Information Security Framework for ABCD Company

Stephen Jenkins

East Carolina University

ICTN 4040: Enterprise Information Security

Instructor: Peng Li

May 24, 2018

Abstract

This paper will emphasize a list of recommendations for establishing an efficient information security network within the ABCD Company. Along with the provided list of recommendations an explanation on how to conform to the requirements of the Sarbanes-Oxley Act. A part of making sure that these security regulations are being met is by using the principle of separation of duties. This paper will indicate how implementing policies physical security, logical security, access control, and network security applications can provide the necessary information security for ABCD Company to meet the necessary confidentiality, integrity and availability of the company information systems.

Executive Summary

There are several objectives for ABCD Company to implement an Information Security Policy that will be effective in securing its network as well as the physical environment of a facility. This policy can be created by combining the knowledge one has gained from word of mouth from peers and from the adopted information security framework practices from institutions such as National Institute of Standard Technology (NIST) or ISO 27000 series. In order for you to create an effective Information Security Policy that will perform and be effective as intended you must rely on principle-based analysis, practices and sound decision making.

There are 12 security principles according to Merkow, M. and Breithaupt, J. (2014) and concepts that should be considered when providing security for a network. Principle 1 is "There is no such thing as absolute security". There is no defined way to providing security. Principle 2 is "The three security goals are confidentiality, integrity, and availability". The third principle of information security is "Defense in depth as strategy. Defense in depth as strategy would include several layers of protection that are implemented to prevent intrusion. Principle 4 is "When left on their own, people tend to make the worst security decisions". This consists of individuals providing usernames and passwords to other users, unauthorized users or the sharing of access passwords between users. Principle 5 is "Computer security depends on two types of requirements: functional and assurance". The functional requirements of a system include indicating if the system is performing as promised. The assurance requirement is whether the system performs the right functions in the right way. Principle 6 of information security is that "Security through obscurity is not an answer". The concept of this principle is that by hiding the details of what the security layers are protecting thinking that this is sufficient enough to prevent an intrusion attack. Principle 7 of information security is "Security = Risk Management".

Principle 8 is the use of three types of security controls preventative, detective, and responsive". This includes creating processes to be followed, implementing controlled security measures to prevent compromise, and responding to compromised attempts on the network environment. Principle 9 of information security is "Complexity is the enemy of security". The basic concept of this principle is that the more complex your system is, the more difficult it becomes to secure it while still allowing it to operate as intended. Principle 10 is "Fear, uncertainty, and doubt do not work in selling security". Principle 11 is "People, process, and technology are all needed to adequately secure a system or facility". Principle 12 includes "Open disclosure of vulnerabilities is good for security". If these principles are all taken into consideration when providing security for ABCD Company you can be assured that all measures will be covered.

ABCD Company has 50 offices in all geographical areas of the United States. With each location having its on local area network that is connected to other location across a wide area network, it is important to ensure security across the wide area network (WAN) so that all data and information is secure from end-to-end transport. With employees frequently traveling between sites and the need for accessing network resources is necessary there must be a plan so that traveling or relocating employees can gain access to the network system efficiently while still providing a high level of security. With information of value passing over an open medium such as the Internet it is critical that this information is protected and safely stored.

ABCD Company have rented office space with power, HVAC system and network connectivity that is ready to get equipment up and running once brought to the site. These sites are known as backup cold sites in case of a disaster. It is our goal to ensure that a well created Business Continuity Plan along with a Recovery Plan has been implemented to getting the network computer system up and running in case disaster strikes.

Physical Security Policy

Threats to a physical security come in different forms which includes natural disasters, emergency situations, and human threats. Natural disasters include threats such as tornadoes, hurricanes, flooding, fire, humidity, ice along with others. Emergency disasters include threats such as a loss of power, surge in power, loss of communications, loss of utilities, or spread of a virus. Human disasters that may occur includes strikes that are being taken by employees, sabotage of a company's operation, personnel loss due to illness, injury, death or termination, theft and threats by unauthorized personnel or individuals. To reduce these vulnerabilities and thwart these attacks a solid physical security policy will need to be established to maintain a secure facility. Physical security is protecting and controlling who has access to a physical constructed facility so that unauthorized users cannot gain access. Physical security domain involves safeguarding against any threats to the physical environment of an infrastructure that are intentional and unintentional. These threats can be minimized or prevented by implementing security checks such as: 24-hour armed security guards, access badges, baggage check and x-ray devices. To minimize security vulnerabilities in the ABCD Company physical security actions such as high fencing around the perimeter of the building should be installed, additional video surveillance cameras added and card scanners at all entrances. Restricting work areas can be an effective attempt to secure company assets and entrances into other accessible areas. This can be done by issuing access cards or badges to allow individuals into specific areas. The use of escorts for visitors can also be an effective ways to controlling visitor access throughout a building. This can be done by requiring visitors to sign in, issuing them a visitor badge and issuing them an employee to escort them throughout the premises. While it is important to

