SOHO: INFORMATION SECURITY AWARENESS IN THE ASPECT OF POLICY

Jason Maurer, Regent University USA, (jasomau@mail.regent.edu)
Brandon Clark, Regent University USA, (brancla@mail.regent.edu)
Young B. Choi, Regent University USA, (ychoi@regent.edu)

ABSTRACT

We seek to build upon the foundation of general security awareness for home and small business owners by looking at how the creation and enforcement of appropriate policy affects successful information security. We will review some general security awareness information, and take a look at the importance of and aspects of planning and policy considerations and some basic techniques to use in order to create effective policy. Finally, we will lay the foundation for creating and implementing policy in your small business office or home office and recommend some practical steps to take.

1. INTRODUCTION

What do you do when you discover that one of your employees has been running an Internet business on their supplied workstation at their desk? Are you legally allowed to do anything about it? How about the employee on your restaurant staff that like to update all their Facebook friends on the newest secret recipe that is being served? What do you do and what can you do? These questions should not be hard to answer. If you find yourself searching for the harshest punishment options in the moment of learning about such actions then you probably are not prepared to handle the situation and you may not be able to take extreme action such as reprimand and termination. If an employee likes to copy all the current projects to their flash drive and take them home every night with the best intentions to get a little extra work in and the bag with the flash drive in it is stolen, what can you do? Some of these examples seem extreme, but are realistic. These are also situations that could have potentially been avoided by establishing guidelines by which all your employees abide by. Many of these situations are a risk to your information and need to be addressed before something as severe as all your client files are lost or your restraint is shut down because your secret recipes were shared with the world due to ignorance or lack of awareness of an employee. Now is the time to act so that you are prepared and your information is kept secure. Information security is about maintaining a balance between securing your information and keeping it accurate while making it accessible to those that are authorized to use it [1]. Our previous research work SOHO: Information Security Awareness was to bring awareness of general threats and vulnerabilities that small business and home office networks face and suggest practical steps of where to begin with information security. Our another research work SOHO: Information Security Awareness 2 built upon the foundation of general security awareness and looked deeper into ways to protect against social engineering, viruses, spyware, and other malicious code and focused on some of the threats to your computer system's security and discussed protecting your information as well as recommended steps to aid in recovery. Our research work SOHO: Information Security Awareness 3 showed the importance of thinking ahead and planning for events that may penetrate through all your layers of prevention and disrupt your operations. All the techniques and strategies to protect your information that have been covered previously in our previous research can all be combined and be managed with the use of effective policy which is the topic of this paper. We will take a look at how the creation and enforcement of appropriate policy affects successful Information Security. We are going to focus on security policy. Let's begin with a basic review of Information Security.

2. INFORMATION SECURITY REVIEW

First, let's take a look at what Information Security is. Many may think it is having an antivirus program installed on their personal computer. Even though that is one very small and important way to help secure your information, Information Security is much more involved and complex. Information Security encompasses a broad concept that applies to every bit of information used by an individual or organization, whether digital or physical, classified or public. "The main goals of information security are Confidentiality, Integrity and Availability [2]." This simply means that information needs to be easily accessed by the people that should have access to it and the

information needs to be accurate. This is commonly known in the information security field as the CIA triangle which is visually represented and summarized in **Figure 1** below.

