Final persuasive essay

Science, Computer Science

Associate Level Material Appendix B Information Security Policy Student Name: University of Phoenix IT/244 Intro to IT Security Instructor's Name: Date: Table of Contents Table of Contents1 1. Executive Summary1 2. Introduction2 3. Disaster Recovery Plan4 4. Physical Security Policy7 5. Access Control Policy11 6. Network Security Policy14 7. References17 Executive Summary Due in Week Nine: Write 3 to 4 paragraphs giving a bottom-line summary of the specific measureablegoalsand objectives of the security plan, which can be implemented to define optimal security architecture for the selected business scenario.

There is no such thing as complete security. Offensive security measures are always being devised to compromise the integrity of a network. Security precautions are constantly being developed in order to battle this constant onsalught of attacks. Any professional organization who cares about the security fo their system, is pretty much guaranteed to put some sort of physical or logical security measures in place. Physical security measures are procautions that inckude things such as security cameras, guards, Id badges, or even a tridtional lock and key.

These types of defense are designed to be preventative of external attakcs or infiltration. Logical Security systems include things such as user admin accounts, passwords, and principles like least privelage that prevent unecesary access all contribute to the prevention of external as weel as internal threats. With the proper security measure in place, Sunica Entertainment Co. should be well on their way to ensuring the integrity of their network as well as increasing the eficciency of support and access. With

the new servers, administrators will also be able to login to access information or perform maintenance from any Sunica branch.

This improved control and security will only improve thehealthof this company. Introduction Due in Week One: Give an overview of the company and the security goals to be achieved. 1 Company overview As relates to your selected scenario, give a brief 100- to 200-word overview of the company. I decided to go with the SunicaMusicand Movie Franchise. Sunica is a multimedia media chain with four different locations. The four stores lack thetechnologyto synchronize their sales as well as their inventories. The four stores needs to implement a system that will collaborate the information from all four locations to one central database.

This insufficient technology has cost Sunica unnecessary staffing as well as spending. By implementing a central web server, Sunica can ensure that all the locations will have access to information regarding inventory, accounting, or any up-to-date information the customer may want to know. 2 Security policy overview Of the different types of security policies—program-level, program-framework, issue-specific, and system-specific—briefly cover which type is appropriate to your selected business scenario and why.

Sunica could actually benefit from implementing multiple policies such as program-framework and system-specific to ensure the company has a secure foundation. A system-specific policy would ensure that the administrators and the employees had specific policies to abide by. 3 Security policy goals As applies to your selected scenario, explain how the confidentiality, integrity, and availability principles of information security will be addressed

by the information security policy. 1 Confidentiality Briefly explain how the policy will protect information.

Just like any effective system, there must be a hierarchy of rights and capabilities. In order to establish a truly secure VPN workspace, the company needs to create user-specific logon. 2 Integrity Give a brief overview of how the policy will provide rules for authentication and verification. Include a description of formal methods and system transactions. With user-specific logons, the system will not be publicly accessible. Secure data logs should be backed up on servers in order to track employee accessibility to make sure there is no internal problems. 3 Availability

Briefly describe how the policy will address system back-up and recovery, access control, and quality of service. To ensure a successful and thriving system, Sunica needs to implement a disaster plan that is capable of backup and recovery. If the disaster plan is configured correctly both physically and at the application level, then Sunica can back up and log critical information to the company such as payroll, email, finances, etc. Disaster Recovery Plan Due in Week Three: For your selected scenario, describe the key elements of the Disaster Recovery Plan to be used in case of a disaster and the plan for testing the DRP. Risk Assessment 1 Critical business processes List the mission-critical business systems and services that must be protected by the DRP. A well designed Disaster Recovery Program can help any business over come imminent disasters likeMother Nature, security breaches, equipmentfailure, outside threats, etc. First off, a rick analysis should be put together to understand the potential problems that could occur and how to resolve them. The mission-critical business systems should include all of the

companies valuable information that is required to keep the business profitable.

