Week 5 Case Study -

Risk Management Policy

Anthony Meunier

DeVry University

SEC 280

Week 5 Case Study – Risk Management Policy

The importance of information security cannot be understated. That importance is multiplied exponentially when your corporation is multi-international and you are tasked with securing confidential data of the amount of customers that come along with a company of this size. First and foremost, having a policy and plan in place before a breach in security occurs is vital to quickly dealing with any potential threats and breaches to the system. Securing customer trust is the number one priority in running a successful business. Losing their trust is the number one way to see your business fail. In order to prevent failure, it’s important to understand potential risks and develop a recovery plan to keep customers feeling safe.

In considering information security, having an understanding of where potential threats lie is key. Threats are ever-present from outside entities, but often times it’s the threats from the inside that can be just as dangerous. In addition, unforeseen threats can be just as devastating if and when they do occur. Hackers, competitors, sabotage, user errors are some examples of “predictable” threats. An organization must also remember that unpredictable threats exist as well; some examples being technical systems failures and environmental threats. You combat predictable threats with preventative security measures while you can combat the unpredictable threats with proper recovery systems.

It is not realistic or possible to always prevent or eliminate every threat. That being said, having systems and protocols in place to greatly minimize the chance of threats (or impact of successful attacks) is vital to an organization’s health and longevity. A risk management policy and its objectives are therefore key in any organization, especially when sensitive customer data is at hand. Some objectives of a policy should include: protecting the organization from particular risks of significant likelihood and consequence; providing a consistent risk management framework which constantly identifies risks and uses processes to review and control identified risks; encourage proactive management rather than reactive management; meets legal and regulatory standards; and overall assists in safeguarding the organization’s assets (which includes customer data as the number one priority).

Every level and aspect of security in the organization must be taken into account. Physical security, password security, and use of protective software are just a couple examples of providing added layers of network defense. In addition to these layers, implementing additional levels of security such as user-access levels can help go a long way in overall security. Individuals in the company need to be properly informed and management needs to uphold a commitment to security that reflects on the entire organization. Greatly reducing user error as well as accessibility to important and sensitive information can help cut down on a large number of potential threats.

Lastly, a strong disaster recovery plan needs to be included in any information risk management policy. Appropriate off-site/remote location backup of systems is one critical example of disaster recovery. If something was to happen and data was lost, it would already be too late; having these systems in place before a disaster is crucial. Risk management should be ever-evolving and viewed and discussed as a continuous process. Evaluation of policies and updates that reflect the current scope of the organization are necessary for the organization to remain on the cutting edge of information management and preservation of customer trust.

References

Harris, S. (2006, April). How to Write an Information Risk Management Policy. Retrieved November 29, 2014, from <http://searchsecurity.techtarget.com/tip/How-to-write-an-information-risk-management-policy>

Hinson, G. (2014, February). Addressing the Rhetorical Question: Why Do We Need Security Awareness? Retrieved November 29, 2014, from <http://www.noticebored.com/html/value_of_awareness.html>