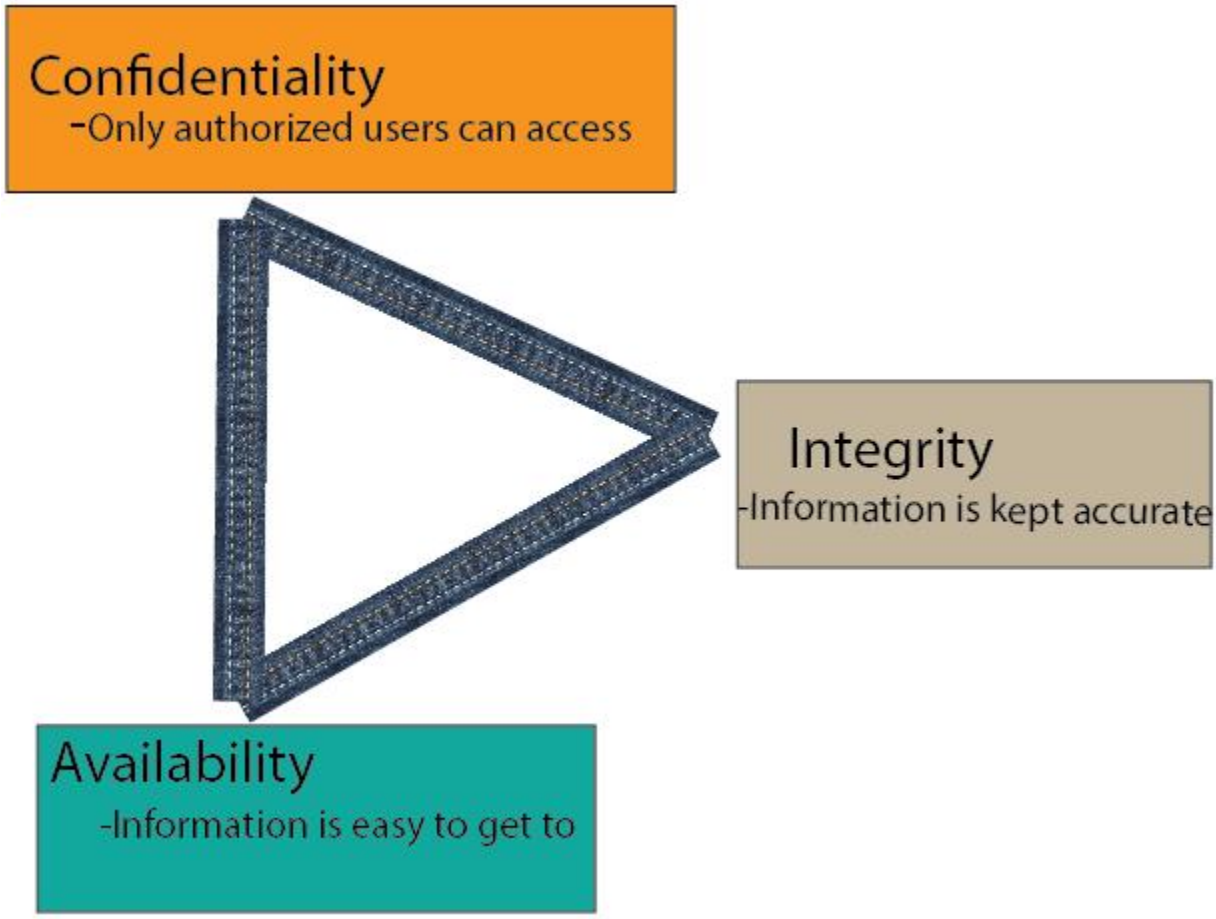

Figure 1. CIA Triangle

Every home office and organization is going to have its own unique situation in regards to the types of information and the laws and regulations and responsibilities associated with maintaining the security of that information. Sometimes it may be easy to maintain confidentiality, integrity and availability, and in other cases it may be extremely difficult. It is about finding the balance of these areas that creates success. "The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption [3]." It is the creation of effective policy that is going to be the foundation of a successful Information Security strategy. Before jumping into policy, we need to look at the larger picture.

3. GOVERNANCE

Creating Information Security policy is a critical step in the larger picture of governance. "Information Security policy is an essential component of Information Security governance—without the policy, governance has no substance and rules to enforce [7]." According to NIST document SP 800-100, which is where much of the information in this paper was retrieved from, Governance involves "… establishing and maintaining a framework and supporting management structure and processes to provide assurance that Information Security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk [7]." To put this in simple terms, governance is the process of making sure things are secure and making sure the things

people do, the technology that is put in place, and the actions of management are legal and abide by policies that support the vision and atmosphere desired by upper management.

4. POLICY

Take your shoes off at the door. Wash your hands before you eat. Do not watch TV two hours before bed. Sync the photos folder with the external hard drive in the safe every time new photos are uploaded to the folder. Create passwords with at least eight characters. No personal activity on business equipment. These are all examples of policy. Some are simple rules that children may have to abide by. Others may be used in a home or small office setting. In a home setting, these rules are put in place to accomplish a general objective; usually the purpose is to keep family and information safe, such as family photos in the example above. In the workplace, an organization will set an atmosphere that encourages or discourages certain behavior whether realizing it or not. This behavior is going to either open the organization to additional threats or help to prevent incidents. Policy that is developed and implemented correctly is going to shape an entire organization and influence the people, technology used to mitigate incidents and even play a role in influencing the environment as represented in **Figure 2** below.

