Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

A Reading Preference and Risk Taxonomy for Printed Proprietary Information Compromise in the Aerospace and Defense Industry

Joshua D. Stalker
Nova Southeastern University, stalker@nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Yoram Eshet
Open University of Israel

James L. Parrish
Nova Southeastern University

A Reading Preference and Risk Taxonomy for Printed Proprietary Information Compromise in the Aerospace and Defense Industry

Joshua D. Stalker[1]
Graduate School of Computer and Information Sciences, Nova Southeastern University,
Ft. Lauderdale, FL, USA

Yair Levy
Graduate School of Computer and Information Sciences, Nova Southeastern University,
Ft. Lauderdale, FL, USA

Yoram Eshet
Department of Education and Psychology, The Open University of Israel,
Rannana, Israel

James L. Parrish
Graduate School of Computer and Information Sciences, Nova Southeastern University,
Ft. Lauderdale, FL, USA

ABSTRACT

The protection of proprietary information that users print from their information systems is a significant concern. Researchers have repeatedly indicated that human behaviors and perception are important factors influencing the information security of organizations and have called for more research. In this study, we focused on the investigation of user reading preference, user perceived risk, and seven demographics in the context of compromising printed proprietary information. A Reading Preference and Risk (RPR) taxonomy was developed to classify users respective to potential risks to printed proprietary information. Results of a Web-based survey show that employees were dispersed across the RPR Taxonomy with 15.1% identified as potentially problematic. Our results also showed an overall reading preference for print materials and a high-perceived risk for compromising printed proprietary information. Significant differences between the constructs and demographics suggest that a user's likelihood

[1] Corresponding author. stalker@nova.edu +1 407-335-9377

to compromise printed proprietary information is affected by frequency of user exposure, confidentiality level, and previous user experience with the compromise of proprietary information. Additionally, age, gender, and a user's desire to retain e-training content in memory had a significant effect on user reading preference.

Keywords: Information security, perceived risk, reading preference, proprietary information, e-training security, e-learning security, cognitive load, protection motivation

INTRODUCTION

This study addressed the problem of protecting an organization's proprietary information managed within its information systems (Bernard 2007; Da Veiga and Eloff 2010; Goel and Shawky 2009; Pacini et al. 2008). The significance of this problem is evidenced by the magnitude of the negative consequences resulting from compromised proprietary information highlighted in current research, ranging from hundreds of billions of dollars in annual economic losses, millions of jobs lost, and threats to national security (Carr et al. 2000; Pacini et al. 2008). The relevance of this study is supported by the current and considerable research into understanding information security risks posed to organization's proprietary information and mitigating negative consequences (Bernard 2007; Da Veiga and Eloff 2010; Pacini et al. 2008; Wiant 2005).

According to Albrechtsen and Hovden (2009), more research is needed on the relationship of risk perception and information security. This appears to be relevant since user risk perception is known to influences user behavior (Besnard and Arief 2004). Further, the approaches used to steal an organization's proprietary information will constantly evolve and any vulnerability will likely be exploited (Dlamini et al. 2009). Additionally, Chang and Ley (2006),

Eshet-Alkalai and Geri (2007), Levy (2008), as well as Spencer (2006) appear to suggest that the amount of printed proprietary information in an organization is influenced by user reading preferences and likely extend into e-training and e-learning contexts. In the context of e-learning systems, Levy and Ramim (2009) suggested a need for additional e-learning security research stating "researchers have raised a valid criticism that information security in e-learning research is scarce" (p. 381). Levy and Ramim (2009) also stated that "there is a substantial interest for additional research on issues related to e-learning security" (p. 381). Thus, this research built upon prior research in information security, user perceived risk, user reading preference, and e-training (Albrechtsen and Hovden 2009; Bernard 2007; Besnard and Arief 2004; Eshet-Alkalai and Geri 2007; Hazari et al. 2008; Kraemer et al. 2009; Levy and Ramim 2009; Spencer 2006). Further, this research problem is present in the aerospace and defense industry, as well as e-training environments in that industry and, thus, was selected as the context for this study (Kambourakis et al. 2007; Kritzinger and von Solms 2006; Levy and Ramim 2009). The main contribution of this study is the extension of research in information systems security related to user behaviors and user risk perception specifically in the context of highly specialized proprietary industry. The results of this study promise to contribute to information security body of knowledge by providing researchers and practitioners more insight to what influences users to print proprietary information, which could be compromised. These communities of interest will, therefore, be able to use the results of this study to shape future research and shape industry practices to mitigate the compromise of printed proprietary information. Thus, reduce the negative consequences associated with compromising proprietary information. The following section will outline the theoretical background for this study and provide the taxonomy proposed. Following, the methodology will be outlined, then the data collection and results will be

discussed. Then, limitations and avenues for future research are provided, while the paper commences with discussions and conclusions.

