Week 1 You Decide -

Information Systems Use Security Policy

Anthony Meunier

DeVry University

SEC 360

Week 1 You Decide – Information Systems Use Security Policy

An information systems use policy is critical to any business’s success and/or continuity. Now that Sunshine Machine Works has grown by adding 10 times the amount of employees and upped their ratio of computers-to-employees from 1:3.3 to 1:2 it is vital that they get this policy in place not only to meet the regulations and standards that dictate the company does so, but also simply to protect the company’s data itself and that of all its customers, suppliers and so forth as well. By establishing a plan now, any potential threats and their impact are greatly reduced, because these policies themselves exist to address threats – without threats there would be no need for a policy, but unfortunately it is necessary to create a policy because threats are ever present. In order to keep the business operations running when a threat does occur, and in order to keep timely and efficient work flow throughout, integrating the various aspects of a workplace and its IT systems into one cohesive policy helps achieve these business objectives.

To start with, based on the analysis and interviews provided, there are some critical pieces of information that must be taken into account when beginning to view and think of establishing a policy as a whole. First off, there are many computer systems in the workplace and even more employees. An acceptable use policy must be integrated into the security policy so that these employees can have guidance as to what is acceptable to use the systems for and what is not. Notifying the employees that computer use is monitored is one step in achieving this, as it will already discourage employees from partaking in any frowned upon activities. Another property of general and acceptable use is to encrypt all data transaction that takes place on the network. This helps protect the user, the company, and the customers. Some other examples of related points/policies that go into creating an overall systems use policy are: security and proprietary information (such as password requirements, etc.), define unacceptable use, what enforcement entails, any term definitions for those who are not IT-savvy, and revision history of the policy so that changes can be documented both so employees know there have been changes and also so the company can see growth in the policy to suit changing business needs.

A commitment from management is key in not only creating a solidified policy, but also in integrating and enforcing the policy company-wide. In the interviews with management some things were mentioned that need to be addressed. The CEO mentioned that work may be expanding to the field. If this happens, communication from the field would need to occur with the company’s data which would be housed locally on the servers. In order to achieve best security practices here, the company would need to explore options for VPNs so that field employees could securely connect to the company’s servers in order to access data they need while not at the main offices. The CFO mentioned that currently only the 3 managers (CEO, CFO, and GM) have access to the company’s sensitive information and must be the ones to manually retrieve and provide the data upon request. This is understandable from a security perspective, but from an efficiency perspective this is not realistic especially with this many employees. What can be done instead is to set up some kind of database and administrator system in which employees could be admins who manage the data and lower level employees could have less privileges such as only being able to view specific data (depending on their security level). This would greatly improve efficiency and speed of business as well as allow management to focus on other issues. The general manager mentioned that the staff may need to be able to access personal information such as email and banking. From a security standpoint this is not acceptable as there are too many backdoors into the network if employees are permitted access to an overabundance of websites and so forth. Traffic must be limited and secured, and this means that employees more than likely will need to only use company email and not access personal information like banking, as again this would be even more to secure.

Another point to touch on in addition to the term “use” is physical use of the equipment as well. While much of the equipment and systems are data-related, users must be educated in what “good practice” entails when using these systems. This is sometimes overlooked but user error or misunderstanding accounts for a very large number of IT and security issues. In addition, because the company now has so many employees on the premises, it can be hard to watch what everyone is doing. A food remedy for this is to physically secure equipment, such as making an equipment room that only certain individuals have access to, as well as physically securing and locking other equipment so it cannot be easily tampered with.

Aside from specifics, a good policy in general will be straightforward and easy to implement and use. Changes are able to be made as new requirements are introduced, such as if the companies adds more equipment or employees. Management must stand behind the policy and its enforcement and be receptive to the fact that good security and use is vital to the business’s continued success. Management and the IT security team must constantly reevaluate how processes are working and see if there are opportunities to strengthen areas of the policy, and it should always be a work in progress. At the end of it all, a policy sets the framework for use and security and serves as a defense against threats to the organization.

References

Breithaupt, M. M. a. J. *Information Security Principles and Practice*. [VitalSource Bookshelf version]. Retrieved from <http://devry.vitalsource.com/books/9781256058328/id/app03>

Lee, D. (2001). Developing Effective Information Systems Security Policies. Retrieved September 13, 2015, from <http://www.sans.org/reading-room/whitepapers/policyissues/developing-effective-information-systems-security-policies-491>