For Sunica, the systems could include anything along the lines of inventory, email, pricing, communications, etc. 2 Internal, external, and en 3 Internal, external, and environmental risks Briefly discuss the internal, external, and environmental risks, which might be likely to affect the business and result in loss of the facility, loss of life, or loss of assets. Threats could include weather, fire or chemical, earth movement, structural failure, energy, biological, or human. As stated earlier, disasters are imminent within any organization.

Natural disasters are unpredictable, inescapable, and can often times be detrimental to an organization. Earthquakes, fires, floods, tornadoes, etc; these are all examples of natural disasters that can cripple any company's systems. Internal disasters could be anything from an internal security breach all the ay t sabotage. If an organization keeps a close eye on its employees and systems, it can sometimes detect signs of foul play before it starts. External disasters are things outside of the company that cannot be controlled, such as the economy, popular trends, unions, strikes, etc. 2 Disaster Recovery Strategy

Of the strategies of shared-site agreements, alternate sites, hot sites, cold sites, and warm sites, identify which of these recovery strategies is most appropriate for your selected scenario and why. Because Sunica is updating its systems to use a WAN in order to collaborate information, a third party site for backup is essential to the success of their new systems. Before the upgrade, Sunica had no choice but to store their data on site at each

location. Because of the accessibility of the new systems, Sunica can backup their data to a third party server and use a warm-site to take control if the main systems are compromised. Disaster Recovery Test Plan For each testing method listed, briefly describe each method and your rationale for why it will or will not be included in your DRP test plan. 1 Walk-throughs A walk-through test is the only way to fully ensure that the system has a solid foundation that is free of any errors. The test will spot out weak points in the systems design, as well as necessary changes and adjustments. The results of the test should be implemented in the system to increase its success and productivity. 2 Simulations

This section of the plan should be self explanatory given the title. Generally a fake disaster is created in order to implement the companies DRP and measure its effectiveness. 3 Checklists Another self explanatory title that basically goes over the requirements Sunica needs in order to operate effectively with the new system. This can also be an incredibly useful resource to use while testing and learning the new systems. 4 Parallel testing Parallel testing a pretty simple concept, but an important step in the recovery plan.

For parallel testing, the company must run their current systems in juxtaposition to the systems at the warm site. This will measure the functionality and efficiency of the data transfer between the two systems. 5 Full interruption Full interruption is the final stage of the plan which indicates you are ready to take the training wheels off. This is not a drill people; this test literally shuts off the systems like the case of a real disaster and does a

final test to ensure that that Sunica experiences the least downtime possible during an actual emergency.

Physical Security Policy Due in Week Five: Outline the Physical Security Policy. Merkow and Breithaupt (2006) state, “ an often overlooked connection between physical systems (computer hardware) and logical systems (the software that runs on it) is that, in order to protect logical systems, the hardware running them must be physically secure” (p. 165). Describe the policies for securing the facilities and the policies of securing the information systems. Outline the controls needed for each category as relates to your selected scenario. These controls may include the following:

Physical controls (such as perimeter security controls, badges, keys and combination locks, cameras, barricades, fencing, security dogs, lighting, and separating the workplace into functional areas) Technical controls (such as smart cards, audit trails or access logs, intrusion detection, alarm systems, and biometrics) Environmental or life-safety controls (such as power, fire detection and suppression, heating, ventilation, and air conditioning) 1 Security of the building facilities 1 Physical entry controls Physical systems are essential to the foundation of a company and it's logical systems.

Without secure hardware to host the logical operations, the whole system would be useless. Physical security can include anything from security cards, photoID badges, security cameras, etc. These precautions are implemented to protect against natural occurring and man made physical threats. As far as Sunica's physical security is concerned, security cameras and alarms at each of their locations would help ensure the physical security of each of their branches. Access ID badges also may be implemented at the location of

the warm site for access to the servers that store the company's data. 2 Security offices, rooms and facilities

The off-site location used to manage SMM's systems should be managed by a small security force that implements the use of security badges and access ID checks. There will have to be rooms set aside for monitoring equipment to keep tabs on both the security cameras, and system access to the logical systems through administrative users. 3 Isolated delivery and loading areas Delivery and loading areas need to be in a secure location that is sut off from the secure portions of the building. By having physical guards and cameras to monitor the delivery and loading areas, they can help ensure that physical security breaches are kept to a minimum.

