Analysis of end user security behaviors

Article *in* Computers & Security · March 2005

Impact Factor: 1.03 · DOI: 10.1016/j.cose.2004.07.001 · Source: DBLP

4 authors, including:

Jeffrey M Stanton
Syracuse University
103 PUBLICATIONS **2,769** CITATIONS
SEE PROFILE

Kathryn R. Stam
State University of New York Institute of Te…
20 PUBLICATIONS **456** CITATIONS
SEE PROFILE

Computers & Security (2004) ■■, ■–■

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Analysis of end user security behaviors

Jeffrey M. Stanton[a,*], Kathryn R. Stam[a], Paul Mastrangelo[b], Jeffrey Jolton[b]

[a]*4-125 Center for Science and Technology, School of Information Studies, Syracuse University, Syracuse, NY 13244-4100, United States*
[b]*Genesee Survey Services, 3136 Winton Road South, Rochester, NY 14623, USA*

Received 29 March 2004; revised 9 June 2004; accepted 12 July 2004

KEYWORDS
Computer security;
Behavioral information security;
Passwords;
User behavior;
Organizational management;
Surveys

Abstract Many information security specialists believe that promoting good end user behaviors and constraining bad end user behaviors provide one important method for making information security effective within organizations. Because of the important of end user security-related behaviors, having a systematic viewpoint on the different kinds of behavior that end users enact could provide helpful benefits for managers, auditors, information technologists, and others with an interest in assessing and/or influencing end user behavior. In the present article, we describe our efforts to work with subject matter experts to develop a taxonomy of end user security-related behaviors, test the consistency of that taxonomy, and use behaviors from that taxonomy to conduct a U.S. survey of an important set of end user behaviors. We interviewed 110 individuals who possessed knowledge of end user security-related behaviors, conducted a behavior rating exercise with 49 information technology subject matter experts, and ran a U.S. survey of 1167 end users to obtain self-reports of their password-related behaviors. Results suggested that six categories of end user security-related behaviors appeared to fit well on a two-dimensional map where one dimension captured the level of technical knowledge needed to enact the behavior and another dimension captured the intentionality of the behavior (including malicious, neutral, and benevolent intentions). Our U.S. survey of non-malicious, low technical knowledge behaviors related to password creation and sharing showed that password ''hygiene'' was generally poor but varied substantially across different organization types (e.g., military organizations versus telecommunications companies). Further, we

☆ An earlier version of this manuscript was presented at a conference: Stanton JM, Caldera C, Isaac A, Stam KR, Marcinkowski SJ. Behavioral information security: defining the criterion space. In: Mastrangelo PM, Everton WJ. (Eds). The Internet at work or not: preventing computer deviance. Symposium presentation at the 2003 meeting of the Society for Industrial and Organizational Psychology, Orlando, FL, USA; 2003, April.

* Corresponding author. Tel.: +1 315 443 2911.
E-mail address: jmstanto@syr.edu (J.M. Stanton).

0167-4048/$ - see front matter
doi:10.1016/j.cose.2004.07.001

documented evidence that good password hygiene was related to training, awareness, monitoring, and motivation.

Over recent decades most work organizations have come to depend on information technology for internal operations such as record-keeping, external transactions such as financial transfers, and mediated communications of all types (e.g., email). As connectivity among devices has increased, so has the likelihood of intrusion, theft, defacement, and other forms of loss. Surprisingly, although organizations tend to be more concerned about vulnerability to external threats, recent industry research suggests that a substantial proportion of security incidents originate from inside the organization. Estimates of this proportion vary: a report by Ernst and Young (2002) suggested that more than three-quarters of security breaches resulted from inside activity whereas the most recent Computer Security Institute report indicated that about half of all incidents arose from inside activity (Gordon et al., 2004, p. 4). At the low end, losses from security breaches have been estimated at approximately $20 billion per year (counting U.S. organizations only; Security Wire Digest, 2000). 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. A substantial IT subindustry designs, develops, and markets of security devices such as firewalls.

One organizational constraint that impacts the effectiveness of these technologies, however, lies in the behaviors of the human agents who access, use, administer, and maintain information resources (e.g., von Solms and von Solms, in press; Vroom and von Solms, in press). 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. In the present article we focused on developing a systematic understanding of the range of end user behaviors that may influence information security effectiveness in organizations. We constructed and tested a taxonomy of information security behaviors and we surveyed employees in a large number of organizations with respect to one of the key end user behaviors that appeared in the taxonomy, namely password management.

