INCIDENT RESPONSE: FORMING AN INFORMATION SECURITY MANAGEMENT PROGRAM

Ronald Stammand Young B. Choi
Department of Business, Leadership, and Information Systems
College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464
USA
e-mail: ronasta@mail.regent.edu, ychoi@regent.edu
Tel: (757) 352-4949

Abstract

In today's information technology world, information security is a hot button topic that many organizations have left unchecked for way too long. Experts in information security management are being sought out to assist organizations with developing information security management programs that can stand up to the increasingly demanding pressure that hackers, the government, and the general consumer are placing on them. This research paper will provide a general overview of the development process that goes into an information security management program and the major factors that come into play during that process.

Keywords: Information Security Management, Baseline Evaluation, Cost Benefit Analysis, Risk Management, Policy, Laws, Ethics

Incident Response: Forming an Information Security Management Program

One day, while reviewing logs on his network Tony, a network administrator for a medium-sized regional logistics company notices several failed connection attempts to sequential IP addresses on port 80on his Intrusion Detection and Prevention System (IDPS). Upon further review, the network technician discovered that the night before they had been infiltrated through a network printer that prints manifests for shipping orders from multiple site offices. It was not properly secured on the network firewall to only allow traffic from specific IP addresses. Upon further investigation, Tony discovered that some of the personally identifiable information (PII) that the company held in their databases was compromised. After gathering the proper information to fix the issue, Tony opened up the firewall on the router and prepared to write a new entry in for this vulnerability, but knew he would have to take the firewall down to do so. He contacted the IT department head, Frank, to notify him of this issue and to get guidance on moving forward with this incident. After Frank heard the issue he told Tony that the firewall could not be taken down until after business hours and that he would have to come in then to apply the changes. Tony acknowledged Frank's orders and suggested that the issue of not having a third shift network administrator coupled with not having documented procedures or adequate training for responding to incidents caused their network to be infiltrated. He said that he had been doing research on Information Security Management programs for college and mentioned the concept to Frank. Frank noted Tony's concerns and said this has been an issue that had been put on the backburner for a while and will definitely need to be addressed as soon as possible.

This research paper will focus on forming an Information Security Management program and the different aspects that go into such a meticulous and cumbersome undertaking. Starting with the strategic planning process and values, vision, and mission statements, Risk Management, and how the Cost-Benefit Analysis goes into determining

the level of risk an organization is willing to accept. After those elements of an Information Security Management program have been discussed, this research paper will discuss the information Security Policy Development Process to include how to determine whichtypes of policies will need to be emphasized for an organization, determining roles and responsibilities, and how employees will comply with these new policies and what enforcement looks like if they do not comply. Finally, this paper will discuss the human factor of Information Security Management and how to create an effective information security training and awareness program along with how laws and ethics play into the overall Information Security Management program.

Problem

Technology is an amazing thing. Fifty years ago the first "modern" computer, the Data General Nova, was big built that were still very large compared to today's standards, but not quite the size of an entire room with large vacuum tubes the size of a VW Beetle like the beloved ENIAC. In these modern times, however, a smartphone has exponentially more memory and processing power than the Nova ever had. As technology progressed and more and more people became linked together by the Internet it has become easier than ever to reach out to someone a world away – even for malicious purposes. It is in the news every day about some company getting hacked for their credit card databases and how it affects 50 million people worldwide. A lot of organizations have established industry accepted "best practices" that may include how best to mitigate certain areas of risk and what policies have worked for other organizations, which has served them well. Other organizations, however, have thought that their company is too small to have to worry about business-crippling threats or were too trusting of their employees, which caused malicious content to be introduced into their network. If an organization does not have an Information Security Management Program in place they will run the risk of losing not only their sensitive data, but also credibility in their industry and with their consumer base. Because of these increasingly frequent threats, CERT, the organization started by Carnegie Mellon University to handle computer security incidents, explains that new laws and regulations from the government are requiring organizations to protect their information assets on a deeper level (2012). This all stems from an inadequate Information Security Management program and can be greatly helped by taking the time, even though the process will be painstaking, to form one. It is imperative that even smaller organizations develop and maintain some sort of Information Security Management Program.

