Managing Information Security in the Age of the Pervasive Internet

David C. Shields

University of Maryland University College

Table of Contents

Introduction 3

The Facts: What's really at stake? 3

The Man in the Box – Insider Threats 4

The Pervasive Internet 5

Concept for Change: Formulating a Security Plan 7

The Human Touch: User Security Awareness 9

Securing the Invisible Borders 10

Conclusion 11

Bibliography 13

Managing Information Security in the Age of the Pervasive Internet

Introduction

The day has just begun in the office of XYZ Corporation. The managers have their systems booted up and are checking through the emails they missed last night, the accounting department is already busily reviewing spreadsheets, some of the employees are already in a meeting with their customers, and already an information security hole is open before the information security analysts have even finished their morning coffee. The problem is not the network and software policies XYZ Corp has implemented, or the Identity Management initiative launched early in this quarter, it is not even the traffic on the e-commerce site. The vulnerability lies in the everyday user sitting at their desk with their smart phone, their tablet, their USB thumb drive, and even in the heart of the user themselves. IT Managers must work more expeditiously on training users of the countless security problems such items as personal electronics or the ever-present Internet connections found on everything from mobile music players to personal smart phones and how the user's actions can have a profound impact on the security of the information they work with.

The Facts: What's really at stake?

For any organization of any size, a security breach can cost countless tangible and intangible losses. Based on analysis of data provided to Ernst and Young by a large sampling of companies, businesses lost an average of $350,000 in 2007 due to information security breaches (Richardson, 2007).

But those figures are only a small fraction of the companies who actually lost data due to such breaches as few companies are willing to actually admit losses for fear of tarnishing their image or scaring investors on Wall Street (D'Arcy, Hovav, & Galletta, 2009, p. 79). Even with such negative outlooks hanging in the balance, a vast majority of modern companies do not consider security awareness as a vital part of their business (Spears & Barki, 2010, p. 503). As a result, many companies are leaving themselves wide open to vulnerabilities from both internal and external sources.

The Man in the Box – Insider Threats

When the average office worker in America hears about information security vulnerabilities, it is likely that their mind conjures up imagery of a hacker from some dark apartment room in China trying to use some sort of complex tools to penetrate the network. They might be surprised to find that the reality is quite different as over 50% of security incidents are actually carried out (sometimes unknowingly) by people working right there in the office (D'Arcy, Hovav, & Galletta, 2009, p. 79). It is important to note, however, that a number of these incidents are likely unintentional such as the user clicking on a link in a phishing email or mentioning something on a social networking site without realizing the error of their ways. Beyond these incidents, it very well may be that a disgruntled employee decides to break the policy out of spite or to sell information to suit their own purposes.

In the face of such obstacles, an IT security manager must be ready to combat these insider threats both proactively and reactively. Proactively, the single greatest technique in a situation such as this is to foster a strong security awareness program that is thoughtfully created and revised often as the environment changes so rapidly.

If the users receive high quality training in acceptable computer use policy and are provided with frequent reminders of the ongoing security posture of the organization, they will be more likely to respond appropriately in the event of a real security incident (Yeo, Rahim, & Ren, 2008, p. 232).

The challenge to applying a strong information security policy and laying out the expectation that it will be followed is how to motivate the users to abide by the security policy set in place. Studies have shown that users who were warned of disciplinary action for improper use of their computers were less likely to break security guidelines for fear of punishment or reproach (D'Arcy, Hovav, & Galletta, 2009, pp. 91-92). In comparison, additional studies have found that employees who are taught security policies in a positive manner have a universally more positive outlook on said policies and will be inclined to follow them due to altruistic sentiments (Yeo, Rahim, & Ren, 2008, p. 237). Therefore, it can be inferred that positive reinforcement is more likely to create a generally better adherence to policies and encourage user ownership of security challenges than negative reinforcement.

The Pervasive Internet

A large, but not separate challenge faced by IT Managers attempting to enforce security and prevent data leakage is the ever present connection to the internet and social media that is manifested in the modern world. The Web 2.0 is awash with social networking sites (e.g. Face Book, Twitter, Google+) which blur the lines of personal, business, and private affairs and have gained a considerable amount of popularity in recent years (Valacich & Schneider, 2010, p. 215). Additionally, the late 2000's saw the rise of the smartphone and high speed data services to meet that rise.

As a result, the smartphone has been permanently ingrained in the society we live in and its connections allow always-on access to social networking and the Internet as a whole. When these ingredients are mixed together and simmered in an environment with lax information security guidelines, the result is a recipe for a major security problem. While these Internet-capable devices can certainly be used to revolutionize the way a business operates, if left unchecked, they can almost certainly generate a security leak.

The proverbial double-edged sword in smartphones is that although they do allow almost constant contact to the outside world, the security policies used on them may only be controlled by the owner's service provider. Once the data travels on to the carrier's network, a complete loss of visibility into the communications the owner makes with the device will occur. Adding insult to injury, requesting network usage records from data carriers without legal action may be a challenging undertaking indeed (Van Eeten & Bauer, 2009, p. 227).