Information security and end user behavior: an overview

Much 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 (see, e.g., Dhillon and Backhouse, 2000). We believe that an important additional layer in this assortment of approaches lies between the human–computer interface and management concerns for risk, business processes, and finances. Specifically, several researchers have begun to develop concepts, theory, and research relevant to human behavior in organizations and how that behavior affects information security. For example, von Solms and his colleagues have described and analyzed a variety of organizational issues related to information security behavior including auditing (Vroom and von Solms, in press), compliance with information security policies (von Solms and von Solms, in press; also see Straub, 1990), and security awareness (Thomson and von Solms, 1997; also see Spurling, 1995).

Another line of research has emerged on counterproductive computer usage including projects by Loch and Conger (1996), Young (1998), Armstrong et al. (2000), Stanton (2002), Morahan-Martin and Schumacher (2000), Siponen (2001), and Trompeters and Eloff (2001). At the extreme end of counterproductive computer use, the ''insider threat'' to information security has also received considerable research attention (e.g., Anderson et al. 1999; Dhillon, 2001; Schultz, 2002; Shaw et al., 2002). Insider threat refers to intentionally disruptive, unethical, or illegal behavior enacted by individuals who possess substantial internal access to the organization's information assets.

In Secrets and Lies, Schneier (2000) delivered his verdict on information security behavior, ''Mathematics is logical; people are erratic, capricious, and barely comprehensible.'' In contrast, the research cited above suggests that information security behavior may indeed be understandable, organized, and meaningful both for those who work at making sense of it. Below, we present our efforts to catalog, characterize, organize, and analyze a range of end user security behaviors in organizations.

A taxonomy of information security end user behaviors

We began by conducting 110 interviews with information technology professionals, managers, and regular employees during which we asked respondents to describe both beneficial and detrimental behaviors that information technology users within organizations enact that may affect information security. From the transcripts of these interviews we compiled a raw list of security-related behaviors. Ten information security subject matter experts sorted these behaviors into categories of their own individual devising. By collapsing across the many similarities among these expert-generated categories, we developed 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 perhaps 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.

Table 1 and Fig. 1 depict the six categories arranged on these two dimensions. To illustrate with contrasting categories, ''aware assurance'' refers to positive security practices conducted by well-trained end users, while ''detrimental misuse'' refers to the inappropriate and intentional behaviors of inexpert individuals who misuse information resources.

Table 1 Two factor taxonomy of security behaviors

Expertise	Intentions	Title	Description
High	Malicious	Intentional destruction	Behavior requires technical expertise together with a strong intention to do harm to the organization's IT and resources. Example: employee breaks into an employer's protected files in order to steal a trade secret.2
Low	Malicious	Detrimental misuse	Behavior requires minimal technical expertise but nonetheless includes intention to do harm through annoyance, harassment, rule breaking, etc. Example: using company email for SPAM messages marketing a sideline business.
High	Neutral	Dangerous tinkering	Behavior requires technical expertise but no clear intention to do harm to the organization's IT and resources. Example: employee configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars.
Low	Neutral	Naïve mistakes	Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources. Example: choosing a bad password such as ''password.''
High	Beneficial	Aware assurance	Behavior requires technical expertise together with a strong intention to do good by preserving and protecting the organization's information technology and resources. Example: recognizing the presence of a backdoor program through careful observation of own PC.
Low	Beneficial	Basic hygiene	Behavior requires no technical expertise but includes clear intention to preserve and protect the organization's IT and resources. Example: a trained and aware employee resists an attempt at social engineering by refusing to reveal her password to a caller claiming to be from computer services.

