Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations

Kenneth J. Knapp
The University of Tampa

Claudia J. Ferrante
United States Air Force Academy

To minimize the probability of costly information security incidents, organizations should be highly motivated to communicate, enforce and maintain security policies. With insight from the workplace deviance and organizational learning literature, we investigate a model exploring the impact of policy awareness, enforcement and maintenance on the effectiveness of information security programs in organizations. Utilizing a sample of 297 certified information security professionals located in the United States, we found support for the model as well as a second-order version of a modified structure. Before concluding, we discuss our results, study limitations and offer implications for research and practice.[1]

INTRODUCTION

Frequent media reports of major data breaches, such as the 2011 Citibank and Sony incidents where hackers accessed millions of customer accounts, has highlighted the critical need for businesses and governments to strengthen information security programs. Organizations should assess all possible threats and weaknesses when evaluating their information security risks. Secure business processes are central to controlling corporate information and preventing a rogue employee, for example, from anonymously giving sensitive information to a competitor or a site like Wikileaks. Key in this regard is the importance for organizations to develop and maintain sufficient security policies and ensure employees are aware of them. The desire to eliminate security breaches which, if publicized, can damage an organization's reputation should be a strong incentive to tighten internal policies. Organizations with sensitive information need formal policies that are actively maintained, updated and properly communicated to employees to prevent such incidents (Knotts, 2011).

Digitized information is the lifeblood of modern organizations that are increasingly reliant on technology to conduct everyday operations. Due to this digital dependence, information security programs have become essential to protecting sensitive information. Likewise, policy is critical because it sets the rules and expectations about how employees are to behave when handling information and using computer systems. Organizational policy must balance the need for security with the requirement for accessibility to these systems. In other words, excessive security can restrict the access and handling of information that may hurt profitability and work against achieving business goals. Likewise, too little security increases the risk of an incident resulting in compromised information, competitive disadvantage, lawsuits and damaged reputation. An organization's information security policy is a vital business document that must address this delicate balance and ultimately promote security effectiveness.

Our study addresses the essential elements of security policy management and their relationship to overall security effectiveness in organizations. In the rest of the paper, we provide a literature review of information security policy as a basis for our theoretical model and hypotheses. We then describe our research methodology and share the results. We conclude with a discussion of our findings and their implications and offer suggestions for future research.

THEORETICAL MODEL AND HYPOTHESES

Security policies are a critical safeguard to help employees understand how they need to behave in regards to protecting organization information and systems. The prevailing literature on organizational policy offers a foundation for the information security field. An internal policy is a general rule or expectation that limits the discretion of employees in an organization (Simon, 1957). It may be considered a plan of action or set of expectations for employee behavior when confronted with a specific set of circumstances that is addressed in the policy. Some believe that policies should evolve over time and be adapted to or derived from operating decisions as a response to repetitive situations (Ansoff, 1965; Wrapp, 1967). From a general deterrence framework, security policy depends on the same core mechanisms as societal law in that organizational policies clarify what is deemed unacceptable versus acceptable conduct as well as the appropriate punishment for illicit behavior (Lee & Lee, 2002). In regards to information security, policy addresses the integrity, availability, and confidentiality of data stored and transmitted between information systems and is necessary before implementing effective deterrents (Straub, 1990). Managing information security policy in organizations involves a cyclical process of activities to develop, implement, communicate and enforce approved policies while performing regular risk assessments to maintain established policies (Knapp, Morris, Marshall, & Byrd, 2009).

Information Security Program Effectiveness in Organizations

In our research model, we measure *effectiveness* to capture whether an information security program is accomplishing its objective of protecting information in the organization. This is a useful measure because with the increasing attention and spending on information security, organizations should know if their security programs are working. We titled the dependent variable of our study *information security program effectiveness*. While published *information system* effectiveness studies exist in significant numbers, few studies with a comparable *security effectiveness* variable exist in the research. Straub (1990) measured computer abuse using qualitative and quantitative items with criminal sociology as a field of reference. A different study used a perception variable of security effectiveness with participants responding to overall security deterrence, prevention and protection levels of computer hardware, software, data, and services (Kankanhalli, Teo, Tan, & Wei, 2003).

Security effectiveness can be challenging to measure, because it is nearly impossible to know if hard data such as the number of incidents or the amount of financial loss is accurate and complete. Moreover, organizations face potential financial losses by publically reporting security incidents due to reputational damage, reduced consumer confidence and stock price decreases. Thus, a financial incentive exists not to report security incidents or to deliberately underreport them. Furthermore, security incidents may not even be detected at all or go only partially detected (Richardson, 2003). As a consequence, research subjects may not be forthcoming in providing hard numbers about security incidents or in admitting general ineffectiveness due to the sensitivity of security matters (Kotulic & Clark, 2004).

Our dependent variable measures how effectively the organization's information security program protects the company's information resources and whether the program is achieving its security goals. Rather than collecting hard numerical data, we measure effectiveness using the professional judgment of certified security specialists. Furthermore, to address the wariness that respondents may have regarding answering effectiveness and policy management questions, we used a survey instrument developed specifically to not sound meddling or excessively intrusive. We discuss these efforts in the methodology section.

Having identified our dependent variable, we now review the independent variables of our model. In the next segment, we discuss information security policy awareness. Next, we reference the workplace deviance literature in regards to the policy enforcement variable. Finally, we cite the organizational learning literature in formulating the policy maintenance variable.

Policy Awareness as Vital to Effectiveness

In the current context, awareness is a general state of employee knowingness or mindfulness about security concepts. Awareness represents a user's raised consciousness and understanding of security issues and strategies of how to deal with them (Dinev & Hu, 2007). Examples of awareness enhancing activities include security briefings, formal training, regular reminders, ethical codes of conduct as well as the promulgation of organization policy describing the appropriate use of system resources (D'Arcy, Hovav, & Galletta, 2009; Parker, 1981).

The notion of awareness is often interchangeably used with training and education; the terms are frequently mentioned together such as in reference to security education, training and awareness (SETA) programs (Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy, Hovav, & Galletta, 2009). Regardless of the term, the goal of awareness and training programs is to enhance knowledge of corporate policies and improve employee security behavior in organizations. It is common practice for organizations to train employees about handling security threats and encourage employees to support security policy in the course of their daily work (ISO/IEC, 2005). This is vital because the human worker is the endpoint of an information system and considered the weakest link in protecting organizations from both external attackers and internal security violations (Hu, Xu, Dinev, & Ling, 2011; Warkentin & Willison, 2009). General awareness of security risk is understood to be fundamental to effective information security (Spears & Barki, 2010). For developing corporate security policies, some suggest that deterrence against violations should be articulated clearly in policies, and firms should ensure that employees are fully aware of the consequences of violating policy (Dinev & Hu, 2007). Similarly, security-aware employees who are knowledgeable about policies translate to a more secure organization. Thus, we hypothesize that:

> *Hypothesis 1: Information security policy awareness is positively associated with information security program effectiveness.*

Policy Enforcement as Minimizing Workplace Deviance

In a sociological context, *general deterrence* assumes that people will engage in negative behaviors if they do not fear punishment. Policies, norms, laws and their enforcement are intended to create awareness that negative behaviors will be detected and violators appropriately punished (Keel, 2005). The related concept of *social deviance* is defined as normative violations especially where breaches of norms risk serious sanctions (Best, 2006). Within organizations, workplace deviance refers to voluntary employee behavior or condition plainly different from the norm that can be a prevalent and costly problem for organizations and its members. (Aquino, Galperin, & Bennett, 2004). Workplace deviance is commonly divided between *interpersonal deviance* which targets individuals such as by gossip or theft from coworkers and *organizational deviance* such as by damaging company property or intentionally working slowly (Berry, Ones, & Sackett, 2007). In regards to security policy, workplace deviance can manifest itself in employee disobedience toward official policy by, for example, providing a whistle-blower site with confidential company information. To help minimize deviance, general deterrence aims to reduce the probability of negative deviant behavior in employees through controls such as organization security policy, which sets to establish what constitutes deviant behavior coupled with awareness of the punishments for violating policy.

Organizations can promote awareness of punishments by enforcing approved policies. If an employee knowingly violates a policy, the company can enforce it by appropriately reacting to the deviant behavior. The act of enforcement may promote employee observance of official policy and encourage employees to respect corporate policies through their behaviors and daily activities. If an employee deviates from policy, the organization can enforce it through punishments such as an official reprimand, monetary penalty, job demotion, work suspension or job firing. In the context of organizations, general deterrence theory predicts that the greater the certainty and severity of punishment for a deviant or illicit act, the more employees are deterred from such acts (Gibbs, 1975). The effectiveness of policy awareness on employee perception of punishment severity is key because it can be a preventive influence to deviant acts targeting information systems (D'Arcy, Hovav, & Galletta, 2009) and thus advance information security. We suggest the following:

> *Hypothesis 2: Information security policy enforcement is positively associated with information security program effectiveness.*

Policy Maintenance as Organizational Learning

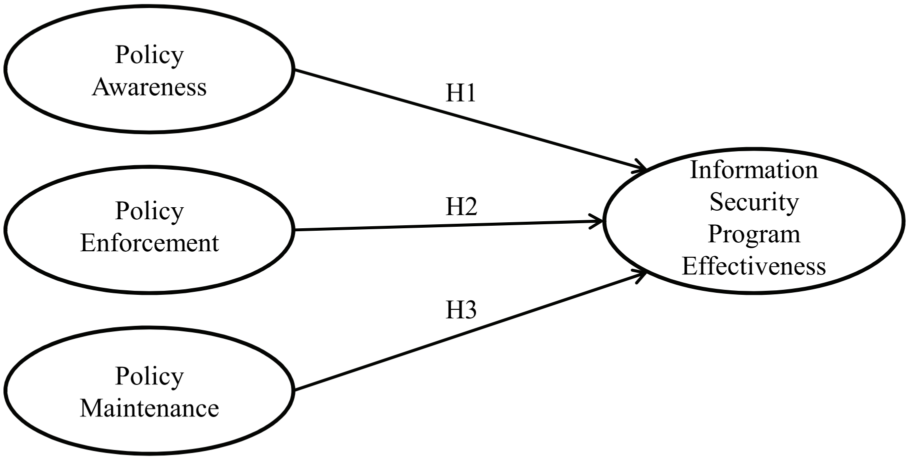
The theory of organizational learning has its roots in the strategic management literature and is the notion that organizations develop insights and changes in states of knowledge over time (Argyris & Schon, 1978). By gaining knowledge, organizations adapt and develop new structures and adjust to their environment to remain competitive for their long term survival under the assumption that change will improve performance and effectiveness (Fiol & Lyles, 1985). Within an organization, individual members and executives alike may come and go, but corporate memory, norms and values will adapt over time (Hedberg, 1981). In order for a process of acquiring skill and knowledge, or learning to occur, organizations make a conscious decision to change behaviors in response to a change in conditions or environment. Organizational learning has not occurred, however, until the knowledge is in the shared collective and stored in organizational memory so that it may be accessed, communicated and used to achieve goals and objectives (York University, 2010).

In regards to the current study, the goal of maintenance is to ensure policies are still working for the organization by protecting its valuable information and systems. Policies must be current, relevant, in 'good working order' and help to minimize the risk of costly incidents by articulating clear guidance about what is expected as proper employee behavior in regards to information security. Companies maintain their policies by updating or at least reviewing them on a cyclical (e.g. annual) or as needed basis (e.g. to address an emerging threat). Once updated, companies must approve or recertify their policies with an appropriate senior manager followed by some type of employee awareness campaign. Continually maintaining, updating, documenting and disseminating corporate policy helps ensure that learning is occurring in the organization. The consequence of not conducting maintenance is that policy can become outdated, neglected and thus irrelevant to shaping employee behavior (Knapp, Morris, Marshall, & Byrd, 2009). Moreover, failing to maintain policy may even demonstrate a general lack of top management support for information security overall. Hence, considering the importance of policy maintenance, we propose:

> *Hypothesis 3: Information security policy maintenance is positively associated with information security program effectiveness.*

Our complete theoretical model of information security policy and program effectiveness is a first-order nomological network containing four variables (see Figure 1).

FIGURE 1
MODEL OF INFORMATION SECURITY POLICY AND EFFECTIVENESS



METHODOLOGY

Data, Respondents and Survey Procedure

The respondents consist entirely of Certified Information System Security Professionals (CISSPs), representing a non-probability, judgment sample for our study. The requirements to earn the CISSP designation at the time of our study include passing a rigorous exam covering ten domains of information security knowledge, consenting to an ethical code and possessing a minimum of four years of professional experience in the field or three years of experience plus a college degree. Once certified, a person must earn continuing professional education (CPE) credits to maintain the designation. The CISSP certification program is managed by a non-profit organization called the International Information Systems Security Certification Consortium [$(ISC)^2$].

We collected data in two phases to minimize the potential validity threat of common method variance, which is a type of method bias where variable correlations are vulnerable to artificial inflation or deflation due to the collection approach. As a source of measurement error, common method variance can potentially threaten the validity of empirical research especially with self-report surveys where the predictor and criterion variables come from a matching source (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Fortunately, data collection procedures exist that can minimize this validity threat. For this purpose, we collected data in phases five days apart to increase the probability that participants were in a different cognitive disposition when giving responses to the predictor and criterion variables. Moreover, this five day gap decreased the probability of participants attempting to hypothesis guess (Straub, Limayem, & Karahanna-Evaristo, 1995) and desiring to answer in a socially acceptable manner (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). While it is impossible for time gaps to remove all method biases, our goal was to reduce the plausibility of this measurement error influencing the associations in the model.

We sent a single email to all CISSPs based in the United States requesting participation in our study. The official $(ISC)^2$ email contained other items of organization business. We had a 4.2% response rate from 9,600 CISSPs. This response rate was expected considering the email approach of seeking research participants with neither follow-up reminders nor professional incentives. After matching responses across the two collection periods, we obtained a useful sample of 297 CISSPs. Table 1 lists the reported industry of the respondents and Table 2 provides the size of respondents' organizations. Additional sample demographics are provided in Appendix C.

TABLE 1
INDUSTRY OF RESPONDENTS

Industry	Count	Percent
Government	83	28%
Info Tech, Security, Telecom	56	19%
Finance, Banking, Insurance	51	17%
Manufacturing	24	8%
Other	24	8%
Healthcare	22	7%
Education, Training	22	7%
Utilities	9	3%
Consumer Products, Retail	8	3%
Professional Services (legal, HR, etc.)	8	3%
Energy	5	2%
Non-Profit	4	1%
Transportation, Warehousing	4	1%
Travel, Hospitality, Entertainment	3	1%
TOTAL	323	100%

n = 297; respondents could choose multiple industries

TABLE 2
SIZE OF RESPONDENTS' ORGANIZATIONS

Size of Organization	Count	Percent
less than 500	57	19%
between 500-2,499	55	19%
between 2,500-15,000	81	27%
over 15,000	104	35%
TOTAL	297	100%

n = 297.

Measures

The survey contained questions examining respondents' perception of policy awareness, enforcement, and maintenance and information security program effectiveness in their organization. During survey development, questionnaire items that may have appeared to be excessively intrusive to potential study participants were removed. Because information security can be a sensitive research topic, a cautious approach to data collection has been recommended (Kotulic & Clark, 2004) due to a general suspicion of any research study that measures the behaviors of security practitioners especially in their own organizational context. In this effort, an expert panel of twelve security practitioners evaluated all candidate survey items on perceived intrusiveness using a *willingness-to-answer* scale (Knapp, Marshall, Rainer, & Ford, 2006) as well as construct validity based on an *item-to-construct* scale (Hinkin, 1998). Items with low construct validity or considered as potentially intrusive by the panel were removed from the instrument. The 18 survey items making up our research instrument are listed in Appendix A.

We assured participants that their individual responses would be confidential and only aggregated data would be published. We used a web-based survey with communication encryption and randomized the order of the question items during both survey phases. All participants responded using a 5-point Likert scale where 1=strongly disagree and 5=strongly agree. Knapp, Marshall, Rainer, & Ford (2005) provides further information about survey development. We averaged each variable's responses into an index and coded so that a high score indicates a high value for each variable. Sample items and Cronbach alpha (α) reliabilities for each variable follow:

Information Security Policy Awareness. Five items, one of which stated: "In the organization, necessary efforts are made to educate employees about new security policies" (α = 0.92).

Information Security Policy Enforcement. Four items, one of which stated: "In the organization, employees caught violating important security policies are appropriately corrected" (α = 0.87).

Information Security Policy Maintenance. Four items, one of which stated: "In the organization, information security policy is consistently updated on a periodic basis" (α = 0.91).

Information Security Program Effectiveness. Five items, one of which stated: "In the organization, generally speaking, information is sufficiently protected" (α = 0.92).

RESULTS

We used structural equation modeling software (Amos 17) to test the research model. Table 3 provides the measurement model: standardized factor loadings, critical value (z-statistic) and squared multiple correlations (SMC) for each of the 18 items in the instrument. Table 4 presents the means, standard deviations and zero-correlations for the variables. We modeled each of the measured factors in isolation, then in pairs, and then as a collective network following procedures from Segars & Grover (1998). To support convergent validity, all survey items loaded on the intended factor with no significant cross-loading present; all loadings were statistically significant and above 0.707, indicating that the latent construct is capturing over half the variance. An item loading and cross-loading matrix is supplied in Appendix B, which also supported initial convergent and discriminant validity.

TABLE 3
MEASUREMENT MODEL (n=297)

Constructs	Indicators	Loadings	Critical Value	SMC
Information Security Program Effectiveness	IE1	.86	---	.73
	IE2	.84	18.6	.71
	IE3	.76	15.8	.58
	IE4	.91	21.0	.82
	IE5	.81	17.1	.65
Information Security Policy Awareness	PA1	.71	13.7	.51
	PA2	.81	---	.66
	PA3	.91	19.5	.83
	PA4	.93	19.8	.87
	PA5	.86	17.4	.73
Information Security Policy Enforcement	PE1	.82	---	.67
	PE2	.82	15.5	.67
	PE3	.85	16.2	.72
	PE4	.72	13.0	.51
Information Security Policy Maintenance	PM1	.91	---	.82
	PM2	.77	17.3	.60
	PM3	.80	18.6	.64
	PM4	.92	24.7	.85

Note: All loadings significant at $p < .001$.

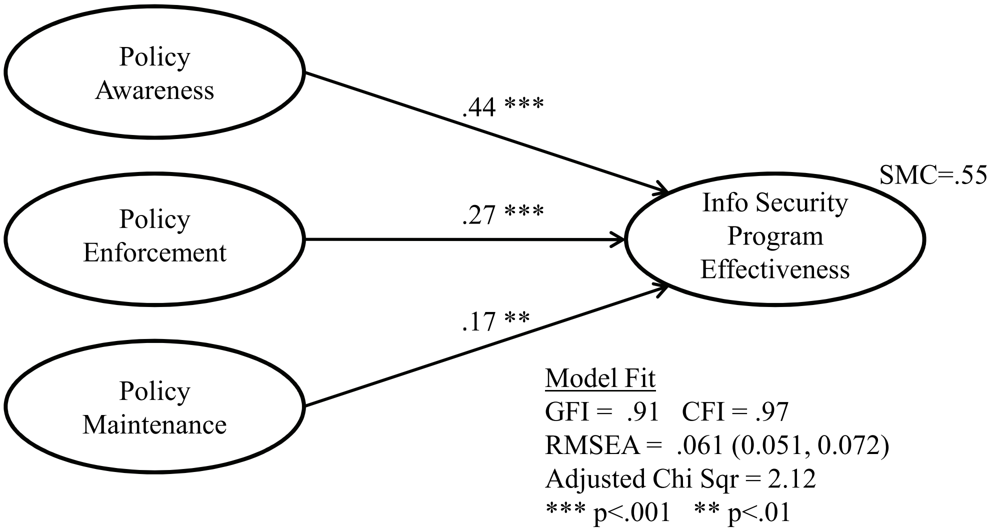
TABLE 4
MEANS, STANDARD DEVIATIONS AND CORRELATIONS [a]

Variable	Mean	s.d.	1	2	3	4
1. Security Policy Awareness	3.28	0.96	(.92)			
2. Security Policy Enforcement	3.45	0.86	.60**	(.87)		
3. Security Policy Maintenance	3.59	0.88	.56**	.46**	(.91)	
4. Security Program Effectiveness	3.56	0.80	.70**	.58**	.53**	(.92)

[a] n = 297. Items in parentheses are Cronbach alpha reliabilities.
** p < .01.

Figure 2 presents the path model (n=297): the standardized causal path findings, selected fit indices, and SMC value for the endogenous dependent variable, information security program effectiveness, in the upper right of the construct. All of the paths were significant. Additionally, supporting both convergent and discriminant validity, GFI, CFI and RMSEA are within acceptable ranges (Straub, Boudreau, & Gefen, 2004). Based on this data analysis, we found support for hypotheses 1, 2 and 3.

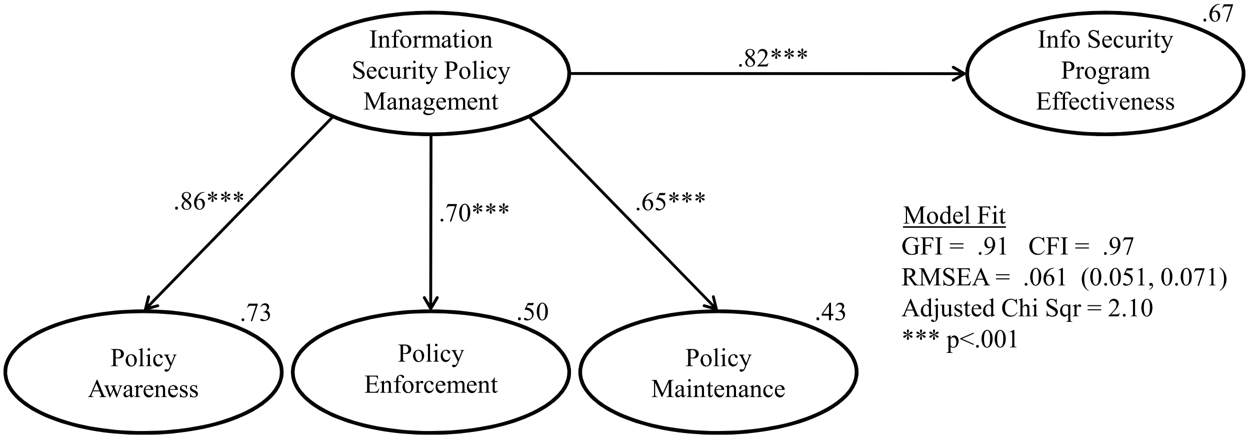
FIGURE 2
PATH DIAGRAM OF THEORETICAL MODEL (n=297)



Model Fit
GFI = .91 CFI = .97
RMSEA = .061 (0.051, 0.072)
Adjusted Chi Sqr = 2.12
*** p<.001 ** p<.01

We also tested a second-order model to provide an additional perspective on the factor analytic structure of the original. Our reason for testing this alternative model is the belief that a general latent construct may shape the first-order latent constructs. Thus, the three independent constructs may be influenced by a second-order factor that does not have direct effects on the observed variables of the study (Bollen, 1989). This second-order factor offers a diverse way of thinking about the relationships among the three independent constructs. Our interpretation of the second-order factor is *information security policy management*. In the second-order model, policy management represents the repeated actions of management to promote information security effectiveness by ensuring employees are aware of polices, and that policies are enforced and maintained in the organization.

FIGURE 3
PATH DIAGRAM OF SECOND-ORDER THEORETICAL MODEL (n=297)



Empirical support for both the original and second-order models were found in the magnitude and significance of the estimated parameters as well as the amount of variance explained by the structural equations (Segars & Grover, 1998). Unlike the original model, all paths in the second-order model were significant at $p < .001$, and the amount of variance explained in the dependent variable by SMC was higher in the second-order model (0.67 versus 0.55). Additionally, fit indices for both models were acceptable. The improved variance explained by the second-order model does not necessarily mean it is the better of the two. The original model, for instance, had the advantage of measuring the magnitude of the direct effect of each independent variable on the dependent variable. This advantage is lost in the alternative model due to the inclusion of the second-order factor.

DISCUSSION

In this study, we explored a theoretical model examining the impact of three dimensions of information security policy on information security program effectiveness. Specifically, our findings highlight the important direct effects that information security policy awareness, enforcement and maintenance have on the effectiveness of information security programs in organizations as well as the significance of considering these three dimensions as a combined effect of policy management. We found that awareness of an organization's policy has the largest direct impact on program effectiveness, whereas maintenance of the policy has the smallest effect, although still statistically significant. These findings suggest theoretical implications for the research literature and practical implications for managers of information security programs.

In the literature, to our knowledge, this study is the first to unite two distinct research streams (workplace deviance and organizational learning) to examine their applicability to information security policy. Our parsimonious model also helps practitioners focus on the fundamentals of policy management (i.e., awareness, enforcement and maintenance) as it impacts program effectiveness. Our study suggests that information security managers should prioritize their efforts and focus largely on policy awareness, as it had the largest impact on effectiveness. Also significant but secondary to awareness, managers should enforce existing policies as well as keep them relevant through regular maintenance. If an organization does a sufficient job of positive and proactive security awareness through adequate training, reminders, and employee orientation programs for example, it is reasonable to expect that enforcement will become less critical. In this sense, positive awareness can be more impactful in affirming security behaviors rather than enforcement, which tends to emphasize the negative. With enhanced awareness, employees may become more security minded and the organizational culture more acclimated and accepting of security goals. It is plausible that organizations with stronger awareness programs will encourage more security-minded employees to conduct informal ‘self-monitoring’ of each other making formal enforcement and sanctions less critical or even necessary. Ultimately, our research suggests the three-pronged approach to information security policy management of emphasizing awareness, enforcement and policy maintenance will ultimately minimize corruption of organizational information and contribute to the bottom-line by reducing the costs of mediating information security breaches.

Moreover, we suggest that managers implement comprehensive security programs that focus on areas beyond what our models covers. For example, recent research shows that how employees perceive benefits of complying with security rules and their moral beliefs can have a significant impact on employee intention to violate security policies (Vance & Siponen, 2012). Others stress that when handling sensitive data such as a person’s credit card or medical information, organizations should screen employees and seek those with higher levels of self-control and compatible moral beliefs in addition to the requisite technical skills and job experience (Hu, Xu, Dinev, & Ling, 2011).

Study Limitations and Future Research

Although our study produced fruitful findings, it has limitations. Our respondents were not pulled from a sample of general employees in organizations, but were professionals in the field of information system security. Thus, our results are not generalizable to other populations of employees. Second, our study had limited scope as we examined only three elements of information security policy, whereas security policy management includes other aspects such as policy development, managerial approval, employee monitoring and security risk assessment.

Based on these limitations, we offer a few suggestions for future research. First, we suggest surveying a wider group of employees whose expertise is not information system security. The insights of workers outside this professional realm undoubtedly hold promise for enhancing information security program effectiveness. Second, we suggest exploring the mechanisms through which organizations enforce their information security policies to minimize workplace deviance. It is possible that the incorporation of workers from various levels and sub-cultures of the organization will influence employees’ adherence to the policies. Finally, it would be very interesting to explore the impact of electronic monitoring of workers and the effect of policy enforcement and penalties for security breaches on workers’ day-to-day security practices.

CONCLUSION

Because the reality of security incidents causing major data losses will likely continue, it is essential for organizations to take systematic action to secure their information. Attention to information security policy management is a critical avenue that can meaningfully improve an organization’s overall information security effectiveness. Based on our research, a systematic approach to policy management that principally focuses on awareness but also on enforcement and maintenance will significantly advance the safeguarding of information in organizations.

NOTE

A previous version of this paper was presented and published in the *Proceedings of the Southern Management Association*, November 10, 2011, Savannah, Georgia.

REFERENCES

Ansoff, H. I. (1965). *Corporate Strategy*. New York: McGraw-Hill Book Company.

Aquino, K., Galperin, B. L., & Bennett, R. J. (2004). Social Status and Aggressiveness as Moderators of the Relationship Between Interactional Justice and Workplace Deviance. *Journal of Applied Social Psychology, 34*(5), 1001-1029.

Argyris, C., & Schon, D. A. (1978). *Organizational Learning*. Reading, MA: Addison-Wesley.

Berry, C. M., Ones, D. S., & Sackett, P. R. (2007). Interpersonal Deviance, Organization Deviance, and Their Common Correlates: A Review and Meta-Analysis. *Journal of Applied Psychology, 92*(2), 410-424.

Best, J. (2006). Whatever happened to Social Pathology? Conceptual Fashions and the Sociology of Deviance. *Sociological Spectrum, 26*(6), 533-546.

Bollen, K. A. (1989). *Structural Equations With Latent Variables*. New York: John Wiley & Sons.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548.

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

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formulation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

Fiol, C. M., & Lyles, M. A. (1985). Organizational Learning. *Academy of Management Review, 10*(4), 803-813.

Gibbs, J. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier.

Hedberg, B. (1981). How Organizations Learn and Unlearn? In P. C. Nystrom & W. H. Starbuck (Eds.), *Handbook of Organizational Design* (pp. 8-27). London: Oxford University Press.

Hinkin, T. R. (1998). A Brief Tutorial on the Development of Measures for Use in Survey Questionnaires. *Organizational Research Methods, 1*(1), 104-121.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM, 54*(6), 54-60.

ISO/IEC. (2005). *Information Technology - Code of Practice for Information Security Management* (No. ISO/IEC 17799:2005 (renumbered to ISO/IEC 27000 series in 2007)): The International Standards Organization/The International Electrotechnical Commission.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Keel, R. O. (2005). Rational Choice and Deterrence Theory: Sociology of Deviant Behavior. Retrieved January 15, 2011, from http://www.umsl.edu/~keelr/200/ratchoc.html (University of Missouri-St. Louis)

Knapp, K. J., Marshall, T. E., Rainer, K. R., Jr., & Ford, F. N. (2005, October 25). Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness. *Auburn University, Alabama; (ISC)^2 Inc., Framingham, Massachusetts* from https://sites.google.com/a/usafa.edu/kennethknapp/cv/selected-papers

Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Ford, F. N. (2006). Information Security: Management's Effect on Culture and Policy. *Information Management & Computer Security, 14*(1), 24-36.

Knapp, K. J., Morris, R. F. J., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model *Computers & Security, 28*(7), 493-508.

Knotts, C. (2011). 5 Ways to Make Sure You Aren't the Next Wikileak, Network World. Retrieved 8 March, 2011, from http://www.networkworld.com/news/tech/2011/021511-wikileak-security.html

Kotulic, A. G., & Clark, J. G. (2004). Why There Aren't More Information Security Research Studies. *Information & Management, 41*(5), 597-607.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 55-63.

Parker, D. B. (1981). *Computer Security Management*. Reston, Virginia: Reston Publishing Company.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common Method Bias in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology, 88*(5), 879-903.

Richardson, R. (2003). *8th Annual Computer Security Institute and Federal Bureau of Investigation Computer Crime and Security Survey*. San Francisco, CA: Computer Security Institute.

Segars, A. H., & Grover, V. (1998). Strategic Information Systems Planning Success: An Investigation of the Construct and Its Measurement. *MIS Quarterly, 22*(2), 139-163.