THEORETHICAL BACKGROUND

Researchers suggest that user behavior can lead to information security risks, while additional research is needed to understand reasons for such risks (Besnard and Arief 2004; Herath and Rao 2009; Kraemer 2009). Cognitive Load Theory (CLT) posits that when a person is engaged in a learning activity, they are engaging two memory structures, their short term working memory (WM) and their long term memory (LTM) (Sweller and Chandler 1994). CLT also posits that people have a limited amount of WM to store and process information (Sweller and Chandler 1994). Researchers have suggested that reading in digital environments increases the reader's cognitive load as compared to reading from print (Eshet-Alkalai and Geri 2007). Further, research has suggested that people will act to decrease the cognitive load they are experiencing by printing online learning material because it may be causing physiological discomfort (Chang and Ley 2006; Spencer 2006). Thus, CLT appears to suggest that information systems users may exhibit a reading preference for print materials in an effort to reduce cognitive load, especially when the content of e-training must be retained in memory. Thus in this study, we explored the user behavior of reading preference, which appears to influence the printing of proprietary information that subsequently must be protected from compromise to preserve information security breach.

Researchers have also emphasized the influence of user risk perception on user behavior to mitigate risks and have called for more risk perception studies in information security (Albrechtsen and Hovden 2009; Workman et al. 2008). Protection Motivation Theory (PMT) suggests how an individual's cognitive appraisal of fear in a given situation motivates their

behavior (Herath and Rao 2009). PMT attempts to explain how people initiate and sustain protective behaviors based on the risk they perceive, the desire to avoid negative outcomes, and while simultaneously weighing the costs of the protective behaviors versus their expected benefits (Rogers 1975). Thus, PMT appears to provide theory that indicates users perceived risk will influence actions they may take to avoid negative consequences.

Considering CLT and PMT, the scope of this study was focused on the crossroad between user reading preference and user perceived risk of compromising printed proprietary information. These two constructs were used to develop the RPR Taxonomy for Printed Proprietary Information Compromise (See Figure 1), which provides insight on the potential for a given user to compromise printed proprietary information based on behavioral preferences and perceptions of risk.

