Jessica Ward
ISQS 3360
Security Policy Paper
December 7, 2010

Security Policy Paper

Policies are an important aspect of business for day to day transactions such as having employees, maintaining safety especially in times of disaster, but in the 21st century, no policy may be as important as the computer security policy developed and maintained by the organization.

The goal of any security policy is to mitigate risk. Risk management is the first step in developing a sound security policy. The risk assessment will show an organization where they are vulnerable and what assets carry the most value, and therefore would be the ultimate targets of attacks. An organization wants to put the most protection around these target areas. For the purpose of this discussion, I will describe each area of a security policy and try to relate it to my experience in the pharmaceutical industry, though I did not work in the IT department, this policy affected my life every single day.

The first policy that should be created should be the higher level, general senior management statement of policy. This statement of policy should be something like:

Our company acknowledges the importance of the computing resources to our success and to the success of all of those who are associated with our organization. We are committed in our support through resources and funding to these endeavors throughout our organization in order to make sure that the utmost due care is taken. We hold with the utmost importance our responsibility to safeguard and enforce the standards, procedures, and guidelines set forth by this organization and we will have no tolerance for an entity that chooses to not exercise these controls to their fullest.

This statement is important because it sets the tone for the whole organization. It provides public support and sets the norms for acceptable practices and the due care that should be exercised by each member of the organization. If the organization takes it seriously, that will rub off on all of the employees. This statement needs to be repeated throughout all aspects of the other policies and shared just frequent enough to make it common place by employees. This statement is meant to be shared with employees, customers, shareholders, etc.

The next step is to implement the regulatory policies that are required due to compliance, regulation or other requirements of the government. These policies are detailed and organization specific. For instance, in my experience working in the heavily government regulated pharmaceutical industry, our regulatory policy most likely contained references to the FDA (Food and Drug Administration) approval process, what information about trademark and proprietary information was allowed to be accessed, HIPAA (Health Insurance Portability and Accountability Act of 1996) requirements regarding patient's classified information or research study participants classified data, the development, manufacturing, quality control, shipping and other logistics of pharmaceutical medications and the reporting and tracking of financial information. In addition, I am quite certain there are regulatory policies regarding social media sites such as Facebook and Twitter coming sometime soon due to the regulation of every aspect of what pharmaceutical companies are allowed to say to the public. There doesn't appear to be any regulation by the government in this department at the moment, but I think it would be prudent of companies to protect themselves in this area and a sound security policy would most likely have some type of policy in this area that falls under the umbrella of the FDA. Lawsuits of this variety are very costly to pharmaceutical companies and they would want to be protected I would assume. It seems as though most pharmaceutical companies use these sites for strictly news about the company which, reflects they have policies regarding this issue.

The next set of policies that need to be developed are the advisory policies. These are policies that are not required to be followed, but are strongly suggested to be followed and may even have serious consequences if they are not followed. Most policies in any organization fall under this category. According to the textbook, these policies can have many exclusions or application levels meaning they do not apply equally to all employees. There may also be special events that allow for members of the organization not to follow these procedures or follow an emergency procedure. In my particular job as a pharmaceutical representative in the pharmaceutical industry, a policy that was an advisory policy was that all representatives were "required" to sync their HP ipaq each night with the home system in order to log the number of physician calls and drug samples used each day. Technically, it was required, and was an offense that could result if termination if ignored, but nothing ever really came of it if a representative missed a day, unless the employee was already putting up red flags for other events. There were however, circumstances such as if you were on an out of town trip and did not have internet or if the company VPN was down, or if you were on vacation, which you were exempt from this policy. Another advisory policy was that employees were not supposed to send any company, drug, competitor, and etc. information via email; instead phone calls were required for this type of information. Another advisory policy in place regarded the weekly sales figures and the prescription volume documents. These documents were elaborate spreadsheet documents and were sent via email. Employees were required to sign in to view them and before they were able to view the document, they had to check a box stating they agreed to not transmit this data to any third party and that this document would not leave the company computer under any circumstances. Since most policies in an organization fall into the advisory category, it is my opinion that having the right norm set forth by senior management regarding a security policy is vital for success. It will be harder to get people to adhere to advisory policies if company norms aren't set in place.