Simon, H. A. (1957). *Administrative Behavior* (2nd ed.). New York: The Free Press.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly, 34*(3), 503-522.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validating Guidelines for IS Positivist Research. *Communications of the AIS, 13*(24), 380-427.

Straub, D. W., Limayem, M., & Karahanna-Evaristo, E. (1995). Measuring System Usage: Implications for IS Theory Testing. *MIS Quarterly, 41*(8), 1328-1342.

Vance, A., & Siponen, M. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41.

Warkentin, M., & Willison, R. (2009). Guest Editorial: Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105.

Wrapp, E. H. (1967). Good Manager's Don't Make Policy Decisions. *Harvard Business Review, 45*(5), 91-99.

York University. (2010). Organizational Learning Theory. *Theories Used in IS Research: www.fsc.yorku.ca/york/istheory/wiki (site maintained by http://istheory.byu.edu in 2012)* Retrieved March 9, 2011, from www.fsc.yorku.ca/york/istheory/wiki/index.php/Organizational_culture_theory

APPENDIX A
SURVEY INSTRUMENT

Items used a 5-point Likert scale: 1=strongly disagree, 5=strongly agree (Knapp, Marshall, Rainer, & Ford, 2005). Each item begins with the phrase, "In the organization".

Information Security Program Effectiveness

E1 The information security program achieves most of its goals.
E2 The information security program accomplishes its most important objectives.
E3 Generally speaking, information is sufficiently protected.
E4 Overall, the information security program is effective.
E5 The information security program has kept risks to a minimum.

Policy Awareness

PA1 Employees clearly understand the ramifications of violating security policies.
PA2 Necessary efforts are made to educate employees about new security policies.
PA3 Information security awareness is communicated well.
PA4 An effective security awareness program exists.
PA5 A continuous, ongoing security awareness program exists.

Policy Enforcement

PE1 Employees caught violating important security policies are appropriately corrected.
PE1 Information security rules are enforced by sanctioning the employees who break them.
PE3 Repeat security offenders are appropriately disciplined.
PE4 Termination is a consideration for employees who repeatedly break security rules.

Policy Maintenance

PM1 Information security policy is consistently updated on a periodic basis.
PM2 Information security policy is updated when technology changes require it.
PM3 An established information security policy review and update process exists.
PM4 Security policy is properly updated on a regular basis.

APPENDIX B
FACTOR LOADING MATRIX

To assess initial validity of the measurement instruments, a cross-loadings matrix was constructed using principal components factoring with varimax rotation. Each item loaded on its theoretical construct more than on the other constructs, supporting convergent and discriminant validity.

Item	Security Effective	Policy Aware	Policy Enforce	Policy Maint
E1	**.778**	.280	.194	.211
E2	**.814**	.163	.192	.233
E5	**.796**	.199	.162	.174
E4	**.793**	.301	.241	.194
E3	**.764**	.216	.148	.163
PE1	.198	.204	**.791**	.161
PE2	.084	.157	**.796**	.155
PE3	.216	.166	**.810**	.176
PE4	.243	.136	**.821**	.137
PA1	.236	**.627**	.450	.164
PA2	.337	**.796**	.186	.232
PA3	.305	**.756**	.227	.232
PA4	.257	**.775**	.135	.266
PM1	.217	.163	.162	**.799**
PM2	.179	.192	.127	**.872**
PM3	.186	.186	.200	**.858**
PM4	.226	.224	.177	**.723**

APPENDIX C
ADDITIONAL SAMPLE DEMOGRAPHICS

TABLE C1
DEDICATED SECURITY OFFICE IN THE ORGANIZATION?

Response	Number	Percent
Yes	245	82.5%
No	51	17%
No Response	1	< 1%
TOTAL	297	100%

TABLE C2
POLICY APPROVAL LEVEL IN ORGANIZATION

Response	Number	Percent
Executive or upper management	246	83%
Middle management	43	14%
The org has policies, but mgt does not approve them	3	1%
Other management	3	1%
The organization does not have approved policies	1	< 1%
No response	1	< 1%
TOTAL	297	100%

ABOUT THE AUTHORS

Kenneth J. Knapp is an Associate Professor of Information & Technology Management at the University of Tampa. He received his Ph.D. at Auburn University. Dr. Knapp's research focuses on information and cyber security effectiveness in organizations and has been published in journals such as *Computers & Security*, *Government Information Quarterly, Information Systems Management* and the *Communications of the Association for Information Systems*.

Claudia J. Ferrante is a Professor of Management at the United States Air Force Academy. She earned her Ph.D. at Carnegie Mellon University and has been published in journal outlets such as *Human Resource Management, Group and Organization Management, Journal of Management Education* and *Trends in Organizational Behavior.*