available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security policy: An organizational-level process model

Kenneth J. Knapp[a,*], R. Franklin Morris, Jr.[b], Thomas E. Marshall[c], Terry Anthony Byrd[c]

[a]John H. Sykes College of Business, The University of Tampa, 401 W. Kennedy Blvd, Tampa, FL 33606-1490, USA
[b]School of Business Administration, The Citadel, Charleston, SC 29409, USA
[c]College of Business, Auburn University, Auburn, Alabama 36849, USA

ARTICLE INFO

Article history:
Received 11 October 2007
Received in revised form
8 July 2009
Accepted 10 July 2009

Keywords:
Information security policy
Governance
Policy development
Policy management
Policy process model

ABSTRACT

To protect information systems from increasing levels of cyber threats, organizations are compelled to institute security programs. Because information security policies are a necessary foundation of organizational security programs, there exists a need for scholarly contributions in this important area. Using a methodology involving qualitative techniques, we develop an information security policy process model based on responses from a sample of certified information security professionals. As the primary contribution of this research study, the proposed model illustrates a general yet comprehensive policy process in a distinctive form not found in existing professional standards or academic publications. This study's model goes beyond the models illustrated in the literature by depicting a larger organizational context that includes key external and internal influences that can materially impact organizational processes. The model that evolved from the data in this research reflects the recommended practices of our sample of certified professionals, thus providing a practical representation of an information security policy process for modern organizations. Before offering our concluding comments, we compare the results of the study with the literature in both theory and practice and also discuss limitations of the study. To the benefit of the practitioner and research communities alike, the model in this study offers a step forward, as well as an opportunity for making further advancements in the increasingly critical area of information security policy.

© 2009 Elsevier Ltd. All rights reserved.

1. Introduction

Organizations are more dependent than ever on the reliable operation of their information systems. Yet institutions worldwide face increasing security threats that can undermine the operation of these systems. Considering today's high-threat cyber environment, organizations need security controls to protect their valuable information. According to Hone and Eloff (2002, p. 402), ''Undoubtedly, the singularly most important of these controls is the information security policy''. Other researchers state that the development of an information security policy is the first step toward preparing an organization against attacks from internal and external sources (Whitman et al., 2001). Some even argue that managerial polices may be more effective at reducing computer security incidents than many electronic devices (Buss and Salerno, 1984).

Information security policy addresses the integrity, availability, and confidentiality of electronic data held within and transmitted between information systems and is the

* Corresponding author. Tel.: +1 813 253 3969.
E-mail address: kknapp@ut.edu (K.J. Knapp).

0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.07.001

precondition to implementing effective deterrents (Straub, 1990). Policies act as clear statements of management intent and demonstrate that employees should pay attention to information security (Wood, 1995). Without an approved policy document, overall guidance may be lacking and managerial support called into question. With security and privacy issues ranking among the top issues for IT executives (Luftman and Kempaiah, 2008; Luftman and McLean, 2004) and with legislation now requiring organizations to govern security policies (Volonino et al., 2004), organizations should be highly motivated to establish and maintain an effective information security policy process.

The primary focus of this study lies in the development of a practice-based organizational model describing a comprehensive security policy process. We could not find a similar model in the academic or practitioner literature. The proposed model reflects an information security policy process in modern organizations based on recommended practices from a sample of certified information security professionals. The model evolved from the data using qualitative techniques to identify the primary policy processes, key environmental and organizational influences, and the underlying linkages among them. Such a model promises to provide relevant guidance for practice and theoretical insight for research. The next section provides a literature background of our topic.

2. Information security policy literature background

A policy is a general rule that has been laid down in an organization to limit the discretion of subordinates (Simon, 1957). The phrase *business policy* describes the knowledge, skills, and attitudes constituting the general management of a total enterprise (Andrews, 1987). In some cases the term policy is interchanged with the term strategy while in other cases the term denotes a specific response to repetitive situations (Ansoff, 1965). Some suggest that well-defined policies do not necessarily lead to well-managed institutions and that good managers should delegate policy decisions to others. This does not imply that organizational policies are not necessary, but instead that policies should evolve over time from a mix of operating decisions (Wrapp, 1967).

In the domain of information systems, policy has been defined in a planning and control context to establish limits of acceptable behavior, decision confines, and standards (Davis and Olson, 1985). Policies are especially important to information systems security as they provide the blueprints for an overall security program and create a platform to implement secure practices in an organization (von Solms and von Solms, 2004b). The objective of policy is to provide management direction and support for information security in agreement with business requirements and relevant laws and regulations (ISO/IEC, 2005). While practitioner-oriented literature offers valuable guidance on how to develop and manage security policies (Bacik, 2008; Barman, 2002; Howard, 2003; ISF, 2005; Lowery, 2002; NIST, 1996; Peltier, 2002; SEI/CMU, 1997; Wood, 2002), there have been few scholarly studies using scientific methodologies that have specifically targeted this important area.

In our literature search for related policy studies, we found research that has (a) proposed a policy development model based on expert knowledge (Olnes, 1994), (b) offered a framework using a business objectives and gap analysis approach (Palmer et al., 2001), (c) illustrated an e-business security policy framework for software applications (Rees et al., 2003), and (d) explored the formulation of security policies in emerging organizations (Baskerville and Siponen, 2002). Our search identified additional studies in this research stream, including a published survey of UK-based senior IS executives finding that, while security policies are widely applied, there is little commonality in terms of their content and dissemination (Fulford and Doherty, 2003). Another article explored how sudden business opportunities may require temporary violations of predefined information security policies (Siponen and Iivari, 2006). A paper by Whitman (2008) described the development of information security policy by focusing on enterprise, issue-specific, and systems-specific policy levels in an organization. Finally, a study by Karyda et al. (2005) developed a contextual framework for the application of IS security policies. It is revealing that Karyda et al. (2005, p. 258) note in their study that ‘‘hardly any empirical accounts on the issues of implementing security policies exist’’. In fact, our literature search did not identify any empirical research using robust methodologies to illustrate the overall process of developing and managing information security policy within the organizational context.

The need for empirical research in this area provides a strong motivation for our research. Thus, the purpose of this article is to offer an exploratory study based primarily on qualitative techniques to describe an information security policy process model at the organizational level that is comprehensive and results in an enforceable information security policy. This study’s model goes beyond the models illustrated in the literature by depicting a larger organizational context that includes key external and internal influences that can materially impact organizational processes. Because many existing models often differ in their scope and intent (e.g. Hare, 2002; Olnes, 1994), the model of this study is noteworthy in its representation of a comprehensive framework based on recommended practices of a large sample of certified professionals. Thus, our model should be relevant to practitioners as well as open to comment and refinement by them. To this end, we provide a three-phase validation process to include: (a) an expert panel of practitioners, (b) on-location interviews with security managers at two technology-intensive organizations, and finally (c) a presentation at a well-regarded information security conference. During the three evaluation phases, participants offered independent assessments of the model based on its relevance, accuracy, and completeness.

The organization of the remainder of the paper is as follows. The next section reviews the methodology used to develop the model. The Methodology section is followed by the Results section, which also includes the evaluations of the model. Before presenting our conclusions, we discuss relationships with theory and practice, offer potential limitations, and highlight contributions of our study.

3. Research methodology

Our qualitative methodology was based largely on a grounded theory (Glaser and Strauss, 1967) approach involving a series of structured steps that include the systematic comparison of units of data and the gradual construction of categories that describe the observed phenomena. Thus, the description of the phenomena evolves directly from the data. After development of the model, we conducted a three-phase validation process that led to improvements to the model. The following sections offer details concerning the major methodological steps applied in this study.

