

Examining the Linkage between Organizational Commitment and Information Security*

Jeffrey M. Stanton
School of Information Studies
Syracuse University
jmstanto@syr.edu

Indira Guzman
School of Information Studies
Syracuse University
iguzmand@syr.edu

Kathryn R. Stam
School of Information Studies
Syracuse University
krstam@syr.edu

Cavinda Caldera
School of Information Studies
Syracuse University
ccaldera@syr.edu

Abstract – *Several new lines of research have begun to focus on a sociotechnical approach to information security by simultaneously considering the behavioral and managerial elements of security together with the technical aspects. In this paper, we examine the influence of organizational commitment on some aspects of security behavior in organizations.*

Keywords: Information security, organizational behavior, management, job attitudes.

1. Introduction

Over recent decades work organizations have come to depend on IT for operations, external transactions, and mediated communications (e.g., email). As connectivity among devices has increased, so has the likelihood of intrusion, theft, defacement, and other forms of information resource loss. Surprisingly, although organizations tend to be very concerned about vulnerability to external attack, recent industry research by Ernst and Young [5] suggests that more than three-quarters of security breaches result from activity within organizations. At the low end, losses from security breaches cost approximately \$20 billion per year across all U.S. organizations [11]. These losses have spurred increased spending on information security specialists and technology: According to a 2002 industry survey by Information Security Magazine, very large organizations spend an average of \$6 million per year apiece on information security. Smaller organizations spend on average nearly 20% of their overall information technology budgets on security related products. This ocean of cash has spawned a large new sub-industry dedicated to the design, development, and marketing of security-related devices such as firewalls, biometrics, and security scanners.

Product development in this new sub-industry has received intellectual backing from academic research

programs on cryptography, public key infrastructure, watermarking, access control, intrusion detection, and related topics. The CiteSeer automated indexing facility (<http://citeseer.nj.nec.com>) lists more than 10,000 academic science and engineering articles related to information security. Computer scientists, network engineers, information technology specialists and others have worked diligently over past decades to develop solutions for fundamental information security problems: how to restrict information resource access to authorized individuals, how to transmit and receive information privately, how to keep public information accurate and available in the face of malicious intrusion, and so forth [20]. The list of accomplishments in these areas is long, and many of these developments have resulted in positive business, economic, and societal outcomes [4].

A constraint appears in all these efforts, however, in the form of the human behavior of those who access, use, administer, and maintain information resources. The success of information security appears to depend in part upon the effective behavior of the individuals involved in its use. Appropriate and constructive behavior by end users, system administrators, and others can enhance the effectiveness of information security while inappropriate and destructive behaviors can substantially inhibit its effectiveness. Human behavior is complex and multifaceted, and this complexity defies the expectations for control and predictability that developers routinely assume for technology. As the Organisation for Economic Co-Operation and Development's [8] Guidelines for the Security of Information Systems states, "The diversity of system users—employees, consultants, customers, competitors or the general public—and their various levels of awareness, training and interest compound the potential difficulties of providing security." Even this statement belies a certain system-centric view of security: Security is something that is *provided* (ostensibly by technology)

rather than something that is *enacted* by users and system administrators.

The present research takes a different perspective on this topic by focusing on “behavioral information security:” the complexes of human action that influence the availability, confidentiality, and integrity of information systems. Our goal for this study was to examine the extent to which information security behaviors related to a common job attitude variable known as organizational commitment. This variable has known positive linkages to job performance and citizenship behavior and negative linkages to counterproductive workplace behaviors such as theft. We hypothesized that organizational commitment would relate positively to the enactment of beneficial information security behaviors such as regularly changing passwords and following acceptable use policies.

2. Behavioral Information Security

Most research on information security focuses on algorithms, methods, and standards that support the four basic functions of information security: confidentiality, integrity, availability, and non-repudiation. In addition to this basic research in computer science and mathematics, human factors experts have worked to simplify and rationalize the user interfaces of security-related systems. Likewise, management experts have analyzed business risks associated with information systems and have drafted organizational policies to cope with these risks. We believe that an important missing layer in this assortment of approaches lies between the human-computer interface and the business-level concerns of management. In particular, we believe that information security research presently gives too little attention to the antecedents of behavior in organizations.

As an example, despite the ready availability of encrypted email products as well as ubiquitous organizational policies decreeing the importance of secure communications, relatively few individuals and few organizations use such products. Each research camp might offer a plausible explanation: Technologists might lament the lack of a widely accepted industry standard, human factors scientists might criticize the user interfaces for securing email as too complex and counterintuitive, and management scholars might say that the risk of costly disaster has historically been too low to bother enforcing the relevant security policies.

The behavioral information security perspective would offer a different scenario: Workers find the use of encrypted email very inconvenient, particularly in light of the fact that they are under pressure to get a lot of work accomplished without delays. Additionally, workers see

little information of value in their routine correspondence and in those rare cases when there is a sensitive message to pass, a phone call or face-to-face meeting can suffice. Finally, the worker sees that even top management never uses the secure email function, never mentions it as a high priority to the organizational mission, never offers training on its use, and never rewards those few workers who use the feature diligently. In *Secrets and Lies*, Bruce Schneier [9] says, “Mathematics is logical; people are erratic, capricious, and barely comprehensible.” On the contrary, our encrypted email example suggests that behavior is understandable, organized, and laden with meaning both for those who enact it and those who try to make sense of it.

Researchers have long used this foundational assumption as the basis for understanding and influencing behavior in organizations; a few have even begun to take tentative steps toward applying research in organizational behavior to information security problems. For example, Straub [17] investigated the impact of sanctions and other forms of obtaining compliance in organizations to ascertain the extent to which the severity and certainty of sanctions would influence “computer abuse.” This early effort preceded a new line of research on counterproductive computer usage that has included projects by Loch & Conger [6]; Armstrong, Phillips and Saling [3]; Stanton [15]; Morahan-Martin and Schumacher [7]; and others.

Interestingly, these projects and related work on the “insider threat” to information security (e.g., Anderson et al. [2]; Schultz, [10]; Shaw, Post, & Ruby, [12]) have all tended to focus on the intentionally disruptive behavior enacted by a small proportion of the workers in any given organization.

The few exceptions to this focus on troublesome actions have included examinations of the importance of user awareness and training (e.g., Spurling, [15]; Thompson & von Solms, [18], [19]), and analyses of the ethical guides that may influence security related behavior (e.g., Siponen, [13]; Trompeter & Eloff, [14]). We believe that projects like these hold substantial promise for helping to shift research away from the common assumption that workers are wrongdoers whose behavior must be carefully circumscribed. In contrast to that common assumption, our own research, as described below, explored positive and negative security-related behaviors.

3. Method

We conducted two studies, one involving 110 interviews with managers, information technology professionals, and regular employees, and another that comprised a survey of 298 workers and managers who routinely used IT on the job.

From the transcripts of the first study's interviews, we compiled a list of 94 security related behaviors. Ten subject matter experts (graduate students and faculty in information science) sorted these behaviors into self-generated categories. Fifty additional subject matter experts confirmed the predominant categorization scheme developed by the initial group of experts. This categorization scheme formed a six-element taxonomy of security behavior that varied along two dimensions: intentionality and technical expertise.

The intentionality dimension appeared to capture whether the behavior described was intentionally malicious, intentionally beneficial, or somewhere in between (i.e., absent explicit intention to help or harm). The technical expertise dimension focused on the degree of computer or information technology knowledge and skill that the actor needed to have in order to perform the behavior described on the card. Three of the six categories were considered low technical expertise behaviors and the other three were considered high technical expertise behaviors.

In the subsequent survey study, we focused on asking respondents who were not security professionals only about behaviors that required low technical expertise (e.g., choosing a hard to guess password). We focused on these low expertise behaviors in the hope that these would be high base rate behaviors and therefore more susceptible to prediction. We included a mix of nine different positive and negative security-related behaviors including three different types of counterproductive computer usage, poor password management practices, taking security training when offered, discussing security policies with coworkers and abiding by acceptable use policies.

The survey study randomly sampled 800 employed adult participants from the StudyResponse Project online panelist service (<http://www.StudyResponse.org>). Given the 298 usable responses we obtained, this procedure yielded a response rate of 37.25%. Post hoc demographic comparisons revealed only minor differences between respondents and non-respondents on age and other demographic variables.

Participants completed a brief survey that included a measure of organizational commitment (Allen & Meyer, 1990), demographic data, and a sample of nine of the low technical complexity behaviors from our security behavior list. We inquired about these behaviors in two different ways. First, we asked respondents about their own behavior, then we asked them to report the typical behavior of their coworkers.

4. Results

Before starting our substantive analysis we used simple regression procedures to reallocate the variance in the two sets of behavioral measures. Specifically we regressed "other" behavior on "self" behavior and saved the predicted and residual values from this analysis. The predicted value from each analysis represented the variance that the self and other behaviors had in common. Thus, this measure captured behavior that was consistent between the respondent and the typical coworker. The residual from this analysis represented the variance in self-reported behavior that was unique to the respondent (i.e., that did not correspond with the behavior of a typical coworker).

Dividing behavior in common and unique components provides a useful perspective into organizational behavior because of the influence of organizational climate, culture, and environment on worker behavior. In all organizations, prevailing conditions such as management style, economic health of the organization, and industry norms all exert common influences on workers. To the extent that certain resultant behaviors occur similarly across multiple workers, we can attribute at least part of the cause of these behaviors to environmental factors. The remaining variance in behavior can be attributed to personal motivating factors including stable influences (e.g., dispositional factors such as conscientiousness) and transient influences (e.g., personal finances).

To test the influence of organizational commitment on common and unique behaviors we conducted a MANOVA analysis with common and unique behaviors as the dependent variables, gender and supervisory status as control variables, and organizational commitment as the predictor variable. We wanted to control for gender and supervisory status so that these variables did not interfere with the interpretation of the relations between organizational commitment and behavior. Although it would not be unreasonable to expect gender differences or differences between managers and non-managers on security behaviors, such differences were beyond the scope of the present study. Supervisory status was operationalized as the number of direct reports to the respondent. Presumably, a higher number of direct reports corresponded to greater supervisory responsibilities. Gender was coded dichotomously and was missing on three cases.

The omnibus test for the effect of organizational commitment on behavior was statistically significant, Wilk's Lambda = .791, $F(18,255) = 3.75$, $p < .001$. The omnibus test for supervisory status was also statistically significant, Wilk's Lambda = .854, $F(18,255) = 2.42$, $p = .001$. The omnibus effect of gender was not statistically significant. Table 1, below, shows the detailed results of the MANOVA. For each behavior we show the unstandardized coefficient (like a B-weight in multiple regression) as well as the partial eta-squared value, which is a standardized measure of effect size.

Table 1: MANOVA Results for the effects of organizational commitment on low skill security-related behaviors

Behavior	Common		Unique	
	B-Weight	Eta ²	B-Weight	Eta ²
Reveal password	.05	.01	.07	.00
Write password	.06	.02*	.07	.00
Password training	.11	.02*	-.07	.00
Personal web surfing	-.09	.02*	.08	.00
Personal email	-.09	.04*	.09	.00
Personal gaming	-.12	.05*	.20	.02*
Acceptable use training	-.06	.05*	.08	.01
Discuss acceptable use	.08	.01	.14	.02*
Abide by acceptable use	-.06	.02*	-.18	.03*

Note: Eta-squared values marked with an asterisk show effect sizes statistically significantly different from 0, $p < .05$ or better.

Results depicted in Table 1 show that organizational commitment successfully predicted seven out of nine of the common behaviors, but only three out of nine unique behaviors. The negative sign of the B-weight on three common counterproductive behaviors (using company computers for personal web surfing, personal email, and personal gaming) suggests that individuals with higher levels of organizational commitment are less likely to engage in these behaviors. Interestingly, however, results surrounding acceptable use policies ran counter to expectations: Those with lower levels of organizational commitment tended to report higher levels of compliance with acceptable use policies.

Note that the MANOVA procedure intrinsically corrects for study-wise inflation of alpha, so the large number of significance tests did not capitalize on chance. All of these partial eta-squared values constitute small effect sizes, but it is important to note that these values represent the unique variance attributable to a single predictor (organizational commitment) over and above any common variance with supervisory status or gender. On both counts, the MANOVA and associated weights and effect sizes comprise a conservative test of the relation between organizational commitment and these behaviors.

5. Conclusions

The goal of the present study was to assess whether a familiar and ordinary job attitude variable, organizational commitment, would demonstrate any significant relations with a variety of information security-related behaviors. Our list of nine behaviors emerged from an initial qualitative study in which we elicited and classified a large list of security related behaviors. For the present study, we focused on good and bad security-related behaviors from our list that required minimal technical

skills (such as using company computers for personal game playing and abiding by company acceptable use policies). We focused on these because of the likelihood that these low skill behaviors could be routinely enacted by non-technical organizational members such as rank and file workers, managers, and supervisors.

Our results showed that organizational commitment does predict a range of security-related behaviors, albeit with relatively small effect sizes. One intuitively appealing result that emerged suggested that people in an organization may be less likely to enact counterproductive computer behaviors that put company systems at risk if their organizational commitment is high. For those individuals whose organizational commitment is high, they may be spending more time on productive work activities and thus have less time for personal web surfing and related non-productive or counterproductive computer uses. Alternatively, those with high organizational commitment may take seriously the admonition often heard from technical personnel that using company systems for personal gaming, chat, or instant messaging puts systems at risk from malware. Other explanations are possible as well, because these data did not lend themselves to ascertaining causal relations for the observed effects.

Our results also showed a counterintuitive result with respect to acceptable use policies. Specifically, those with high levels of organizational commitment reported lower degrees of compliance with acceptable use policies both by themselves and by co-workers. This result raises a number of interesting possibilities. First, it is possible that organizations that engender high commitment differ in some way from those that do not. For instance, an organization that worked hard to ensure employee loyalty and commitment might have less need to routinize, publicize, and enforce acceptable use policies than other organizations. In contrast, an organization that was experiencing problems with employee loyalty or commitment might have no choice but to strongly emphasize the criticality of abiding by acceptable use policies.

Another alternative on a more individualistic level might reflect a psychological process called reaction formation. When individuals have rules imposed upon them, with a concomitant reduction in personal choice, they often form a negative reaction to the restriction and work to overcome it. It is possible that individuals with high levels of organizational commitment consider themselves entitled to substantial freedom of action and resent the imposition of acceptable use policies upon them.

Regardless of the speculative explanation that one adopts for these results, our survey study suggests that job attitude variables may provide a useful set of predictors for information security-related behaviors. Future research

should explicitly adopt a motivational framework for understanding and predicting security-related behaviors that incorporates job attitudes as predictor constructs. In this way, research on behavioral information security can continue to uncover the sociotechnical elements of information security in organizations. Based on the results of the present study, understanding behavior as it relates to information security practices seems like a fruitful complement to purely technical approaches.

Results of the present study should be interpreted in light of the strengths and weaknesses of our research methods. First, neither our interview study nor the survey included direct observations of security related behaviors. Instead, in the interview study we relied on the reports of information security professionals and others to derive our list of relevant behaviors. In the survey study, we relied upon self reports of job attitudes and behaviors. Self reports are always subject to some distortion from events or behaviors as noted by an observer. Second, both the interview and survey studies were cross-sectional, that is, all data were collected from each respondent at a single point in time. For this reason and others, one may not learn much if anything about the causal precedence of variables we examined.