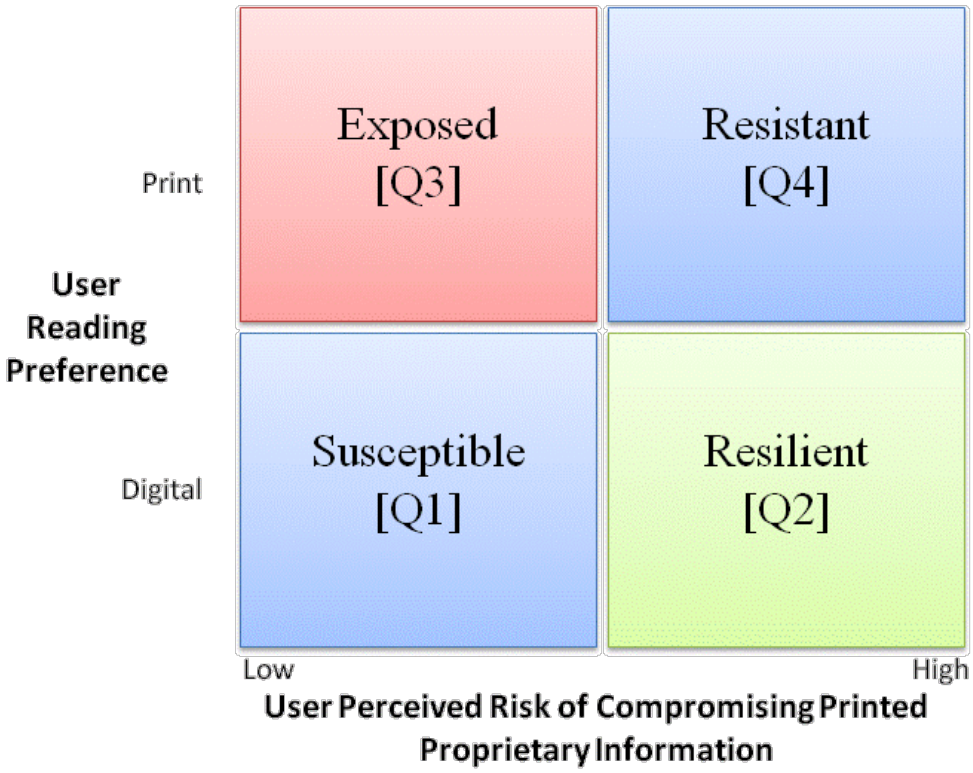

Figure 1: Reading Preference-Risk Taxonomy for Printed Proprietary Information Compromise

The main research question presented for this study was: how are e-training users in the defense industry classified in terms of their potential for compromising printed proprietary information based on user reading preferences and user perceived risk of compromising printed proprietary information in the defense industry? Based on this overarching perspective, the first specific research question (RQ1) was: how are the aggregated scores for user reading preference and user perceived risk of compromising printed proprietary information positioned on the RPR Taxonomy for users? The second, and final specific research question (RQ2) was: do significant differences exist in user reading preference and user perceived risk of compromising printed proprietary information based on the seven demographics: (1) age, (2) gender, (3) frequency of a user exposure to proprietary information, (4) confidentiality level of the proprietary information a user is regularly exposed to, (5) user previous experience with the compromise of proprietary information, (6) user organizational role, and (7) user education level? RQ2 was addressed by exploring seven null hypotheses (H1 – H7) that examined whether significant differences exist between each construct based on each demographic variable.

METHODOLOGY

A Web-based survey was developed based on current and relevant research literature on user reading preference and user perceived risk. Survey items were drawn from those presented the literature and modified slightly to the context of this study in order to support internal validity (Straub 1989). Further, an expert panel and pilot test were performed to ensure the survey instrument was effective. The survey consisted of three sections (See Appendix A). The first section consisted of seven items focused on perceived risk dimensions deemed applicable to the context of this study, i.e. financial risk, physical risk, prosecution risk, disciplinary risk, psychological risk, social risk, and time-loss risk. The second section of the survey instrument

consisted of five items focused on user reading preference. Participant responses in the first two sections were aggregated using a summary function and then normalized on a 0.0 – 1.0 scale for subsequent placement in the RPR Taxonomy and associate analysis according to RQ1 and RQ2's seven hypotheses. Lastly, the third section of the survey consisted of seven items, each item solicited participant data for each of the seven aforementioned study demographic variables. The selected case study organization was a privately held mid-sized business in the aerospace and defense industry whose employees regularly deal with proprietary information, especially when they participate in e-training activities.

DATA COLLECTION AND RESULTS

Data was collected using the Web-based survey instrument from employees in the case study organization. The initial draft of the survey instrument was refined based on direct feedback from the expert panel and subsequent pilot test. An invitation was sent by email to 1,728 employees and reminders were followed few days later. After pre-analysis data cleansing, a total of 311 usable responses remained, for a response rate of 18%. The demographics of the participants, in terms of age, gender, organization role, and education level reflected those of the overall organization as well as the aerospace and defense industry as a whole. Tests for validity using principal components analysis confirmed that the items load on their respective constructs. Further, tests showed support for reliability using Cronbach's α with results of .793 and .776 for the constructs: user reading preference and user perceived risk of compromising printed proprietary information, respectively. Then, appropriate analyses and statistical tests, including one-way ANOVA, Pearson's r, t-tests, and Kruskal-Wallis, were performed to assess the research questions and test the hypotheses. Table 1 summarizes the overall results with respect to hypotheses H1 – H7.

The results of the first research question (RQ1) showed that cases were dispersed across all four quadrants (Q1 – Q4). A concern identified was that 15.1% of the employees in the target organization were located in the more problematic Q3: Exposed, suggesting this portion of the population is likely the most exposed to the potential to compromise printed proprietary information.