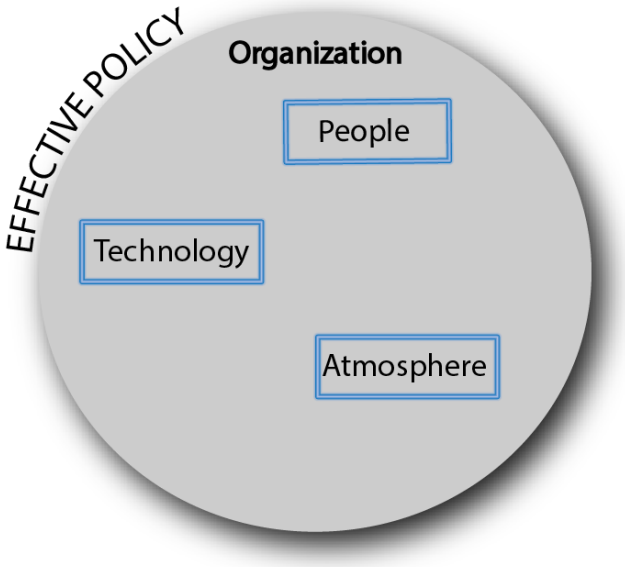

Figure 2. Effective Policy

4.1 INFORMATION SECURITY POLICY

Although there are many areas that policies can cover, we are focusing on Information Security policy which is directed specifically at actions and procedures that affect organizational information security. "Information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information [7]." This could be acceptable use, unacceptable use, and even procedures for storing, backing up and recovering information. According to NIST, information security policy should include information on which roles are responsible for certain tasks, information about baseline standards for security controls, and behavior guidelines for employees and consequences for not complying with the policies [7]. "It is thought that the root cause of 80% of security incidents could be avoided by 'doing the basics well [5].'" Policy is something basic that, with proper development and maintenance, can be done well and have greater impact on the security of your information more than any available anti-virus software ever developed. Some believe that "Organizations can reduce the risks to their business by building up capabilities in three critical areas – prevention, detection and response [4]." **Table 1** below shows how developing specific goals and establish policies in each of these areas are applied to Management, Processes and Technology.

	Prevention	Detection	Response
Management and organization	Appointing cyber crime responsibilities	Ensuring a 24/7 stand-by (crisis) organization	Using forensic analysis skills
Processes	Cyber crime response tests (simulations) Periodic scans and penetration tests	Procedures for follow-up of incidents	Cyber crime response plan
Technology	Ensuring adequate desktop security Ensuring network segmentation	Implementing logging of critical processes Implementing central monitoring of security incidents	Deactivating or discontinuing IT services under attack

Table 1. How developing specific goals and establishing policies in Prevention, Detection, and Response are applied to Management Process and Technology [4]

4.2 Education

While the process of education may seem like a simple one, it can be a challenge to ensure that everyone has not only seen the developed policy but also understands is and agrees to it [10]. Security awareness can positively influence the attitudes of employees towards policy compliance. "Many users can pose a challenge to an organization in that they could be ignorant, make mistakes, and just cause deliberate acts against the information systems [9]." Education is one of the most important parts of an information security policy. The importance of achieving goals and the importance of training as a countermeasure is paramount. It is a way to show your employees the information they need to do their jobs. Training programs will ensure that employees have the information and resources to properly use and protect the information systems that they use every day. It also is a way to show the responsibilities of the various people working with the information systems and how they should use them. It is also shown that companies that have trained their employees have had a higher rate of success [7].

4.3 Enforcing

Consider the situation that you are a small business owner with a handful of employees that each has their own computer systems in their work spaces. Over a period of time, you become suspicious that two of your employees are consistently using their computers for personal business. You haven't said anything to them and there is no policy in place that specifically says that they are not allowed to, but you assume that everyone knows that using work resources for personal business is not okay. You have known about employee X for a long time now and a new employee Y has started doing something similar to employee X over the last few months. This is when you decide a policy must be created. However, you get busy and forget to send it out. The next day you see employee Y doing some more personal work. You decide to say something to employee Y because they are taking things a little too far and you could tolerate the amount that employee X was doing. If employee Y refuses to stop their activity, are you allowed to fire them for their actions? They get their work done. They are not breaking any laws. If you fire them on the grounds of using work resources for personal use, which is against policy. Can they sue you and the company for their termination? There are many more legal factors involved in this case than the scope of our research will cover, but from the angle of policy, they could sue. A company must have in place a solid policy with no gaps that allow undesired behavior to slip through. Regarding policy compliance, we may think that people either obey it or not and we must make the consequences clear to intimidate compliance. In an article called "Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition," Princely Ifinedo studies the relation of compliance to policy and the social relationships and environment and the general knowledge of security awareness in general. "Data from a survey of business managers and IS professionals confirmed that social bonds that are formed at work largely influence attitudes towards compliance and subjective norms, with both constructs positively affecting employees' ISSP compliance [8]." He found that social relationships formed in the workplace positively affected the compliance to security policy by employees. He refers to these as socio-organizational factors and says that it influences the attitude of employees in turn influencing their compliance. While the article dives into the hypothesis and raw data, the

summary of these findings is impactful and should influence how we develop policy and be strategic in encouraging compliance.