3.1. *Data collection and model development*

In September 2003, an announcement was placed on the International Information Systems Security Certification Consortium [(ISC)^2] home page[1] requesting participation from Certified Information Systems Security Professionals (CISSP) interested in this research project. (ISC)^2 is a non-profit, ISO/IEC 17024[2] compliant organization that manages the CISSP program. Among the requirements to receive certification at the time of our study, candidates must (a) pass a rigorous exam, (b) possess a minimum of four years of professional experience in the field (or three years plus a college degree), (c) agree to a code of professional ethics, and (d) receive sponsorship from a member of the constituency. Once certified, a CISSP must earn professional development credits to maintain currency. As an incentive to volunteer in this project, (ISC)^2 offered professional development credits to each participating member. We selected the CISSP population for this study due to the comprehensive understanding of information security required to pass the CISSP exam. The exam covers the information security field across ten domains that address not only technical considerations but also managerial and organizational aspects of information security. Given the holistic understanding of the field required to pass the CISSP exam, we felt this population was ideal considering the goals of our study.

Based on the CISSPs who responded to the announcement, we sent 220 participants an open-ended question asking for the top five information security policy issues facing organizations today. We also asked participants to provide a short title and rationale for each of their five issues. This question had two primary objectives. The first objective was to gather information about the processes organizations use to develop, approve, implement, enforce, and review information security policy. The second objective was to collect information about the organizational issues that substantially influence policy development. We received 198 usable responses, complete with a short title and rationale for each of the five issues as requested.

After consolidation of the issues into logical categories that emerged from our analysis of the responses, a committee of two university faculty members and one (ISC)^2 board member reviewed the categories for clarity and accuracy resulting in minor changes. During this entire process, we sent multiple follow-on questions to individual participants as needed for the purposes of on-going clarification and feedback. In the end, we accumulated a database containing over 146,000 words of question responses suitable for the purposes of this study.

By asking respondents to identify and describe their top issues, we took as our starting point the concerns of the participants, which is a viable approach for studies that seek to describe phenomena directly from the data (Galal, 2001). In addition, we found that asking open-ended questions to a larger sample maximized the collection of a wide variety of issue-oriented practitioner viewpoints present in the data. This approach proved essential in developing a comprehensive process model rather than one more narrowly focused. Throughout this study, we oriented our evaluation towards addressing many of the practical issues raised by the participants from their organizational perspective. This is noteworthy because, if followed, it means that the resulting model offers practical guidance concerning the security policy process that can help organizations avoid the very problems that our sample identified in this study.

While the sample was homogeneous to the (ISC)^2 constituency, respondents came from over 25 countries and various industries. Appropriate for this study, consultants provided a valuable perspective since many work with companies representing multiple industries and organizations of various sizes. Overall, the research sample provided a broad and valuable cross-section of industry and employee viewpoints that would have been difficult to replicate using an on-site, case study approach. Table 1 presents a summary of key characteristics of the sample. Later in the paper, we discuss the limitations of the methodology employed.

As a part of our methodology, we used a form of content analysis in which we categorized the data into concepts that originate from the data rather than from an outside source. Specifically, respondents' short-titles of each issue along with a frequency analysis of key words and phrases contained in the respondents' descriptions of the issues were the first steps in synthesizing the key categories from the data. Table 2 contains a partial listing of our quantitative results that aided the identification of the *policy review* and *senior management support* categories, which we offer here as an example.

Glaser and Strauss (1967) argued that preconceiving research projects could limit the possibilities that the end result will emerge strictly from the data. Therefore, the authors made a conscious decision and an on-going effort to not predefine or assume *a priori* any of the categories that might be found in the data. Following this approach, the first two authors developed categories independently of each other. Through an analysis process of (a) interplay between the researchers and the data (Strauss and Corbin, 1998, p. 13), (b) clarification with respondents as necessary, and (c) reconciliation of any differences between the first two authors, an eventual list of logical categories emerged. These categories describe the conditions, events, experiences, and consequences associated with developing and managing information security policies.

For example, one respondent stated, "*An information security policy document should be reviewed at least quarterly to ensure*

[1] (ISC)^2 and CISSP are registered trademarks. See www.isc2.org.

[2] The International Standards Organization/The International Electrotechnical Commission, (ISO/IEC) 17024 provides general requirements for bodies operating certification of persons.

Table 1 – Summary of sample demographics.

Respondents:	220 certified information system security professionals (CISSPs)
Country:	- United States (72%) - Canada (5%) - India (4%) - Hong Kong (3%) - United Kingdom (3%) - New Zealand (2%) - 22 other countries represented (France, Japan, Mexico, etc.; less than 2% from each country)
Industry:	- Government (21%) - Consulting (15%) - Banking & finance (15%) - Information technology (12%) - Manufacturing (11%) - Telecommunication (8%) - Healthcare (7%) - Energy (4%) - Retail (3%) - Education (3%) - Others (1%)
Job position:	- Top management & business owners (11%) - Middle management (34%) - Professional/administrative (32%) - Other management (23%)
Information Sources[a]:	- Information Security magazine - SANS Institute - Security Focus - SC Magazine - CERT web site - CSO magazine

[a] Participants named their two primary sources of security information, whether electronic or print based. Lists of top six sources identified.

that it is still relevant and adding value to the business in appropriate areas''. As we applied our methodology, this statement stood out during the categorization process considering the phrase 'information security policy document' and the word 'reviewed'. We assessed this statement as evidence supporting the *policy review* category as it expressed the importance of a regular organizational process of reviewing a policy for continued relevance. In another case a respondent stated, ''*…without top management support and involvement, the creation, training and enforcement of the organization's security policies would not occur…*'' This statement helped justify the creation of the category we titled *senior management support* because the statement highlighted the critical role of senior leadership regarding overall policy management.

As we further developed the categories, it became evident that most fell into two general divisions: (1) those categories directly involved with policy development and management, and (2) those representing influences, either internal or external to an organization that can affect the policy management process. We classified information security governance as an overarching category since it did not neatly fit into either general category. This classification scheme allowed us to describe from the data the policy management categories as well as the overall organizational environment. After a number of iterations and reexaminations of the data, the framework of the information security policy model evolved as shown in Table 3.

The essential organization of the model is that of a cyclical but evolutionary sequence of steps. In some cases, identifying the sequence and relationship of the categories was straightforward. For example, since it is ideally desirable to first gain approval for a policy before it is implemented, the category *policy approval* is a clear logical antecedent to the category *policy implementation*. Other relationships were not inferred by logical sequence, but required studying the data and clarifying with respondents in a search for key words that conveyed cues of sequence among the categories. For instance, we classified *audits* and *automated tools* as subcategories of *monitoring* based on respondent statements such as the following: ''*Once the policies are in place, you need the continued backing of management as well as the ability to know when policy has been violated. For tools, we need auditing and real-time monitoring products…*'' This rich statement emphasized not only the value of obtaining management support but also the value of audits and automated tools in helping to monitor and identify when

Table 2 – Frequency counts of key words or phrases.

Key word or phrase (selected examples)	Individual count	Category subtotal	Potential category for related grouping
Update	111		Review
Review	110		Review
Maintenance	28		Review
Policy review	9		Review
Policy update	8		Review
Policy maintenance	7	**273**	Review
Senior management	45		Sr mgt support
Management support	31		Sr mgt support
Executive support	30		Sr mgt support
Top management	27		Sr mgt support
Top management support	5		Sr mgt support
Management backing	5		Sr mgt support
Executive support	3		Sr mgt support
Senior management support	2	**148**	Sr mgt support

Table 3 – Information security policy categories by classification.

