Va information security

Law, Security

Information security policies are measures taken by organizations to ensure the security and safety of information of an organization (Stallings, 1995). The policies of an organization pertaining to information and data are bench marks and core resource in any organization. This paper looks at the information security situation in the United States Department of Veteran Affairs (VA) with an aim of analyzing the organization's information security policies, standards and measures used by the organization to ensure confidentiality of its information.

VA has in the recent years been on the spotlight concerning its information security breach specifically it has been accused of being very vulnerable to information security breaches. VA lacks information control system which is vital in access to the organization's information system. VA also lacks enough physical protection of computer facilities, something which leaves its information stored in computers very vulnerable to burglary.

In terms of the human factor in information, security the organization data and vital information is easily accessible to a wide range of staff some of whom do not require access to the information. VA is currently facing the threat of information security in the areas of personal identification information, loss of data, accessibility of data to unauthorized persons, or misuse of information and should deal with the above issues in order to ensure maximum information security.

The information security policies at VA include well laid out procedures for implementing and handling of day-to-day data and information, controlling the employees' access to data and information, careful selection of security

controls. VA has enacted steps aimed at protection its information systems, further it has safeguarded the nearby buildings by making sure that recommended fire protection as well as other hazards such as floods and wind. The equipment at VA is also safe guarded from any hazards such as , natural, environmental, as well as unauthorized access.

In addition, access of data in VA is well safe guarded by use of not-easy-to-hack passwards. These are comprehensive and in compliance with ISO standards. At VA, such are updated very regularly. There is also a full pledged department for supporting the information system of the organization. Since human factor plays a very vital role in information security, alongside the technological issues are human oriented efforts such as awareness campaigns and seminars aimed at enhancing security in VA.

Examples of technological based security measures adapted by VA include the installation of firewalls, installation and constant upgrading and updating of antivirus software, Alongside the above, VA ensures the security measures are controlled through use of security alarms, when there is impending danger as well as ensuring that all incoming emails are scanned. VA has invested in qualified staff and therefore, the quality of security management is guaranteed. In terms of physical security, VA has invested in security management.

In terms of reacting to security breaches, VA has a clear reporting system which culminates in thorough investigations and appropriate course of actions once breaches are reported to the management Disasters can, and do strike when least expected and if no proper systems are in place for data

recovery, massive damage and loss of information as well as equipment can be suffered. The cost is very high and sometimes it is irreparable. Any data protection measure must take into account the facilities, data, hardware and network safety (Summers, 1997).

At VA, the data is invaluable and is crucial since it entails details of veterans' information and if this was to be lost, it can not be regained. Perhaps the hardware, the facilities, and the networks can all be reconstructed. The data protection strategies at VA include, back ups; there exists hard copies of data stored in different locations. Such back ups also are available in online backups and disks. It will be wise though, for VA to include snapshots of disks to act as back ups in the event of data corruption as well as carrying out these back ups regularly.

VA can significantly improve its information security by; training all staff on the information policies as well as standards and make sure such are comprehensive and updated (Neumann, 1995). This is necessary and relevant to VA because some of the information breaches reported there, in the past were related to lack of stringent policies. By ensuring that, evaluation of systems is done properly before system change over in order to avoid setbacks. By training employers on enhanced security measures such as use of passwords; ensuring commitment from top management to safeguard information.

Virus attacks are common in computer networks; therefore it is highly commendable that, VA ensures installation of effective anti-virus software. There is a need to have secure and restricted areas for systems. Although

data encryption is highly commended, access should be guaranteed to make sure that no an authorized person gains access to the back-ups. System hardening is highly recommended since data in VA system is potentially useful and of interest to hackers and therefore it is not unlikely that hostile networks may attempt to hack the information.