Offsetting these limitations, we obtained large and diverse samples of respondents, thereby ensuring that a wide range of organizations and personal perspectives were represented. The great variety of ideas and behaviors described in the interview transcripts and the substantial variability of all quantitative measures both suggest that we succeeded in tapping a range of attitudes and behaviors. Further, there was systematic concordance between the two studies: The security-related behaviors described by security professionals and others in the interview study were reported as frequent occurrences in actual organizations (as determined by respondents' reports of self and other behavior on the survey). Finally, by linking a reliably measured, familiar job attitude variable to these behaviors, we demonstrated an attitude-behavior linkage that serves as a proof-of-concept for the behavioral information security approach. Together, these strengths and weaknesses suggest that the present study provides a useful stepping-stone to future behaviorally oriented research on information security and that the use of job attitudes within an appropriate motivational framework may provide substantial utility in understanding and predicting information security-related behaviors.

References

- [1] Allen, N.J., & Meyer, J.P. (1990). The measurement and antecedents of affective, continuance and normative commitment to organizations. *Journal of Occupational Psychology*, 63, 1-18.
- [2] Anderson, R. H., Feldman, P. M., Gerwehr, S., Houghton, B., Mesic, R., Pinder, J. D., Rothenberg, J., & Chiesa, J. (1999). *Securing the U.S. defense information infrastructure: A proposed approach*. Washington, DC: Rand.
- [3] Armstrong, L., Phillips, J. G., & Saling, L. L. (2000). Potential determinants of heavier Internet usage. *International Journal of Human-Computer Studies*, 53 (4), 537-550.
- [4] Dhillon, G. (Ed.) (2001). *Information security management: Global challenges in the new millennium*. Hershey, PA: Idea Group Publishing.
- [5] Ernst and Young LLP. (2002) *Global Information Security Survey*. Published in the UK by Presentation Services.
- [6] Loch, K. D., & Conger, S. (1996). Evaluating ethical decision-making and computer use. *Communications of the ACM*, 39(7), 74-83.
- [7] Morahan-Martin, J., & Schumacher, P. (2000). Incidence and correlates of pathological Internet use among college students. *Computers in Human Behavior*, 16 (1), 13-29.
- [8] OECD (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Organisation For Economic Co-Operation And Development. Available at: <http://www.oecd.org/pdf/M00033000/M00033182.pdf>.
- [9] Schneier, B. (2000). *Secrets and Lies*. New York: Wiley.
- [10] Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers and Security*, 21 (6), 526-531.
- [11] Security Wire Digest. (2000, March 27) *CSI/FBI study says: Security breaches on the rise*. Author. Available: http://www.lexias.com/1.0/securitywiredigest_27MAR2000.html
- [12] Shaw, E. D., Post, J. M., & Ruby, K. G. (2002). *Inside the Mind of the Insider*. Available at: <http://www.securitymanagement.com/library/000762.html>.
- [13] Siponen, M. T. (2001). On the role of human morality in information systems security. *Information Resources Management Journal*, 14 (4), 15-23.
- [14] Trompeter, C. M., & Eloff, J. H. P. (2001) *A Framework for the Implementation of Socio-ethical*

Controls in Information Security. *Computers & Security*, 20, 384-391.

[15] Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3 (2), 20-26.

[16] Stanton, J. M. (2002). Company profile of the frequent Internet user: Web addict or happy employee? *Communications of the Association for Computing Machinery*, 45 (1), 55-59.

[17] Straub, D.W. (1990). Effective IS security: an empirical study. *Information System Research*, 1 (2), 255-277.

[18] Thomson, M.E. and von Solms, R. (1997). An effective information security awareness program for industry. Proceedings of the WG 11.2 and WG 11.1 of the TC11 IFIP.

[19] Thomson, M.E. and von Solms, R. (1998). Information security awareness: educating our users effectively. *Information Management & Computer Security*, 6 (4), 167-173.

[20] Won, D. (Ed.) (2001). Proceedings of the Third International Conference on Information security and cryptology (ICISC 2000), Seoul, Korea, December 8-9, 2000. Berlin: Springer.