

Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices

Jeffrey M. Stanton
Syracuse University
jmstanto@syr.edu

Paul R. Mastrangelo
Genesee Survey Services, Inc.
paul.mastrangelo@gensurvey.com

Kathryn R. Stam
Syracuse University
krstam@syr.edu

Jeffrey Jolton
Genesee Survey Services, Inc.
jeff.jolton@gensurvey.com

ABSTRACT

Information security is a multibillion-dollar problem faced by commercial and government organizations around the world. Through their adverse effects on organizational information systems, malware, hackers, and malicious insiders jeopardize organizations' capabilities to pursue their missions effectively. Although technology-based solutions help to mitigate some of the many problems of information security, even the best technology cannot work successfully unless the people in organizations do the right thing. In two national survey studies (N=1167 and N=298) we explored some of the motivational antecedents surrounding the practices of information security by end users. Results revealed that organization type, job role, job satisfaction, and organizational commitment each showed relations to some key security behaviors of end users.

Keywords

Information security, organizational behavior, motivation.

INTRODUCTION

Over recent decades, most work organizations have come to depend on information technology. As connectivity among computers has increased, so has the likelihood of intrusion, theft, defacement, etc. Surprisingly, although organizations sometimes focus more on vulnerability to external attack than internal, recent industry research by Ernst and Young (2002) suggests that over 75% of the cost of security failures results from insider activity. Computer scientists, network engineers, information technology specialists and others have developed technological solutions for these information security problems (e.g., Won, 2001), and a large industry of software and hardware development is dedicated to the design and marketing of security-related devices such as firewalls and biometrics.

Many of these developments have resulted in positive business and economic outcomes (Dhillon, 2001), but a constraint appears throughout in the behaviors of the human agents who access, use, administer, and maintain information resources. The success of security appears to depend 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 inhibit its effectiveness. As the Organisation for Economic Co-Operation and Development's (OECD, 2002) 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."

The present research focuses on the human actions that influence the confidentiality, integrity, and availability of information systems. In the present research, the authors have investigated these behaviors and their motivational antecedents by conducting two survey studies of end user behavior. The first study, a survey study of organizational factors and security behaviors, was exploratory, so we intentionally defer our introduction of theory until the introduction of Study 2.

STUDY 1

Overview

Most research on information security focuses on algorithms, methods, and standards that support the three basic functions of information security: confidentiality, integrity, and availability. 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 motivational 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, few individuals and few organizations appear to use such products on a regular and consistent basis. 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 serious pressure to get a lot of work accomplished without delays. Additionally, the 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 will suffice commendably. 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 (2000) says, "Mathematics is logical; people are erratic, capricious, and barely comprehensible." On the contrary, the above example suggests that behavior is understandable, organized, and laden with meaning both for those who enact it and those who work at making sense of it. Researchers have long used this foundational assumption as the basis for developing theory and practice 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 (1990) 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 line of research on counterproductive computer usage that has included projects by Loch and Conger (1996); Armstrong, Phillips and Saling (2000); Stanton (2002); Morahan-Martin and Schumacher (2001); and others.

Interestingly, these projects and related work on the "insider threat" to information security (e.g., Anderson et al. 1999; Schultz, 2002; Shaw, Post, and Ruby, 2002) have focused primarily on the highly disruptive behavior enacted by one or more "rogue" workers in an organization. For our research, we wished to focus on both positive and negative security behaviors that an individual worker might enact. Thus, we used a comprehensive list of 91 end user security-related behaviors compiled by Stanton et al. (2003) as a starting point for our investigation. Stanton et al. uncovered six areas of security related behavior arranged on a grid that represented different motivations and different skill levels involved in the behavior. For the present study we focused on the positive or benign security-related behaviors that could be enacted by employees who did not possess specialized security training (e.g., regularly changing passwords). Because little research exists on the base rates of these behaviors in organizations, we determined that an important next step would be to assess the behaviors in a large-scale, national survey and to screen the behaviors against a set of organizationally relevant predictors. At the conclusion of the study we expected to ascertain a set of patterns relating personal and organizational factors to security behaviors that we could then use as a basis for selection of a theoretical framework.

Method

Each year, Genesee Survey Services, a consulting firm based in Rochester, NY, conducts a nationwide study of U.S. workers from a variety of industries. The National Work Opinion Survey (NWOS) serves as a source of normative data on measures of organizational concern including job security, employee retention, workload, compensation, benefits, organizational support, and job satisfaction as well as a variety of other areas. The NWOS is distributed by postal mail to a random sample of U.S. employees (using a professionally compiled sampling frame) along with a postage paid return envelope. In addition, in recent years the NWOS has been administered to a portion of the sample via the Web.