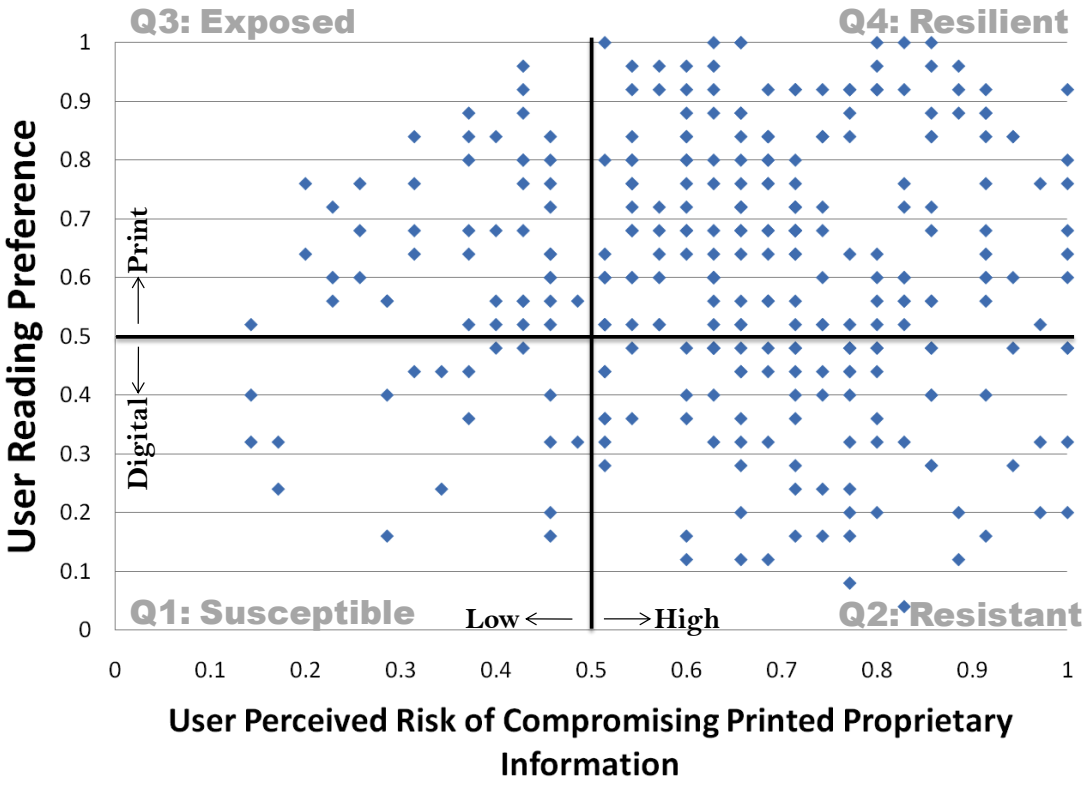

Figure 2: RPR Taxonomy Scatter Plot of Participant Responses

Overall, considering the mean score scale of 0.0 – 1.0 shown in Figure 2, RQ1 results also showed that the population had a reading preference for print materials (M = .61, N = 311) and a high perceived risk for compromising printed proprietary information (M = .65, N = 311), as demonstrated with the most number of cases located in Q4: Resistant. RQ1 results also showed that females had a higher preference for print materials as compared to males, a finding consistent with prior research (Eshet-Alkalai and Geri 2007; Levy 2008). Though not explicitly

hypothesized, a significant finding associated with RQ1 was that respondents had a significantly higher user reading preference for e-training materials to be printed when it was necessary to retain the content in memory as compared to when the e-training content was purely informational.

Table 1. Summary of Hypothesis Results

	Hypothesis Analysis	
H1	H1(a) There are no statistically significant differences in *user reading preference* based on *age*.	Reject
	H1(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on *age*.	Failed to Reject
H2	H2(a) There are no statistically significant differences in *user reading preference* based on *gender*.	Reject
	H2(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on *gender*.	Failed to Reject
H3	H3(a) There are no statistically significant differences in *user reading preference* based on *the frequency of user exposure to proprietary information*.	Reject
	H3(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on the *frequency of user exposure to proprietary information*.	Reject
H4	H4(a) There are no statistically significant differences in *user reading preference* based on *the confidentiality level of the proprietary information a user is regularly exposed to*.	Failed to Reject
	H4(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on *the confidentiality level of the proprietary information a user is regularly exposed to*.	Reject
H5	H5(a) There are no statistically significant differences in *user reading preference* based on *user previous experience with the compromise of proprietary information*.	Failed to Reject
	H5(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on *user previous experience with the compromise of proprietary information*.	Reject
H6	H6(a) There are no statistically significant differences in *user reading preference* based on *user organizational role*.	Failed to Reject
	H6(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on *user organizational role*.	Failed to Reject
H7	H7(a) There are no statistically significant differences in *user reading preference* based on *user education level*.	Failed to Reject
	H7(b) There are no statistically significant differences in *user perceived risk of compromising printed proprietary information* based on *user education level*.	Failed to Reject