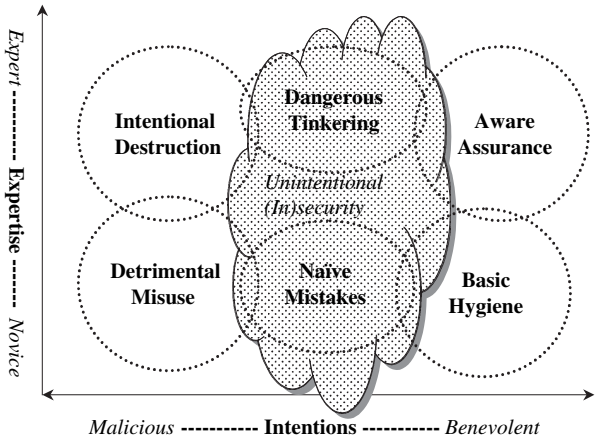

Figure 1 Two-factor taxonomy of end user security behaviors.

An example of aware assurance would be when a well-trained end user discovers a backdoor on her desktop PC by using the task and process list to investigate unusual hard drive activity. An example of detrimental misuse would be when a worker uses the company's email to spam his coworkers with pitches for his sideline business. In Fig. 1, each category shows a slight degree of overlap with its neighbors in recognition of the likely existence of behaviors near the borderlines. For instance, forging an email header to make it seem like the boss has distributed a rude joke requires some expertise and some malicious intent.

In Fig. 1, the central "dark cloud" of unintentional (in)security suggests that sometimes individuals act without explicit intentions either to harm or help information security behavior, even though the outcome may suggest otherwise. Our experts' list of behaviors contained many examples of "naïve mistakes" (e.g., using one's social security number as a password) that suggested a lack of awareness of basic information security principles rather than an intention to cause harm. Similarly, dangerous tinkering suggests that an individual with a higher degree of technical expertise might affect information security as an unintended consequence of his or her ability to setup a more complex technology configuration with unintentional properties (e.g., by deploying a wireless network gateway that allowed non-company personnel to use the company's network).

Next, we tested this six-category taxonomy to ascertain whether a larger panel of subject matter experts could agree on the classification of behaviors into the categories we had defined, to obtain ratings of the level of expertise required, and to ascertain the apparent intent associated with each behavior. Respondents for this part of the research comprised 49 advanced degree students (e.g., M.S. and Ph.D.) in information technology who completed a survey by rating a series of 94 statements such as, "He brought a wireless gateway device into his office, and installed it on the network without authorization." We distributed a total of 75 of these surveys for a response rate of 65 percent. Respondents rated the intentionality of each behavior on a scale ranging from 1 ("Highly malicious intentions to compromise resources") to 5 ("Highly benevolent intentions to preserve resources"), and the degree of necessary technical know-how on a scale ranging from 1 ("No special expertise or training required") to 5 ("A lot of special expertise and/or training required"). Respondents also made a separate designation that assigned each behavior to one of the six categories.

We used the "modal" category designation (i.e., the category chosen by the greatest number of respondents) to assign each behavior to one of the six categories. As an example, 39 out of 49 raters assigned item 11 ("She did not change her password for over two years.") to the "Naïve Mistakes" category, and so we placed this item in the low expertise condition (expertise factor) and the neutral intentionality condition (intentionality factor). In the case of three behaviors, there were ties between two neighboring categories. In these three cases, we assigned the behavior to one of the tied categories at random. Next, we aggregated the ratings across all 49 raters to form an average rating of intentionality and expertise for each behavior. In this way, we created a map of all 94 behaviors on the two-dimensional space depicted in Fig. 2.

The map of average ratings in Fig. 2 makes it clear that survey respondents did not distribute the items evenly across the two-dimensional

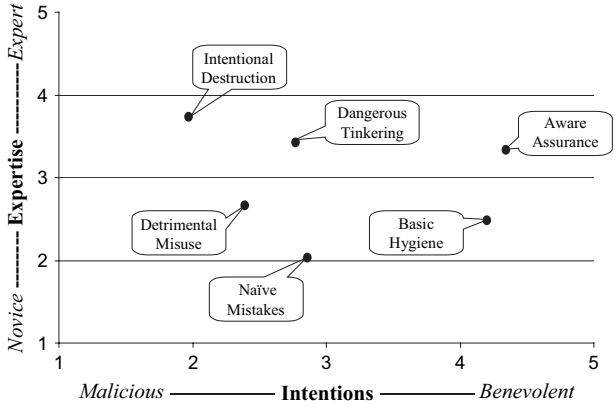

Figure 2 Map of the average ratings for behaviors in each category.