You also need to make sure there is no access to any secure part of the building from the delivery areas, unless it is protected with the proper security restrictions. 2 Security of the information systems 1 Workplace protection Workplace protection in the information systems require several different levels of monitoring, access, and administration. As discussed earlier in the physical security, a designated and secure area should be selected for monitoring equipment on both the physical and logical security systems. 2 Unused ports and cabling

Unused ports and cabling can be an access point for all types of infiltration if not properly secured. All unused ports should be immediately secured when not in use. If external visitors require access to these ports, advances notice should be given to the network admin in order to provision temporary user access. 3 Network/server equipment Network and server equipment are the backbone of Sunica's information systems and must be secured at all cost.

The server rooms should not be accessed regularly except for inspection and maintenance.

The network equipment should be kept a secure climate-controlled room that is cut-off from most natural disasters or occurrences that could be out of the company's control. Access should be monitored with proper restrictions to only those with proper access to this vital equipment. 4 Equipment maintenance Equipment maintenance is something that should be done on a regular but sparingly basis. Server rooms should not be accessed often in order to reduce possible infiltration to the information that is critical to Sunica's systems. Maintenance can include anything from updates, replacing tapes, repairing ports/cables, and even climate control.

The rooms containing this important equipment needs to be well ventilated and cooled due to the touchy reactions to heat this equipment demonstrates. 5 Security of laptops/roaming equipment The security of laptops and other mobile equipment used by employees can be a huge vulnerability in the security of Sunica's systems. Each employee who is assigned any sort of mobile equipment must sign a legal disclaimer against any unlawful uses. Security features must also be implemented by the network administrator, in order to prevent and monitor any suspicious behavior on the company's roaming equipment.

Access Control Policy Due in Week Seven: Outline the Access Control Policy. Describe how access control methodologies work to secure information systems 1 Authentication Describe how and why authentication credentials are used to identify and control access to files, screens, and systems. Include a discussion of the principles of authentication such as passwords,

multifactor authentication, biometrics, and single-sign-on. Access controls are a collection of synchronized applications and mechanisms that ensure the integrity of an information system's security.

By ensuring that every login to the network is on a constantly monitored system, a network administrator can spot errors in the network or possible security infiltrations before they get out of control. In order for any employee to access the database, they will need a secure login and password with access to only systems necessary to complete their duties. 2 Access control strategy 1 Discretionary access control Describe how and why discretionary access control will be used. Include an explanation of how the principle of least privilege applies to assure confidentiality.

Explain who the information owner who is responsible for the information and has the discretion to dictate access to that information. The Discretionary access control (DAC) mechanism is the dictator of networking systems in the sense that it assigns an individual information owner who decides who gets control of what. Although the system may seem unfair, it is a necessary precaution to ensure that the principle of least privelage is applied correctly. The DAC sets the foundation for Sunica's systems and will ensure that they are running as efficiently and securely as possible. Mandatory access control Describe how and why mandatory access control will be used. A Mandatory access control (MAC), also referred to as a nondiscretionary access control is a mechanism that determines who gains access to information based on a system of objects and labels. In a MAC system, duristiction is based on levels of access that each contain secure information only accessible to those selected to receive it. MAC is most

commonly seen in the military. Its that classic manilla folder with “ top secret” stamped on it that is slapped on the presidents desk after a major crisis has occurred.

SMM is not a military, its a media company; and this level of security would only overcomplicate their needs. 3 Role-based access control Describe how and why role-based access control will be used. Role-based access control (RBAC) is exactly that; it sorts users into role-based groups with the same common needs to complete a given task. RBAC can be handy for impromptu granting and revoking of access to individual groups. By having a pre-determined access control for a certain area of information, it is easy to just shuffle people back and forth as needed.