Classification	Category
I. Broad Categories	1. Information Security Governance 2. Organization Information Security Office[a]
II. Policy Management Phases	1. Risk Assessment 2. Policy Development 3. Policy Approval 4. Policy Awareness & Training 5. Policy Implementation 6. Monitoring (Audits & Automated Tools) 7. Policy Enforcement 8. Policy Review 9. Policy Retirement[a]
III. External Influences	1. Economic Sector 2. Technology Advances 3. Industry Standards 4. Legal & Regulatory Requirements 5. External Threats
IV. Internal Influences	1. Senior Management Support 2. Business Objectives 3. Organization Culture 4. Technology Architecture 5. Internal Threats

[a] Category was added during the evaluation phase.

employees may be violating security policy. Overall, we liken this process in our study to that of assembling a jigsaw puzzle that begins to take shape as each piece of the puzzle finds its place. Eventually, as we placed each piece in its appropriate position, the overall pattern became discernable.

In summary, the categories and sequences evolved directly from the wealth of participant responses (i.e., the data). In fact, for this study, these responses provided the primary source and means for developing the model's categories and sequences. This rich set of responses contains detailed descriptions of the issues and concerns involved with information security policy in organizations. While it is impractical to include the complete set of data with this article, the Appendix offers a sample of participant statements for each variable in the model. Readers can benefit from examining the Appendix to gain insight into some of the issues identified by our sample of security professionals. Such insights can increase understanding of the model and deepen appreciation for how it can help organizations avoid these same types of problems when developing and managing information security policy.

3.2. *Model evaluation*

A way to judge if our developed model is an accurate account is to determine whether practitioners look upon it favorably. Since the model reflects a practice-based view of an information security policy process, the model should be relevant, accurate, and enlightening to practitioners who have familiarity with policy management. Accordingly, we subjected the proposed model to three rounds of scrutiny. In the first round, an expert panel of ten CISSPs who had not previously participated in the study, independently reviewed and critically assessed the model. We solicited the members to be part of this panel based on the high quality and insightful answers they gave in a previous but unrelated research project. In the second round, we conducted interviews with an information security manager at two technology-intensive organizations. Each interview was on-site, face-to-face, and lasted two hours. The first individual interviewed had multiple professional certifications including a CISSP and was the lead security engineer on a large software development project working for a Fortune 100 company. The second individual did not have professional certifications at the time and was the top information assurance officer for a federal government organization. Both organizations are located in the western United States and have between 5000 and 10,000 employees located at the interview site. The first author digitally recorded the interviews with permission and discussed every aspect of the model with each interviewee seeking opportunities for model refinement and clarification. Both managers had ample time to study the model prior to questioning. Open-ended and specific questions were asked. Each interview concluded with the following questions: *What is your overall impression of the given model? Would you add or change anything to the model? Do you have any suggestions for improvement?* Finally, in the third round, we presented the full model at a well-regarded information security conference (Knapp, 2007). The project background, research methodology and model were presented to over 200 attendees during a 60-min session. In addition to a 30-min question and answer period during the session, each attendee was given the author's email address to provide an opportunity to forward commentary on the model.

This three-round evaluation process resulted in changes and refinements to the model. Most of the suggestions were minor to include variations in the wording of the titles that describe the management processes and environmental influences in the model. Based upon these suggestions, we adjusted several titles to improve clarity and understanding (e.g. *Policy Awareness* became *Policy Awareness & Training*). The most significant improvements emerged from the on-site interviews. First, we added the *organization information security office* as the construct underlying the policy management phases listed in Table 3. The rationale was initially based on the first interviewee's argument that the information security professional should have a place in the model that clearly illustrates the important role they provide in policy management. In many ways, the information security professional facilitates and is most responsible for the success or failure of the overall process. Second, we added the iteration arrows for three of the policy management phases that exhibited a more ongoing nature rather than a sequential one. From the conference, we added the one-way arrow between risk assessment and policy development to retirement based on a suggestion from an attendee during the presentation. Most significantly, all improvements to the model were consistent with the data collected earlier in the project.

Additionally, the first interviewee stated that the model would be useful in a training environment for new information security employees and added that, "the security concerns that surfaced within your study truly represent the civilian, Federal, and Department of Defense security communities''. The feedback from the security conference as well as the follow-on e-mail correspondence with over thirty of the session attendees was overwhelmingly favorable. For instance, a sample correspondence stated, ''I've distributed (the presentation slides) to my team. We'll be using your chart as a guideline. I must say that the problems described and solutions offered were nearly an exact match for what's going on in my company''.

Overall, the three evaluation rounds provided favorable reviews of the model. We would not say that we experienced dissenting, conflicting or negative views among the various evaluators. Instead, we received positive and neutral statements about the model. In doing so, the evaluators expressed and emphasized different dimensions and aspects of the model based on each person's experiences and expertise. We captured a representative cross-sample of evaluation statements in Table 4, which provides six responses from the ten-member expert panel.

4. Results

We now unpack the model in two steps. The first step, as shown in Fig. 1, depicts the policy model as a repeatable organizational process. The figure shows the general flow and major interactions among the categories (i.e., processes). The second step, as shown in Fig. 2, illustrates the complete model with the ten internal and external influences as well as the broad categories of *Information Security Governance* and the *Organization Information Security Office*. The complete model in Fig. 2 shows each of the identified categories grouped according to the general classifications represented in Table 3.

While the respondent statements provided in the Appendix offer guidance concerning many aspects of the model, we now provide additional comments explaining the flow of activities illustrated in Fig. 1. The double arrows between four of the policy management processes (i.e., *policy review*, *risk assessment*, *policy development*, and *policy approval*) represent the frequent interplay and iteration among these activities that occur in organizations. For example, if an authority disapproves a proposed policy, the developers may have to rewrite or review a policy based on the feedback from the approval authority. The single arrows illustrate the general sequential flow from the *policy approval* to the *policy review* phase. Still, this general sequence does not imply a rigid linear progression, as some phases have concurrent dimensions. The dotted line to *policy retirement* reflects that sometimes during *policy review*, *risk assessment*, and *policy development*, an organization may decide that certain policies are no longer needed and thus should be retired. In the *monitoring* phase, the dotted lines lead to two key subcategories (*audits* and *automated tools*). For example, respondents often mentioned the helpfulness of using automated tools to assist in the tedious job of monitoring employees. The semicircular, iteration arrows represent phases that have a vital, ongoing dimension. Such is the case with the *policy awareness and training* phase. While substantial awareness and training should follow the formal approval of many policies, study respondents emphasized the necessity of reoccurring training events to remind employees about important policies. Overall, our model illustrates iteration of individual processes (e.g. *policy awareness and training*), iteration of portions of the model (among *policy review*, *risk assessment*, *policy development*, and *policy approval*) and iteration of the processes of the complete cyclical model.

Table 4 – Sample responses from the expert panel.

- ''[The model] seems to sum up the very essence of knowledge needed to run a strong info-sec organization. Our organization struggles with many of the issues and reading this was like a cliffnotes version of both the things that we struggle with and things that we have some strength in''.
- ''It's concise but will require that the uninitiated reader study it for a few minutes before the principals you put forth come through to such a person''.
- ''I have seen these [the model] depicted in various charts, flows, swim lanes, wheels and graphics over the years…you don't seem to be treating this process flow any differently. You have the appropriate steps in the process and have depicted them in a sensible graphic flow''.
- ''I think that your most critical point about senior management support is displayed first [in the list of internal influences]…as it should be, and all other evidence is very valid and critical to operating a security organization''.
- ''You have identified many areas in policy development that urgently need improvement. The model is concise, yet thorough enough to convey the inherent complexity of the process''.
- ''The model is a good one. If an organization uses the model, they will find value and be successful''.