Table 2 Ten most extreme end user behaviors on expertise

Category assignment	Expertise rating	Item text/behavior description
High expertise behaviors		
Intentional destruction	4.29	He created a denial of service attack on a competitor's website using the company's computers.
Dangerous tinkering	4.24	She set up a packet spoofing application to test out her programming ability.
Dangerous tinkering	4.20	He set up a network monitoring scanner on his PC.
Intentional destruction	4.13	He built a special script that disabled other users' terminal sessions.
Intentional destruction	4.04	She forged routing information to make it seem like someone else had sent some packets.
Low expertise behaviors		
Naïve mistakes	1.68	She wrote her password on a sticky note and put it on her monitor.
Naïve mistakes	1.61	She chose a password consisting of four digits.
Naïve mistakes	1.60	He used his social security number as a password.
Naïve mistakes	1.55	She wrote her password on a slip of paper and taped it under her keyboard.
Naïve mistakes	1.53	She shared her account information with a friend.

taxonomy. In particular, it is clear that the items assigned to the intentional destruction category were more extreme with respect to both malicious intentions and required expertise than either of the neighboring categories. The intentional destruction plainly appears to capture the range of behaviors one would normally attribute to individuals involved in an ''insider threat'' to information security. Another notable discovery from Fig. 2 is that relatively little space existed between naïve mistakes, detrimental misuse and dangerous tinkering. This may reflect a belief on the part of these respondents that when end users cause problems with security, it may often be difficult to judge the degree to which the problem was caused by ignorance, negligence, or mischievous intent. Additionally, the same relatively inexpert users may possibly exhibit behaviors in more than one of these categories at different points in time. In contrast, Fig. 2 makes evident both the required expertise and the clear beneficial intentions of behaviors in the aware assurance category. In Tables 2 and 3, we provide a sampling of the items from the most extreme ends of each dimension as a way of illustrating the data used to build Fig. 2. Table 2 shows the behaviors with the most extreme ratings on expertise.

In Table 2, note how most of the high expertise behaviors appear in the intentional destruction category. Referring back to Fig. 2, this is reflected in the fact that the intentional destruction category has the highest average level of expertise of all of the six categories. An anonymous reviewer pointed out an interesting correlate: some of these behaviors also require the actor to have a high degree of access or administrative rights in addition to their high expertise. In contrast, note that both Table 2 and Fig. 2 show how the naïve mistakes category contains the items with the lowest values of expertise. It is also notable that four out of five of the least expert naïve mistakes behaviors refer to password management issues. Next, Table 3 shows the behaviors with the most extreme ratings on intentionality.

In referring to Table 3, note that the five-point intentionality scale was bipolar and ranged from 1 (''Highly malicious intentions to compromise resources'') to 5 (''Highly benevolent intentions to preserve resources''). In the top half of Table 3, the highly benevolent behaviors are about evenly split between aware assurance and basic hygiene categories, and this is reflected in Fig. 2 by the rightmost positioning of these two categories on the map. Most of the malicious behaviors in Table 3 appear in the intentional destruction category in correspondence with the leftmost positioning of this category on the map in Fig. 2. As a final note, we conducted statistical analysis comparing averages from each of the six categories depicted in Fig. 2 that showed statistically significant differences for all categories on both dimensions.

A national survey of naïve security mistakes

The map of categories in Fig. 2 and the other results from our taxonomy of end user security behaviors suggested that one viable strategy for improving security performance in organizations

Table 3 Ten most extreme behaviors on intentionality

Category assignment	Intentionality rating	Item text/behavior description
Benevolent behaviors		
Aware assurance	4.75	He did a training program to learn about the sensitivity and criticality of special company files so that he could apply appropriate protective measures when handling the information.
Aware assurance	4.64	She did a training program to become familiar with indicators of virus infection and learn how to report operational anomalies to resource administrators.
Basic hygiene	4.62	She reported a discovered security vulnerability to the appropriate authorities.
Basic hygiene	4.60	He would not release non-public company data/information to a reporter.
Basic hygiene	4.57	She used excellent access codes (passwords and usernames) and changed them periodically.
Malicious behaviors		
Intentional destruction	1.83	She forged her email header information to make it look like her boss had sent a message.
Intentional destruction	1.82	She forged routing information to make it seem like someone else had sent some packets.
Detrimental misuse	1.80	He transmitted a harassing message using the company's email.
Intentional destruction	1.75	He used a file decryption program to discover the contents of a file containing trade secrets.
Intentional destruction	1.63	He intentionally introduced a Trojan horse program into the network.