protect the unauthorized access to the physical building it is also important to take into consideration site selection of your data operations center and any other departments that may contain pertinent information concerning employees or data regarding the operations of ABCD Company. It is important to keep the data centers containing this information inconspicuous with upscale security. Moving data centers and human resource department along with server rooms from all entrances and preferably not located on the first flow, is highly recommended. This prevents these departments and rooms from being easily access in case of a breach from the outside.

Access Control Policy

The logical security in a company is controlling who has access to what is inside the physical constructed compound. Logical security is the software that provides protection to what is inside or is of value. The item that is inside or has value is known as the company's assets. There are specific types of principles and controls that need to be implemented to protect these assets. Separation of duties is an important principle that should be considered when handling extensive database that contains chemical inventory, personal identifiable information, confidential information and corporate data. Separation of duties is a type of security control that prevents an employee from having excessive privileges that exceeds past the necessary privileges needed to complete their job duties. With the use of separation of duties principle and applying access control techniques this will provide protection to those assets. Identification is a concept of access control that can be used. The issuing of badges or identification cards will provide an authentication factor to identify authorized or unauthorized individuals on premise or in the workplace. Authentication is another concept of access control which is used along with identification. Authentication credentials allow the system to recognize an individual's

identification and identify the permissions or rights someone has to gain access to an asset, system or location within the facility. To authenticate a person it could be something that a person know, have or is that will grant them access. Privileged and special account access is the component that ensures confidentiality amongst specified employees who have authority to perform a transaction or have access to an asset that is not accessible to other users. I would recommend this concept to be used for determining which employees will have clearance to gain access to facilities, departments, data centers, servers, network devices and any other assets that store valued information throughout ABCD Company network. The Microsoft Corporation (2010) website indicates that before a user can gain access to a network device, the user must identify itself to the security subsystem in order to connect to the operation system. This can be used with the implementation of authentication, authorization and accounting (AAA) systems. An extended access control system consisting of AAA is necessary to provide a framework that will authorize access to IP networks and transport services. The decisions on authorization is dictated by the level of confidentiality, technical requirements and financial aspects of the resource. Authentication is based on the type of identity being used such as a personal user IDs, key fobs, biometrics or IDs for hardware devices. The accounting component records, collects and stores accounting records in relation to service utilization (C. Resing, M. Karsten, B. Stiller, 2002). Due to traveling employees from location to location I would recommend that the permissions be set by an employee's job title or their department. Permissions can be defined by who the user is, their job tasks or based on the group that they belong.

With employees working from remote locations this creates security problems of securing the network because of the connection between local corporate offices. Addressing

these issues require access control mechanisms that will minimize or eliminate these connections from being hacked into by hackers and attackers. A virtual private network (VPN) is a means to access a network from a remote location over a WAN across the internet. These systems use encryption and other security mechanisms so that only authorized users can access the network and the stored data. Golen (2010) indicates that there are many reasons why a VPN should be used for remote access; reasons such as sensitive data security and the possibility of users losing passwords. VPN can prevent network traffic from being intercepted between locations and administration is able to manage user access easily. From the economic stance creating a VPN can be less expensive than maintaining leased lines. It is cost-efficient and any Microsoft Windows base device can be used as a VPN client and can be configured to the VPN server. This will eliminate any problems concerning traveling employees between plant locations that need to access the network with their laptops.