We illustrate the complete organizational model in Fig. 2. *Information security governance* is an overarching category directly affecting the entire policy management process; doing so also stresses that governance is not merely an internal organizational process but can consist of external attributes such as the involvement of a board of directors. The *organization information security office* is depicted as a category supporting the policy management phases. We depict the internal and external influences as general influences on the entire policy management process because, according to our respondents, the influences tend to impact each category in varying ways. For instance, while the external influence of *legal and regulatory requirements* will affect the content of an organization's security policies (e.g. Sarbanes-Oxley Act of 2002), legal requirements also can restrict how companies engage in employee monitoring and surveillance (George, 1996). Finally, double arrows illustrate the two-way interaction between the policy management processes and the internal and external influences. For example, developed policies can address vulnerabilities in an organization's network *technology architecture*. Once approved, such policies will shape network equipment purchases, which in turn can change the architecture. Once operational, the modified architecture can influence future risk assessments and policy developments. In addition, best and worst practices of a single organization can affect the external environment. The Enron scandal demonstrates how problems in one organization's processes can affect the general legal environment. The scandal helped inspire legislators to create the Sarbanes-Oxley Act, which in turn affected a myriad of organizations in the U.S. (Moulton and Coles, 2003).

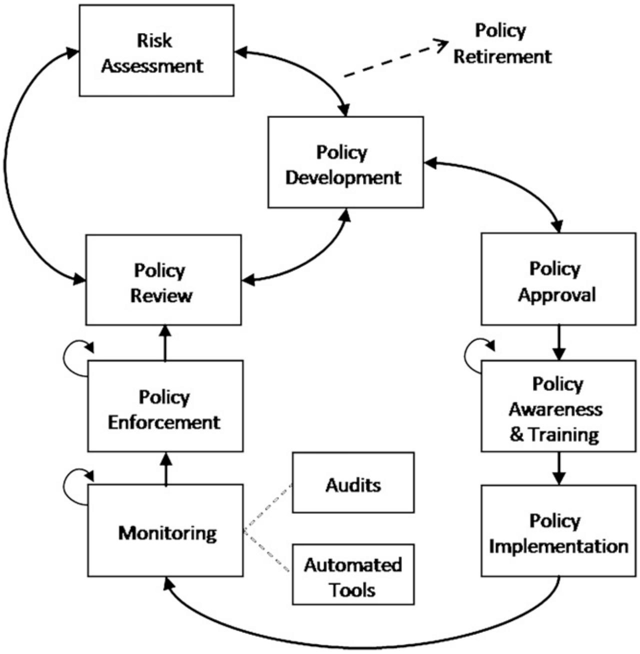

Fig. 1 – Information security policy as a repeatable organizational process.

5. Relationships with theory and practice

In this section, we further discuss this study's resulting model, as illustrated in Fig. 2, and compare it with existing theory and common practice found in both the academic and practitioner literature. While many aspects of this study's model have ties to the literature, here we highlight five of the model's most salient and relevant aspects that are supported in the literature. These five include the emphasis on training and awareness, the necessity of policy enforcement, the cyclical nature of policy management, the role of corporate governance, and the effect of the internal and external influences on the policy process.

5.1. *Emphasis on training and awareness*

Simon (1957) classifies training as a mechanism of organizational influence. Organizations train and indoctrinate its members to internalize knowledge and skill that enables the worker to make decisions consistent with organization objectives. Applied to security, the topic of training is intertwined with awareness. An organizational awareness program is often the initial phase of a broader security training program. Awareness alerts employees to the issues of information security (Straub and Welke, 1998) and prepares users to receive the basic concepts of security through a formal training program. Security awareness helps reinforce training materials through cyclical and ongoing security reminders and events (Hansche, 2002). Training and awareness programs can be used to influence the culture of an organization (Schein, 1995) by promoting favorable security practices and mindsets.

One of the basic steps in coping with information security risk is the establishment of a training awareness program. Organization's are urged to train employees about security threats and to encourage employees to support organizational policy in the course of their daily work (ISO/IEC, 2000). The

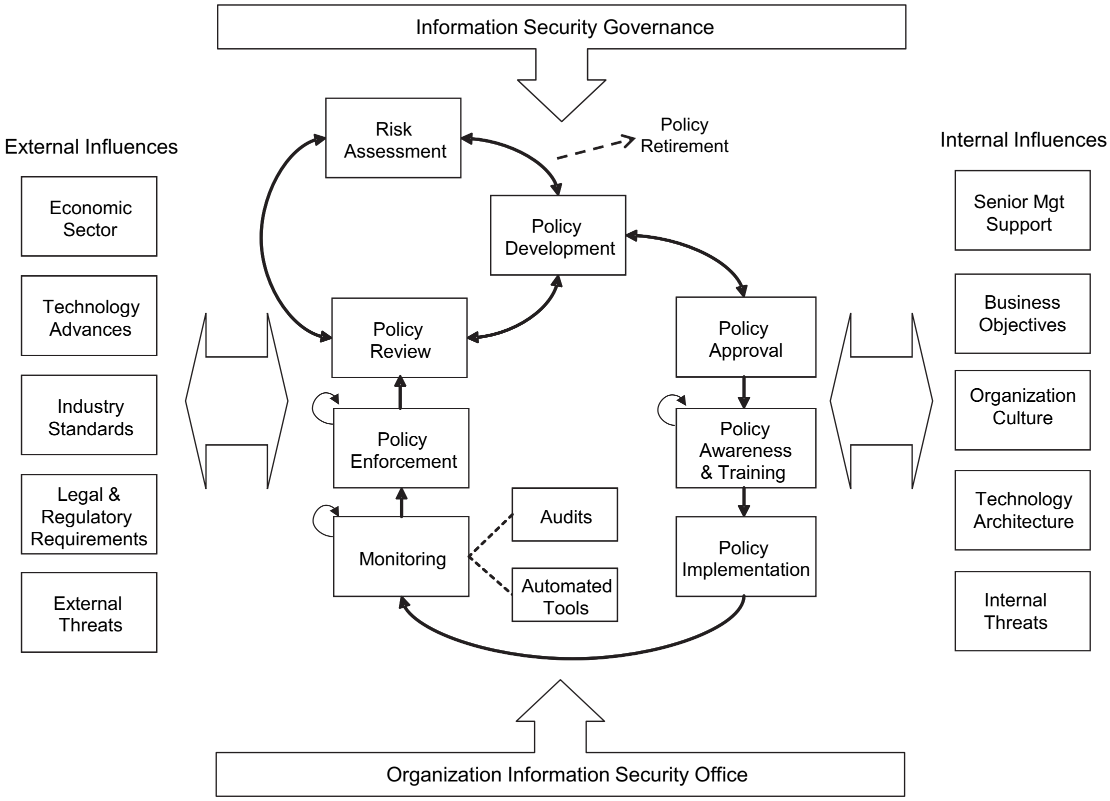

Fig. 2 – Comprehensive information security policy process model.

model developed in this study illustrates the process of *policy awareness & training* immediately following *policy approval*. However, awareness and training is consistently described by the respondents of this study as an ongoing process. This point is emphasized in the model of this study by including a semicircular arrow in the upper left corner of the process. Barman (2002, p. 32) makes it clear that the significance of this function is paramount: ''The importance of security awareness training and education cannot be overstated. By taking the policy seriously and teaching all of the stakeholders about their role in maintaining it, they will embrace the policy as an integral part of their jobs''. Whitman (2008, p. 140) agrees by stating, ''Of extreme importance in the process of implementing information security policy is the need to keep the policies fresh in employees' minds .... Employee awareness is recognized as one of the greatest challenges in implementing security in general''. Others in the literature take a broader view of awareness that addresses user behavior, of which training is one part of improving overall user conduct. Additional factors can influence user security behavior including the perception of senior management commitment and a user's personal values and standards of conduct (Leach, 2003).

