Bead bar consultant activity

The informationtechnologyaspect is a rapidly booming industry in the present influences almost all of the relevant activities in the social and economic fields. Because of this significant influence, most of the major social and economic industries rely much to the value of information and the effects of their exchange in the operations of each respective organization. However, because of the dependence of most economic and social transactions to the value of information, several risk issues are now being considered influential and significant to the information operations.

Included in this aspect are the security threats imposed by (1) poorly written software or improperly configured systems, (2) computer viruses and worms, (3) external breaches, and (4) internal breaches. The first issue posts some significant threat because poorly written or configured software are more vulnerable to breach attack and viruses. Aside from this, poorly made softwares are also likely to become unstable and unreliable for actual use because of the negative characteristics that are likely to have been overlooked in the use of the system.

Computer viruses and worms on the other hand tend to alter the normal processes in the information system causing significant leaks or instability in the operations. External and internal breaches are both threats on the literal means as they manifest unauthorized access to the informations though they vary only from the nature of the source. 2. Develop a security awareness-training plan for employees and franchisees. Knowing the significant threats to information security is an important aspect in the development of a security awareness plan for each organization.

In general, the plan must be able to address each of the known threats including anticipation, development of a defense, and the prevention of future occurrences. The security awareness plan must classify mainly into two approaches namely the information protection and the physical security plan. The first encompassed the protection of the information through firewalls and security system, the protection of the storage facilities, and the access of these informations. The physical security must encompassed the actual factors involve in the protection such as the people involved in the information and others.

The security plan must mainly anticipate the threat through developing a protection against known breach and virus infection, scrutinize and identify the access, prevent any unauthorized connection, and report the possibilities of leaks and the cases of intrusion. Most importantly in the security plan is the constant update, regular development and the close monitoring of the protection system to ensure its effectiveness and reliability against the threats to the information system. 3.

Which Internet-based data backup plans should be used? Part of the security plan, which the organization itself must consider critically, is the aspect of recovery and backup for any intrusion disaster to their information system. Included in this concern is the backup system of the information system and operation of the organization, which is significant for their recovery process. Some of the common approaches to address this need are establishing a security partner to act as a storage facility of the backup data of the organization.

These security partners are commonly internet-based serving as the primary data backup plan of most organization for situation of critical intrusion, infection or breach. The development of the internet-based data backup plan must also be extensive as they are similarly critically to the security plan. Several issues and aspects must be satisfied in this data backup plan such as their protection in terms of alteration, tampering or intrusion, isolation, and the constant update of the backup solution.