> "Our findings showed that the proposed factors indeed affect ISSP compliance in organizations. To a large degree, the study's results indicated that socio-organizational factors affect individuals' attitudes towards ISSP compliance and subjective norms, which in turn affect ISSP compliance behavioral intentions. In addition, social influence and individuals' perceptions of their control and competence with regard to IS security issues have a positive effect on ISSP compliance behaviors. By focusing on the constructs considered in this study, knowledge of ISSP compliance is augmented and diversified [8]."

This tells me that setting a good balance between comprehensive policy and having a good working relationship with employees that can allow them to see that a manager has some trust and can give them some freedoms within acceptable guidelines is important and can be more beneficial than ruling with intimidation, overbearing policy and micromanagement.

4.4 Maintaining

Creating a policy and educating others how to comply with it is only effective if the policy remains up-to-date. "Some attempts fail because there is a lack of management support, some attempts fail because there is no enforcement, and others fail because of a lack of experience. But the most common problem is neglecting the security program once it is implemented [6]." The world of technology, as we all know, is a fast paced one with things constantly changing and old ways becoming obsolete sometimes before we even fully understand them. "…effective cyber security policy and strategy should be based on continuous learning and improvement [4]." Because of these changes security professionals need to constantly learn new ways, learn about new threats and adapt current policy to apply to this ever changing world. It is suggested that "To ensure that information security does not become obsolete, agencies should implement a policy review and revision cycle [7]." In order for a security program to be effective, there are suggested actions to take regarding policy, and as mentioned above, this involves a continuous cycle of "review of policies and procedures, daily administration, and verification audits" by management and legal counsel [6]. Following this continuous cycle ensures that all policies are not just "maintained," but it ensures they are up-to-date and applicable to the current environment and situations facing an organization.

5. PRACTICAL RECOMMENDATIONS

We did not show comprehensively enough to give strategies on finding threats to your organization, determining the best way to handle or prevent them, and writing effective policy to mitigate all these threats. What we can do though is encourage you to think about the behavior an employee should have and what things they can and cannot do with company equipment and what actions would threaten the well-being of the organization and its information. Essentially this is stepping back and looking at what you have that may be at risk, whether it's your public image or classified company files and determining what actions, standards and technologies are acceptable and needed and what actions are not acceptable and this becomes your policy.

5.1 Proactive versus Reactive

When a situation arises that needs a policy to help avoid further damage or a repeat occurrence, then it is too late. Start before the need arises. Get the information into the hands of your employees before they take a client's file home and lose it. Be proactive. Always be on the offensive looking for new issues that need to be addressed. How should the new 50" TV in the lobby be used, March madness or live stock information and news that affects the company?

5.2 Detailed and Comprehensive versus Vague

When developing these new policies be thorough and detailed versus only covering the minimum information. Don't be vague when setting rules. Say "Facebook, twitter and other social networking sites are not permitted to be viewed on company computers." Instead of "No personal activity is allowed on company time."

6. CONCLUSION

As we have seen, policy can encompass many areas and is one of the key aspects of having a successful information security program that maintains confidentiality, integrity, and accessibility to an organization's information. Policy affects everything down to even the workplace environment. There are always going to be new systems and areas that need to be addressed by the continuous updating via a repeating cycle of review and revision. Start now and be detailed and thorough.

REFERENCES

[1] OIT Communications Group. (2014). definition-information-security. Retrieved 11 29, 2014, from oit.unlv.edu: https://oit.unlv.edu/network-and-security/definition-information-security

[2] Information security. (2006). Retrieved April 10, 2014, from http://ubiquity.acm.org/article.cfm?id=1117695

[3] Swanson, M. et al. (2010). Contingency Planning Guide for Federal Information Systems. SP 800-34. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[4] KPMG LLP. (2014). Cyber security: it's not just about technology. Retrieved from kpmg.com: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-security-not-just-technology.pdf

[5] Schreiner, S., Carpenter, M., Hamerstone, A., Coffey, C., Webb, N., & Rottinger, J. (2013). CyberOps Quick Start Guide: Human Factors, Version 1.2. Retrieved from TMForum: http://www.tmforum.org/GuideBooks/GB968CyberOpsQuick/50365/article.html

[6] Jarmon, D. (2002). preparation-guide-information-security-policies-503. Retrieved from sans.org: http://www.sans.org/reading-room/whitepapers/policyissues/preparation-guide-information-security-policies-503

[7] Pauline Bowen, Hash, J., & Wilson, M. (2007, March 07). Information Security Handbook: A Guide for Managers. Retrieved from csrc.NIST.gov: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[8] Ifinedo, P. (2015). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 69-79.

[9] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. MIS Quarterly, 34(3), 523-A7.

[10] Whitman, M., & Mattord, H. (2010). *Management of Information Security.* Boston, MA: Course Technology.