Good essay on the network system of the institution

Law, Security

Information security plan

Executive summary

Information security plan is meant to protect any resource that relates to information from multiple security threats so that the continuity is maintained. The security plan is meant to cover all the organization's information technology assets against any possible threat. To achieve an effective information security mechanism, a suitable set of controlled crucial. The control includes processes, procedures, and policies organizational structure and software functions. The controls need to be formulated, implemented tracked reviewed and improved to make sure the particular security and business goals of the organization are attained.

The plan guides the confidentiality, privacy and security of an organization in particular critical data and roles of individuals and department for involved data. Information security measures are meant to protect organization assets and keep the confidentiality of the organization's entities. The plan should conform to the information security compliance policy requirements.

A successful information security measure requires the involvement of all the organization's employees.

An information security plan us meant to ensure integrity, availability and confidentiality of information technology assets. It also specifies the documentation procedures and policies that support the goals and the objectives of an organization to meet the ethical and legal objectives in respect to the information technology assets.

Overview of the organization

Overview of the organization

The University of Barton is in the institution of higher learning whose has strived to ensure its information technology assets meets the international standards. The information technology asset is meant to support the student and the administration in running their day to day activities. It is an integral part of the learning facility as the students uses the internet in research and other learning activities.

In this institution, the information technology system is considered a very crucial asset. As such an effective and a robust information system security paramount. A very critical facet of information system security is the ability of the security team to detect or to response to a security failure within the shortest time possible. As such an effective security plan is required

The information system disaster recovery in the organization is carried out by emergency council. Their responsibility is to monitor the security of the information technology asset including overseeing any disaster. The university preparedness plan governs any action performed by this team. The team's key goals ensure that the critical operation in the organization is not interrupted as a result of system security breach.

Organization's alternative network system

Security plan policy

Scope

The security plan covers all the institutions information technology infrastructure, and service delivery in case a disaster strikes. It, therefore,

means an alternative network system is also considered. The alternative network system is an institution’s subsystem that that enables the institution to perform its critical service delivery activities in case the network system is undergoing system downtime. The recovery plan is a section of the entire security plan which spans to any security threat in the organization. Currently, the institution’s system security status has never experienced a major security threat. The key issue is the rate at which the university expands which warrants for a well-established system security. The team’s key objective is to ensure that the response team undergoes an effective and prompt mobilization when a security disaster strikes. The technical results of any security situation are put under consideration in order to provide a technical solution to any security breach. The procedures and steps followed in case a security breach befalls the system is also put under consideration. The plan is also meant to lower the impact of any security threat to both data and service delivery. It also gives a detailed strategic plan for restoring the system.

In general, the security state of the institution’s information system is stable. However, the growth of the university calls for a detained and well formulated security plan so that the institution’s service delivery is not interfered at any situation. The scope of the information technology assets is also identified. It includes the procedures and guideline of using these assets by different users.

It also includes Data security policy guidelines that as organizations have put in place to ensure business continuity and compliance. It includes any

activity relating to virtualization, compliance to objective, logging and monitoring and business continuity (Beiver 2010)

Possible IT security breach scenarios

The security of the data center is very critical for any information system. Attackers always target the data center since they are aware of the critical state of the information therein. Any attack that targets the data center regardless of its origin is a potential threat to the system. As such, it should be accorded high priority. The challenge comes in the system is trying to meet the grown demands of the system. In such situation, the system tends to get compromised hence making it vulnerability to attacks.

Another possible threat related to change in the user. In some situation, the network administrator keeps user accounts that are not functional. It implies that someone can get into the system through such weakness.

Procedures for Disaster recovery

The security disaster recovery process undergoes the following steps

Disaster recovery procedures

Information Security Plan Overview

An organization’s information system and network system are critical assets that need maximum security. The security in this context entails both physical and logical security. For an institution to ensure security of its network system, they have to invest heavily in security. The rate at which automation is done in the business sector is very rapid and therefore calls for intense network system security to ensure that the company’s business and financial information is kept safe. The most significant information in a the

company is the software code repositories, employee information, the information concerning the customers, financial information such as billing data and the employee's information (Yar, 2009). The information or rather data should be kept in the datacenter and mechanism is supposed to be put in place to ensure that the data is protected and preserved. In addition, access to this information should be restricted so that the organization's data integrity is maintained.

Risk Assessment –TBD

Potential physical vulnerabilities and threats

The company's information system faces the following physical risks. The most prevalent physical threats are:

- Physical theft of information system assets-Physical theft is where the company's information system asset such as hardware or data is stolen. For instance, a puppet master accesses the premise and exploit the physical vulnerability to steal the router

- Physical destruction by fire- A fire can destroy both hardware and data in case there is an a fire breakout in the pharmacy's premises

The most common physical vulnerability is a lack of adequate physical security. Compromised physical security gives room for thieves, unauthorized individuals and terrorist. On the other hand, fire breakout can occur as a result of faulty electricity connection, explosion as a result of reactive chemicals in the chemist.

Potential logical threats and vulnerabilities

Weak passwords are the greatest issue to the institution's information system. The risk mostly affects the system users who give commonly known username and password as default credential is unauthorized access via default credential

The most prevalent logical threat which the company faces is abuse of system access rights. This kind of threat is mostly executed by the employees in a company in and intention of vengeance or sabotage. Detecting such issue is cumbersome since the intrusion will be taking place internally and hence task tracking may be a challenge. The employees use his or her right to access the system to make alteration and modification of data. The motive is financial gains. One example is an employee in the IT department of a water providing company can change the figures of some specific customer details then liaise with the holders of those accounts for payment.

