Security monitoring

Security Monitoring Amy Smart CMGT/442 University of Phoenix Online Instructor: James Summerlin April 15, 2013 Security Monitoring In this paper we will be discussing security monitoring techniques that can and should be used within an organization to help put together an solid action plan when there is an risk identified. For any business or organization to ensure that they are conducting quality business to their customers as well as achieving their businessgoalsshould consider risk management as an huge part of their organization. Security Monitoring Process

The organization IT department and e- commerce applications are the ones that conduct security monitoring and measuring. Security monitoring is very important, because it is the process of preventing attacks and responding to threats that could happen in the future. An organizations can prevent small risk from turning into a bigger and more expensive problem by taking preventative steps. The IT department should be monitoring the system at all times and it must be implemented both externally and internally. However the first step each organization should take when starting the monitoring system is to first discuss what a potential risk is.

For an organization to truly have an secure system they must determine an list of risk. Businesses and organizations can use security monitoring to ensure both integrity and confidentiality for sensitive information. As well as holding IT administrators responsible for keeping their organizations sensitive and financial assets safe and secure from unwanted eyes. Internal IT and Secure Monitoring Processes The security monitoring activities that should be conducted in an organization with both internal IT payroll, human resources, inventory, general ledger, inventory monitoring.

However these internal structures constantly grow and increase revenue and the possible risks are also always growing and increasing. So for an organization to make sure that there information is safe and secure they will have to make sure that they have their network secure. There are an number of tools an business or organization could use to help keep the network secure, but we will only be discussing a few. The first step would be to create an good an strong password. The pros on having an password would be that it helps to protect unwanted users on their computers.

However employees could forget the password so the organization would have to decide if that was an problem then they may want to have an only IT members knowing the password. Then we would have to decide which network firewall would work best for their business. The network firewall is very important to have, because it protects the network from unwanted users and can be used from small company networks to large corporate system. Another great tool to use to keep the organization network secure internet filtering software and monitoring tools, which would be used to protect their employers from inappropriate usage from their employees.

Lastly vulnerability assessment and penetration testing is an very great tool to use, because any company that does any business online should and needs to perform an regular vulnerability assessment on their network. The next step in keeping all the organization personal and financial information secure would be to set in place an antivirus protection. Antivirus is important to have because it will protect the computer and the information store in it safe from virus that can wreak havoc on your computer and the information store upon it as well.

However antivirus cannot do it alone so by also making sure the organization computer are always up-to- date and running properly is another step closer to being fully protected. Some examples of Antivirus software would be Norton, AVG, Shield Deluxe, or Panda Antivirus Pro, and all are very good antivirus software to use to keep their computers safe and secure. Data security is the next step in which an organization needs to take to make sure that their whole system is safe and secure from the inside out. Establishing an strong password is the first level of defense to keeping data secure.

The next would be to make sure that there is an strong firewall, by having firewalls in place will help to keep the network properly protected from viruses and hackers. Data security is also achieved by having antivirus and anti- malware which is an systems last line of defense if everything else has failed. Having an organizations computer systems up to date and running properly is another great step to keeping their data safe, because if their computer software is not up to date then it won't be able to provide the upmost protection towards their personal data.

Performing backups to the external hard drive is the best way to insure that all the data is stored safely. Then lastly is to have their IT department monitor diligently so that they can look for specific information coming out of their network. In conclusion we have discussed the security monitoring activities that should be conducted in an organization with both internal IT payroll, human resources, inventory, general ledger, inventory monitoring. As well as how important each one of these activities are and how they help to monitor and keep their system safe and secure from unwanted eyes.