CORE Metadata, citation and similar papers at core.ac.uk

Provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Mindful Administration of IS Security Policies

James L. Parrish, Jr.
University of Central Florida, jparrish@bus.ucf.edu

John R. Kuhn, Jr.
University of Central Florida, jkuhn@bus.ucf.edu

James F. Courtney
University of Central Florida, jcourtney@bus.ucf.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2008

Recommended Citation

Parrish, Jr., James L.; Kuhn, Jr., John R.; and Courtney, James F., "Mindful Administration of IS Security Policies" (2008). *AMCIS 2008 Proceedings*. 270.
http://aisel.aisnet.org/amcis2008/270

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2008 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Mindful Administration of IS Security Policies

James L. Parrish, Jr.
University of Central Florida
jparrish@bus.ucf.edu

John R. Kuhn, Jr.
University of Central Florida
jkuhn@bus.ucf.edu

James F. Courtney
University of Central Florida
jcourtney@bus.ucf.edu

ABSTRACT

Managers of information systems have ethical, moral and legal obligations to protect their organization's intellectual property. They often look to frameworks such as the Control Objectives for Information and related Technology (CobIT) to guide them to what data needs to be secured or standards such as the ISO/IEC 27000 series to provide best practices regarding their policies on how to safeguard this information. However, these policies are either vague in the details or not fluid and flexible enough to account for the unexpected security events that may render them obsolete. For example, Google recently released an online suite of applications that would allow an organization's employees to collaborate on items of intellectual capital stored on Google's servers outside the control of the organization's information technology (IT) department. Additionally, new techniques have been discovered to break the encryption of data that was previously thought to be lost when the device containing it was powered off. While these events certainly have utility to practitioners, they also pose new threats to the security of intellectual capital created and stored on IT artifacts. This paper advocates mindfulness (Weick and Sutcliffe, 2001) as a necessary component of choosing and adapting security policies to better predict the unexpected security threats that may come as a result of technological change, environmental forces, or organizational use of IT.

Keywords

IT security, IT security policy, mindfulness, security standards, ISO, CobIT.

INTRODUCTION

In 1986, Richard Mason enlightened researchers in information systems (IS) to four ethical issues associated with information systems. He simplified these dilemmas into a single acronym, "PAPA," which stood stands for privacy, accuracy, property, and accessibility (Mason, 1986). In Mason's model, privacy dealt with issues related to personal information that is embedded within intellectual capital. Accuracy was focused on those issues related to the validity of the intellectual capital and who was responsible for ensuring that validity. The property dimension of the model was concerned with ownership of the intellectual capital and the technologies used to store and transmit it. Finally, accessibility was relevant to those issues of what information individuals or organizations had the right to access, and the conditions under which it should be accessible (Mason, 1986).

As technology and organizations evolve, never have the issues regarding securing our information been more prevalent than today. For example, organizations are turning more to mobile computing devices such as laptops and hand held devices such as Blackberries and Palm Pilots. This change moves the technology outside the workplace and puts more ethical responsibility on the individual to safeguard intellectual property stored on mobile devices. Recent events only highlight these dilemmas. Take, for example, the discovery that cooling random access memory (RAM) chips allows memory once thought to be gone to be accessed for hours after the device in which they are embedded is powered down. This method also allows breaking of encryption schemes on the data stored on the RAM.

Another example can be seen in the advances in web technologies that have enabled the creation of such applications as the Google Team Suite. This suite of applications allows organizational members to collaborate and to create, share, and store items of intellectual property on the web, outside the organizational boundaries of the corporate information technology department, its policies and procedures, and the protection of its firewalls. This type of application is illustrative of all the issues described in Mason's model. For example, consider the following questions?

- Do employers have the right to know that their employees are using this application suite (Privacy)?