might lie in shifting the enactment of behaviors in the naïve mistakes category toward the enactment of basic security hygiene behaviors. The layout of Fig. 2 suggests that only a relatively small increase in security expertise or awareness would be needed whereas a more substantial boost in benevolent intentions or motivations is warranted. To explore these ideas, we conducted a U.S. national survey of end user behaviors across a wide range of organizations using a sampling of the behaviors reflected in the naïve mistakes and basic hygiene categories. As noted above in the narrative description of Tables 2 and 3, many of these behaviors pertained to the selection of passwords and the frequency of changing passwords. Thus, we focused our attention on asking end users about these behaviors.

We conducted our survey with the assistance of Genesee Survey Services of Rochester, NY, a firm that conducts an annual nationwide study of U.S. workers from a variety of industries including financial, manufacturing, health, military, government, and telecommunications. Their National Work Opinion Survey (NWOS) serves as a source of normative data on a variety of measures of organizational concern. 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 2003, the NWOS was distributed to $N = 4000$ individuals and $N = 2011$ usable surveys were returned for a response rate of approximately 50%. In 2003, the survey was offered in several versions, and not all of the versions contained our security items. With this consideration, we obtained $N = 1167$ surveys with usable data on the nine items adapted from our naïve mistakes and basic hygiene categories. The set of items included three items pertaining to password management behaviors (e.g., frequency of changing the password), three items pertaining to password sharing behaviors (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.'').

Results of our survey showed that 62.5% of respondents never used numbers or punctuation marks in their passwords, 48.5% of respondents had not changed their passwords in the last six months, and 27.9% of respondents wrote down their passwords to help remember them at least once in the last six months. Results also indicated that 23% of respondents sometimes reveal their

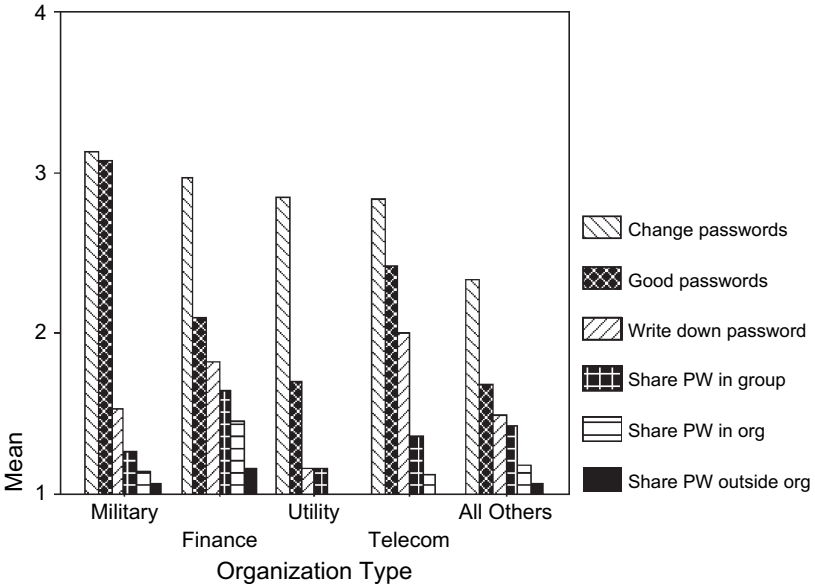

Figure 3 Average password behavior frequencies for different types of organizations.

passwords to members of their work groups, 7% share their passwords with someone in their company but outside their work group, and 4.1% share their passwords with someone outside their company. With respect to training and awareness, 35% have never taken any type of security training, 34.9% work in settings where they have not been told how their computer activities are monitored, and 19.9% work in companies that do not enforce their acceptable use policy (AUP).