Discussion

An Information Security Management Program is made up of multiple smaller areas that reach from the IT department, to legal, to Human Resources, as well as other areas within an organization. To from an effective Information Security Management Program, an organization should focus on the following elements: mission, strategies and goals; senior management approval; how the organization approaches information security and their attitude towards it;the flow of communication upwards and downwards; what methods and metrics will be used to determine how the Information Security Management Program will function; and, finally, how the Information Security Management Program fits into the overall goal and mission of the organization.

Strategic Planning

Any plan should begin with a review of the values,vision, and mission statements that an organization currently has in place. In their book *Management of Information Security*, Michael E. Whitman and Herbert J. Mattord (2010), explain that in order to implement effective planning "…an organization's leaders should begin from previously developed positions that explicitly state an organization's ethical, entrepreneurial, and philosophical perspectives" (p40). In a world of scandals the magnitude of Enron and Fannie Mae, organizations need strong, well-defined values statements that they can stand by from the top down to the bottom. This is what will set an organization apart from others. By establishing in a good values statement, "…a formal set of organizational principles and qualities…benchmarks for measuring behavior…an organization makes its conduct and performance standards clear to its employees and the public" (p40-41). Having a well-crafted values statement will show an organization's consumers, as well as their stakeholders, that they have integrity and want to uphold right in a world filled with so much wrong.

The second area to consider when working with strategic planning is the vision statement. An organization must assess where they currently are and then develop a vision for where they want to be. A vision statement can encompass multiple areas of an organization and each department could have their own vision statement. This is actually a better route to take. According to The Society of Human Resource Management (2012), an effective vision statement "…is inspirational and aspirational…creates a mental image of the future state that the organization wishes to achieve…should challenge and inspire employees." The vision statement is going to build upon the values statement in that it is going to incorporate the organization's ethical values into its' mission and give employees as well as consumers a clearly defined and powerful statement that will energize and motivate people.

Lastly, and organization must have a clearly defined mission statement. Whitman and Mattord (2010) define a mission statement as, "…concise, [it] should reflect both the internal and external operations, and [it] should be robust enough to remain valid for a period of four to six years" (p42). It is not a 10 page long exposition of the intricacies of the organization, but rather a short statement of who the organization is, what it does, and for whom it does it.According to *Idealist.org*, a leading online resource for non-profit organizations, a mission statement is so important because by not having one, or having one that is not clearly defined and concise, "...organization members can waste time "barking up the wrong tree"…may not think broadly enough about different possibilities if its mission statement is unclear or overly narrow…may not realize when it is time to go out of business" (Action Without Borders, 2014). Without a mission, an organization will have no direction and will not perform to its' full potential and could ultimately fail.

Having a clearly defined set of values, vision, and mission, an organization can now focus on the strategic planning process of developing the Information Security Management Program. This starts with a general (but concise) strategic statement, which it turn is taken by each department who will then create response statements that will guide their individuals departments' progress toward the overall goal of creating the Information Security Management Program. The organization's overall strategic plan is likewise translated into strategic goal for each major milestone of the plan development process. As the plan goes lower into the organization, different and more specific objectives will surface at a divisional level. The strategic plans are used to create tactical plan, which in turn are used to create operational plans (Whitman and Mattord, 2010, p45). The lower the overall strategic (long-term) plan goes into the organization, the more defined (and shorter) the goals are. There will be lists and checks that will be made to measure progress in order to give employees and management a good gauge as to where each part of the organization is in the overall Information Security Management Program progress. With a strategic plan thoroughly in place, the organization can then turn it's attention to the next major area of the Information Security Management Plan – Risk Assessment.