In order to compete with the ever-present, ever-active Internet access allowed on smart phones, an IT manager must take calculated action when considering how best to counteract the possibility of data leakage using this medium. While it is possible to forbid the use of phones inside the company walls, this option will not only appear overly oppressive to the users but also could cause severe privacy and security challenges in the event of emergencies both personal or company related (Spears & Barki, 2010, p. 74). It would be a wise decision for the IT Manager to take a more inclusive and persuasive approach that not only allows for the privacy but also generates a desire for the users to make educated choices as they are all pieces of the puzzle. When the users are engaged in a Security Education, Training and Awareness (SETA) curriculum, they will be more likely to take personal ownership of security responsibilities (D'Arcy, Hovav, & Galletta, 2009, p. 83).

Concept for Change: Formulating a Security Plan

As the previous pages have outlined, the security and integrity of information is one of the company's greatest assets and IT managers should see the need for security policies that are well implemented and modernized enough to combat such things as smartphone usage and social media. The careful balancing act that must be carried out by businesses to insure security without too heavy of an impact on privacy is not a minor undertaking. Furthermore, making the same system universal is such a daunting task that even the US Government admits that it is not properly prepared to manage the problem (Sandham, 2008, p. 70). However, with proper consideration to the needs of the people and the organization coupled with ongoing measures to engage employees in security awareness can create an ecosystem that will greatly minimize the risks of data leakage. All of these things require a framework, a system of governance that binds the guidelines together and can be shared with the organization – this item is simply known as a security plan.

The first step in creating a security plan is to research the organization in which the plan will be implemented and requires the IT Manager to clearly consider many questions such as: What risks can be found in the infrastructure? How are these risks being monitored and mitigated at this very moment? Of the risks uncovered, how many of them are the company willing to pay to mitigate and how much remaining risk is the company prepared to deal with? All of these things fall under the banner of what is better known as 'Risk Mitigation' (Prowse, 2011, p. 222). In order to convince the upper management of the need for a better quality Security Awareness program, an IT manager would be wise to show the results of a comprehensive risk analysis of the organization and gather their input to determine the level of risk they are willing to take.

Once the upper management has signed off on the risk factors and level of mitigation they wish to endure, the IT Manager should use the data from the risk analysis to determine the current level of security that the organization supports on their IT infrastructure and isolate any areas where critical system updating is needed. An example of such a critical challenge are machines that are off network and not receiving operating system updates or virus definition updates and they could pose a severe threat to the environment. Once severe issues are mitigated, a more cohesive baseline for the 'general population' can be created.

Once the initial 'baseline' is complete, the IT manager's team should then focus on any technologies needed to keep the systems as closely in compliance with the general baseline as possible. Some technologies that might fill this need can include such things as Group Policies in Microsoft's Active Directory framework or Microsoft Systems Management Server (SMS) to name a few (Prowse, 2011, pp. 69-73). The integrity of the network can be maintained by installing a good network monitoring solution and protective devices such as Network Intrusion Prevention Systems (NIPS) and firewalls (Hazari, Hargrave, & Clenney, 2008, p. 7). These technologies can be automated in such a way that they can be constantly monitoring the network and will send alerts based off preset criteria to allow the IT team constant insight into the state of the network, some of the machines can even be automated to the point that they can automatically execute a response based off certain actions (i.e. dropping a network connection to a compromised computer) (Prowse, 2011, pp. 144-145).

The Human Touch: User Security Awareness

Once the background infrastructure has been created and is running smoothly, an IT manager might be prone to think that the hardest part is over whereas in reality, it has only just begun. Regardless of how well the security plan on the backend has been orchestrated, security is only as strong as the weakest link which is often the user (Liang & Xue, 2010, p. 405). As the earlier part of this document discussed, it is vitally important for the IT manager to create a strong user security awareness program that not only provides guidance in easy-to-follow terms but also creates a sense of ownership and responsibility among users.

For the program to be a success, the IT manager will want to create a security program that endorses positive reinforcement and is geared toward self-awareness and awareness of others. Research has shown that although many users will react with compliance to security guidelines that are geared toward negative reinforcements or fear they are not the best model to ensure compliance as they can create negative responses and threat avoidance mentalities (D'Arcy, Hovav, & Galletta, 2009, p. 82). Furthermore, employees that already carry a negative mentality toward their employers and may intentionally misuse their computer equipment are more likely to retaliate if they feel that the security policy is too demanding (Spears & Barki, 2010, p. 506).

In situations where internal users are engaged actively in not only the creation but also the execution of the security program, IT managers will find that people are far more likely to provide quick responses to incidents, report feedback of existing processes, and even create more refined processes to implement than might otherwise be possible (Spears & Barki, 2010, p. 508).