The results associated with the second research question (RQ2) shown in Table 1 also demonstrate several interesting findings. Analysis of H1 revealed that age did have a significant

effect on user reading preference. Interestingly, per Figure 3, the results demonstrated a u-shaped parabola across the age groups related to reading preference, with the 20 – 29 age group as well as the 50 – 60 age group and >=60 age group showing higher preference for reading in print than both the 30 – 39 and 40 – 49 age groups. These findings appear counterintuitive since one might expect that the youngest generation, i.e. the 20 – 25 year old group, would have the least preference for print materials since they have most recently grown up with digital tools like personal computers, tablets, smartphones, and other digital devices. However, at least at the organization assessed, results show that it is the middle age groups that have the least preference for reading in print.

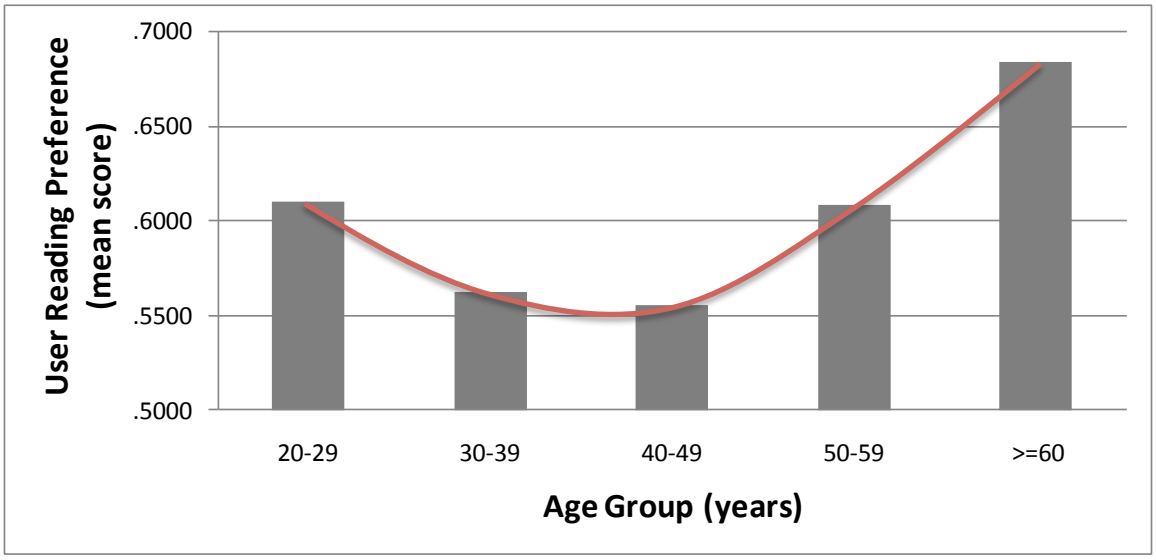

Figure 3. Mean Score Plot of User Reading Preference vs. Age

H1 results also showed that user perceived risk of compromising printed proprietary information did not have a significant difference based on age. Thus, contradicting prior research that found user perceived risk to have a significant difference based on age (Henwood et al. 2008; Cheng 2010). H2 t-test results revealed that user reading preference did have a significant difference based on gender [$t(309) = -2.90$, $p = .004$)] with females showing a higher user

reading preference for print materials than males, a finding consistent with Levy (2008). H3 ANOVA results revealed that both user reading preference [$F(5, 305) = 2.09$, $p = .067$] and user perceived risk of compromising printed proprietary information [$F(5, 305) = 4.34$, $p = .001$] had significant differences based on the frequency of user exposure to proprietary information. Considering the limited research on these relationships, the findings associated with user perceived risk may be significant since it suggests that employees with infrequent exposure to proprietary information have less perceived risk and, thus, may be more likely to mishandle printed proprietary information. H4 results revealed that user perceived risk of compromising printed proprietary information did have a significant difference based on the confidentiality level of the proprietary information a user is regularly exposed to [$F(5, 305) = 8.99$, $p < .001$]. These results appear to suggest that as employees gain access to increasingly confidential information they have a corresponding increase in the risks they perceive with that information. The H5 Kruskal-Wallis results revealed that user perceived risk of compromising printed proprietary information did have a significant difference based on user previous experience with the compromise of proprietary information [$\chi^2(5, N = 311) = 5.96$, $p = .310$]. Though consistent with the availability heuristic, these results are likely significant since they indicate that the more familiar an employee is with a prior situation where printed proprietary information was compromised, they will have a correspondingly higher user perceived risk of compromising printed proprietary information. The H6 and H7 results showed that user organizational role and education level, respectively, did not have a significant difference with either construct.

Limitations and Future Research

A limitation of this study is that this research was performed in only organization in the aerospace and defense industry, thus, confident extrapolation of the results and subsequent

findings may be limited. Additionally, since the case study organization in this study was US-based, the US culture may have played a role in risk perceptions and reading preferences. As such, one key limitation of this study is the US context.

The results of this study suggest several areas for future research. One recommendation would be to perform similar research, using both the RPR Taxonomy as well as the demographic variables in another industry that commonly deals with proprietary information. Future studies may also find it insightful to include a focus on coping appraisal or coping response, both elements of PMT that were not in the scope of this study. Lastly, future studies may use multiplicative models for user perceived risk and compare results.

DISCUSSIONS AND CONCLUSIONS

Several conclusions standout based on the results of this research. First, information systems users in the case study organization in this research have a reading preference for print materials, with females to a slightly higher degree. Additionally, they generally perceive there are high risks in dealing with printed proprietary information. Another conclusion is that users whom participate in e-training will likely have a significantly increased tendency to print the e-training material if it is necessary to retain the content for a test or exam. Another important implication for researchers relates to the findings associated with demographic (D3) frequency of user exposure to proprietary information, and (D4) confidentiality level of the proprietary information a user is regularly exposed to. The results showed that both D3 and D4 demonstrated a significant effect on a user's perceived risk of compromising printed proprietary information, with a corresponding positive relationship. The implication of this finding is that it is likely employees whom have infrequent exposure to proprietary information or are not regularly exposed to at least moderately confidential information; these individuals will likely have lower

perceived risks in dealing with the information. Thus, they may be less likely to take appropriate measures to protect the proprietary information. Another conclusion of this study relates to the findings associated with demographic (D5) user previous experience with the compromise of proprietary information. The results showed that the more familiar an employee is with a prior situation where printed proprietary information was compromised, they will likely have a higher user perceived risk of compromising printed proprietary information. The implication of this relationship is that when practitioners share detailed information regarding instances of printed proprietary information becoming compromised, this likely increases user perceived risks and may lead to increased protective behavior in their organizations. One of the implications for researchers is that the RPR Taxonomy can be used compare the distributions of people in the quadrants across other industries thereby increasing insight into consistencies, or inconsistencies, related to the behavioral preferences and risk perceptions affecting information security. Researchers, especially those investigating models and frameworks for information security assessments, can also leverage insights gained by the RPR Taxonomy to ensure a focus beyond electronic aspects of information security, thus, including more behavioral and human factor considerations as recommended by Bernard (2007), Da Veiga and Eloff (2010), as well as Kraemer et al. (2009). Overall, the results of this study contribute to information security body of knowledge by providing researchers and practitioners more insight to what influences users to print proprietary information, which could be compromised. It addresses calls from researchers and practitioners for an improved understanding of how user behaviors and user risk perception influence information security.

REFERENCES

Albrechtsen, E., and Hovden, J. 2009. "The Information Security Digital Divide Between Information Security Managers and Users," *Computers & Security* (28), pp. 476-490.

Bernard, R. 2007. "Information Lifecycle Security Risk Assessment: A Tool for Closing Security Gaps," *Computers & Security* (26), pp. 26-30.

Besnard, D., and Arief, B. 2004. "Computer Security Impaired by Legitimate Users," *Computers & Security* (23), pp. 253-264.

Carr, C., Furniss, J., and Morton, J. 2000. "Complying with the Economic Espionage Act," *Risk Management* (47:3), pp. 21-24.

Chang, S. L., and Ley, K. 2006. "A Learning Strategy to Compensate for Cognitive Overload in Online Learning: Learner Use of Printed Online Materials," *Journal of Interactive Online Learning* (5:1), pp. 104-117.

Cheng, C. 2010. "A Study of the Role of Perceived Risk in Continuing Education Participant's Learning Motivation," *The Business* Review (16:2), pp. 313-320.