5.2. *Necessity of policy enforcement*

As one respondent stated, ''*A policy may become a 'paper tiger' with no 'teeth' if there is no enforcement*''. In our model, policy enforcement is an on-going activity affording the opportunity for management to put the ''teeth'' into formal policies. If, for example, an employee is caught knowingly violating a policy, managerial-directed corrective action can occur. The literature emphasizes the importance of enforcement: ''Policy must be enforced to make it effective'' (David, 2002); without enforcement, a policy might as well not exist. The criminology theory of general deterrence emphasizes policing as a means of warding off potential abusive acts primarily through the fear of sanctions and unpleasant consequences (Parker, 1981). But while a negative deterrent may help encourage proper security behavior in accordance with policies, Leach (2003) points out that the opposite approach, one that rewards good security can also be an effective means of enforcing policy. Thus, effective policy enforcement can emphasize both negative consequences for poor security behavior and positive reinforcement through rewards to encourage good security behavior. Overall, the model developed in this study is consistent with the literature through its inclusion of the important aspects of policy awareness and training along with policy monitoring and enforcement. The inclusion of these aspects is especially critical as an example of how the model can help guide organizations to more effective security policy management since the behavior of individuals has been repeatedly identified as one of the primary reasons that policies fail. As Leach (2003, p. 686) states, ''Poor or unacceptable user behavior is a significant, perhaps even major, determinant of the level of security incidents suffered by a company''.

5.3. *Cyclical nature of policy management*

Process theory explains phenomena in terms of a sequence of events leading to an outcome. Understanding patterns in events is thus critical to developing a process theory. Using this process approach, the security model illustrated in Fig. 2 may be viewed as a series of phases that, taken together, transform inputs into an output (Garvin, 1998). The central structure of such a model is that of a sequence of steps, each with intermediate outcomes that influence the final outcome, but do not determine it. This is not unlike a common representation in the literature of security policy development illustrated as a circular process starting with phases such as policy evaluation followed by development, approval, publication, implementation and maintenance (e.g. Hare, 2002; Lowery, 2002). The cyclical nature of the model developed in this study highlights the ongoing need to execute some processes on a reoccurring and even frequent basis. For example, this study's model emphasizes the possibility of a continuous cycle among the phases of policy review, risk assessment and policy development. The model also illustrates individual processes, such as monitoring, that have an ongoing or continuous characteristic. In addition, even the entire model with all of its phases can be seen as having an overall cyclical nature. Thus, the model developed in this study is consistent with the cyclical approach that is represented in numerous models in the literature. It is worth noting that other helpful approaches for describing security processes also exist in the literature. Two examples include Olnes (1994), who illustrates a decision tree approach to policy development, and Barman (2002), who provides textual descriptions of policy development with specific examples of actual policies.

5.4. *Role of corporate governance*

Information Technology governance can be defined as representing the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT (Weill, 2004). One respondent in our study felt that information security itself must be viewed as a governance issue stating, ''*Information security is often treated as a technology issue, when it really should be treated as a governance issue*''. Others have suggested that failing to realize that information security is a corporate governance responsibility is the number one 'deadly sin' of information security management (von Solms and von Solms, 2004a). Recent legislation, such as Sarbanes-Oxley in the U.S., has substantially strengthened the link between information security and governance. Newer regulations as well as increasing organizational dependence on IT are forcing information security issues to the level of the corporate board. (Moulton and Coles, 2003; Nolan and McFarlan, 2005; Volonino et al., 2004). Information security has too often been treated as primarily a technical issue rather than an enterprise-wide priority. Today, however, information security needs to be governed by not just senior management but also by the corporate board who should integrate security into the overall IT governance framework (Damianides, 2005). Relating to policy, Warkentin and Johnson (2008) suggest that governance is the means of ensuring that policies and procedures are put into practice in an organization. Thus, the emergence of governance as a critical and overarching category in the policy model is consistent with the literature. As reflected in the model, this insight suggests that a failure to establish adequate governance prior to developing security policies will likely lead to a less effective process, resulting in diminished organizational security.

5.5. *Affect of the external and internal influences*

In addition to the processes such as *policy development* that directly shape, sustain and modify an organization's information security policies, a number of important factors exist that are either external or internal to an organization, yet have the potential to significantly influence an organization's information security policies. The model that evolved in this study depicts five external and five internal influences as illustrated in Fig. 2. In general, an *influence* serves to determine or shape the development and management of policies in an organization. External influences are considered to emanate in the environment outside an organization's boundaries whereas internal influences are considered to reside within an organization's boundaries. In this subsection, we briefly discuss the five external and five internal influences as illustrated in the model.

Over the past decade, numerous industry standards and guidelines have emerged worldwide. While this study's respondents mentioned a variety of available standards and guides affecting information security, the most frequently mentioned was ISO/IEC 17799.[3] This prominent international standard provides both an authoritative statement on information security management as well as procedures to be adopted by organizations to ensure information security (Backhouse et al., 2006). Because such industry standards and guidelines offer recommendations and best practices to help organizations develop policies and implement effective security programs, *industry standards* emerged as one of the five external influences in the model. Three remaining external influences include (1) the *economic sector*, which is important due to the fact that some sectors (e.g. healthcare, finance) have distinctive or specialized security considerations that organizations must not overlook; (2) *technology advances*, which refers to society's inexhaustible drive toward technological progression and change; and (3) *legal and regulatory requirements*, which concerns the growing levels of governmental interest and control in matters affecting information security (e.g. HIPAA).

One of the multifaceted influences with both external and internal dimensions relates to security *threats*. A threat is an indication of an impending undesirable event that may inflict injury or damage to a company's resources (Parker, 1981). A taxonomy offered by Loch et al. (1992) organizes information threats in a manner consistent with this study by categorizing threats as external or internal to an organization. This taxonomy classifies hackers and natural disasters as examples of external threats, while employee error and a facility mechanical failure are examples of internal threats. Recognizing the variety of threats facing an organization, Barman (2002) states, "the only way to understand your infrastructure is to perform a full risk assessment … on the entire enterprise", and then ensure that information security policies appropriately address diverse threats. The words of one respondent emphasized the need to account for all threats: "*Because of the changing nature of the Internet, the security threats faced by an organization also change, leading to updates to security policies. As such, an organization is required to … ensure (that) security policies address all security issues faced by an organization*".

Three remaining internal influences include (1) *senior management support*, which may be described as the degree to which top executives support security priorities; (2) *business objectives*, which pertain to the business or financial goals of an organization; and (3) *technology architecture*, which refers to the existing technologies and architectures currently operating in an organization that suffer from vulnerabilities requiring mitigation. Each of these three internal influences can affect the scope of policies as well as the amount of managerial support and resources available to develop and implement information security policies in an organization. For example, in the case of *business objectives*, security policies should not be overly restrictive or burdensome to the extent that they are inconsistent with the business goals of the organization. The fifth and final internal influence in the model is *organizational culture*. Organizational culture has been defined as the basic assumptions and beliefs (1) that are shared by organizational members, and (2) that have worked well enough to be considered valid and to be taught to new members (Schein, 1996). Considering that information security is, in general, a management problem, then the security culture of an organization will reflect how management handles and treats security problems. Consistent with the literature, organizational culture is a factor that influences security policy development (Ruighaver et al., 2007) because an organization's culture will significantly determine the overall employee attitude about security. For example, if an organization's culture breeds hostility toward a security policy that employees perceive to be unreasonable, the security staff may find it challenging to achieve compliance of the particular policy.

In this subsection, we have briefly described the five external and five internal influences depicted in this study's model. We encourage readers to review the Appendix for additional respondent statements regarding each of the ten influences in the model.

6. Limitations

Like all research, this study is not without limitations. One limitation regards the sample chosen for the study. The model was developed exclusively using responses to questions given to professionals certified by $(ISC)^2$. This constituency tends to support workers in government, finance, and information technology as well as consultants whose clients come from such organizations. Concerns from participants in these demographics may have biased the model in favor of organizations that typically hire $(ISC)^2$ certified professionals. For instance, only 3% of respondents came from the retail sector. In this case, the external influence of legal and regulatory requirements will likely influence organizations in the healthcare and financial industries more than those organizations in the retail sector due to the focus of legislation on the former. Thus, some of the identified external influences could affect some organizations more than other organizations.