Risk Assessment

Risk is inherent in everything the world over. When a person walks outside or logs onto the Web there are literally millions of things that could wreak havoc on their lives. The same stands true for any organization. When doing business, especially if it uses the Internet heavily in its' day to day operations, an organization runs risk from any number of avenues – hacking, DDoS attacks, social engineering, industrial espionage, and the like. An organization must learn to mitigate or manage this risk as much as possible if they are going to adequately function in the business world. This is where Risk Management comes in. Risk management is "…the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization" (Whitman & Mattord, 2012, p. 27). If an organization is coming up in a market with other like vendors, they have the advantage of learning from the misfortunes of those other companies. An organization should also report incidents to incident response organizations such as the United States Computer Emergency Readiness Team (US-CERT) or an Information Sharing and Analysis Center (ISAC) to aid in the formation of new policies and procedures that will help other organizations with Risk Management.With the increase of malicious activity toward organizations from outside entities, the Federal Information Security Management Act (FISMA) was established to mandate certain actions that government organizations must take in the event of an incident. There are other entities, such as ISACs, for the private sector as well. The Presidential *Executive Order – Improving Critical Infrastructure Cybersecurity* explains that the United Sates Government has a policy "…to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats" (Barrack Obama, 2013). According to Cichonski et al. (2012), US-CERT gathers information from many organizations and conducts meta-analyses on the data to discern trends and patterns of malicious activity (p11). This data is then in turn used to create new industry "best practices" that other organization can adopt continuing the cycle of improvement.

In order for an organization to determine their areas of risk, they must perform a Risk Assessment. A Risk Assessment is the process of determining how much risk an organization has. During the Risk Assessment, an organization conducts a Business Impact Analysis (BIA) to determine its' highest risk areas and establish procedures and safeguards to either mitigate or absorb the potential cost of these events occurring. During the BIA process, a Cost-Benefit Analysis is done to determine the "best bang for the buck" that an organization can work with to accomplish its' Risk Management objectives. While there are many technologies out there that do a better job than others at managing vulnerabilities, some are way too expensive for an organization to reasonably use for their Information Security Management Program. In making the determination of what Risk Management strategy to use, an organization must determine if they want to avoid the risk all together, transfer the risk to another area of the

organization (such as a De-militarized Zone), mitigate the risk (with controls), or accept the risk. The thing to keep in mind, according to Whitman & Mattord (2010), is that "…organizations must make sure that they have met a reasonable level of security in all areas, and that they have adequately protected all information assets, before improving individual areas to meet the highest standards" (p249). The goal of any risk control strategy is to reduce risk to within acceptable limits. These acceptable limits are known as the Risk Appetite. Risk Appetite is defined as, "…the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility" (Whitman & Mattord, 2012, p.163).An organization must thoroughly understand the risks that they are accepting in determining their level of Risk Appetite. Lastly, there are times that no matter what an organization does it cannot completely control risk. This is called residual risk. Residual risk is defined as, "…a combined function of (1) a threat less the effect of threat-reducing safeguards, (2) a vulnerability less the effect of vulnerability-reducing safeguards, and (3) an asset less the effect of asset value-reducing safeguards" (Whitman and Mattord, 2010, p312). In these instances an organization might consider purchasing additional insurance to help cover the costs should an incident they could not control ever occur. Now that risk has been covered, the Information Security Policy Development Process will now be covered.

Information Security Policy Development Process

After the Risk Assessment has been performed and the risk controls established, an organization must work on policy development. Policy development does not have to be a "start from scratch" endeavor. Using existing policies, or even memorandums, can help an organization gauge where they are currently in a certain area to where they want to be in that area. There could even be different enforcement of the same policy in different areas of an organization. This can also be taken into account to implement a broader (but not necessarily less restrictive) organizational policy. There are some things to take into account when developing Information Security Policy. Roles and responsibilities must be clearly defined from the top down with specific duties assigned to specific individuals or divisions. The key personnel need to be identified so they can be contacted should an immediate decision need to be made. Next, the essential policies, the ones that apply to the widest (largest risk) audience, must be identified and efforts made to disseminate these policies to the entire organization in the most efficient format possible. Next, make determinations on how the policies will be reviewed, acknowledged, and enforced as well as what disciplinary actions should be taken should these policies be broken. Dissemination depends on the audience to which you are targeting. If the audience is the personnel on the assembly line and the method of dissemination is via company email, this is most likely not going to get seen by the right audience. If training is required because of the new policies, the awareness and training program must support"…the business needs of the organization and be relevant to the organization's culture and IT architecture" (Wilson & Hash, 2003). The method of delivery of training, just like the method of policy distribution, depends on the audience and their level of knowledge and understanding. Now that Information Security Policy Development and training and awareness have been established, the last topic is how people play into the overall Information Security Management Program.