- Who is responsible for the accuracy of the items of intellectual property created through the collaborative efforts of employees mediated by information systems that are not the company's property and not subject to its policies (Accuracy)?
- If the employees are creating intellectual property while they are being paid by the organization, but storing and modifying that intellectual property on another organization's servers, who really owns it (Property)?
- Do employees have the right to create, access, and modify intellectual property on servers external to the organization? Do the owners of the servers have rights to access it since they own the servers (Accessibility)?

While ethical issues and security breaches are not the same, it is easy to see how ethical questions such as the ones mentioned can impact how an organization secures its systems and data.

For the most part, IT professionals turn to tools such as standards created by the International Organization for Standardization (commonly referred to as ISO) to assist with securing information systems, however as technology and the way we use it continue to evolve, a single innovation can render the most stringent standards obsolete. Other tools provide general frameworks on what should be done (e.g. CobIT) but do not provide specific guidance on how security policies should be implemented. When writing about the adoption of security standards by European small and medium enterprises, Bartlette and Fomin (2008) note that some information standards received criticism for not being suitable or adaptable for businesses. There certainly seems to be a need for organizations to be able to adapt their standards and frameworks in response to the unexpected events that arise as a result of technological innovations.

The purpose of our research is to highlight the ability of technological innovations to affect current security standards and policies and to examine the relationship between organizational mindfulness and the way that organizations manage their security policies. Organizational mindfulness (Weick and Sutcliffe, 2001) is the extension of mindfulness theory (Langer and Moldoveanu, 2000) to the organizational level. Weick and Sutcliffe created the concept by examinining the qualities of high-reliability organizations. High-reliability organizations are organizations such as aircraft carriers and nuclear power plants that experience a very small amount of unexpected events. Weick and Sutcliffe (2001) attributed the small amount of events to five factors: (1) Preoccupation with failure, (2) reluctance to simplify expectations, (3) sensitivity to operations, (4) commitment to resilience, and (5) deference to expertise.

The remainder of this paper will be structured as follows. First, we will provide a brief overview of two of the major tools that organizations are using to protect their information systems and data (ISO and CobIT). We will then review these standards in the context of the Google Team Suite and mobile computing to identify any weaknesses that may exist in this context. Next, we will present the concept of organizational mindfulness and present seven propositions to assist with identification of the qualities of organizations that take a mindful approach to implementing and modifying IT security policies and procedures. Finally, we will conclude with an outline for future research.

THE ISO STANDARDS

ISO is a non-governmental, standard-setting organization comprised of a network of national standards institutes for 157 countries. ISO develops and publishes international standards for industry and commerce ranging from agriculture to railway engineering. Over 17,000 standards have been issued to date and an average of 1,100 new standards are created per year (ISO 2008a). The organization's goal is to "promote the development of standardization and related activities in the world with a view to facilitating international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity" (ISO 2001). Research has shown ISO significantly influences the diffusion of organizational practices across organizations, companies, nationalities, and cultures (Guler et al. 2002).

In order to eliminate redundant IT standards, ISO formed a joint task force with the International Electrotechnical Commission (IEC) to develop, maintain, and promote IT standards in the global marketplace that must be characterized by interoperability, portability, and cultural and linguistic adaptability. The task force directives define the scope of IT standards as those related to "the specification, design and development of systems and tools dealing with the capture, representation, processing, security, transfer, interchange, presentation, management, organization, storage and retrieval of information" (ISO, 2008b). As this study focuses on information security, the ISO/IEC 27000 (ISO27k) series of standards hold particular relevance as they contain best practice recommendations for information security management (ISM). ISO27k "provides the means to implement effective information security management in compliance with organizational objectives and business requirements" and the recent publication "is a big event in the world of information security and one that has been eagerly awaited" (Humphreys, 2006). However, ISO27k is far from complete. Only three standards have been officially published (27001, 27002, and 27006) covering implementation and maintaining an ISM system, guidelines for conducting ISM in an organization, and guidance for bodies that provide audit and certification of ISM systems. The joint commission announced plans for at least ten other standards that include a focus on ISM (IsecT Ltd., 2008).

This timing raises several concerns. Companies have been using IT in normal day-to-day business processes for over 30 years and Internet access for employees has been the norm for over a decade. Why has it taken this long for ISO to develop standards addressing ISM? Given the heavy reliance on ISO standards by companies globally, managers and shareholders should be concerned about the lack of ISM standardization. Are their companies truly adhering to best practices and moreover, what are those best practices? Are their companies able to adapt to the constantly changing security threats as technology becomes easier to use and abuse? In the case of Google Team Suite, how would these standards protect systems and data from misuse if the data resides on systems outside the organization? These are only a few of the questions that should be addressed by organizations that rely on the ISO standards to protect their systems and data.

THE COBIT FRAMEWORK

CobIT, a product of the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI), provides a set of "best practices" and a framework to develop IT governance, security, and control policies and procedures. Released in 1992, the framework gained popularity for the development of governance structures because its scope encompasses business requirements, IT resources, and IT processes (See Figure 1). Since the focus of this paper is security and the processes and practices that are used to ensure it, we focus on the face of the CobIT cube associated with IT Processes (all of the documents of CobIT may be obtained free of charge at www.isaca.org).

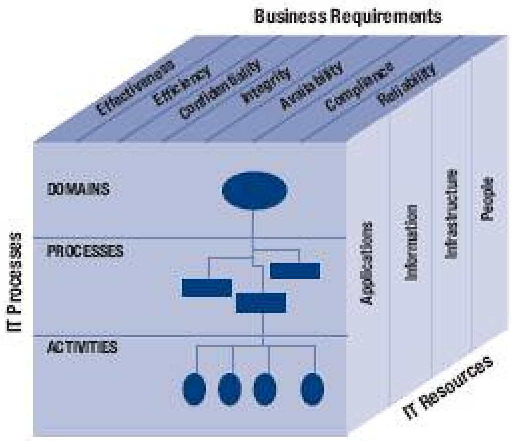


Figure 1. The CobIT Cube (ITGI, 2005)

According to CobIT, the various IT processes are controlled through the definition of high level and detailed control objectives arranged into four domains: (1) Plan and Organize, (2) Acquire and Implement, (3) Delivery and Support, and (4) Monitor and Evaluate. Objectives are implemented through the use of control practices (a.k.a. internal controls) and measured through management guidelines such as key performance and goal indicators and maturity models. Figure 2 depicts the relationship between business and IT processes, control objectives, control practices, and management guidelines.

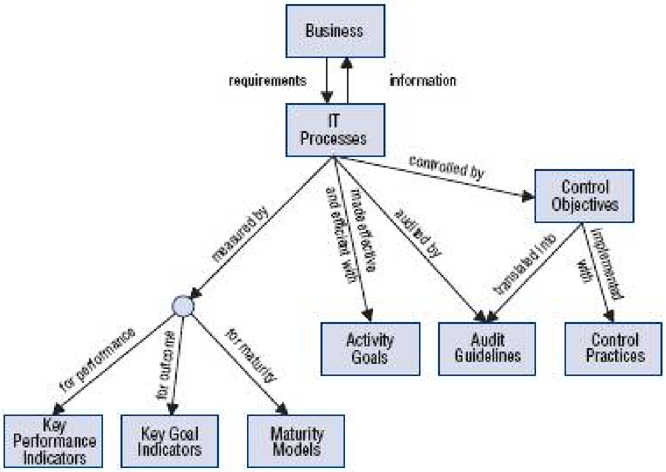


Figure 2. Interrelationships of CobIT components (ITGI, 2005)

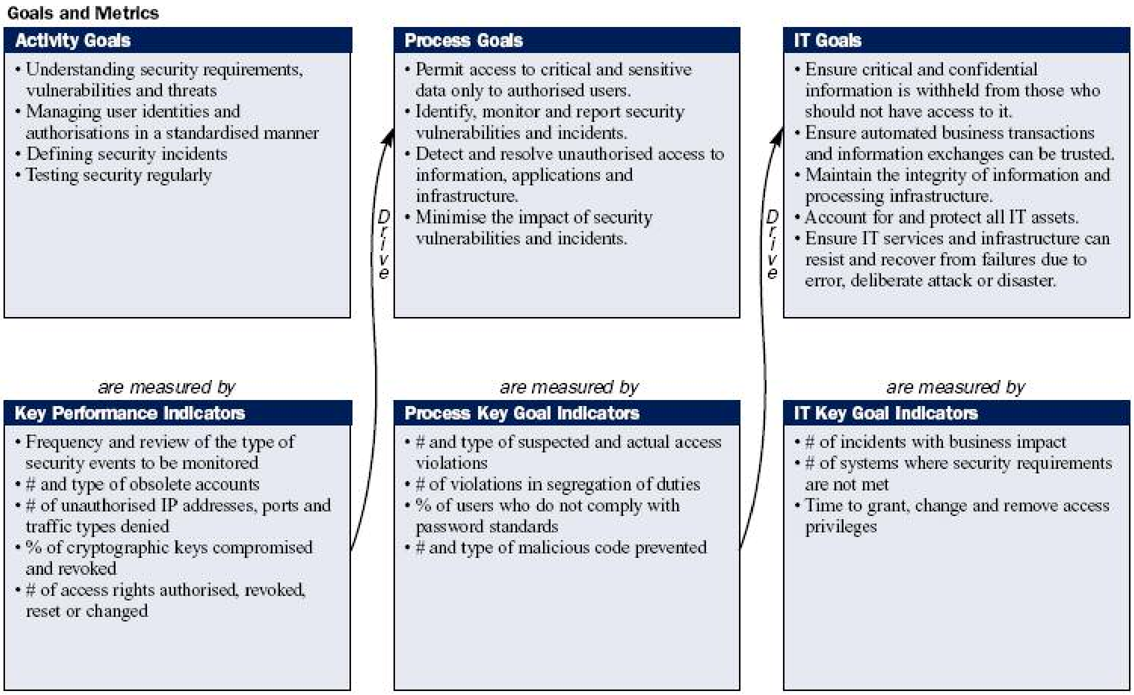
Of the four domains listed, Deliver and Support provides the most guidance on IT security, particularly on how IT solutions perform and their level of efficiency. The high level control objective associated with security of systems is "DS5 – Ensure Systems Security". DS5 seeks to maintain the integrity of information and infrastructure and minimize the effects of any security vulnerabilities or incidents through security testing, standardized user management, and understanding of the security environment (ITGI, 2005). Table 1 summarizes the 11 detailed objectives associated with DS5.

No.	Title	Description
DS5.1	Management of IT Security	IT Security management should be consistent with business requirements and done at the highest appropriate level in the organization.
DS5.2	IT Security Plan	An overall IT security plan should be put together, implemented through policies and procedures, and communicated to organizational members.
DS5.3	Identity Management	All system users should be uniquely identifiable and any access they have to the system should be approved by managers and in line with specific job descriptions.
DS5.4	User Account Management	Any items that pertain to user accounts (creating, modifying, issuing, suspending, and closing) should be addressed by policy.
DS5.5	Security Testing , Surveillance, and Monitoring	The IT implementation should be tested in a proactive manner and unusual activities logged.
DS5.6	Security Incident Definition	The characteristics of security incidents should be defined so that they are properly treated.
DS5.7	Protection of Security Technology	Security-related technology and documentation should be kept with a low-profile
DS5.8	Cryptographic Key Management	Policies should be in place to keep cryptographic keys from being compromised or disclosed without consent.
DS5.9	Malicious Software Prevention, Detection, and Correction	Ensure that measures to protect systems against malicious software are in place and updated.

DS5.10	Network Security	Techniques and procedures should be in place to ensure network security
DS5.11	Exchange of Sensitive Data	Sensitive transaction data should be sent only over trusted paths with controls to provide for authenticity and proof of submission, receipt, and non-repudiation of origin.

Table 1. Detailed Objectives for the Ensure Systems Security high-level objective (ITGI, 2005)

Management guidelines related to DS5 provide the means to measure organizational progress in developing security policies and procedures. Figure 3 lists the goals and metrics for DS5.



Goals and Metrics

Activity Goals

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Defining security incidents
- Testing security regularly

Process Goals

- Permit access to critical and sensitive data only to authorised users.
- Identify, monitor and report security vulnerabilities and incidents.
- Detect and resolve unauthorised access to information, applications and infrastructure.
- Minimise the impact of security vulnerabilities and incidents.

IT Goals

- Ensure critical and confidential information is withheld from those who should not have access to it.
- Ensure automated business transactions and information exchanges can be trusted.
- Maintain the integrity of information and processing infrastructure.
- Account for and protect all IT assets.
- Ensure IT services and infrastructure can resist and recover from failures due to error, deliberate attack or disaster.

are measured by

Key Performance Indicators

- Frequency and review of the type of security events to be monitored
- # and type of obsolete accounts
- # of unauthorised IP addresses, ports and traffic types denied
- % of cryptographic keys compromised and revoked
- # of access rights authorised, revoked, reset or changed

are measured by

Process Key Goal Indicators

- # and type of suspected and actual access violations
- # of violations in segregation of duties
- % of users who do not comply with password standards
- # and type of malicious code prevented

are measured by

IT Key Goal Indicators

- # of incidents with business impact
- # of systems where security requirements are not met
- Time to grant, change and remove access privileges

Figure 3. Goals and Metrics for the Ensure Systems Security High-Level Objectives (ITGI, 2005, p.128)

CobIT primarily addresses "what" to do to ensure systems security but provides little guidance on the control practices that depict "how" that is actually done (Casper, 2004). Some have argued for CobIT to be used in conjunction with other standards such as ISO 27001, where the ISO standards would form the basis of the control practices (Johnson, 2006). From our earlier discussion, however, we see ISO lacks standardization and completion. Even with a complete set of standards to serve as the control practices, any practices implemented may be static while the IT environment around them is highly dynamic. Furthermore, who is to say that the control practices of today cannot be rendered ineffective or obsolete by a technological innovation tomorrow?

To demonstrate this point, return to the example of the Google Team Suite. The release of this application allows users to interact with one another outside the controls of the organizational IT department. For instance, assume the organization in our example uses CobIT as a framework for its IT security. How would it affect the goals and goal indicators if some employees started using the Google Team Suite application to create items of intellectual property? Well, things might not be all that different if everyone in the organization is happy and employed. However, consider the case of a terminated employee. One of the CobIT activity goals is to manage user identities and that is measured in part by the number of access rights that are changed, added, or revoked in a timely manner. For the sake of this example, say our disgruntled employee has his access revoked immediately. From the diagram we can see that these performance indicators drive the process goals.

This is where things begin to break down in the case of the employee's use of the Google Team Suite. Some of the goals in this section relate to permitting access to sensitive data only to authorized users and to detect unauthorized access. If the application that contains the sensitive data exists outside the organization's control, how are these goals achieved? An even more frightening scenario would be if the organization was not even aware of the external application at all. This would cause the organization to *believe* that it meets all of its security goals when, in fact, implemented control practices fail to account for certain violations because of intellectual property stored externally unbeknownst to the organization.

ORGANIZATIONAL MINDFULNESS

Organizational mindfulness is a theory described by Weick and Sutcliffe (2001) that extends the idea of individual mindfulness theory from Langer and Moldoveanu (2000) to the organizational level. Weick and Sutcliffe observed the qualities of mindfulness in what they termed "high reliability organizations" (HRO's). Examples of such organizations include aircraft carriers and emergency rooms. From their observations, they identified 5 qualities related to organizational mindfulness. The five qualities are presented and summarized in table 2 below.

		Quality	Description
Anticipation	1.	Preoccupation with failure.	Success makes organizations complacent because they feel that what they are doing is the best way of doing it. This leads them to become intolerant of other ideas and interpretations that can blind them to the little events that could become crises.
	2.	Resistance to simplify interpretations.	Simplifying interpretations leads to a dependence on expectations that can cause us to ignore evidence that the unexpected is about to occur.
	3.	Sensitive to operations.	When the focus is what is going on at the operational level, small events get big attention and seldom blossom into crisis situations.
Mitigation	4.	Commitment to resilience.	Don't ignore errors that have already occurred. Correct them before they become bigger errors that can cause greater damage.
	5.	Defer to organizational expertise.	Flexible leadership structures allow the person with the most expertise to be empowered to make decisions, allowing organizational proficiencies to be made use of in a crisis. However, higher level managers are readily accessible should events become more than the local experts can address.

Table 2 – The Qualities of Mindful Organizations (Weick and Sutcliffe, 2001)

The use of mindfulness in IS is not a new concept. For example, Swanson and Ramiller (2004) argued that mindfulness theory could form the basis for a strategy for IT innovations. According to them, firms mindfully innovated with IT when the innovation was grounded in their own organizational context. This was contrasted with the mindless IT innovation strategy that did not include context and the innovation was driven more by the fact that other enterprises had already undertaken projects involving the IT innovation. Surprisingly, the two strategies are not mutually exclusive and the authors show how at times one strategy could be favorable over the other (Swanson and Ramiller, 2004)

Butler and Gray (2006) advance mindfulness as a key component for those seeking to increase the reliability of information systems. They state that although routines, policies, procedures, etc. can help to ensure the reliability of systems in static environments, it takes more than that to provide system reliability in more dynamic environments (Butler and Gray, 2006). It is mindfulness that they believe can help organizations and individuals go beyond the consistent actions dictated by procedures to achieve the "properly situated cognition [that] is ultimately the basis for reliable performance." (Butler and Gray, 2006, p.4)

MINDFUL ADMINISTRATING IT SECURITY

Before we discuss how IT security policies are administered by mindful organizations, it would be prudent to make a few comments on how a mindless firm would administer their policies. Mindless firms are rooted in expectations. Therefore, they would expect that since they have had no noticeable breaches in security, their policies must be sufficient to protect them. This is caused, in part, because they are unable to detect the stimuli that could cause an unexpected event due to the predisposition to see situations through the lens of the plans they have created (Butler and Gray, 2006). In contrast to this plan-based focus, the mindful firm focuses its efforts on the perception of cues that could lead to an unexpected situation, how it interprets those cues, and how fast it can take action as a result of its interpretations (Butler and Gray, 2006).

To see how a mindful organization would administer security, we can look at the previously discussed elements of mindful organizations and apply them in this context. For example, an organization that is preoccupied with failure would be concerned that their security policies would be able to address any type of existing or potential threat. Any potential violation of security policy would be taken seriously and addressed immediately in the organization. The lessons learned from the failure would be incorporated back into the security policy. This attention to the possibility of failure acts as a buffer to the complacency and inattention that security policies often receive when small failures are not noticed by the organization or when the security staff develops too much confidence in the policies that they have in place (Weick and Sutcliffe, 2001; Butler and Gray, 2006). The foregoing leads to Propositions 1 and 2:

P1: Mindful organizations amend their IT security policy as a result of identified violations more frequently than mindless organizations.

P2: Mindfulness will be exhibited more prominently in organizations that have recently changed IT security policies or implemented a new IT security policy.

A reluctance to simplify interpretations means that the organization does not simply see things from one or two perspectives, but that it brings in many different perspectives in its attempts to interpret phenomenon (Butler and Gray, 2006, Weick and Sutcliffe, 2001). By bringing in multiple perspectives, mindful organizations increase their ability to notice small changes in their environments or small deficiencies in their security policies that could possibly lead to much larger security breaches. For example, the Sarbanes-Oxley act of 2002 requires the evaluation of all deficiencies regardless of individual impact. In fact, a group of smaller, related deficiencies can be viewed as a material weakness in internal controls. This is significant because SOX requires that material weaknesses are reported in the financial statements and how they will be addressed. Only an organization with a requisite level of mindfulness can recognize and interpret the interrelationships of the smaller deficiencies in the context of the larger, additive impact on the organization. In addition to detecting small differences, however, we argue that by looking at issues from multiple perspectives overcomes the deficiencies of a single perspective (Courtney, 2001) and potential threats from security can be unearthed that may have gone unnoticed in larger, more noticeable events as well. Propositions relating to these concepts are:

P3a: Mindful organizations report a greater number of minor security violations than mindless organizations.

P3b: Mindful organizations report a lesser number of major security violations than mindless organizations.

Sensitivity to operations presumes an understanding of the interrelationships of the different operational facets of the organization. This allows for the organization to understand that plans may actually serve to cover some of the potential problems because they were never considered in the plan (Butler and Gray, 2006, Weick and Sutcliffe, 2001). This is overcome by spending effort focusing on what is ***actually*** done on the operational level of the organization as opposed to what ***should*** be done. Here, the mindful organization understands that there may not always be a "faithful" (DeSanctis and Poole, 1994, Butler and Gray, 2006) appropriation of IT within an organization and the security policies can not be based on how the IT was designed to be used, but rather how it actually is used. Additionally, the persons responsible for the organizational IT security policy should have a great deal of "laterality," (Tiwana, 2000) meaning that they are able to bridge the gaps between operational groups and understand the interrelationships between them. We therefore propose that:

P4: Mindful organizations amend their IT security policy based on the actual use of IT within the organization.

P5: The persons responsible for the IT security policy in mindful organizations possess cross-functional organizational knowledge.

A commitment to resilience focuses on an organization's ability to tend to problems as they arise (Butler and Gray, 2006, Weick and Sutcliffe, 2001). In the context of the IT security policy of the mindful organization, this implies two things. The first implication is that the mindful organization is constantly adjusting its policies. Many times, organizations that follow a planning paradigm to adjust their security policy will wait until the standards organizations release new recommendations, or set a predetermined schedule to adjust their security policies. In contrast, the mindful organizational members would spend great efforts to identify the latest trends in IT innovation and use to ensure that their policies address them proactively.

P6: Mindful organizations amend their IT security policy as a result of environmental changes more frequently than mindless organizations.

One way that an organization is able to make these changes immediately is by exhibiting the final quality of mindful organizations: deference to expertise. This quality is exhibited by organizations that collapse the traditional hierarchical structure and allow decision making to flow to the persons in the organization with the requisite expertise to make the decision in question (Butler and Gray, 2006, Weick and Sutcliffe, 2001). The implication of this with regards to mindful IT security policy is that adjustments to the IT security policy are made in a timelier manner, by the persons that are most qualified. This eliminates the need for the persons responsible for amending the policy to work their requested changes up the corporate ladder and, thus, delaying their implementation and possibly opening the organization up to vulnerabilities in the IT security policy.

P7: Requested changes in the IT policies of mindful organizations are implemented in a timelier manner than in mindless organizations.

CONCLUSIONS

These seven propositions lay the groundwork for our future research in this area. The first step along this path will involve the evaluation of our propositions using survey research. In the book, *Managing the Unexpected*, Weick and Sutcliffe (2001) provide several tools for evaluating organizational mindfulness. . Since our propositions are founded on the individual tenets of organizational mindfulness, we will have to evaluate each of the propositions as it relates to the tenet from which it was derived. This is because an organization could have high levels of some characteristics of mindfulness and lower levels of others, thus making the overall construct insufficient to evaluate the individual propositions. Fortunately, instruments to assess each individual characteristic are included by Weick and Sutcliffe with the aforementioned tools. In addition to evaluating the propositions, we will also look to utilize expectation confirmation theory to examine the relationships between security policy and organizational mindfulness by assessing the expectations that are associated with the adoption of security standards and how those expectations affect the perceived performance of the standards and the level of disconfirmation. We hypothesize that organizations that are less mindful with their security policies will rely on standards and that those standards will influence the development of expectations that adherence to the standards will be enough to provide adequate protection, thus having a positive impact on the perceived performance of the standards. The level of mindfulness is also hypothesized to moderate the link between expectations and disconfirmation in that less mindful companies will simplify interpretations of events that could have a negative impact on disconfirmation.

Another interesting area is to consider the role of IT itself in the development of organizational mindfulness. Van de Walle and Turoff (2007) discuss the use of a group decision support system (GDSS) in the context of security response that was found to have an impact on the overall mindfulness of the organization that utilized it. Additionally, it would be interesting to see how other applications of IT artifacts and skills can enhance mindfulness when it comes to the detection of security vulnerabilities. One such application would be the utilization of computer forensics techniques and software to review web logs for possible threats. The security of information systems is a fertile ground for research and should continue to present us with many interesting questions to investigate.

REFERENCES

1. Barlette, Y., & Fomin, V. V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, 308-308.
2. Butler, B. S., & Gray, P. H. (2006). Reliability, Mindfulness, and Information Systems. *MIS Quarterly, 30*(2), 211–224.
3. Casper, C (2004). Complicated Compliance. Available at: http://searchcio.techtarget.com/news/article/0,289142,sid182_gci955397,00.html
4. Courtney, J. F. (2001). Decision making and knowledge management in inquiring organizations: toward a new decision-making paradigm for DSS. *Decision Support Systems, 31*(1), 17-38.
5. DeSanctis, G., & Poole, M. S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science, 5*(2), 121-147.
6. Guler, I., M. F. Guillen, and J. M. Macpherson. 2002. Global competition, Institutions, and the Diffusion of Organizational Practices: The International Spread of ISO 9000 Quality Certificates. *Administrative Science Quarterly* 47(2): 207-232.
7. Humphreys, T. (2006). State of the art information security management systems with ISO/IEC 27001:2005. *ISO Management Systems* (Jan-Feb): 15-18.
8. Johnson, E. (2006). Security Awareness: Switch to a Better Programme. *Network Security* (Feb):15-18.
9. International Organization for Standardization. (2001). TC176 on Quality Management and Quality Assurance. Available at: http://www.tc176.org.
10. International Organization for Standardization. (2008a). ISO Standards. Available at: http://www.iso.org/iso/iso_catalogue.htm.
11. International Organization for Standardization. (2008b). ISO/IEC JTC 1 Directives, section 2.1.3. Available at: http://isotc.iso.org/livelink/livelink.exe/fetch/2000/2489/186491/186605/Foreword.html?nodeid=5541785&vernum=0.
12. IsecT Ltd. (2008). ISO27001 Security. Available at: http://www.iso27001security.com/html/iso27000.html.
13. ITGI. (2005). *CobIT 4.0* (4.0 ed.). Rolling Meadows: IT Governance Institute.
14. Langer, E. J., & Moldoveanu, M. (2000). The Construct of Mindfulness. *Journal of Social Issues, 56*(1), 1-9.
15. Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly, 10*(1), 5-12.
16. Swanson, E. B., & Ramiller, N. C. (2004). Innovating mindfully with information technology. *MIS Quarterly, 28*(4), 553-583.
17. Weick, K. E. and Sutcliffe, K.M (2001) *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. Jossey-Bass.