[3] ISO/IEC 11799 was renumbered as ISO/IEC 27002 in 2007. At the time of the data collection phase of the project, ISO 11799 was considered current. See www.iso.org.

Cross-cultural differences may affect the way organizations go about policy management. Research has shown that certain management practices can be compatible and others incompatible depending on the culture of a society (Hofstede, 1993). For example, highly individualistic societies may accomplish policy development differently than more collectivistic societies. While a significant cultural difference in the sample responses was not detected, the extensive CISSP certification requirements and the global nature of modern Internet security threats may have acted to minimize many cultural differences (Yang, 1986). In a related area, language did not present a difficulty in the frequency analysis or other aspects of the methodology. All study participants responded in English and were able to communicate effectively concerning terminology, composition, clarity, etc. The proliferation of IT certification bodies with rigorous entrance requirements and their role in minimizing differences in culture and language is a potential question for future research.

Furthermore, the proposed process model represents a generalized framework rather than a specific model for a single company. That is, not all aspects of the model will apply equally or in the same manner to all organizations. Consider organizational size as one dimension where this may be the case. Many of this study's participants came from larger organizations that are likely to have an established information security office. Smaller organizations with only one or two workers who regard their security responsibilities as an additional duty may not have such an established office as depicted in the model. Therefore, the inclusion of an information security office in the overall security policy process may not be reflective of smaller organizations. Other aspects of the model such as *legal requirements* can also vary depending on the particulars of the organization, industry, regulatory climate, and country. Thus, we recommend that applications of the model in organization-specific settings (e.g. consulting, case studies) take into account important dimensions such as national culture, regulatory climate, and organizational size. Yet, such organization-specific variance should not affect the general applicability of the model.

Furthermore, our model does not attempt to address exceptional situations that may warrant a temporary violation of predefined policies. For example, in turbulent organizational environments it may be prudent to temporarily suspend rigid policies to take advantage of unanticipated business opportunities (Siponen and Iivari, 2006). Even so, we suggest that our general model can serve as a valuable resource for organizations looking for guidance in developing and improving their security policy processes. The need for such guidance is clearly evidenced by the fact that some organizations don't have any formal IS security policies in place (Whitman et al., 2001) while others have deficient policies with, as one participant stated, ''*inconsistent formats, inappropriate scope, incomplete structure and coverage of subjects, ambiguous wording, and weak coupling between risk and intent*''.

7. Contributions to practice and research

A major contribution of this research is that the study used scholarly techniques and methodologies that allowed the data to guide the model development. This is significant because the model that evolved from the data in this research reflects the recommended practices of our sample of certified professionals, thus providing a practical representation of an information security policy process for modern organizations. This data-centered approach to model development also led to a primary contribution of this research study: a more inclusive model that illustrates a general, yet comprehensive policy process in a distinctive form not found in existing professional standards or academic publications. Another key contribution of this research is that the model goes beyond other models illustrated in the literature by depicting a larger organizational context that includes key external and internal influences that can materially influence organizational processes. Specifically for practitioners, the model provides an illustrative framework that can guide the management of information security policy in organizations. Most importantly, the model should greatly aid practitioners in improving or establishing a policy management program in their organization and as a training resource to teach about security policy development and management. Practitioners can use the model to develop and analyze their current policy programs from a holistic or systems viewpoint that takes into consideration the overall flow, interacting phases, as well as internal and external influences as important factors in the policy process. For researchers, given the scientific approach of the study and considering that it's one of the first to apply such methodologies to the development of a holistic policy process model, this study can serve as a basis for other research projects concerning information security policy. This study may prove particularly helpful to research focused on the question of how internal and external organizational influences can affect policy process.

8. Conclusion

This paper presented the findings of an exploratory study that developed an information security policy process model for organizations. The model generated in our study suggests that a security governance program together with the organization's information security office, an ongoing process of interrelated policy management activities, and the proper gauging of key external and internal influences together contribute greatly to the success of an organization's information security policies. This model provides unique value through its comprehensive, real-world representation of an information security policy process in modern organizations. The final model evolved through a data-centered approach that lead to identifying the primary policy processes, the key environmental and organization influences, and the important linkages among them. The data used in the development of the model is rooted in the broad-based experiences of those who have been most active in developing and implementing organizational information security policies. Thus, this unique and comprehensive model provides a more complete, practice-based framework that informs organizations and researchers concerning the interactions of key processes and influences that form an effective information security policy process.

Appendix.

Examples of respondent statements gathered during original data collection are presented in this Appendix. Examples are provided for the nine policy management categories, the information security office and governance categories, as well as the ten external and internal influences. These examples employ underlining to identify words and phrases that were key in categorizing the statements and in developing the overall model. We placed these statements in their most appropriate category given that some responses provided evidence of more than a single category. Readers are encouraged to review these statements to gain a fuller appreciation of the model illustrated in Fig. 2.

Examples of respondent statements for each category.

Policy management phase	Example respondent statements
Information Security Governance (overarching category)	• "Especially in larger organizations, there may be separate policies within distinct branches or divisions. A formal process needs to be in place to ensure there is standardization and consolidation of policies to ensure governance of info sec is uniform across the enterprise". • "Strong and effective governance is required when it is necessary to consolidate policies, especially when certain departments are entrenched in following their own respective policies". • "The determination of responsibility and authority must be clearly established before security policies and the enforcement of those policies can occur. Employees need to know that someone has the authority to make and enforce the rules. Without [governance] the organization is simply not secure".
Organization Information Security Office (supporting category)	• "Deployment of new applications or network changes that are not reviewed by the security group can lead to vulnerabilities in the organization's security infrastructure". • "There is little threat of retribution (of a security violation) unless a VERY serious breach is discovered, and then only if the information security group escalates the issue". • "Policy is not effective without an active … program to monitor and enforce compliance. This is by far the most labor intensive part of an information security program. Typically, the security organization is small compared to the total number of IT and network personnel".
Risk Assessment	• "Economically responsible security should only address the threats and risks that an organization can reasonably be expected to encounter". • "Part of consensus building is defining what a policy will cover that is actually pertinent to the organization as opposed to implementing security for security's sake. Just because it may be best practice and good security to implement certain controls does not mean it is meaningful to a given organization. Consequently, risk analysis and vulnerability assessment MUST precede policy development". • "In order to implement a successful security policy, a risk assessment which quantifies and evaluates business risk should be done first. It's essential to know what is protected and how much it's worth before deciding how to protect it. Otherwise unsuccessful policies which cost millions of dollars are implemented".
Policy Development	• "Laying the groundwork for new policy is a very involved and highly iterative process that must include representatives and/or input from all of the stakeholders. Many are affected by the final outcome, so even though senior management drives policy, many others must provide valuable input in order to shape the policy documents accordingly". • "It is a mistake to hire consultants to develop the policy document, then see the organization fumble the ball when it tries to implement the policy by itself".

(continued on next page)

Appendix (*continued*)

Policy management phase	Example respondent statements
Policy Approval	• ‘‘Most companies do not have an established process for policy development and approval since it is often viewed as a one-time-effort’’. • ‘‘Approvals often require the ISO/CISO to work with Legal, HR and a multitude of departments to achieve some consensus. Also, as policies work through these areas, they are often ‘watered down’ to least common denominators further weakening the end result. Lack of process also allows other groups to develop a policy, even though it may be outside their scope of expertise’’. • ‘‘A clearly defined course of action for approval can expedite the process and result in stronger policies that are enforceable’’.
Policy Awareness & Training	• ‘‘It is important that all the stakeholders understand not just the policy, but also the rationale behind the policy and the risks of non-compliance’’. • ‘‘If the employees do not know that a security policy exists and how it fits into the organization, chances are enforcement will be unsuccessful or even non-existent. It’s easy to get focused on technology as the silver bullet and overlook the fact that people ultimately make or break an organization’s security efforts’’. • ‘‘Regular end-user security awareness trainings must follow security policy development’’.
Policy Implementation	• ‘‘Management can often agree to adopt certain information security policies only to change their minds when the reality of implementation hits them’’. • ‘‘The team responsible for developing the policy should also be made responsible to implement the policy’’.
Monitoring	• ‘‘Without the monitoring of logs, transactions, etc. it is impossible to see if any policy breaches are taking place unless a highly visible, public event occurs, such as a virus outbreak’’. • ‘‘Without some type of monitoring in place, it is almost impossible to determine if employees are following policy’’. • ‘‘Because so much of policy enforcement [depends on] monitoring and reporting, policies are not effective if employees feel the (y) … are not being monitored’’. • ‘‘Regular audits against your IS Policy are very important. This enforces accountability for each department within your organization to follow the Corporate IS Policy’’. • ‘‘There are lack of tools and resources to monitor the compliance of security policy, standards & ‘guidelines’’’.
Policy Enforcement	• ‘‘A policy may become a ‘paper tiger’ with no ‘teeth’ if there is no enforcement. The enforcement standards need to be formalized, standardized, and written into the policies for the policy communication and rollout. Therefore, the repercussions and consequences of policy violation are understood by all parties upfront and can be objectively applied in a regulated and fair manner. For example, the risk of facing unlawful dismissal is minimized with a documented and employee acknowledged ‘3 strikes and you’re out’ policy for inappropriate internet usage’’.
Policy Review	• ‘‘An information security policy document should be reviewed at least quarterly to ensure that it’s still relevant and adding value to the business in appropriate areas. If it’s found that a policy is no longer adding value – then it should be modified or scrapped’’. • ‘‘There appears to be a common belief that with the exception of virus protection, a security policy is put in place one time and does not require maintenance, updating, monitoring, or revisiting the policy to make adjustments’’.
Policy Retirement	• ‘‘As an organization’s business model changes and technology requirements change, policies need to be reviewed for their relevancy, and modified or retired where appropriate’’.

Appendix (*continued*)

Influential factors (external & internal)	Example respondent statements
Economic Sector	• "Organizations … should engage a reputable information security company with specific industry domain knowledge to assist in developing the information security policy". • "In finance and health industries, compliance to regulations is mandatory and companies need to ensure that there is formal compliance auditing and policy enforcement".
Technology Advances	• "Chances are if you haven't updated your Information Security Policy in a while you are probably missing the boat on major technological advances. Wireless PDAs, Internet ready cell phones and wirelessly enabled laptops…were not around 5 years ago … it's important to review IS Policy at least once a year". • "It is all too common that a security team (if it exists) is too small for the enterprise resulting in an improperly maintained or executed security policy…and is not keeping up with the urgency of policy implementation in today's constantly changing security environment".
Industry Standards	• "With the emergence of attention on security and the importance of policies and procedures, it is now possible to buy prewritten policies or engage a service to update current policy on a regular basis". • "Writing a good policy is more than taking the words from ISO 17799 and saying you have a policy – I have seen many of these!"
Legal & Regulatory Requirements	• "Automated monitoring tools may be resented and covert monitoring may be illegal; while internal audits may be biased and third-party audits are often not thorough". • "With the increasing introduction of legislation and regulation with respect to information security, it is becoming more difficult to ensure that policies are being kept up-to-date, and that they are compliant with the legislation, especially … translating legislation and regulation into practical terms".
External Threats	• "A policy quickly delivered may achieve short-term gain for your organization but, in the long term, may well not be broad and deep enough to properly protect your organization's information assets from the wide range of potential threats". • "Because of the changing nature of the Internet, the security threats faced by an organization also change, leading to updates & modifications to organizational security policies".
Senior Management Support	• "In most companies today, even those with largely effective individuals at the CIO/CxO level, it is extremely rare that these individuals take a direct leadership role with regards to security issues within their company. Policy/procedure development, enforcement, and ultimately support, is too often relegated to lower-level management where it sits in the queue with other day-to-day operational imperatives of the business, ultimately diminishing the focus, support, and effectiveness of the security organization". • "… without top management support and involvement, the creation, training and enforcement of the organization's security policies would not occur or would not be taken seriously by the employees". • "Top management support must happen first if the other issues are to be handled effectively".
Business Objectives	• "To make policies effective, policy writers must align policy content with business issues and revenue considerations". • "Corporate security policy needs to reflect and support the overall corporate business goals and objectives".

(*continued on next page*)

Appendix (*continued*)

Influential factors (external & internal)	Example respondent statements
Organizational Culture	• "Most managers, technical staff and end users generally see security as an imposition that interferes with their mission accomplishment rather than as an aid to help them accomplish their mission securely. As a result, people tend to ignore or try to circumvent security policies and controls". • "The subjective enforcement of violations of information security policies leads to a culture of some individuals in an organization being above the law. When others in the organization see this they are less inclined to follow the policies". • "Without an established and widespread awareness and education effort, it is difficult if not impossible to integrate security into the corporate culture".
Technology Architecture	• "It is important that the individuals writing the policies understand the operating system, hardware, protocols, applications, etc. as all can have their own security vulnerabilities". • "Many organizations lack a clear, coherent, comprehensive policy as to how to "harden" the configuration of servers, databases, routers, firewalls, and other key components in the systems environment". • "Organizations must remember to update their security policies when implementing new advances to their network security architecture". • "… new vulnerabilities in existing technologies are discovered daily … even the most well thought out policy cannot anticipate every newly emerging threat".
Internal Threats	• "Most organizations believe that if they have a firewall, intrusion detection system, VPN, or other technical gadget, that they are operating in a safe environment. They don't realize that policy, process, and procedures are equally important, in some cases more so, especially to defend against the internal threat or against accidents that compromise the integrity or availability of data".

REFERENCES

Andrews KR. The concept of corporate strategy. 3rd ed. Homewood, Illinois: Irwin; 1987.

Ansoff HI. Corporate strategy. New York: McGraw-Hill Book Company; 1965.

Bacik S. Building an effective information security policy architecture. Boca Raton, FL: CRC Press; 2008.

Backhouse J, Hsu CW, Silva L. Circuits of power in creating de jure standards: shaping an international information systems security standard. MIS Quarterly 2006;30(Special Issue):413–38.

Barman S. Writing information security policies. New York: New Riders; 2002.

Baskerville R, Siponen M. An information security meta-policy for emergent organizations. Journal of Logistics Information Management 2002;15(5/6):337–46.

Buss MDJ, Salerno LM. Common sense and computer security. Harvard Business Review 1984;84(2):112–21.

Damianides M. Sarbanes-oxley and IT governance: new guidance on IT control and compliance. Information Systems Management 2005;22(1):77–85.

David J. Policy enforcement in the workplace. Computers & Security 2002;21(6):506–13.

Davis GB, Olson MH. Management information systems – conceptual foundations, structure, and development. 2nd ed. New York: McGraw-Hill Book Company; 1985.

Fulford H, Doherty NF. The application of information security policies in large UK-based organizations: an exploratory investigation. Information Management & Computer Security 2003;11(3):106–14.

Galal GH. From contexts to constructs: the use of grounded theory in operationalising contingent process models. European Journal of Information Systems 2001;10:2–14.

Garvin DA. The process of organization and management. Sloan Management Review 1998;39(4):33–50.

George JF. Computer-based monitoring: common perceptions and empirical results. MIS Quarterly 1996;20(4):459–80.

Glaser BG, Strauss AL. The discovery of grounded theory: strategies for qualitative research. New York: Aldine de Gruyter; 1967.

Hansche SD. Making security awareness happen. In: Tipton HF, Krause M, editors. Information security management handbook. 4th ed., vol. 3. New York: Auerbach Publications; 2002. p. 337–51.