Da Veiga, A., and Eloff, J. H. P. 2010. "A Framework and Assessment Instrument for Information Security Culture," *Computers & Security* (29), pp. 196-207.

Dlamini, M. T., Eloff, J. H., and Eloff, M. M. 2009. "Information Security: The Moving Target," *Computers and Security* (28), pp. 189-198.

Eshet-Alkalai, Y., and Geri, N. 2007. "Does the Medium Affect the Message? The Influence of Text Representation Format on Critical Thinking," *Human Systems Management* (26), pp. 269-279.

Goel, S., and Shawky, H. A. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information and Management* (46), pp. 404-410.

Hazari, S., Hargrave, W., and Clenney, B. 2008. "An Empirical Investigation of Factors Influencing Information Security Behavior," *Journal of Information Privacy & Security* (4:4), pp. 3-20.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organizations," *European Journal of Information Systems* (18), pp. 106-125.

Henwood, K. L., Parkhill, K. A., and Pidgeon, N. F. 2008. "Science, Technology, and Risk Perception: From Gender Differences to the Effects Made by Gender," *Equal Opportunities International* (27:8), pp. 662-676.

Kambourakis, G., Kontoni, D. N., Rouskas, A., and Gritzalis, S. 2007. "A PKI Approach for Deploying Modern Secure Distributed E-Learning and M-Learning Environments," *Computers &* Education (48), pp. 1-16.

Kraemer, S., Carayon, P., and Clem, J. 2009. "Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities," *Computers and Security* (28), pp. 509-520.

Kritzinger, E., and von Solms, S. H. 2006. "E-learning: Incorporating Information Security Governance," *Issues in Informing Science and Information* Technology (3), pp. 319-325

Levy, Y. 2008. "An Empirical Development of Critical Value Factors (CVF) of Online Learning Activities: An Application of Activity Theory and Cognitive Value Theory," *Computers and Education* (51)*,* pp. 1664-1675.

Levy, Y., and Ramim, M. 2009. "Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)," *Interdisciplinary Journal of E-Learning and Learning Objects* (5), pp. 379-397.

Pacini, C. J., Placid, R., and Wright-Isak, C. 2008. "Fighting Economic Espionage with State Trade Secret Laws," *International Journal of Law and Management* (50:3), pp. 121-135.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology* (91), pp. 93-114.

Spencer, C. 2006. "Research on Learner's Preferences for Reading from a Printed Text or from a Computer Screen," *Journal of Distance Education* (21:1), pp. 33-50.

Straub, D. W. 1989. "Validating Instruments in MIS Research," *MIS* Quarterly (13:2), pp. 147-169.

Sweller, J., and Chandler, P. 1994. "Why Some Material is Difficult to Learn," *Cognition and Instruction* (12:3), pp. 185-233.

Wiant, T. L. 2005. "Information Security Policy's Impact on Reporting Security Incidents," *Computers & Security* (24), pp. 448-459.

Workman, M. 2008. "A Test of Interventions for Security Threats from Social Engineering," *Information Management & Computer* Security (16:5), pp. 463-483.

APPENDIX A - SURVEY INSTRUMENT

Reading Preference and Perceived Risk Survey

Thank you for taking part in this brief, voluntary, and anonymous research survey that investigates user reading preferences and user risk perceptions associated with printed proprietary information. The results of this study promise to be of value to our organization, our customers, and our industry. Your participation is voluntary and all responses will be strictly confidential.

Section 1. User Perceived Risk Dimensions

The items in Section 1 below are related to the risks you perceive associated with the compromise of printed proprietary information that you regularly deal with. Proprietary information refers to information that your organization takes steps to protect from being publicly known.
Some examples of proprietary information in our organization, which you may deal with occasionally in printed form, includes financial information (e.g. in Monthly Performance Reviews), business plans (e.g. the business opportunities or acquisitions we are considering), human resources data (e.g. employee information), business processes (e.g. documents on how we perform internal processes), customer information (e.g. technical information on systems or projects), government classified information, and trade secrets.
The term "compromise" refers to proprietary information being viewed by unauthorized individuals.

Please rate how probable you think each of the following risks are by indicating one of the options from 1 (Strongly Disagree) to 6 (Strongly Agree).

Item	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
R1: If the printed proprietary information you regularly deal with were to become compromised, it would likely lead to financial losses for you or your organization.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
R1 Help Text: Note: It may be helpful to refer to the examples of proprietary information above.						
R2: If the printed proprietary information you regularly deal with were to become compromised, it would likely lead to risks to the physical safety of people or property.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
R3: If the printed proprietary information you regularly deal with were to become compromised, it would likely lead to attempts to legally prosecute you or members of your organization.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
R4: If the printed proprietary	(1)	(2)	(3)	(4)	(5)	(6)

Item	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
information you regularly deal with were to become compromised, it would likely cause you personal feelings of anxiety or tension.	Strongly Disagree	Moderately Disagree	Somewhat Disagree	Somewhat Agree	Moderately Agree	Strongly Agree
R4 Help Text: Note: The context of this question refers to your actions (or inaction) resulting in the compromise of the printed proprietary information.						
R5: If the printed proprietary information you regularly deal with were to become compromised, your colleagues, business associates or supervisors would likely think less highly of you.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
R5 Help Text: Note: The context of this question refers to your actions (or inaction) resulting in the compromise of the printed proprietary information.						
R6: Taking the recommended precautions to prevent compromising printed proprietary information never feels like a waste of your time.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
R6 Help Text: For example: placing printed proprietary information in proper disposal containers, or properly shredding documents						
R7: If the printed proprietary information you regularly deal with were to become compromised, it would likely lead to disciplinary action against you or your organization.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree

Section 2. User Reading Preference

These items (P1 - P5) are related to whether you prefer to read material in print form or a computer screen. The first two items (P1 - P2) ask about specific e-training situations. The term "e-training" refers to any training or learning, instructor-led or self paced, supported by information technology (e.g. online briefing of material you need to know - such as policies, processes, work procedures, business plans; formal training material you are studying for a test or certification). The remaining items (P3 - P5) are more general.

Note: You may find that some questions feel similar in nature, but this is intentional based on prior research.

Please rate your reading preferences below by indicating one of the options from 1 (Strongly Disagree) to 6 (Strongly Agree).

Item	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
P1: When studying for a test or exam, you prefer to print the e-training material instead of reading it from a	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree

Item	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
computer screen.						
P1 Help Text: The intent of this question relates to information you need to memorize.						
P2: When the e-training content is just informational, you prefer to print the e-training material instead of reading it from a computer screen.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
P2 Help Text: "Informational content" is intended to mean information you do not need to memorize. Examples could include: an overview of new policies, a briefing on business plans, a briefing on financial information.						
P3: You strongly prefer to read important information from a piece of paper rather than a computer screen.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
P4: You n ever mind reading from printed material.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree
P5: You get tired of reading from a computer screen.	(1) Strongly Disagree	(2) Moderately Disagree	(3) Somewhat Disagree	(4) Somewhat Agree	(5) Moderately Agree	(6) Strongly Agree

Section 3. Demographics

The items in Section 3 below are related to demographics about our survey participants.

Please respond below by indicating using the provided options.

Item	Responses					
D1: Age	(1) <20	(2) 20-29	(3) 30-39	(4) 40-49	(5) 50-59	(6) >= 60
D2: Gender	(1) Male	(2) Female				
D3: How frequently are you exposed to proprietary information?	(1) Never	(2) A Few Times per Year	(3) A Few Times per Month	(4) A Few Times per Week	(5) A Few Times per Day	(6) Many Times per Day
D3 Help Text: Proprietary information refers to information that your organization takes steps to protect from being publicly known.						
D4: How confidential is the proprietary information that you are regularly exposed to?	(1) Not at all	(2) Very Low	(3) Low	(4) Moderate	(5) High	(6) Very High
D4 Help Text: "Confidential" refers to your understanding of how important your organization considers the proprietary information. In some cases the level of confidentiality is explicit.						
D5: Do you have familiarity with any situation where proprietary information was compromised?	(1) Not at all familiar	(2) Vaguely Familiar	(3) Slightly Familiar	(4) Moderately Familiar	(5) Very Familiar	(6) Extremely Familiar
D5 Help Text: This may include situations that you were personally involved in or learned about in some way.						

Item	Responses					
D6: What is your organizational role?	(1) Junior-level Non-Management	(2) Middle-level Non-Management	(3) Senior-level Non-Management	(4) First-level Management	(5) Middle Management	(6) Senior Management
D7: What is the highest level of education that you completed?	(1) Grade school or some high school	(2) High School or GED	(3) Community College or Technical School	(4) Bachelor's Degree	(5) Master's Degree	(6) Doctoral Degree or Ph.D.