Another Potential logical threat is malware. It is a malicious code that is built to obtain illegally, track and block the right of the user to get access to the system. An example of this threat is where someone or an individual tries to log on to the system or a website like an email account, but the system, or the site fails to authenticate the user.

The second logical threat is SQL injection. It is a unique threat that targets the web pages of the system application. It cuts down the communication between the database and the system application interface. This threat is common in the organization where system implementation is taking place. An example is a situation where an attacker alters the name of the database

and hence disconnects it from the user interface.

Another threat is where the rogue user gets illegal access to the system via weak ACLs or when the configuration of an ACL is done wrongly. It gives a loop-hole to attackers to get access to the system and perform destructive task that can hinder the operation of a system or event can result to complete denial of services

The second vulnerability is violation of acceptable system user policies. In some companies, the system once logged in by the user will remain on till logged out. A user can negligently abandon the system while logged in and go out. It can give an opportunity to an unauthorized person to access the system and facilitate any harmful event like altering the data with the intention of causing an embarrassment to the company or the owner. An example of this is where somebody forgets to log from his email account, and another person comes and sends abusive or vulgar mails to some group of people. It can be a detrimental to the user's attribute because everybody believes that the message comes from the rightful owner of the account. To eliminate this threat, everybody should be careful while using such system by ensuring that the log out process has been affected anytime you can quit from using the system.

Security Standards for Development and Deployment –TBD

The security plan will comply with the requirement of National institute of standards and technology. NIST develops and gives guidelines that should be adhered to by any business or institution. The body also gives directive on the security policies and the information security best practice.

The body demands that the company itself be responsible in ensuring that the developed policies are implemented and observed by the employees. They also recommend the most effective security tools. For instance, virtualization IS Citrix XenDesktop. This technology uses granular policies to separates the interaction of the end uses that are using virtual desktop and other application from the partition where these programs are installed. All the work station computers users make use of virtual replication of the critical data. When they make any alteration, the changes are facilitated via the network to the database in the datacenter.

Vulnerability Management –TBD

Implementation of secured information system infrastructure

The Security challenge that company's management face is ensuring that the security of their sensitive information is achieved and guaranteed at the simplest way possible. As such, they should look for a way of ensuring the data is stored in place where the information cannot get out in any way. The best way to do this is keeping the data in the datacenter so that that sophisticated tools for watching, controlling and monitoring can be used. In addition, there are EISA policies that regulate the access to sensitive data location (Palmer, 2010).

Strategy for dealing with logical vulnerabilities and threats

Major areas that an organization should work on to ensure data and information security in their system are confidentiality, integrity and availability. Information confidentiality enables the organization's sensitive information to be a secret so that it does not fall into the hands of

unauthorized persons, for example, the competitors. Information integrity ensures that the data that is stored is accurate and serves the purpose and is always up to date. Data availability enables information to be present any time the organization required. It is by preventing any vulnerability for example denial of service (Straub & Baskerville, 2008).

Use of a firewall is also necessary because there is some information that are supposed to be known by the management only hence the information that the other employees get should be filtered. In their network, there should be two firewalls: enterprise firewall and DMZ firewall that are used to facilitate data confidentiality by filtering the information that the some employee's access. In addition, the entire workstation computer should have the latest version of anti-viruses to deal with upcoming viruses.

The solution to curb this access control is using access gateway from Citrix. This gateway is the most secure remedy for access control. It can be placed as a component Citrix platform that combines a variety of performance and security component or as an SSL VPN that is dedicated to one component (Palmer, 2010). This gateway uses SSL/TLS standardized encryption to ensure that the configuration across the network that is based in the headquarters and at the same time facilitate a user authentication that is dual-factor. There is a need to use access gate-way as the only way to access the data in the datacenter for every workstation used by the healthcare and the employees in the headquarters. It will facilitate a secure connection via encrypted and secure media that ensures network and information security.

The best method assessing the security of the system and ensuring

assurance is performance-tracking. Tools such as those used to track and rate the DNS server tasks using system tracker, for example, is the statistical counters. Platform SDK for a particular system also has the tools that can be used to trouble shoots the DNS for examples a network application that uses java can be troubleshoot using the jdk. To ensure these, the component of the site should have a way of tracking the data that pass through the network to curb all the cyber-crime that may be involved.

Windows Server backup and restore are the components of windows environment that enables you to create a backup and retrieve the data or information using the windows properties. Active Directory backup and restore is where the backup is created within the system using system properties that are related to each other. For example system start-up files and system registry files, Active Directory defragmentation where the administrator used the group policy group objects of the active directory to slit and manage the different groups of computer users

References

Blokdijk, G. (2008). Disaster recovery 100 Success secrets – IT business continuity, disaster recovery planning and services. Lulu. com.

Books, L. (2010). Business continuity and disaster recovery: Business continuity planning, backup, carbonite, abnormal situation management. General Books LLC.

Rittinghouse, J. (2009). Business continuity and disaster recovery for InfoSec managers. Digital Press.

Roebuck, K. (2011). Business continuity and disaster recovery: High-impact

technology. Emereo Pty Limited.

Snedaker, S. (2007). Business continuity and disaster recovery planning for IT professionals. Syngress.

Middleton, B. (2005). Cybercrime investigator's field guide. Auerbach Publications.

Ransome, J., & Rittinghouse, J. (2009). VoIP security. Digital Press.

Rosenberg, R. S. (2006). The social impact of computers. Emerald Group Publishing.

Salomon, D. (2007). Data privacy and security. Springer.

Trevor, J. (2011). Cyber Threat: Improving Prevention and Prosecution" Hearing Before the Subcommittee on Technology, Terrorism. General Books.

Wall, D. (2009). Crime and the Internet. Routledge.

Wiles, J., & Cardwell, K. (2007). The best damn cybercrime and digital forensics book period. Syngress.