Hare C. Policy development. In: Tipton HF, Krause M, editors. Information security management handbook. 4th ed., vol. 3. Baca Raton: CRC Press; 2002. p. 353–83.

Hofstede G. Cultural constraints in management theories. Academy of Management Journal 1993;7(1):81–94.

Hone K, Eloff JHP. Information security policy – what do international standards say? Computers & Security 2002;21(5):402–9.

Howard PD. The security policy life cycle: functions and responsibilities. In: Tipton HF, Krause M, editors. Information security management handbook. 4th ed., vol. 4. Boca Raton: CRC Press, LLC; 2003.

ISF. Standard of good practice for information security (V4.1). from:. Information Security Forum www.isfsecuritystandard.com; 2005. Retrieved July 15, 2006.

ISO/IEC. Information technology – code of practice for information security management (No. ISO/IEC 17799:2000(E)). The International Standards Organization/The International Electrotechnical Commission; 2000.

ISO/IEC. Information technology – code of practice for information security management, ISO/IEC 27002:2005. The International Organization for Standardization/The International Electrotechnical Commission; 2005.

Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective. Computers & Security 2005;25(3):246–60.

Knapp KJ. Development of an organizational information security policy process model (PROF-303; session commentary offered by Steve Lipner, Microsoft Corporation). In: Paper presented at the RSA Conference; 2007, February 2. San Francisco, CA.

Leach J. Improving user security behavior. Computers & Security 2003;22(8):685–92.

Loch KD, Carr HH, Warkentin ME. Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly 1992;16(2):173–86.

Lowery JC. Developing effective security policies. Dell Powersolutions; 2002, November. pp. 77–79.

Luftman J, Kempaiah R. Key issues for IT executives 2007. MIS Quarterly Executive 2008;7(2):99–112.

Luftman J, McLean ER. Key issues for IT executives. MIS Quarterly Executive 2004;3(2):89–104.

Moulton R, Coles RS. Applying information security governance. Computers & Security 2003;22(7):580–4.

NIST. SP 800-14, generally accepted principles and practices for securing information technology systems. Access at. Washington D.C.: National Institute of Standards and Technology; Computer Security Resource Center (CSRC), http://csrc.nist.gov/publications/nistpubs/; 1996.

Nolan R, McFarlan FW. Information technology and the board of directors. Harvard Business Review 2005;83(10):96–106.

Olnes J. Development of security policies. Computers & Security 1994;13(8):628–36.

Palmer ME, Robinson C, Patilla JC, Moser EP. Information security policy framework: best practices for security policy in the e-commerce age. Information Systems Security 2001;10(2):13–27.

Parker DB. Computer security management. Reston, Virginia: Reston Publishing Company; 1981.

Peltier TR. Information security policies, procedures, and standards: guidelines for effective information security management. 1st ed. CRC Press; 2002.

Rees J, Bandyopadhyay S, Spafford EH. Prires: a policy framework for information security. Communications of the ACM 2003; 46(7):101–6.

Ruighaver AB, Maynard SB, Chang S. Organizational security culture: extending the end-user perspective. Computers & Security 2007;26(1):56–62.

Schein EH. Coming to a new awareness of organizational culture. In: Kolb DA, Osland JS, Rubin IM, editors. The organizational behavior reader. 6th ed. Englewood Cliffs, New Jersey: Prentice Hall; 1995.

Schein EH. Defining organizational culture. In: Shafritz JM, Ott JS, editors. Classics of organizational theory. 4th ed. New York: Harcourt Brace College Publishers; 1996.

SEI/CMU. RFC 2196-site security handbook. Access at. Pittsburgh, PA: Software Engineering Institute/Carnegie Mellon University, http://rfc.net/rfc2196.html; 1997.

Simon HA. Administrative behavior. 2nd ed. New York: The Free Press; 1957.

Siponen M, Iivari J. Six design theories for IS security policies and guidelines. Journal of the Association for Information Systems 2006;7(7):445–72.

Straub DW. Effective IS security: an empirical study. Information Systems Research 1990;1(3):255–76.

Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Quarterly 1998; 22(4):441–69.

Strauss A, Corbin J. Basics of qualitative research. Techniques and procedures for developing grounded theory. 2nd ed. Thousand Oaks, CA: Sage; 1998.

Volonino L, Gessner GH, Kermis GF. Holistic compliance with sarbanes-oxley. Communications of the Association for Information Systems 2004;14:219–33.

von Solms B, von Solms R. The 10 deadly sins of information security management. Computers & Security 2004a;23:371–6.

von Solms R, von Solms B. From policies to culture. Computers & Security 2004b;23:275–9.

Warkentin ME, Johnson AC. IT governance and organizational design for security management. In: Straub DW, Goodman S, Baskerville RL, editors. Information security: policy, processes, and practices. Advances in management information systems, vol. 11. Armonk, NY: M.E. Sharpe; 2008. p. 46–68.

Weill P. Don't just lead, govern: how top performing firms govern IT. MIS Quarterly Executive 2004;3(1):1–17.

Whitman ME. Security policy: from design to maintenance. In: Straub DW, Goodman S, Baskerville RL, editors. Information security: policy, processes, and practices. Advances in management information systems, vol. 11. Armonk, N.Y.: M.E. Sharpe; 2008. p. 123–51.

Whitman ME, Townsend AM, Aalberts RJ. Information systems security and the need for policy. In: Dhillon G, editor. Information security management. Global challenges in the new millennium. Hershey, PA: Idea Group Publishing; 2001.

Wood CC. Writing infosec policies. Computers & Security 1995; 14(8):667–74.

Wood CC. Information security policies made easy. 9th ed. Houston, Texas: PentaSafe Security Technologies; 2002.

Wrapp EH. Good manager's don't make policy decisions. Harvard Business Review 1967;45(5):91–9.

Yang KS. Will societal modernization eventually eliminate cross-cultural psychological differences. In: Bond MH, editor. The cross-cultural challenge to social psychology. Newbury Park, CA: Sage; 1986.

Kenneth J. Knapp is an Assistant Professor at the University of Tampa. He received his PhD from Auburn University in 2005 and spent seven years teaching at the U.S. Air Force Academy between 1999 and 2009. His research focuses on topics relating to information security effectiveness and has been published in numerous outlets including *Information Systems Management*, *Information Systems Security*, *Communications of the AIS*, *Information Management & Computer Security*, *International Journal of Information Security and Privacy*, *Journal of Digital Forensics, Security, and Law*, as well as multiple articles in editions of the *Information Security Management Handbook* edited by Tipton & Krause. Dr. Knapp is the editor of a peer-reviewed book titled, *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*.

R. Franklin Morris, Jr. is an Assistant Professor of Management Information Systems at The Citadel in Charleston, SC. He received his Ph.D. in Management Information Systems from Auburn University, Auburn, Alabama. He holds an MBA from Georgia Southern University and a Bachelor of Science degree in Aerospace Engineering from Georgia Institute of Technology. Dr. Morris has more than twenty years of experience working in private industry and has been published in various outlets including *Communications of the AIS, International Journal of Electronic Marketing and Retailing, Journal of Learning in Higher*

Education, and the 2008 *edition of the Information Security Management Handbook* edited by Tipton & Krause.

Thomas E. Marshall is an Associate Professor of Management Information Systems at Auburn University, Alabama. He is a CPA and has been a consultant in the area of accounting information systems for over twenty years. His publications include *Information & Management*, *OMEGA*, *Journal of Computer Information Systems, Information Management & Computer Security*, *Information Systems Security* and the *Journal of Database Management*.

Terry Anthony Byrd is a Professor of Management Information Systems at Auburn University, Auburn, Alabama. His research appears in *Journal of Management Information Systems*, *MIS Quarterly*, *Decision Sciences*, *Journal of the AIS*, *Communications of the AIS*, *OMEGA*, *Interfaces*, and other leading journals.