ISSN: 2167-1435
v30 n2578

A New Value for Information Security Policy Education

Garry L. White
gw06@txstate.edu
Department of Computer Information Systems & Quantitative Methods
Texas State Univeristy
San Marcos, Texas, 78666 U.S.A.

Abstract

Security breaches are a result of poor policies, not the technology used. This paper presents critical issues an information security and assurance policy course should cover. Some of the problems with policies are: 1) failure to address unique systems configurations due to be belief compliance to standards provides full protection, 2) deal with situations that do not yet exist due to new and changing technologies, 3) lack of addressing the external due to globalization and outsourcing, 4) no relationships between security best practices policies and the incidence or severity of security breaches, and 5) the lack of policies being people focus.

A good security policy course should teach students how to deal with these problems and write, develop, and implement good policies. These new policies must go beyond required compliance so as to address unique system configurations, deal with the dilemma of security hindering productivity, and finally, focus on people.

Keywords: education, policy, security, assurance, curriculum..

1. Introduction (White, 2009)

Strategic management answers the question "why do security enterprise problems exist?" This question of security leads to developing security policies that deal with people issues, and evaluates internal/external risks.

Policies:
Policies are "a set of rules combined to create a management framework that dictates how an organization will function" (Greene, 2006, p. 542), while, standards are "specific minimum requirements in policies" (Greene, 2006, p. 543).

Information security policy provides a framework to ensure that systems are developed and operated in a secure manner. Such policies must consider internal and external threats and risks. They must address issues such as privacy and be current to changing technologies. Additionally, policies must complement and be compatible with federal, state, and local laws.

Zhang & Suhong (2006) indicated the need for secure information sharing policies in Internet-based supply chain management. Such policies enhance the competitive advantage by promoting trust with partners, a strategic goal. However, the literature, with regard to the formulation of the information security policy, has generally tended to ignore the important relationship with the strategic information systems plan (Misra et al, 2007).

People issues:
Strategic management is not focused on technologies, but on higher-level issues of functionality for all stakeholders. Stakeholders in information security include government regulators, shareholders, customers, employees and business partners. (Vijayan, 2005).

Additionally, laws, ethical principles, codes of conduct, and society-driven needs are considered. Relationships with people, effective communication and human resources management are required. Security professionals deal with people, both criminal and non-criminal. (Armstrong & Jayaratna, 2002; Zhang & Suhong , 2006).

A proactive approach to new threats and risks, is a component of strategic management, as well as enterprise strategic planning. A business impact analysis identifies threats and possible attacks where potential damage is then assessed (Whitman & Mattord, 2005, p. 209). Evaluating these threats and risks prioritizes investments for information security and the establishment of new security policies. Enterprises must adapt themselves to rapidly changing circumstances in order to survive in changing external environments (Kim & Leem, 2005). As the environment changes, so do the threats and risks. A proactive approach to these new threats and risks, instead of reacting to incidents, is to modify or create new security policy.

Development of security policies requires a common vision shared by planners, constructors, and administrators. It integrates management processes and policies for enterprise information security (Kim & Leem, 2005). The security professional must be able to advise top management on strategic policy security decisions.

2. PROBLEMS WITH POLICIES

An increasingly important business document is the information security policy (Doherty & Fulford, 2005). "Of all the tools at the information security manager's disposal, none is more widely valued and used than the information security policy" (Stahl, et. al., 2012). Policy provides organizations guidance on the means if information security management as well as the desired end results (Stahl, et. al., 2012). Policies emphasizing management's commitment to and support of information security (Stahl, et. al., 2012). Unfortunately, generalized policies cannot address unique needs (Malin, 2007) or new technologies such as mobile devices. There is a need to update policies due to new and changing technologies and standards.

