Timothy Rine

ISDS 4120

Security Assignment

4/3/2018

Effective security management is a vital component of running a successful organization. The security assignment that was completed illustrated just a sample of how many different ways organizational security can be breached. Information is perhaps the most valuable asset that a company owns and as such it is of the utmost importance that a company’s information is safe. If a company can’t protect its information, then the value of that company is greatly diminished into almost nothing. Security is also important from an individual morale standpoint. An employee won’t want to work for a company that isn’t actively trying to keep its employees and information safe. Workplace safety includes both physical security and information security. This is also valuable because good security measures help protect a company from liability, insurance, and other expenses.

A few threats that I had not previously considered are natural disasters, hardware failure, and internal theft. It makes sense that a company should have a plan of action in the event of a natural disaster, but I never thought about that. The same goes for hardware failure. As a company you really don’t want your hardware to fail and realize that you don’t have a backup. With the advent of cloud storage this becomes less of an issue, but it is still worth preparing for. As far as theft goes, I always think of the person stealing as coming from outside of the company. I still find it baffling that half of company thefts come from within the organization. That threat makes security, backups, and logs very important. In order to prevent internal theft you want to have good physical security measures as well as data encryption and network security. Although an internal member can still access the company information, you should make sure that employees only have access to information that they need for their job and they should have signed liability forms during pre-employment stating that it is illegal to steal company information for any reason.

One area that I was weak at assessing for several of the ten scenarios was the financial impact. I suppose that every security threat, large or small, has a significant financial impact on an organization. As I mentioned earlier, information is the most valuable asset in today’s market economy. Without effective protection of its information, a company is nothing. I think that my security recommendations would get the job done but they are closer to the minimum rather than a comprehensive security plan. In analyzing my recommendations, I see that I was far more likely to suggest individual-level preventive security measures such as dual-factor authentication, anti-virus software, and password controls compared to business-level security measures like response plans, policies, and SETA programs. I believe that may be because I am too trusting of people. I would trust my employees to be honest and not steal company information – that is why the statistic about internal theft was so shocking to me.

If I was in charge of designing a security solution for a firm, the policies that I would enforce would be network and personal security policies. Specifically, I think that password controls, dual-factor authentication, firewalls, Wi-Fi security, data encryption, network monitoring, anti-virus software, and application security are the most important. These security measures are the most important in my eyes because they are actively working to ensure security. Policies are great, but they can be broken by a disgruntled employee or criminal. A firewall will actively work to keep bad guys out. In my opinion, the individual level is the most important level of security. If employees are careless with their personal computers, use bad passwords, and generally are negligent in protecting their information then that puts the entire company at risk. As an employer if you really stress the importance of good personal security practices then I think that increases the chances that your information will be kept safely guarded.

Five takeaways from this security assignment are:

1. Security is a vast subject that a firm needs to address very carefully
2. Internal theft is a very real and potential security risk
3. There are multiple ways to handle security of a firm
4. Internal and external threats must be prepared for
5. Security threats pose a heavy risk to the financial department of a firm