Acceptable use policy

Engineering, Computer Security

Acceptable Use Policy Artiesha Artis CIS 462 Security Strategies and Policy Professor Darrell Nerove October 20, 2012 Working in many different arenas while pursuing my degree in Computer Security has opened my eyes to many things, one thing that I have noticed is that some companies felt that they were immune to data breaches. I have worked in smaller organizations that just didn't have the knowledge to protect their network against security breaches. One inexpensive and very productive way to counteract lack of resources or know how is with an Acceptable use police. An acceptable use policy is not put in place to snoop on individuals rather than to protect the businesses assets. The AUP (acceptable use policy) that I want to focus on is one that governs internet usage. Acceptable use policy regarding internet usage normally includes information about websites that are off limits as well as defining a scope for what sites are allowed to be accessed for personal surfing. Most AUP's are put in place to protect the company's employees, partners and the company itself from any illegal or damaging actions by individuals knowingly or unknowingly. Confidentiality, integrity and availability are the founding stables of insuring that information is secure. An acceptable use policy enforces confidentiality, integrity and availability by limiting access and disclosure to authorized users -- " the right people" -- and preventing access or disclosure to unauthorized ones -- " the wrong people. ", as well as requiring employees to authenticate themselves in order to control access to data system resources and in turn hold employees responsible if violations occur under their user id. The company that I presently work for has an acceptable use policy it purposes is to highlight an outline the acceptable use of the computer equipment and systems that we

are granted access to. It is always stated throughout all the acceptable use policies I have seen that users must be aware that data created on corporate systems are property of the company. Employees are to exercise sound judgment regarding personal usage of computer systems. To be quite honest the AUP at my current organization is very straight forward and what I consider to be week. It is literally a blurb in the handbook that states that the internet systems are for business purposes only, and that the company observes the right to monitor the usage of the software. I can only think of a few reasons why the AUP at my organization is so brief. I work in the healthcare industry and because we deal with a lot of member information we are more concerned with HIPPA violations. In conjunction with HIPPA we also focus on making sure we remain in compliance with the HITECH act. Since there are other rules that we become preoccupied with the focus is no longer place on the AUP at my job. You will notice although there is no strict regards to an AUP at my place of employment there are filters and blocks in place so that certain websites are not able to be accessed. I have a few ideas on how I would implement a better AUP at my place of employment. I would first conduct a current policy review. By performing an audit of my current internet usage policy I would compare it with what I want my new policy to be. Taking into careful consideration the degree of policy enforcement required. Next I would want to gain visibility of your network traffic. Using a Web traffic assessment tool, such as a proxy appliance, to identify and monitor Internet traffic and to identify specific areas or groups that are engaging in inappropriate or excessive Web use. This would allow me to analyze how much time users and user groups spend on the Internet during

an " average" workday and what policies may need to be implemented. I would then concentrate on working collaboratively with all departments to enforce my end goal concentrating on the departments that have a bearing on the companywide Internet use policy, especially human resources and IT ensuring that there are no mismatches between the policies established and the ability of the network infrastructure to support them. After all this is completely then we would need to test my new policy by conducting an exercise with key users when the policy is at a draft stage. This will ensure that the policy is both practical in terms of achieving its objectives and sufficiently flexible to accommodate change or emergency situations. Then I would create a plan for announcing the new Internet usage policy throughout the organization to ensure that employee communication is well managed, the policy is understood and the restrictions imposed are fully justified. This would include denying access to Internet resources until users agree to accept the new policy. I would then ensure monitoring employee use is automated through Web monitoring software. I feel it would be a waste of human resources to assign a person or team to monitor the Internet activities of all company employees as a supervisor I know that there is just no time for looking over someone’s shoulder. Web monitoring software would provide efficient and comprehensive reports and data can be accessed within minutes. Stricter automation would allow management to set boundaries for site browsing, prevent downloading and installing of software and has multiple scanning engines to ensure that allowed downloads are free of viruses and other malware. By controlling downloads and browsing in real-time, the network is protected from malware. There is also the prevention of

data leakage through socially-engineered websites and it also helps reduce cyber-slacking, thus boosting employee and business productivity. In order to increase awareness of the importance of AUP and the need for them I would hold formal companywide training. I would also have quarterly reviews on what to do if. I have always believed that the only way for end users to truly embrace and understand the importance of any new policy or procedure implemented is to make them part of it, so during training I would ask for suggestions on how the employees feel they could make things smoother or easier and I would advise them to keep an eye out for violations. Having individuals keep an eye out on violations is the more challenging part of it all because no one wants to be a snitch but in order for any policy or procedure to work well to its fullest all wheels have to turn in the same direction. Of course the responsibility of reporting violations won’t be solely on staff because I would want monitoring in place to assist with that. AUPs are put in place to protect a company's data assets and confidential information while also safeguarding employees and maintaining standards concerning the use of the Internet during working hours. Implementing Web monitoring software is an investment in security and could prevent employees from cyber-slacking or abusing the company's trust with work-related information. By implementing and enforcing a solid AUP and providing ongoing, end-user education and training, a company can minimize risk, allowing them to focus on growing their business rather than the need to repair it. References Gaskin, J. E. (1998). Internet acceptable usage policies. Information Systems Management, 15(2), 20 Johnson , R., Merkow, M. (2011). Security Policies and Implementation Issues. Sudbury, MA: Jones &

Bartlett. Palgi, R. D. (1996). Rules of the Road: Why You Need an Acceptable Use Policy. School Library Journal, 42(8), 32-33. Siau, K., Nah, F., & Teng, L. (2002). ACCEPTABLE INTERNET USE POLICY. Communications of the ACM, 45(1), 75-79.