The 2003 version of the NWOS included nine new and original items customized for the present study based on the list of security-related behaviors from Stanton et al. (2003). The NWOS sample comprised regular managers and employees, so we only sampled from the "novice" items in our taxonomy because we expected relatively few information individuals with professional security training in the sample. We used three items pertaining to password management (e.g., frequency of changing the password), three items pertaining to password sharing (e.g., sharing with others in the work group) and three items pertaining to organizational support of security-related behaviors (e.g., "My company/org. provides training programs to help employees improve their awareness of computer and information security.").

The NWOS was distributed to N=4000 individuals and N=2011 usable surveys were returned for a response rate of approximately 50%. The survey was offered in several versions, and not all of the versions contained the customized items. After accounting for these variations and missing data we had N=1167 surveys with usable data on the security-related items.

Results

We reduced the standard NWOS predictor items to a nine-factor structure using analytical procedures provided by Genesee Survey Services. The factors mapped onto common organizational constructs, contained between three and 10 items, and provided alpha reliability estimates ranging from .70 to .92. Six satisfaction factors included satisfaction with the work itself, satisfaction with coworkers, satisfaction with immediate supervision, satisfaction with pay, and satisfaction with organizational support services (e.g., employee training). Remaining factors included trust in top management, tolerance for diversity, and clarity of mission and goals. The NWOS also captures information about the respondent's organization and demographics. We screened these organizational and demographic variables as possible predictors.

We factor analyzed the security-related items using a principal components extraction and varimax rotation. The results suggested three factors with eigenvalues in excess of 1.0, item loadings above .33 on each factor, and no sizeable cross-loadings. The breakdown of items reflected our original intentions for the items: three items indicating password sharing ($\alpha = .67$), three items indicating organizational support of security-related behaviors ($\alpha = .77$), and three items indicating password management ($\alpha = .56$). This low value of alpha led us to remove an item pertaining to writing down one's password, and this increased that latter alpha reliability estimate to .68. We analyzed the password-writing item separately. Scale scores for each multi-item scale were constructed by computing the mean across all items comprising that scale.

Next we conducted analyses to explore the effects of 1) organizational circumstances, 2) personal demographics, and 3) job attitudes on the outcomes. We used the multivariate analysis of variance (MANOVA) because the four dependent variables in the analysis were intercorrelated to a modest degree. Statisticians recommend MANOVA in such cases because it avoids inflation of the study-wise Type I error rate. In the first analysis we used MANOVA to examine effects of geographic location, size of company, and type of industry on password management, password writing, password sharing, and organizational support for security. Multivariate results indicated that company size, Wilk's lambda = .88, $F(40,1894)=1.5$, $p<.05$, and company type, Wilk's lambda = .88, $F(56,1943)=1.8$, $p<.05$, had statistically significant effects on the outcomes. Wilk's lambda is a summary statistic that ranges from 0 to 1 and is similar to a coefficient of alienation.

Table 1 details univariate tests on each factor. Results showed that employees in larger organizations reported better password management practices (more frequent password changing and selection of stronger passwords); employees from the military, financial institutions, and telecommunications/Internet companies reported better password management practices than employees in other organization types; and more security support was perceived in the military and public utilities than in other organizations. We also examined demographic factors: Multivariate tests revealed that job type, job tenure, union membership, age, and income level had statistically significant effects on the outcome variables, with Wilk's lambda values ranging from .95 (job type) to .99 (union membership; see Table 1 for univariate effects). Administrative personnel, managers, and technicians reported better password management than other job types, but administrative support personnel, managers, first level supervisors, and sales/management personnel also tended to share their passwords with others more frequently than those in other job types. Individuals with longer service reported greater organizational support for secure behaviors (e.g., availability of training). Union members reported slightly less favorable password management practices than those not in unions. Those with higher incomes reported better password management practices and less password sharing than those with lower incomes.