Starting in 1995, corporate business executives recognized that a changing Internet required changes in security policies (Berryman, M. 2008; Harne, 2004; Lindup, 1995). IT security policies develop and mature over time (Frankland, 2008). An example is Bring Your Own Device (BYOD) (Casey, 2012). A few years ago, the technology did not exist where cell phones can be used to do work on the Internet. Today, smart cell phones can now do that. New policies need to be written to deal with this new situation for a business. And there are social networks. They did not exist 10 years ago. Web site or Internet policies of 10 years ago are now outdated (Berryman, 2008). Policies lag behind technologies. Future corporate leaders need to know how to write new policies for situations that do not yet exist.

Globalization has created another problem; outsourcing, especially to a foreign country. Policies must address these external third parties (outsourcing) (Kemp & Kemp, 2005), especially foreign laws. Unfortunately, policies tend to deal with internal systems, where the organization has the most control.

Another problem research has shown is no statistically significant relationships between the adoption of information security best practices policies and the incidence or severity of security breaches (Doherty & Fulford, 2005). Five possible reasons for this are as follows:

1. Difficulties of raising awareness (Sipponen, 2000). Let alone getting employees to read the policy and take the policy seriously (Hinde, 2002; Wood, 2000).
2. Fail to impact the users (Hone & Eloff, 2002).
3. Inadequate resources to monitor and enforce policies (Doherty & Fulford, 2005).
4. Policy standards are too complex and time consuming to apply (Doherty & Fulford, 2005).
5. Failure to tailor polices (Doherty & Fulford, 2005).

Sometimes, being compliant to regulations can be a problem. One size, such as "best practices," does NOT fit all. Being compliant does not guarantee best fit. To deal with unique computer configurations may require going beyond compliance or best practices. This may also help explain Doherty & Fulford (2005) findings.

Finally, security incidents are not due to technology, but due to poor policies which is a people problem. The five reasons from Doherty & Fulford (2005) focus on people. And different people require different policies. Therefore, separate policies need to be written for IT staff and business users (Vijayan, 2006).

3. NEEDS

Effective security starts with policies (Andress, M., 2001). Current security courses tend to deal with current technologies. A policy course is different. Policies dictate technology through stating results to be accomplished. Policies do not dictate what technologies to use, only the objectives security technologies must accomplish. This is how a policy course is different from a security course.

To know how to development and implement of a good policy is needed. For example, know how to identify the security policy requirements for various computer systems (Malin, 2007), especially for new technologies that yet to exist. These requirements can be based on the network attack data (Zhdanov, 2007) or government regulations.

Security policies need to be easily enforceable. (Vijayan, 2006). And good policies must be updated; continually reviewed and improved (Andress, 2001; Bielski, 2005). Authors of policies need to know these aspects and learn how to resolve them. What students need to learn is how to create new policies that deal with new and changing technologies and situations. Just as laws lag behind technology, so do corporate polices.

Policy course content:
A good policy course will focus on procedures; internal (policies), external (laws and regulations), strategic aspects of access control and data classification, strategic decisions involving corporate security and assurance issues. Students need to learn how to write security policies that clarify thinking and agenda (Bielski, 2005), be broad in scope and clear in meaning (Berryman, M. 2008), be compliant with laws and regulations, protect corporate data, ensure operation continuity, and deal with new technologies yet to be developed. The impact of a good policy course on employers will be having future managers who can create good information security policies to protect corporate data and ensure continue operations during a cyber-attack.

The primary goals of a policy course are to introduce students to the issues and concepts of information systems security policies along with the methods and /procedures to assure compliance and how to develop good policies. It should teach how to deal with new situations that yet to exist because these future managers will be held accountable for these new situations. Another issue is how information security hinders productivity. The course should also teach how to write a policy to deal with this dilemma in the corporate world. (Zhdanov, 2007).

4. CONCLUSION

"No matter how many sophisticated security tools a company has, it also needs good security polices …" (Anthes, 1995). A good security policy course should teach students how to write good policies for new technologies yet to exist, go beyond required compliance so as to address unique system configurations, deal with the dilemma of security hindering productivity, and finally, focus on people -- not the technology used. Such a course should be more than just an elective.

