The role of information security policy essay sample

Law, Security

“ An Information Security Policy is the cornerstone of an Information Security Program. It should reflect the organization’s objectives for security and the agreed upon management strategy for securing information”(Bayuk, 2009). Finding out how management views security is the first step in composing a security policy. The human element is the biggest security vulnerability for any organization. Policies, standards and training are the best ways to mitigate the human element risk. Employees need to be educated and trained on the dangers and risks associated with information security. Roles of Employees

“ Roles and responsibilities are the descriptions of security responsibilities executed by departments other than the security group”(Bayuk, 2009). Human factors must be included in the organizations security policies and an effort must be made to inform employees about the policies, standards, procedures and guidelines. In any organization’s security plan people are the weakest link. Employees must be watchful against social engineering and phishing attempts, as well as other attempts like physical security and other human-oriented intrusion attempts. There are serious consequences for the organization and employees for any information compromises and employees must know and understand this. Different levels of security

“ In a world of viruses, malware, and hackers, information security is a big deal. One single method of IT security cannot insure protection of mission-critical data. In the enterprise IT environment, layering multiple tactics and security processes can help close all of the gaps” (Wikibon Blog, 2010). The first level would be for the organization to do a risk assessment analysis.

Second a security policy is written which may include an acceptable use policy which is a policy that a user agrees to follow in order to be granted access to a network, also an explanation of how security measurements will be carried out and enforced. Third, logging, monitoring and reporting-management regularly monitors performance results and as well as establishes and documents performance metrics. Forth, virtual perimeters-authentication is reintroduced into personal computers as the systems grow and become more powerful.

Fifth, environmental and physical information-mainframes, servers and routers are housed in an secure area that protects the devices from fire, explosions, man-made or natural disasters and physical access. Sixth, platform security-a model used to protect and secure the platform and the entire span of the software on the platform. It also provides an increased level of integrity. Seventh, information assurance-manages risks that can be related to use, storage, processing of information or data. Eighth, identity and access privilege management-each subject is uniquely identified and given access to the lowest level of privileges. This limits damage that can result from error or unauthorized use. Authentication/authorization system can be as simple as a password challenging system. Polices and Standards

” Policies outlines security roles and responsibilities, defines the scope of information to be protected, and provides a high level description of the controls that must be in place to protect information. Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or

software”(P, 2009). Microsoft’s goals are “ to operate our services with the security and privacy you expect from Microsoft, and to give you accurate assurances about our security and privacy practices.

We have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction” (Microsoft, 2015). Microsoft have a lot of policies, standards, audits and certifications that cover both their united states customers and international customers. Also every year they audit all of the third party organizations associated with them. The security management service manager function guides leaders through issues that should be considered for developing an effective security policy. The SMF reviews tactics and practices to increase staff awareness and improvement. Managing different levels of security

Security clearances for the differing personnel is a great way to manage the different levels of security required for differing levels of personnel. This goes back to the eighth level of Information security which is identity and access privileges. Depending on the level of the personnel determines what level of security and what data of the organization the employee can access. For example in the military there are I think two levels of security, secret and top secret. Both require an in depth background and credit check. Doing this ensures that data is not seen or given to personnel who does not have right level of security.

References

Bayuk, J. (2009, June). How to write an information security policy. Retrieved from http://www. csoonline. com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy. html Microsoft. (2015). Security, Audits, and Certifications. Retrieved from http://www. microsoft. com/online/legal/v2/en-us/MOS_PTC_Security_Audit. htm P, J. (2009, February). What are Policies, Standards, Guidelines and Procedures? Retrieved from http://mindfulsecurity. com/2009/02/03/policies-standards-and-guidelines/ Wikibon Blog. (2010, October). 8 levels of Information Security. Retrieved from http://wikibon. org/blog/8-levels-of-information-technology-security/