The next aspect of a security policy is the informative policies. These are policies that exist to inform the reader whether it is customers or employees. These policies are general and will not breach security of they are shared with third parties. In the pharmaceutical industry, this could include rules on what information third party companies like the VPN provider is allowed to access or what the corporate ISP is allowed to access. It could also include policy made available to customers for reference regarding the use, storage, etc. of their personal data. There were also policies for the information transmitted electronically to third parties regarding employees such as the travel agents, marketing companies, drug sample delivery companies, etc. In addition, we received an elaborate employee handbook that stated the company's technology policies in detail, but as part of the security policy any employee leaving the company is required give all handbooks back to the company. It would not be the end of the world if one of these handbooks got out, but it is just an extra precaution they take.

The last set of policies that should be developed is the standards, guidelines and procedures, which are the most technical and the most detailed regarding computer security policy of the organization. These policies discuss details of how they should be used and when and how each procedure should be used. Each type of policy focuses on a different audience whether it is employees, customers, technical support employees, CEO’s, CTO’s, etc. and are written specifically for each area.

Standards specify the use of specific technologies in a standardized way. This standardization is helpful when implementing a sound security policy because it allows everything to be uniform throughout an organization. Guidelines are similar to standards, but are just recommended actions to consider when developing standards. They are also better at taking into account the differing nature of information systems. Procedures are the details of how to carry out these standards. In the pharmaceutical industry, these standards would include policies such as the acceptable use policy. This policy states how each employee is allowed to use their company laptop, the software installed on that laptop, what software the user is allowed to or not allowed to install, their hand held devices, the internet, including restrictions on personal use and what times of the day you were allowed access and whether or not you are allowed wireless access, email use, the corporate network, the VPN, etc. There was also policy regarding how often the user’s passwords needed to be changed and detailed the users passwords needed to be. In addition, there were policies such as having to have 4 different logins to access the system. For example, to access the system fully, the user had to log into their hand held device and prepare it to sync, log into Windows, log into the VPN and then log into the company’s portal. If there was ever a problem, the user had no authority on the system and had to contact the IT help desk for even the smallest details. IT support personnel were allowed to see procedures that most other employees were not allowed to see. For example, users were not even allowed to fix the clock on their own hand held device. If you called technical support, they would randomly generate a password that was only good for three minutes and that would allow you to change the clock. Computers and hand held devices were scanned fully once a week and an activity log was transmitted back to the company, which were used to generate several reports and track the user. There was also a detailed policy about how you are supposed to pack your computer and hand held device for travel, how you are supposed to conceal them in your car and what to do if they get lost, stolen or damaged. If an employee left the company, there was a detailed policy describing how they had to pack and ship each piece of equipment back to the company before the employee would be given their last paycheck. All of these areas were fully covered in training and we continued to receive education regarding these policies as they were needed. The human resources department is a very integral part of this level of security policy in the pharmaceutical industry as well. They are responsible for upholding standards, guidelines and procedures for running background checks, credit checks, developing job requirements, developing training and education, etc. all of which are important safeguards that play a key in having a secure organization from a technological standpoint. It is human resources that will hopefully let the most trustworthy individuals into the company as well as individuals that are competent to use the technologies, know when something is wrong and be able to take the right steps to help fix a problem if one arises. In addition, to these policies, this section of policy would also include things like safeguards and procedures for who and how individuals would be allowed to access proprietary information such as the development of new drugs, technologies, etc.

This policy overview did not even scratch the surface to what an actual security policy should entail. The development of a security policy is a never ending battle because technology always changes and there is always someone or something looking for the weak link. It takes a team of people, various technologies and a watchful eye and even then, you better have a really good lock on the door.

References:

Krutz, Ronald L. & Vines, Russell Dean, *The CISSP Prep Guide*. New York: Wiley Computer Publishing, 2001.

Professor John Durrett Lecture Notes