Mis security threats

Types and Categories of Threats to IT systems

The management information system helps in the production of all crucial information that is necessary for the effective operation of an organization. Management information system has been considered to be an important part of the control internal system in a given organization. The management information system focuses on the application the documents, various procedures, technology and the people, that the management accountants use in solving their business problems like product costing, service costing service or the development of a business strategy. There are various types of MIS security threats which includes; Hardware theft (servers, Laptop and Desktops theft.); Hardware destruction (Hardware can be destroyed by disasters, like fires, floods, and earthquakes. It can be destroyed by people as well.); Physical data device theft (Thieves can steal data storage devices. Hard disks, CDs, USB flash disks, laptops, desktops, and servers can all be stolen for the data they contain); Accidental release of physical data devices.); (Currie and Galliers, 25). Data destruction by software this the most common security threat in MIS. Programs secretly planted on machines can destroy data.

A virus is a self-replicating program that copies itself from machine to machine, usually over a network. Viruses spread by attaching themselves to other programs. They have various effects, from displaying harmless messages to erasing hard disks. Unlike worms, viruses focus on damaging local data (Oz, 19). A virus can be embedded in a Trojan horse. A Trojan horse is a useful program, like a game, that has malicious software

deliberately embedded within it. There are other poorly written software which are vulnerable to an SQL injection attack.

MIS is security threats can be categorized in the following programs: worms, these are malicious program that largely exploit the operating system to spread itself; Viruses are Programs that infect other programs, adding their own code to them to gain control of the infected files when they are opened; Risk ware are dangerous applications that include software that have no malicious features but could form part of the development environment for malicious programs or could be used by hackers as auxiliary components for malicious programs. Trojans are a category of Programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang ad stealing confidential information. Spyware, they are Software that collects information about a particular user or organization without their knowledge; Root kits, are used to conceal malicious activity.

CISSP

Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by the nonprofit . the body has duties to a collection of topics relevant to information security professionals around the world. The CISSP establishes a common framework of information security terms and principles that allow information security professionals worldwide to discuss debate and resolve matters pertaining to the profession with a common understanding.

Forensic Investigation Methods

Forensic Investigation Methods is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of forensics investigation is to examine digital media in a forensically sound manner with the aim of preserving and recovering, analyzing and presenting reality of information. It is mostly used in investigation of a wide variety of computer crime and computer civil proceedings. The investigation method involves similar techniques and principles to data recovery and other steps and practices designed to create a legal audit trail. Evidences from computer forensics investigations are usually subjected to the same guidelines and practices of other digital evidence.

Legal Requirement for Reporting

The law requires that any information on MIS security threats be treated with due care and should not be misused (Lucey, 17). Information should be confidential and no an authorized user should access. The reporting should comply with the laws and should never go beyond the legal requirement.

Qualifications of Personnel to Hire and Salary

The qualification of personnel is that he or she must have a minimum knowledge and skill necessary to qualify for a specific watch station or maintain a specific equipment for example for management position it requires a bachelors degree. Advancement like leadership is also paramount for the managerial position. The salaries for the personnel vary by specialty and level of responsibility. eg annual wages for the manager varies from that of other personnel’s. Other than getting salaries personnel who are at higher

levels often receivee employment related benefits such as bonuses, insurance covers and stock option plans (Davis, and Olson, 99).

Mitigation

MIS security is day to day process of exercising due care to protect information and information system. To ensure that MIS well protected from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Organization and individuals should ensure that their system is well built in strong passwords to limit access. They should also make sure that their systems are also protected from viruses and worms by installing and keeping on updating their antivirus. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review of information (Rocheleau).

One also has to make sure he or she has adequate anti-virus software and is regularly updated for their computer. Scanning the computer network should be done regularly to eliminate any malware, viruses, spyware and other harmful problems. The firewall should always be turned on; it is a digitally created barrier that helps ones computer system from hackers getting into it.

One should always ensure that important information is always encrypted so that it is not compromised. One can utilize encryption software, the software “ garbles” the data and makes it unintelligible for anyone who hacks into ones computer system (Kilkenny, 17). Also one should not provide personal information to website one knows nothing about. This is especially in those

websites that ask for ones name, address, mailing, bank account number and also ones social security number.

An individual or organization should always create strong passwords for websites that have their personal information stored. To create strong passwords one should use numbers, lower and upper case and also symbols in the password. One should also secure their wireless network and other networks with very strong encrypted passwords a good password should have at least 32 set of characters.

To protect you computer and network from the risk of Intentional network based attacks and cyber threats (data theft, identity fraud and Hacking) and also malicious software such as viruses, Trojan horse, spyware and adware. One should always ensure that the spam blocker is always turned on. This will prevent any unwanted message, like fraudulent emails and phising emails do not get to your inbox.