The constant application, validation, and re-assessment of policies that are created in such a user-focused model will greatly increase the quality of the procedures and allow for testing of circumstances that the IT management team may not have even considered in the initial scope of the program. The resulting program will be more of a living, organic, security policy that unifies the users and the IT management in a trusted and flexible model.

One minor note of caution in an open ended model such as the one outlined above is that for all the positives it can offer, it is not without its own challenges. Users who are so active and 'plugged in' to this style of policy can also create a false sense of security or consider themselves 'above the system' (Liang & Xue, 2010, p. 396). Thusly, it would benefit the organization a great deal if they were to provide an education system for information security that does not stress any form of invincibility. Users must be made aware that no matter how well the system is secured and how well the training and reporting model is, no system is bulletproof. The focal point is not so much 'if' but 'when' a security violation will occur.

Securing the Invisible Borders

No security plan would be complete without a method to deal with Internet capable smartphones and the various leakages it creates. In a strong armed approach to security, the IT manager might consider an outright ban on bringing smartphones into a facility and some secure processing facilities such as DoD organizations do require such measures. Even still, the requirement to remove these devices in a standard business environment is superfluous and will likely generate considerable dissatisfaction amongst users.

Instead of banning wireless devices, an IT manager might opt to include special instructions regarding the use and possession of these devices that clearly explains to the users what expectations are placed on them for allowing such devices. Furthermore, the security plan should include concise directions about the use of social networking applications by employees both on their personal devices and on company owned information systems (Kachhi & Link, 2009, p. 75). If the user has specific instructions for how they are expected to use such items and networks, there can be little question of responsibility in the event of a security violation.

The challenge faced with securing data outside of the standard company's IT infrastructure does not end with smartphones; it extends to the Internet as a whole. The safest practice for protecting your network from unauthorized data leakage, phishing attacks, and social engineering is to completely remove access to the Internet. This method is a double edged sword however as it also prevents users from having access to the wealth of information the Internet has to offer and may isolate the company from achieving a competitive edge over their competition. A much more amicable method for reducing the risk of leakage on the Internet is to utilize intelligent content filtering and URL filtering technologies which can be trained to recognize sites that are likely phishing sites or insecure venues that would facilitate a leak (Hazari, Hargrave, & Clenney, 2008, p. 7). On a cautionary note, while automation of such tasks can certainly reduce operational overhead, there is still little that compares to a competent analyst who can interpret the data from angles that computer software simply cannot replicate.

Conclusion

IT managers face countless challenges day in and day out with creating the best possible solution to protect the data that they and their teams have been entrusted with.

While there are certainly not any ‘one size fits all’ models for security in an organization, a careful analysis of many great practices can produce a wealth of options that can be synthesized into the perfect plan to fit each organization on its own. As the world of information security changes at such a rapid pace and the threats change even faster, the single greatest vulnerability is in the lack of a flexible security plan that can be engineered to evolve as the company it is protecting evolves. If an IT manager works carefully, they can create a high profile Security Awareness program that embraces the culture of the company and also engages the users in an ever-evolving and positively reinforced environment.

The best security environments that can be found in organizations today are those that have been created with the business needs at the forefront of the plan but with a strong backend of dedicated professionals, equipment, measurement tools, and safeguards. The plans have contingencies in place for the ever-present Internet and social networks and an audit trail that can be implemented when the inevitable data leakage occurs. Most importantly, however, the best security plans are those that are guided and evaluated by the very people they are to protect.

Bibliography

D'Arcy, J., Hovav, A., & Galletta, D. (2009, March). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 20*(1), 79-98. doi:10.1287/isre.1070.0160

Hazari, S., Hargrave, W., & Clenney, B. (2008). An Empirical Inevestigation of Factors Influencing Security Behavior. *Journal of Information Privacy and Security, 4*(4), 3-20.

Kachhi, D., & Link, M. W. (2009, March). Too Much Information: Does the Internet Dig Too Deep? *Journal of Advertising Research*, 74-81. doi:10.2501/S0021849909090047

Liang, H., & Xue, Y. (2010, July). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems, 11*(7), 394-413.

Prowse, D. L. (2011). *CompTIA Security+ SYO-201 Cert Guide.* Indianapolis: Pearson Education.

Richardson, R. (2007). *CSI/FBI Computer Crime and Security Survey.* San Francisco: Computer Security Institute.

Sandham, D. (2008, November-December). fragile web. *Engineering and Technology*, 68-71.

Spears, J. L., & Barki, H. (2010, September). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 501-522.

Valacich, J., & Schneider, C. (2010). *Information Systems Today: Managing in the Digital World.* Upper Saddle River: Prentice Hall.

Van Eeten, M., & Bauer, J. M. (2009, December). Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications. *Journal of Contingencies and Crisis Management, 17*(4), 221-232.

Yeo, A. C., Rahim, M., & Ren, Y. Y. (2008, December). Use of Persuasive Technology to Change End Users' IT Security Aware Behaviour: A Pilot Study. *Proceedings of the World Academy of Science, Engineering, and Technology, 36*, 232-239.