Password-related behaviors varied substantially across different types of organizations. Fig. 3 shows a breakout of the six password-related behaviors in four separate organization types — military, finance, utilities, and telecommunications — as well as a conglomerate of all other organization types in the rightmost cluster. The bars represent average values on a frequency scale that ranged from scale of one to six, where one was "never do this," two was "have not done this in the past six months," three was "have done this a few times in the past six months," and four was, "have done this 1—5 times per month." Note that the leftmost two bars in each cluster represent behaviors that are preferentially done more frequently (i.e., changing one's password and choosing a hard to guess password), whereas the rightmost four bars in each cluster represent behaviors that are preferentially done rarely, if at all (e.g., sharing one's password outside the company).

Note that with respect to the positive, basic hygiene behaviors of changing passwords frequently and choosing difficult to guess passwords, the respondents from military organizations reported these behaviors as occurring more frequently than for those from other organizations. For the negative, naïve mistakes behavior of sharing passwords, the respondents from the military reported these behaviors as quite infrequent, although the individuals from utility firms reported even lower frequencies than those reported in the military. In general, the "all others" category, which included non-financial service businesses, manufacturing, education, and other sectors, reported the least favorable mix of behaviors, including less frequent positive behaviors and more frequent negative behaviors.

We also used simple correlations to evaluate the degree of relationship between the password-related behaviors and the issues of training and awareness we examined. Table 4 shows the statistically significant[1] correlations between the password-related behaviors and training and awareness. The last column of Table 4 also introduces a new variable that is a composite of the respondent's reports of the use of formal job evaluations and his or her satisfaction with benefits, two organizational issues related to employee rewards. Most of the correlations are positive, which suggest that a greater degree of training and awareness signifies a higher frequency of the security-related behaviors. In general, correlations less than 0.20 are considered small, whereas correlations between 0.20 and 0.50 are considered

[1] Significant at $p < 0.01$, indicating a very low likelihood that the finding could have resulted from sampling error.

Table 4 Correlations between password-related behaviors and training/awareness

Behavior	Training	Enforce AUP	Monitoring	Rewards
Frequency of changing password	0.31	0.43	0.28	0.21
Using numbers and punctuation in password	0.24	0.21	0.26	0.14
Write down password	0.17	0.16	0.11	—
Share password with workgroup	—	—	—	—
Share password in company	—	—	—	—
Share password outside of company	—	—	—	−0.08

medium. Most of the correlations shown in Table 4 fall into the medium range. Note that a positive correlation does not signify that the training or awareness *caused* the improvement in password practices. A positive correlation does, however, imply that the inverse causal relationship is extremely unlikely to exist (i.e., that more training or awareness activities could cause a *decline* in the quality of password practices).

The correlations depicted in Table 4 provide further information about the password-related behaviors we assessed in the survey. Training, enforcement of an acceptable use policy (AUP), letting employees known about how they are monitored, and positive reward practices all appear to have beneficial effects on getting end users to change their password frequently and compose difficult to guess passwords. Note, however, that using frequent password changes and hard to guess passwords probably has the unintended consequence of making it more likely that an individual will have to write down their password in order to remember it. This would account for the results suggesting that increased training, AUP enforcement, and monitoring actually seem to associate with a higher likelihood of writing down one's password. Finally, sharing behavior does not seem to relate to training, AUP, monitoring, or reward except in one isolated case. In particular, positive reward practices were associated with a very slightly lower likelihood of sharing one's password outside the company.

Conclusions

One purpose of this research was to transform a raw list of security-related behaviors into a more manageable taxonomy with recognizable dimensions that had logical appeal. Our results suggested that we achieved a degree of success in this goal. While raters failed to agree on where to fit three of the 94 behaviors, for the remaining 91 behaviors a consensus emerged on where that behavior belonged in our six-element taxonomy. Further, when we used this consensus as a basis for comparing ratings of expertise and intentionality (the two dimensions of our taxonomy) a map of the average ratings clearly showed that as a group our raters assigned normative levels of expertise and intentionality consistent with the classification scheme. We feel confident at this point that most security-related end user behaviors that occur in organizations could be positioned within our six-category taxonomy. We emphasize that what we have created is a scheme for organizing various behaviors, not for describing kinds of people. In all likelihood, many employees and managers could exhibit behaviors from different categories at different points in time.

Our national survey of end users in U.S. organizations shed some additional light on the end user security-related behaviors we categorized as naïve mistakes or basic hygiene. We focused on password-related behavior, which comprised an important subset of the behaviors in both categories. First, our survey suggested that end users have a rather dismal record of enacting the basic hygiene behaviors that security experts suggest are important in maintaining the safety of user accounts (e.g., frequent changes to one's password). Second, we found that the amounts of effective and ineffective behavior varied across organization types, with better performance by organizations whose missions depend upon security. Third, as the taxonomy of end user security-related behaviors would suggest, several mechanisms may help to move end user behaviors from the naïve mistakes category to the basic hygiene category. More specifically, training, awareness, knowledge of monitoring, and rewards exhibited positive associations with changing passwords more frequently and choosing better passwords. Unfortunately, improvements in these areas also seemed to associate with a greater likelihood of writing down one's password. In addition, training, awareness, knowledge of monitoring, and rewards appeared to lack relations with password sharing behaviors, an issue that deserves further research.

Note that other mechanisms with influence over naïve mistakes and basic hygiene are also likely to be important (e.g., judicious enforcement of compliance with an acceptable use policy), but our survey of end users was not geared toward examining these possibilities.

From a practical perspective, this confirmation of our taxonomy may help with the tasks of assessing and auditing security-related end user behaviors in organizations. We recommend that assessments of user behavior attempt to capture, through observations, self-ratings, or audits of computer use, the occurrence of a range of behaviors in every one of the six areas of our taxonomy. Further, different assessment techniques are probably needed across the six areas. The categories with neutral and positive intentions are likely to yield usable self-reports because most users are probably willing to reveal these behaviors on a survey or during an audit. Design and publication of a set of standard instruments for obtaining these self-assessments from users would be of benefit to the security community. In contrast, the behaviors in the malicious zone of our taxonomy are unlikely to be revealed in self-reports and, therefore, must be obtained through other means such as monitoring and logging of access attempts and transactions. Given the diversity of equipment, applications, network structures, and other variables in the environment, obtaining such reports presents a considerably more difficult challenge. Existing technological tools for content filtering and analysis (e.g., of outgoing emails and incoming web pages) as well as intrusion detection may provide at least some of the answers to this challenge.

We also believe that an important characteristic of our taxonomy and the subsequent survey is that they suggest paths that an organization can take towards improving its security status. In general, any reward or motivational interventions that shift intentionality towards the benevolent end of the continuum ought to improve the organization's security status. Effective security organization, positive security leadership, and clear designation of user roles and responsibilities may also help to shift intentionality in the beneficial direction. Likewise, with the exception of those employees who may have malevolent intentions towards the organization, providing training and other forms of expertise development appear to have the potential to benefit the organization's information security.

Note that there are several limitations of the methodologies we used that should temper interpretation of the results. First, although we used over a hundred interviews with individuals who occupied different organizational roles, in all likelihood we did not generate a truly exhaustive list of end user security behaviors. We believe that our list is representative, however, and therefore that the six-category, two-dimensional taxonomy has merit. Additionally, while it is likely that behaviors in all six categories occur in many organizations, it is also likely that smaller organizations, specialized organizations (e.g., military), and organizations that use little information technology may have substantially different distributions of behavior.

Despite these limitations, the data we reported in this article provide useful guidance to promote further understanding and investigation of end user security-related behaviors in organizations. Because end user behaviors intertwine inextricably with the overall effectiveness of security, it is important to have a systematic view of end user behavior that facilitates accurate auditing and assessment of this behavior. Through careful analysis of end user security-related behaviors, organizations can help to ensure that workers have the motivation and knowledge follow the policies that the organization sets to promote its security agenda.

Acknowledgment

This research was supported in part by a small grant from the SIOP research foundation and by an award from the National Science Foundation. Neither SIOP nor the National Science Foundation necessarily endorse the results or conclusions of this study.

References

Anderson RH, Feldman PM, Gerwehr S, Houghton B, Mesic R, Pinder JD, et al. Securing the U.S. defense information infrastructure. A proposed approach, Washington, DC: Rand; 1999.

Armstrong L, Phillips JG, Saling LL. Potential determinants of heavier Internet usage. International Journal of Human—Computer Studies 2000;53(4):537—50.

Dhillon G. Violation of safeguards by trusted personnel and understanding related information security concerns. Computers and Security 2001;20:165—72.