Network Security Policy

Network security is the most important aspect of implementing and having a successful network that will be able to operate with longevity. Keeping a network secure from hackers, attackers, viruses and any other malicious activity is important. There are a few ways of providing this security such as the use of packet-filtering routers, cryptography, intrusion detection prevention systems and firewalls. Packet-filtering is a simple basic way of controlling access to a network by reviewing and analyzing incoming and outgoing packets on network. Packet-filtering firewall identifies and maintains the traffic coming and leaving the network not only by the address of the source and destination but by the port number and the protocol types as well. Any packet that passes through a router has the potential of launching an attack on a network. According to Javin Technologies, Inc. (n.d.), “Network layer firewall is a type of

firewall that works as a packet filter by deciding what packets will pass the firewall according to rules defined by the administrator (Network Layer Firewall, para.1).” Packet-filtering is able to minimize these attacks and makes it harder for intruders to gain access the system. Another method that can be used to secure data transmissions over a wide area network is the use of cryptography. Cryptography uses a method known as scrambling data messages or encryption during transmissions so that the data is secure and tightly controlled during transmission. With the use of this method it prevents unauthorized users gaining access to personal information and enabling secure electronic transmissions and transactions taking place between networks.

Separation of Duties

Separation of duties is an internal control set by an administrator that requires a different set of people to complete certain parts of a task. This principle is used to prevent a single person from defrauding or performing fraudulent acts and threats against an organization. This principle is also used to prevent serious or uncorrectable errors from occurring by a single individual. By applying this principle of who should be granted access into the computer room and what type of access they should have you are limiting fraudulent activities or threats from happening. Even though you have authorized the cleaning person to gain access to the computer room, authentication hasn’t been given to for the same person to gain access to the computer system. Another example would be erasing old data from a mainframe computer. Access may have been granted for an individual to set-up this job tasks, but it takes access from another employee to provide an authentication code to confirm and proceed with this process. This eliminates any unauthorized tasks from being completed. Thurman, M. (2006) indicates that often there is no reason why any full-time employee should be granted full access to an entire network. Someone in marketing shouldn’t be able to access the administrative interface of a

production database that contains financial information about the company. An employee whose Active Directory attribute set identifies him as part of a specified group should be granted access appropriate to someone working on specified network devices or access to a facility that is pertaining to their job function.

Conforming to the Act

The Sarbanes-Oxley Act is used to set guidelines for these corporations to make sure that corporations are being transparent with providing full disclosure of corporate information when they are required to. The Sarbanes-Oxley (SOX) Act ensures that corporations are accepting accountability, working within compliance regulations and adhering to guidelines. If these guidelines are not adhered to there will be criminal and civil penalties for violating security regulations. For a policy to enforceable it must be disseminated, readable, comprehended, agreed upon and uniformly enforced. The recommendations for establishing a secure information system to the requirements of the Sarbanes-Oxley Act is by making sure that you are taking the necessary steps to setting, implementing and adhering to these standardized security regulations. With the use of these recommendations you are implying that you understand the possibility of vulnerable threats, you are issuing guidelines and provisions that are within compliance regulations and you are accepting accountability for setting these standards.

Conclusion

In the operations of an expanding corporation it is important that all aspects of having a secured network should be considered such as physical security, security of information systems, access control policy, network security and separation of duties. These are all important to the information security framework of ABCD Company so that the organization can operate efficiently and meet the expectations of providing confidentiality, integrity and availability.

References

Golen, P. (2010). *Virtual Private Networking*. TechGenix Ltd. Retrieved from (http://www.windowsecurity.com/articles/Virtual_Private_Networking.html)

Javin Technologies, Inc. (n.d.). *Network Layer Firewall*. Retrieved from (http://www.javvin.com/networksecurity/NetworkLayerFirewall.html)

Microsoft Corporation. (2010). *Access Control Overview*. Retrieved from (http://technet.microsoft.com/en-us/library/cc753976.aspx)

C. Rensing, M. Karsten and B. Stiller, "AAA: a survey and a policy-based architecture and framework," in *IEEE Network*, vol. 16, no. 6, pp. 22-27, Nov/Dec 2002. doi: 10.1109/MNET.2002.1081762

Thurman, M. (April 24, 2006). These rules will keep users in their place: the rule of least privilege and separation of duties will keep users out of network places they don't belong. *Computerworld*, 40, 17. p.36(1). Retrieved August 28, 2010, from General OneFile via Gale:

Merkow, M. and Breithaupt, J. (2014). Information Security Principles of Success. Indianapolis, Ind.: Pearson Education.