How People Play into the Picture

People can be the greatest asset or the biggest hindrance within an organization. Personnel security is often overlooked as a security risk within an organization because employers like to believe that all employees are honest and loyal to the organization. In a perfect world all employees would be honest, hard-working individuals – and most of them are. There are those though, given the right motivations, which would conduct malicious activity in order to obtain some sort of personal gain. The employee may be bribed by a competitor, blackmailed into giving out sensitive information, want revenge for being fired, or just simply a victim of social engineering.It all starts with the hiring process. A strict hiring and termination process will begin with "…conducting proper background checks, interviewing past employers, and verifying credentials" (Ozderman & Edmond, 2013). The authors also explain that, "a strict termination process can help mitigate the risk of a breach from separated workers, especially those with administrative privileges" (Ozderman & Edmond, 2013). Ethics in the workplace can be a tricky thing to maintain. It is ultimately up to the security person within the organization to "…deter unethical and illegal acts, using policy, education and training, and technology as controls or safeguards to protect the information and systems" (Whitman & Mattord, 2010, p451). In order to have a good gauge of how ethical an employee is, there are industry certifications such as $(ISC)^2$ and ISACA that have been developed where individuals obtain certifications showing their mastery of a field and then sign a code of ethics essentially stating that they will not use their knowledge for nefarious purposes. Ethics can be difficult to maintain within an organization, but it is ultimately up to the culture of the organization that determines how these new changes will be received.

Conclusion

This research paper covered the formation of an Information Security Management Program to include strategic planning, risk assessment, the Information Security Policy Development process, and how people fit into the picture. An important point to take away is that an organization that does not have an effective Information Security Management program is destined to fail. The Bible says in James 1:5 "If any of you lacks wisdom, let him ask God, who gives generously to all without reproach, and it will be given him" (ESV). In the same way, if an organization lack wisdom, they are not alone and have many resources to lean on should they need to.

References

Action Without Borders. (2014). What should a mission statement say? Retrieved April 28, 2014, from http://www.idealist.org/info/Nonprofits/Gov1#One

Bible Gateway.(n.d.). Bible Gateway passage: James 1:5 - English Standard Version. Retrieved from http://www.biblegateway.com/passage/?search=James+1%3A5&version=ESV

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August).NIST (United States of America, U.S. Department of Commerce, National Institute of Standards and Technology). Retrieved April 23, 2014, from http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Obama, B. (2013, February 12). Executive order -- improving critical infrastructure cybersecurity. Retrieved April 28, 2014, from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Ozderman, E., & Edmond, R. (2013, November 7). Managing the human factor in cyber defense. Retrieved April 28, 2014, from http://www.celerity.com/blog/2013/11/07/ways-manage-human-factor-IT-security-cyber-threats/

SHRM. (2012, December 20). Mission & vision statements: What is the difference between mission, vision and values statements? Retrieved April 28, 2014, from https%3A%2F%2Fwww.shrm.org%2FTemplatesTools%2Fhrqa%2FPages%2FIsthereadifferencebetweenacompany%E2%80%99smission%2Cvisionandvaluestatements.aspx

Whitman, M. E., & Mattord, H. J. (2012).Security and Personnel. In *Principles of Information Security* (4th ed.). Boston, MA: Course Technology.

Whitman, M., Mattord, H. (2010).Principles of incident response and disaster recovery. (2nd ed.). Boston, MA: Course Technology, Cengage Learning.

Wilson, M., & Hash, J. (2003, October). Building an information technology security awareness and training program. Retrieved April 28, 2014, from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf