# Essay on security plan

Business

This paper contains a plan by a university in North Carolina on how to ensure system security of the university's information technology resources. The purpose of this paper is to address issues and problems listed in the article by North Carolina Agricultural and Technical state university on information security. It is a plan that clearly explains the efficient use of resources, especially computer resources like networks and computer systems. To ensure the effective use of all these, there has to be good security so that they function properly and efficiently without any problems. The plan given is meant for the users of computer systems like students in the university, alumni of the university, and vendors among many others. This paper will also look at the issues that need to be improved in the plan contained in this article, so as to eliminate those that will not work.

It highlights the responsibilities of each and every user in ensuring security of the systems and networks in the university are maintained. This includes complying with the laws of the state and those of the university too (North Carolina Agricultural and Technical State University, 2008). The agency and its administration According to North Carolina Agricultural and Technical State University (2008), the administration has an important role to play in the protection of the resources and also in the planning and the administration it makes policies that need to be implemented in the university so that all information is protected against the many threats that it is prone to. The agency of the organization, as explained below has to make necessary changes, for example of the employees who are no longer in the university, so that they are not able to access the information any more, like they used to before. Responsibility to the information technology resources

The responsibility towards ensuring security of the information technology resources in the university is not on one particular person or group of persons, but to all who are in the university fraternity.

The responsibility of various people is discussed below in details (North Carolina Agricultural and Technical State University, 2008). Users Information technology has many resources which include the computer, computer systems, network systems, data, hardware and software. All these components of information technology have to be protected against certain threats that they are exposed to. The components also have to comply with the policies, laws of the university and those of the federal state. It is to ensure that the university is able to meet its goals and mission.

This plan focuses on how the users at different levels in the institution can take responsibility, so that collectively they are able to ensure security of the information technology components (North Carolina Agricultural and Technical State University, 2008). This plan highlights some of the users like the students, personnel in the institution, guest who visit the university, vendors who sell some of the components to the university, and consultants who offer services to the university in regard to the components mentioned above. All these are users of the components, either directly or indirectly. The users should ensure integrity, reliability, confidentiality and availability of the information technology resources in the university. The data in the system should confidential, to mean that there are restricted users to access the data. This is because data in the university includes details of the students which should be private and not be accessed by just anybody.

That is why the users who handle the data should ensure that the systems are safe enough to keep the data safe from such threats. Users also have a responsibility of ensuring that the data and other information technology resources are reliable in terms of the services that they give, like the information that they generate should be reliable. This ensures accuracy and reliance on and of the information, hence of the system too. The resources of the university should be availed to all users who require them, at any time and place, so that they are great benefit to the university’s fraternity. In the long run, with all those responsibilities met by the users, the university is able to meet its goals and missions that have been set.

North Carolina Agricultural and Technical State University (2008) asserts that to be able to meet their responsibilities, the users should do some things that are extra. It includes, logging out their accounts when they are not in use so that no other party has access to the data in the computer systems. Users should also not share any information regarding their accounts with anybody, regardless of who they are, so that privacy and confidentiality is ensured. That means the user is only supposed to trust him or herself, and not any other party. They are not allowed to access any other account that they are not obliged to, regardless of whether the information contained in them was given to them by the account owner. For example, a student should not access the account of another student, especially without the consent of the student to do so; or a personnel working in the finance department is not authorized to access the account of another personnel working in the human resource department.

The university’s resources should be used for the intended purpose, and not any other especially for personal goal or satisfaction. For example, the computers of the university are to be used for the purpose of data entry or processing of activities taking place in the university like students’ details, and not to use them to do personal jobs at the expense of the intended purpose. In case there is any suspected or actual misuse of the university’s resources, it should be reported to administrator or information technology security office (American Institute of Architects, 2007). This is so that immediate action is taken, to ensure that the resources are used well and for the intended purpose to achieve the set goals and mission. Users should also ensure that there is back-up data, in case data is lost, to ensure that they are in a position to access the data again even after it has been lost or been tampered with.

Data may be lost because of various reasons, like due to power interruptions or when the computer systems get spoilt. When data is lost, it might cause a lot of damage to the university because it is vital and very important. If data regarding employees and the salaries status is lost, that means that the employees details and history of the payment of salaries has to be taken again, which is a strenuous activity and may end up not gtting all the data that existed before. American Institute of Architects (2007) stipulates that a firewall can also be used to protect data from unauthorized people, which is in form of hardware or software. As mentioned above, data and information in the university’s system is confidential, hence the need to protect it from access by unauthorized people. Such people may want to access information either for their own selfish gain or to tamper with it so that it suits their needs, or to just access it to get hold of some important information, like bank details among other information.