Table 1: Summary of Study 2 Results: Significant Univariate F-tests from MANOVA

Outcome	Predictor Variable	Univariate F-test
Organizational Support for Security	Job Tenure	$F(5, 854)=4.1, p<.001$
	Organization Type	$F(14,502)=2.2, p<.01$
Password Management	Company Size	$F(10, 502)=2.2, p<.05$
	Organization Type	$F(14,502)=3.5, p<.001$
	Job Type	$F(7,854)=2.1, p<.05$
	Income Level	$F(4, 854)=7.3, p<.001$

Outcome	Predictor Variable	Univariate F-test
	Union Membership	F (1, 854)=6.5, p<.05
Password Sharing	Job Type	F (7, 854)=2.3, p<.05
	Income Level	F (4, 854)=2.6, p<.05

Finally, we ran regression models using demographic and organizational factors as controls (some of which were dummy coded), job attitudes as predictors, and the three password behaviors as dependent variables. Using eight control variables and eight job attitude predictors, all three regressions were statistically significant, as shown in Table 2. Regression diagnostics showed no problems with multicollinearity. The pattern of significant weights for the controls largely accorded with the MANOVA results, so in the interest of brevity Table 2 only displays significant weights for the attitude predictors. Note that the relatively small beta weights reflect the unique variance explained by the predictors over and above the large set of control variables. An interpretation of these results appears below as part of the introduction to Study 2.

Table 2: Summary of Regression Analyses for Study 2

Outcome Variable	Overall F-Test	Predictors (Beta Weights)		
		Satisfaction with Support Services	Pay Satisfaction	Coworker Satisfaction
Password management	F(16,1089)=8.3***	.09*		
Password writing	F(16,1089)=3.9***	-.16*	.08*	
Password sharing	F(16,1089)=2.7***			.11*

STUDY 2

Introduction

Results from Study 1 indicated significant findings for organizational, demographic, and a few attitudinal factors. Individuals in organizations that had “a lot at stake” (e.g., the military, or financial institutions) appeared to have received the training, tools, and incentives needed to enact more effective information security behavior. Likewise, many individuals with longer job tenure and higher incomes may have had substantially more “personal investment” in the organization than those with lower incomes or a shorter history with the organization. As shown in Table 2, an organization that provides supports for people to perform their jobs seems to offer some advantages with respect to the effectiveness information security. In contrast, however, those individuals with greater satisfaction with pay and coworkers seem to have less effective password management habits. In reviewing these results, we were struck by the need for a research framework that considered organizational/environmental factors, personal perceptions about the work environment, and organizational commitment in a unified story that explained productive and counterproductive behaviors associated with information security.

Several available theoretical perspectives explain and predict workplace behaviors with these types of factors. For example, Spector and Fox (2002) recently proposed an integrated model of organizational citizenship behavior (OCB) and counterproductive workplace behavior (CWB) that used affective constructs to provide an unitary mechanism governing both classes of behavior. Organizational citizenship behavior refers to the activities that workers perform that go above and beyond the normal call of duty. Counterproductive workplace behavior refers to those activities – generally not illegal but usually counter to policy – that adversely impact the overall effectiveness of the organization. Spector and Fox centered their model on emotional experiences in the workplace: the good and bad experiences at work that may have strong influences on workers’ attitudes and behavior. These researchers described some of the common antecedents of CWB and OCB, including organizational constraints, role stressors, interpersonal conflict, organizational justice, and psychological contract issues. These researchers also initiated a discussion of the state- and trait-based affective mechanisms that activate OCB and CWB in response to antecedent events. An empirical test of their model supported a number of their primary propositions (Miles, Borman, Spector, and Fox, 2002). Although their framework was not specifically designed for security-related behaviors, we were struck by the similarity of security-related behaviors to OCB, in the case of activities such as good password management, and CWB in the case of activities such as downloading illegal software to workplace computers. Additionally, Spector and Fox’s antecedent model for predictors of OCB and CWB seemed to share much in common with the predictors that succeeded in Study 1.

Thus, for Study 2, we adopted the Spector and Fox (2002) unified framework for OCB and CWB, with positive security behaviors equated with OCB and negative security behaviors equated with CWB. Given the model's attention to both positive and counterproductive behaviors we consequently expanded our outcome measures to include the use of games, chat, and instant messaging (behaviors frequently prohibited by acceptable use policies). We also queried respondents about the avoidance of personal web surfing and email at work. We adopted a subset of the predictors prescribed by the Spector and Fox (2002) model, including organizational commitment and negative emotional events at work. In addition, we queried respondents' technical knowledge (of computers, software, etc.) and the degree of their managerial responsibilities. We hypothesized that organizational commitment would facilitate the performance of positive security behaviors and inhibit the performance of negative security behaviors. We hypothesized that negative emotional events would have the opposite effect. We further hypothesized that individuals with more technical knowledge of computers would perform more positive security behaviors and that individuals with more substantial managerial responsibilities would do so as well.