Dhillon G, Backhouse J. Information system security management in the new millennium. Communications of the ACM 2000;43:125—8.

Ernst and Young LLP. Global information security survey UK: Presentation Services; 2002.

Gordon LA, Loeb MP, Lucyshyn W, Richardson R. 2004 CSI/FBI computer crime and security survey Manhasset, NY: CMP Media; 2004.

Loch KD, Conger S. Evaluating ethical decision-making and computer use. Communications of the ACM 1996;39(7):74–83.
Morahan-Martin J, Schumacher P. Incidence and correlates of pathological Internet use among college students. Computers in Human Behavior 2000;16(1):13–29.
Schultz EE. A framework for understanding and predicting insider attacks. Computers and Security 2002;21(6):526–31.
Schneier B. Secrets and lies. New York: Wiley; 2000.
Security Wire Digest. CSI/FBI study says: security breaches on the rise, <http://www.lexias.com/1.0/securitywiredigest_27MAR2000.html>; 2000, March 27.
Shaw ED, Post JM, Ruby KG. Inside the mind of the insider, <http://www.securitymanagement.com/library/000762.html>; 2002.
Siponen MT. On the role of human morality in information systems security. Information Resources Management Journal 2001;14(4):15–23.
von Solms R, von Solms B. From policies to culture. Computers and Security, 2004;23(4):275–9.
Spurling P. Promoting security awareness and commitment. Information Management and Computer Security 1995;3(2):20–6.
Stanton JM. Company profile of the frequent Internet user: Web addict or happy employee? Communications of the Association for Computing Machinery 2002;45(1):55–9.
Straub DW. Effective IS security: an empirical study. Information System Research 1990;1(2):255–77.
Thomson ME, von Solms R. An effective information security awareness program for industry. In: Proceedings of the WG 11.2 and WG 11.1 of the TC11 IFIP; 1997.
Trompeters CM, Eloff JHP. A framework for the implementation of socio-ethical controls in information security. Computers and Security 2001;20:384–91.
Vroom C, von Solms R. Towards information security behavioural compliance. Computers and Security 2004;23(3):191–8.
Young KS. Internet addition: the emergence of a new clinical disorder. CyberPsychology and Behavior 1998;1(3):237–44.

Dr. Jeffrey M. Stanton, Ph.D. (1997, University of Connecticut, Industrial/Organizational Psychology) is an associate professor in the School of Information Studies at Syracuse University. He has developed an extensive funded research program at the intersection of behavioral science and information technology and has published more than 40 refereed articles on this and related topics. Dr. Stanton's research interest in the area of information security lies in understanding the role of work motivation in guiding the security-related behaviors of employees and managers in organizations, an area of research entitled behavioral information security.

Kathryn Stam, Ph.D. is a senior researcher and associate director of the Syracuse Information Security Evaluation (SISE) project at Syracuse University's School of Information Studies. She earned her Ph.D. in Social Science (Anthropology and Sociology) from Syracuse University's Maxwell School of Citizenship and Public Affairs. Her educational background and research interests are related to information technology, health and social services, and organizational culture. She has published a range of qualitative research on the topics of work organizations, community health, and teaching, and has received financial support for her research from the National Science Foundation.

Paul M. Mastrangelo, Ph.D., has been a consultant at Genesee Survey Services since 2002, where he works with large-scale organizations in the design, implementation, and analysis of employee surveys. Previously, Paul was a tenured associate professor at the University of Baltimore, where he focused on the measurement of attitudes, personality, and biographical information. He received his Ph.D. in Industrial and Organizational Psychology from Ohio University in 1993 and his B.A in Psychology from the University of Rhode Island in 1989, where he was inducted into the Phi Beta Kappa Honor Society.

Jeffrey A. Jolton, Ph.D., is a senior consultant with Genesee Survey Services in Rochester, NY where he has worked with a variety of organizations helping them with the design, implementation and analyses of large-scale employee surveys. He has over 10 years' experience in the design, implementation, and analysis of individual, group, and organization-level assessments. He holds a Ph.D. in Industrial and Organizational Psychology from Ohio University and a B.A. in Psychology from Lawrence University. Jeff is a member of the Society for Industrial and Organizational Psychology and has presented and published in numerous conferences and publications.