Firewall has to be installed properly to ensure its effectiveness. If not installed properly, it might prevent any access to the computer systems and other resources even by the authorized people, because of its configurations. Data custodians and administrators They are actively involved in not only the planning and implementation stages but also in ensuring diligence in the resources of information technology in the university. They ensure compliance with the state and university laws regarding information technology resources. It involves ensuring that the resources are up to the standards set by the necessary regulating bodies.

The policies, procedures, guidelines, processes and practices are supposed to meet the set standards according to the laws given by the state and the university too. They have another responsibility of ensuring that the systems have adequate physical security against such threats like theft and burglary so that they are safe. Physical security mainly entails security of the hardware parts of the resources, like of computer parts or cables that are used in the networking with other components (American Institute of Architects, 2007). It becomes very expensive to replace information technology resources in case they are stolen, because of their high prices to purchase them. Hence the need to ensure physical security, like using door locks that are strong, employ security people to guard the premises where the resources are stored.

The premises should be located in a place that is not prone to theft, which is a place that is more secure. They also have a responsibility of finding out the threats that they are prone to, analyze them and come up with possible management strategy to curb the threats. The possible solutions should be documented for easier implementation. Like the users, they have a responsibility of maintaining data confidentiality, integrity, reliability and availability of the resources to others who need the resources. Data custodians have another responsibility of implementing the management strategy that has been selected, like have a policy of setting of the passwords.

For example, they might set a policy of the required characters in any password that is to be set. The characters should be six and follow the rule of the lower and upper case, letters and numbers or any special character. The passwords also are required to be changed every now and then so that the information is protected against threats (American Institute of Architects, 2007). The users may be required to change their passwords after every two months or so. The administrator should also reset high security accounts after every 30 days.

There should be termination of access to resources once an employee has terminated employment, or when the employment has ended. A person who is no longer an employee of the university should be denied access to the resources, on matters like the passwords that he or she used. The passwords should be changed so that the former employee is not able to access information of the university any more, to ensure privacy and confidentiality of the information in the system. The access should be disabled immediately or on termination of the employment, whether through retirement, death or otherwise. Data owners They possess the data that is contained in the systems and that is being protected against the threats.

They are responsible for data integrity; hence they have a great and critical role to play in ensuring security of their own data. They decide who to give their own information and who not to give. That makes them have some crucial responsibilities in ensuring for the security of their information (Giles, 2008). According to Giles (2008), they have a responsibility of disclosing information to the authorized users or those with the legal requirements and obligations to get the information. Data owners are supposed to know who and when to give their information. For example, students should not give their account passwords to anybody; employees should not give their bank details to anybody but to the relevant finance officers.

That will ensure that nobody else can access your personal information except the authorized personnel. They are supposed to maintain a list of the relevant and authorized personnel in the university so that they are able to protect their information. Data owners should develop a policy of electronic records retention and disposition and also exercise the principle of least privileges and separation of duties. They are supposed to develop procedures relating to the granting of, modification of and denial of access to their information to new or the already terminated employees and the transferred employees. They are also required to have adequate knowledge through being trained on the protection of their personal information against unauthorized persons (Giles, 2008).

They should also classy data according to sensitivity, confidentiality, proprietary value or in another criterion as desired. That way, they are able to know the kind of information to disclose, to who and when to disclose it, that is the circumstances for disclosure. Network security It has the responsibility of protecting the integrity, reliability and the confidentiality of the network, data resources and computer systems in the university that are attached to the network. This is done so that access to the university's wired and wireless network is limited to the authorized users only. All the devices that are connected to the network in the university should be properly registered and configured so that they are recognized to access the network (Giles, 2008).

The standard configuration that can be used is the Dynamic Host Configuration Protocol, such that connection to the network is prohibited unless it is approved by the Division of Information Technology. Giles (2008) stipulates that all the devices that are approved for use in the network should be properly screened and protected from all system vulnerabilities, like have the latest antivirus sooftware. It should also have spyware and have passwords so that they are fully protected against all threats prone to it. Even hardware devices must be approved by the Division of Information Technology before being connected to the university's network. Critiques The plan has very well analyzed the responsibilities of many people in the university towards the protection and ensuring security of the components and resources of the information technology resources of the university.