This is great for places like call centers with a high turnover rate and would be a very simple way to catagorize employee access at Sunica Media Ent. Flexible controls are also needed for constantly entering new members information into the databse. 3 Remote access Describe the policies for remote user access and authentication via dial-in user services and Virtual Private Networks (VPN) Although remote access can be extremely useful for network adminstrators, it must be implemented carefully to ensure that the wrong individual does not have the ability to use this access.

Remote Access services are server based applications that make it possible to dial in to a system's network from any remote location that can establish a connection with their servers. Most companies impliment a Virtual Private Network (VPN) connection that allows remote users to access the corporate infrastructure. Essentially, you are creating a private virtual network on your own ISP by retrieving the information across a WAN from the origin or

servers. VPNs use a very secure ecnryption and authenticates both the senders and receivers on either end.

This allows any SMM employee who requires access to the corporate systems to pull up that information from anywhere with a connection to the internet. This makes sick leave, hospital time, vacations, and other absences less detrimental to the production of the company. Network Security Policy Due in Week Nine: Outline the Network Security Policy. As each link in the chain of network protocols can be attacked, describe the policies covering security services for network access and network security control devices. 1 Data network overview

Provide an overview of the network configuration that the company uses. Discuss each network type of Local Area Network (LAN), Wide Area Network (WAN), Internet, intranet, and extranet. Include how the network type is employed in your selected scenario. Sunica Music Co. needs to implement a solid security policy to make sure their systems are secure. All stores should have extranets thats dial into third party server using an employee login. All employees should have the policy of least security implemented on their user accounts by the system admin.

This will ensure that system traffic is kept to a minimum but allows employees ample access to system information. 2 Network security services For each security service, briefly describe how it is used to protect a network from attack. Include why the service will be used for network security as relates to your selected scenario, or why it is not applicable in this circumstance. 1 Authentication Authenication could include different type of physical and logical security. Anything from access ID badges to

administrative logins could help eensure the integrity of the system. Access control Access control must be maintaned in order to ensures that a system doesn; t get sloppy. Things like the principle of least privelage help ensure that there are no loose ends in the network that could be potential security threats. 3 Data confidentiality Data confidentiality can help be maintained in several different ways. By changing the IP address off the destination of a packet, you can ensure that only the person the message was intended for reads it. Sunica also needs to make sure that the wrong people cant access the right information. Data integrity Data integrity ensures that no sort of change is made without be monitored or recorded to help prevent foul play. Data Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality. 5 Nonrepudiation Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation. 6 Logging and monitoring Loggign and monitoring can be perhaps one of the most critical security features to a system.

By logging all activity, there can evidence to look back upon in order to solidify any information that may pertain to the integrity of the systm; s security. 3 Firewall system Outline the roles of the following network security control devices and how these basic security infrastructures are used to protect the company’s network against malicious activity. Provide a description of each type of firewall system and how it is used to protect the network. Include how the firewall system is or is not applicable to the company’s network configuration in your selected scenario. Packet-filtering

router firewall system There are several different types of firewalls that can help keep Sunics's information protected. Firewalls are like a giant net that surround a network and only allow certified information to enter. When setting up packet filters, you must first determine what filtering capabilities your router has and where you want to filter. 2 Screened host firewall system The screened host firewall combines a packet-filtering router with an application gateway located on the protected subnet side of the router. The application gateway needs only one network interface.

This firewalls is simply a version of a dual-homed gateway that can be used to separate components of the firewall onto separate systems. 3 Screened-Subnet firewall system This firewalls is simply a version of a dual-homed gateway that can be used to separate components of the firewall onto separate systems which achieve greater throughput and flexibility. References Cite all your references by adding the pertinent information to this section by following this example. American Psychological Association. (2001). Publication manual of the American Psychological Association (5th ed.). Washington, DC: Author.