides what is missing through its unique and efficient features. The virtual security strategy of admonition is designed within the system already making it possible to monitor the prompts, commands, or protocols being utilized and then limit or control the use of information within the system in order to prevent breaches and violations to IT system security. It guides individuals on how to handle sensitive or private information and data by informing them of the results and outcomes if particular commands will be implemented to release or publish information. (Seifert, Welch, & Komisarczuk, 2006)On the other hand, the physical design of the IT security system is also protected since admonition establishes the affirmation of laws and policies that are important for members of the organization to remember when handling the IT system or network. Whenever individuals remind other people within the organization to secure information, IT security laws and

policies embodied within the IT security strategies are firmly or strictly implemented, while at the same time, the results and outcomes of the implementation process is monitored or supervised in order to ensure that individuals are abiding by IT security rules and laws.