Testing and monitoring security controls assignment

Testing and monitoring security controls can come in different factors. Monitoring security is by far Important because you need to know what's going on before you can announce It. Networking abuse is by far the biggest baseline anomaly. For employees who have access to the internet, the network can be used to stream media, to access social websites and to download unauthorized software or free software which has vulnerabilities a long with that.

People will always be tempted to go onto the network ND to browse the web on their own. Employees can dollar music or videos and possibly games which hand affect the security controls sometimes when those who don't have authorized access to the network, they will continuously try to attempt to connect. Its best to notify anyone who Is authorized on the network to know that there Is an unauthorized attempt to log In. There are created polices that are made Just to Inform employees of risk managing and prevention. Notify are very Important to the workstation.

All employees must be able to know when there Is authentication failure. Viewing log files can show all the security events which allow an administrator to check into it and find he root causes. Other suspicious indications are a large amount of requests for specific file. This takes a while for a web site to be compromised. This take a lot of trial and error as the hacker has to find exploits to determine access of a URL. The URL that is being attacked will change on each request and chances are the file portion will stay the same.

Given the following list of end-user policy violations and security breaches, select three breaches and identify tragedies to control and monitor each event to mitigate risk and minimize exposure. 1 . A user made unauthorized use of network resources by attacking network entities. You are potentially sabotaged by an employee or employer. Solution can help by viewing the log files and reviewing the activities then confront the user about it. Log files include all security events and it’s very important that these are reviewed first as it can indicate attempted violations or resources or changes in configurations.

Business hours should apply on usage of network. 2. Having a predictable password is the biggest mistake and issue of all time. Passwords are the key to protection and to protect the password it must be difficult and appropriate. Having a user password means vulnerability therefore user passwords should be a minimum of 6-10 characters long including or excluding capitalization. Weak passwords are passwords that meet the requirement like Yahoo! When It comes to security breaches, passwords need to have strict requirements such as mandatory limit of caps, symbols and characters.

Length also has an effect. Anything more than eight harassers have less chance of being cracked. 3. Sensitive laptop data Is unencrypted and susceptible to physical theft. This Is total responsibility of the owner of this confidential and Important Information In the laptop. The responsibility Lies In the hand of the person who DID not encrypt their Information. The solution to this Is to be better prepared to ensure encrypting and that data

Information and hard drives are also encrypted. This way the hacker or the robber can’t access any of the data because it must be decrypted with a key.

Testing and Monitoring Security Controls By beautiful 2 Unit 5 Assignment 1 : Testing and Monitoring Security Controls Testing and far important because you need to know what’s going on before you can announce it. Don’t have authorized access to the network, they will continuously try to attempt to connect. Its best to notify anyone who is authorized on the network to know that there is an unauthorized attempt to log in. There are created policies that are made just to inform employees of risk managing and prevention. Notify are very important to the workstation.

All employees must be able to know when there is authentication t can indicate attempted violations or resources or changes in configurations. That meet the requirement like Yahoo! When it comes to security breaches, characters have less chance of being cracked. 3. Sensitive laptop data is unencrypted and susceptible to physical theft. This is total responsibility of the owner of this confidential and important information in the laptop. The responsibility lies in the hand of the person who DID not encrypt their information.