5. REFERENCES

Anderson, J. E. & Schwager, P. H. (2002). Security in the Information Systems Curriculum: Identification & Status of Relevant Issues. *Journal of Computer Information Systems*, 42(3), 16-24.

Andress, M. (2001). Effective security starts with policies. *InfoWorld*, 23(47), 56-57.

Anthes, G. H. (1995). Security tools and policies go hand in hand. Computerworld, 29(24), 61.

Berryman, M. (2008). IT POLICY: Setting sensible internet policies; a rapidly evolving web environment requires employers to

develop smarter internet-use policies. *New Zealand Management,* February 2008, 43.

Bielski, L. (2005). Getting "front and center" on security policies*. American Bankers Association. ABA Banking Journal,* 97(3), 57-59.

Casey, K. (2012). 6 Risks Your BYOD Policy Must Address. *InformationWeek – Online*, Nov. 19, 2012. Retrieved from http://search.proquest.com/docview/1171331024?accountid=5683.

Doherty, N.F. & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information Resources Management Journal*, 18(4), 21-39.

Frankland, J. (2008). IT security metrics: implementation and standards compliance. Network Security, 2008(6), 6-9.

Green, S. S. (2006). Security Policies and Procedures: Principles and Practices. Pearson Prentice-Hall, Upper Saddle River, NJ. p. 542, 543.

Harne, E. G. (2004). Perfecting Security's Policies. *Security Management*, 48(5), 32-34.

Hinde, S. (2002). Security surveys spring crop. *Computers and Security*, 27(4), 310-321.

Hone, K. & Eloff, J.H.P. (2002). What makes an effective information security policy? *Network Security,* 20(6), 14-16.

Kemp, M. & Kemp, M. (2005). Beyond trust: security policies and defense-in-depth. *Network Security,* 2005(8), 14-16.

Kim, S. & Leem, C. S. (2005). Enterprise security architecture in business convergence environments. *Industrial Management + Data Systems*, 105(7), 919-936.

Lindup, K. R. (1995). A new model for information security policies. *Computers & Security*, 14(8), 691.

Ogut, H. & Cavusoglu, H. & Raghunathan, S., (2008). Intrusion-Detection Policies for IT Security Breaches. *INFORMS Journal on Computing*, 20(1), 112-123.

Malin, A. (2007). Designing Networks that Enforce Information Security Polices. *Information Systems Security*, 16(1), 47-53.

Sipponen, M. (2000). Policies for construction of information systems' security guidelines. In Proceedings of the *15th International Information Security Conference* (IFIP TC11/SEC2000), Beijing, China, August, 2000 (pp. 111-120).

Stahl, B.C. & Doherty, N. F. & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Info System*, 2012(22), 77-94.

Vijayan, J. (2005). Strategic Security. *Computerworld*, 39(15), 48.

Vijayan, J. (2006). Data security policies need focus, execs say. *Computerworld*, 40(15), 12.

White, G. (Spring, 2009). "Strategic, Tactical, & Operational Management Security Model." *Journal of Computer Information Systems, 49(3), 71-75.*

Whitman & Mattord, (2003). Principles of Information Security, Thomson Course Technology, Boston, MA.

Whitman, M. E. & Mattord, H. J. (2005). Principles of Information Security, 2nd Ed. Thomson/Course Technology, Boston, MA.

Wood, C.C. (2000). An unappreciated reason why information security policies fail. *Computer Fraud & Security,* 10, 13-14.

Zhang, C. & Suhong, L. (2006). Secure Information Sharing in Internet-Based Supply Chain Management Systems. *Journal of Computer Information Systems*, 46(4), 18-24.

Zhdanov, D. (2007). Information security in organizations: Drivers, policies, and compliance incentives. *ProQuest Dissertations.*