Method

As in Study 1, we focused on asking about novice behaviors (e.g., choosing a hard to guess password). We included a mix of nine positive and negative security-related behaviors including three 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 randomly sampled 800 employed adults from the StudyResponse panelist service (<http://www.StudyResponse.org>). We intentionally sampled individuals who reported their jobs as *not* in the military, utilities, financial institutions, or telecom so that we would not need to control for organization type. Given the 298 usable responses we obtained, this procedure yielded a response rate of 37.25%. We dropped N=24 respondents from the sample who reported never using a computer on the job. StudyResponse provided demographic comparisons between respondents and non-respondents that revealed slight differences on age and gender: Women and older individuals were slightly more likely to respond. We did not believe that this small degree of non-response bias would affect the substantive conclusion of our study because we had no evidence from Study 1 that gender or age mattered with respect to the focal variables. Participants completed a brief, web-based survey with measures of organizational commitment (Allen and Meyer, 1990), assessments of negative emotional events at work (Miles, Borman, Spector, and Fox, 2002), a count of the number of individuals supervised, a self assessment of technical knowledge, demographic data, and a sample of nine of the novice behaviors from our security behavior list.

Results

Factor analysis of the criterion items produced conflicting results depending upon the extraction, so we opted to conduct MANOVA tests with the nine behaviors as separate dependent variables. Note that using the individual items in the analysis precluded the need for creating composite scale scores. Multivariate results indicated that organizational commitment, negative emotional events, technical knowledge, and number of supervisees all significantly related to at least one of the criterion behaviors with Wilk's lambda values ranging from .87 to .93. Table 3 reports univariate tests showing that greater organizational commitment, fewer negative emotional events, more technical knowledge, and more management responsibilities associated positively with productive security-related behaviors and negatively with counterproductive security-related behaviors. Interestingly, none of these predictors related to two of the criterion behaviors that we examined in Study 1 (password sharing and writing down passwords).

Table 3: Summary of Study 2 Results. Univariate Tests from MANOVA

Outcome Variable	Predictor	Univariate F-test
Abiding by acceptable use policies	Organizational Commitment	F(1,255)=6.2, p=.01
	Span of Control	F(1,255)=10.6, p<.001
Avoiding personal web surfing at work	Technical Knowledge	F(1,255)=6.0, p<.05
Avoiding use of personal email at work	Technical Knowledge	F(1,255)=6.0, p<.05
Choosing to obtain password training	Technical Knowledge	F(1,255)=16.6, p<.001
Counterproductive security behaviors	Negative Emotional Events	F(1,255)=5.6, p<.05
	Organizational Commitment	F(1,255)=5.4, p<.05

Outcome Variable	Predictor	Univariate F-test
Discussing acceptable use policies with coworkers	Organizational Commitment	F(1,255)=6.2, p<.01
	Span of control	F(1,255)=7.8, p<.01

OVERALL DISCUSSION

Recall that our goal with this research was to investigate end-user security behaviors and their motivational antecedents by conducting two national survey studies. Study 1 provided an initial overview of organizational, demographic, and attitudinal factors that predicted the novice behaviors that security professionals consider essential in the end-user's behavioral repertoire: good password management, avoiding sharing of passwords, and obtaining awareness training. Study 2 made an initial pass at applying a theoretical framework onto the criterion behaviors with the intention of choosing predictor variables on a rational basis and developing a framework suitable for future research in this area. Taken together, the two studies did suggest that security-related end user behaviors relate to a combination of relevant situational and personal factors. We believe that these findings support our essential belief that examining the motivational antecedents of information security behavior may prove productive in improving information security within organizations. The potential seems to exist for a variety of practitioner interventions that could influence the enactment of security-related behaviors.

With respect to the substance of our findings, Study 1 raised a number of new questions that Study 2 did not adequately answer. The predictive value of demographic characteristics (e.g., income level) translated adequately into organizational commitment when examined in light of the Spector and Fox model. That is, individuals with longer job tenure and those at a higher level in the hierarchy generally have higher organizational commitment. The results for *type* of organization, however, suggests that this variable must operate as a proxy for other variables of interest. For instance, in some or many military organizations a culture may exist in which the value of information security is continually reinforced through everyday practices, training, and socialization. Similar factors may be at work in financial institutions and utilities, given the overall criticality of their missions.

Unfortunately, the Spector and Fox model does not seem well suited to capture the essence of these "positive security cultures." That model's focus on each individual's positive and negative emotional workplace events and the subsequent behavioral outcomes (OCB and CWB) emphasizes the influence of *unique personal experiences* at work rather than those factors that are shared across a variety of people (e.g., culture, norms, customs, standard practices, etc.). What may be needed here is a theoretical perspective that can explain the importance of common situational influences on behavior that arise in particular organizational settings. As an example, when one contrasts banking – known for its "cultural" emphasis on information security – with university environments, which are known for their openness, the importance of situational influences on security behaviors seems evident. Additionally, Study 1 suggested that particular occupational roles seem to influence the enactment of security-related behaviors. One's status as a manager, an administrator, a supervisor, or a technician seemed to impact the pattern of security related behaviors. Together, these results suggest that some practical opportunities for improving security may lie in changing the culture of the organization (e.g., trying to shift universities into a more secure cultural mindset) and in changing workers' beliefs about the importance of security in their particular job roles (e.g., emphasizing the importance of security even in the most basic, entry level administrative assistant position). Naturally, there are limits to such changes: No university can operate like a bank and few administrative assistants routinely think like information security specialists. Nonetheless, there is probably sufficient latitude for change in many organizations such that well-designed organizational development interventions and training programs could have positive benefits for security.

In our upcoming work on this research program we plan to refine our guiding theory to explicitly incorporate ideas of culture and occupations into our existing theoretical framework. One possibility lies in Trice's (1993) ideas about occupational subcultures. Trice posited the existence of definable subcultures within organizations characterized by unique sets of norms, shared meanings, and shared identities based on occupational roles. As the data from study 2 apparently suggest, the organization, the occupation, and the personal experiences of organizational actors seem to jointly influence the enactment of security-related behaviors. Building on these studies, we hope to advance the application of social science to problems of information security such that social and organizational researchers can contribute practical solutions that improve the information security of contemporary organizations.

REFERENCES

1. Allen, N.J., and Meyer, J.P. (1990). The measurement and antecedents of affective, continuance and normative commitment to organizations. *Journal of Occupational and Organizational Psychology*, 63, 1-18.

2. Anderson, R. H., Feldman, P. M., Gerwehr, S., Houghton, B., Mesic, R., Pinder, J. D., Rothenberg, J., and Chiesa, J. (1999). *Securing the U.S. defense information infrastructure: A proposed approach*. Washington, DC: Rand.
3. Armstrong, L., Phillips, J. G., and 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*. London: Presentation Services.
6. Loch, K. D., and Conger, S. (1996). Evaluating ethical decision-making and computer use. *Communications of the ACM*, 39 (7), 74-83.
7. Morahan-Martin, J., and Schumacher, P. (2000). Incidence and correlates of pathological Internet use among college students. *Computers in Human Behavior*, 16 (1), 13-29.
8. Mangione, T. W., Quinn, R. P. (1975). Job satisfaction, counterproductive behavior, and drug use at work. *Journal of Applied Psychology*, 60:114-116.
9. Miles, D. E., Borman, W. E., Spector, P. E., and Fox, S. (2002). Building an integrative model of extra role work behaviors: A Comparison of counterproductive work behavior with organizational citizenship behavior. *International Journal of Selection and Assessment*, 10: 51-57.
10. Organisation for Economic Co-Operation and Development (2002). *Guidelines for the Security of Information Systems*. Available at: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.
11. Schneier, B. (2000). *Secrets and Lies*. New York: Wiley.
12. Shaw, E. D., Post, J. M., and Ruby, K. G. (2002). *Inside the Mind of the Insider*. Available at: <http://www.securitymanagement.com/library/000762.html>.
13. Spector, P. E., and Fox, S. (2002). An emotion-centered model of voluntary work behavior: Some parallels between counterproductive work behavior and organizational citizenship behavior. *Human Resource Management Review*, 12:269-292.
14. Stanton, J. M. (2002a). Company profile of the frequent Internet user: Web addict or happy employee? *Communications of the Association for Computing Machinery*, 45 (1), 55-59.
15. Stanton, J. M., Stam, K. R., Guzman, I., and Caldera, C. (2003, October). Examining the linkage between organizational commitment and information security. *Proceedings of the IEEE Systems, Man, and Cybernetics Conference*, Washington, DC.
16. Straub, D.W. (1990). Effective IS security: an empirical study. *Information System Research*, 1 (2), 255-77.
17. Trice, H. M. (1993). *Occupational subcultures in the workplace*. Ithaca, N.Y. : ILR Press.
18. 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.