The plan has clearly outlined all the players in the protection of the resources of the information technology components (Giles, 2008). However, it has not properly analyzed the system vulnerabilities and abuse of the resources of the information technology in the university. Especially on matters of the internet, the threats and dangers that the university is prone to when it used the internet. For example threats like hacking, where people access information and use to for their own use and spam messages (Giles, 2008). Where messages are sent to emails of people in the university that contain threats and so on. As result of that, it has not provided the security measures against such threats.

Security This system compares each computer against the checklist in the Security Guide for small ventures. They are running the MBSA (Maiwald & Sieglein, 2002). The following results were therefore produced by these actions: – Spam-filtering software: numerous users are complaining about spam, though there is no protection in place. – Virus protection: antivirus is not present in some computers, others computers have outdated antivirus. In general, nearly all users know the presence of viruses but are a bit unsure about what they could do to prevent them. – Firewall: they thought that the ISP’s router consisted of a firewall, but it doesn’t, so there is none in existence.

-Wireless networking: they are broad open here. It was revealed that after setting this thing up, it started to work immediately, hence, nobody touched any of the settings. The wireless network is open to individuals who have wireless access ability to snoop on the network or freeload on the internet connection. -Web browsing: since everybody thinks that accessing fast internet is a great perk, they are using it all the time without putting into consideration risks associated with its use. It was for instance found through a content filtering audit that 19% of the web browsing was not related to work. It also lack a policy on acceptable use, and no security measures are taken by anyone (Maiwald & Sieglein, 2002).

– Backups: the University backs up data on the server to a Digital Audio Tape drive on a weekly basis, though it has not tested data restoration unless individuals remember to copy local files to the server. This is unsatisfactory because those files are not backed up. The server consists of the University’s primary client database; hence, well-tested backups are crucial just like keeping copies of backup offsite. Skills and knowledge University’s technology consultant is familiar with the entire situation and will be its expert guide. Nevertheless, the University needs to internalize as much of this knowledge as possible by undertaking as much of the work it can.

Doing so will also help the University to save money. Fortunately, university’s technology consultant is a proletarian computer enthusiast. He has attended security training course and is equipped with all necessary skills needed in this sector (Maiwald & Sieglein, 2002). Every member of the project team has read the available security planning guides fromMicrosoftand the Internet Engineering Task Force in preparation.

The University as a whole is sensibly technically literate though they observe computers as tools to get the work done and don’t much regarding how they function. Response planning The University will be contacting technology consultant in the event of a security breach. Technology consultant’s company has a one-hour response policy at all other times to handle serious incidents, like virus infections. Additionally, technology consultant will monitor the server and firewall frequently so as to ensure that no breaches have taken place (Maiwald & Sieglein, 2002). Ongoing maintenance and compliance Manager will be accountable for security on a daily basis, with manager taking the general accountability.

Technology consultant will go on with his own self-education on the subject, subscribe to security bulletins from Microsoft and University’s software supplier, and communicate with technology consultant on a regular basis to supervise compliance with the new rules. Manager will ensure on monthly basis that windows and University’s antivirus software are up-to-date and that the backup and restore processes are functioning efficiently (North Carolina Agricultural and Technical State University, 2008). He will also be accountable for making sure that new computer equipments are configured properly and up-to-date. Technology consultant will also be accountable for making sure that new staff joining the University is trained fully in the University’s security policies and processes. Conclusion In brief, security plan is one of the most significant aspects required in an organization or a company hence needs to be preserved well.

North Carolina Agricultural and Technical State University has been dedicated and doing its best to ensure that it has proper and efficient security plan just like any other company o organization. In order to achieve this, it has hired skilled employees and made use of modern technologies and devices. This has seen it developing its security plan rapidly under the guidance of its newly implemented policies hence placing it in a better place. Nevertheless, since there are some problems that have been encountered in the university despite all measures taken to prevent them while others seems to be unpreventable, the University is supposed to be more vigilant and careful. It should ensure that it makes use of modern technology and all its network and computers are prevented well from viruses and other intruders.

They should all be up-to-date and under care of a highly skilled person with high knowledge of preventing these problem and solving them quickly if they occur.