Computers in Human Behavior 83 (2018) 32–44

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

The impact of information security threat awareness on privacy-protective behaviors

Stanislav Mamonov [a, *], Raquel Benbunan-Fich [b]

[a] Montclair State University, Department of Information Management and Business Analytics, Feliciano School of Business, 1 University Ave, Montclair, NJ 07043, USA

[b] Baruch College, CUNY, Information Systems and Statistics Department, Zicklin School of Business, One Bernard Baruch Way, Box B11-220, New York, NY 10010, USA

ARTICLE INFO

Article history:

Keywords:
Security
Privacy
Protective behaviors
Passwords
Self-disclosure

ABSTRACT

In this study, we examine how to motivate computer users to protect themselves from potential security and privacy threats. We draw on the Information Processing framework which posits that threat mitigation commonly occurs before full cognitive threat assessment and we conduct an empirical study to evaluate the effects of an exposure to general information security threats on the strength of passwords and the disclosure of personal information. Through an online experiment, we compare immediate computer user reactions to potential non-individually specific security and privacy threats in an extra-organizational context. We find evidence consistent with automatic security and privacy protective actions in response to these threats. Computer users exposed to news stories about corporate security breaches limit the disclosure of sensitive personal information and choose stronger passwords. The study complements the existing behavior modification research in information security by providing the theoretical and empirical foundation for the exploration of automatic security and privacy threat mitigation strategies across different contexts.

1. Introduction

Continued integration of technology into everyday life exposes technology users to growing security and privacy risks. According to a survey of Chief Information Officers by PricewaterhouseCoopers, 42.8 million security incidents were detected in 2016, showing a 48% increase over the previous year (PricewaterhouseCoopers, 2017). The economic impact of the security breaches is estimated at nearly half a trillion dollars globally (Ponemon Institute, 2017). Password breaches are one of the most common information security failures. Although there is a considerable body of research on the best practices in secure computing (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013; Yang & Tate, 2012; Zeng, Wang, Deng, Cao, & Khundker, 2012), companies continue to struggle with preventing password breaches. In 2015, the Central Intelligence Agency discovered that 47 government agencies, including the Department of Homeland Security, were compromised, giving the hackers access to over 21 million government employee accounts (Hirschfield Davi, 2015). Equifax, one of the three largest credit agencies, recently reported that it suffered a breach that affected 143 million consumers (McMillan & Knutson, 2017) and Yahoo announced that over three billion user accounts were impacted in the previously reported breach (Andriotis & McMillan, 2017). These events indicate that secure password selection and protection remains a problematic area of practice that merits further research.

News of security breaches feeds a parallel trend in modern society because they exacerbate concerns about potential privacy violations. Increased reliance on technology to store and communicate personally identifiable information exposes technology users to ever-growing privacy risks. Yet, researchers have found that, seemingly in contradiction to increasing privacy concerns, people continue to disclose ever-growing volume of personal information online (Barnes, 2006) and this trend shows no signs of slowing down. Recent social media statistics show that Facebook users share over 300 million images through the social network platform every day (Zephoria Digital Marketing, 2017). The growing frequency of security incidents along with the mounting volume of

* Corresponding author.
E-mail addresses: stanislav.mamonov@montclair.edu (S. Mamonov), rbfich@baruch.cuny.edu (R. Benbunan-Fich).

https://doi.org/10.1016/j.chb.2018.01.028
0747-5632/

technology-mediated information disclosure raises the question of how to motivate technology users to protect themselves.

Interdisciplinary research has established that people have two alternative information processing systems: automatic (fast) and effortful cognitive (slow) (Kahneman, 2011). The cognitive approach to motivating employee compliance with organizational security policies has been a central theme in Information System search (Sommestad, Karlzén, & Hallberg, 2015). However, little is known about the *automatic* reactions of technology users to immediate perceived privacy and security threats. We draw on the Information Processing (IP) framework (Beck & Clark, 1997), which emphasizes automatic threat mitigation in response to threatening stimuli and we conduct an experimental study to evaluate the effects of an exposure to information security threats on the strength of passwords and disclosure of personal information. We manipulate the exposure to information security threats by showing the participants different types of news stories. The control group is exposed to general technology-related news, while the treatment group is exposed to computer security breach related stories. For these two conditions, we evaluate the differences in two behavioral variables: the strength of passwords chosen by participants to protect their responses and the degree of refusal to answer personal questions in a self-disclosure survey.

2. Theoretical background and hypotheses

The focus of our study is on the automatic computer user reactions to potential security and privacy threats. We draw on the IP framework as the theoretical foundation for our study. The IP framework posits that threat mitigation often precedes full cognitive threat assessment (Beck & Clark, 1997). Before we discuss the automatic threat mitigation, we will review the established stream of research which has focused on a related question of how to motivate employee compliance with organizational security policies through cognitive persuasion. This stream of research evolved from the observation that organizational insiders are often responsible for the organizational security breaches (Zadelhoff, 2016). Promoting organizational security policy compliance is seen as a key factor in corporate security breach prevention.

Protection motivation theory (PMT), which was initially developed in health-related behavior modification research (Maddux & Rogers, 1983; Prentice-Dunn & Rogers, 1986; Rogers, 1975), has served as the focal theoretical foundation for the stream of research examining ways to persuade employees to adhere to organizational security policies (Sommestad et al., 2015). PMT research on health-related topics provided evidence that exposure to "persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" can be effective in motivating behavior modification, e.g. in motivating people to quit smoking (Witte, 1992). PMT posits that perceived threat severity, perceived vulnerability, self-efficacy and response efficacy are the key factors that affect individual behavioral intentions (Maddux & Rogers, 1983; Prentice-Dunn & Rogers, 1986). Applying PMT to the organizational security policy compliance contexts, prior research has shown that fear appeals and threats of personal responsibility can have a positive effect on employee intention to follow organizational policies (Ifinedo, 2014; Johnston & Warkentin, 2015). However, the results have not been consistent across the studies. For example, a study of employee intention to comply with organizational security policies in the United States showed no significant effects of perceived threat severity or perceived threat susceptibility after considering the effects of perceived security policy legitimacy and organizational value congruence (Son, 2014). A recent study by Boss et al (Boss, Galletta, Lowry, Moody, & Polak, 2015). involving student reactions to malware threats similarly found no significant direct effects for perceived threat severity and perceived susceptibility on the behavioral intention. Contrary to the predictions of the PMT, Boss et al. (2015) also documented a negative effect of self-efficacy on the behavioral intention. Individually-relevant fear appeals are at the core of PMT because fear is believed to be the core emotion that motivates changes in attitudes and behavioral intentions (Floyd, Prentice-Dunn, & Rogers, 2000; Johnston, Warkentin, & Siponen, 2015). Recent neuroimaging studies have further challenged PMT assumptions in information security research by showing that computer security-related warnings commonly fail to produce activation in the brain regions associated with fear (Warkentin, Johnston, Walden, & Straub, 2016).

In addition to the inconsistencies concerning the effects of the core PMT constructs in information security research, there has also been very little work on examining actual user behaviors using objective security-related behavior measures. The majority of studies applying PMT to examine organizational security policy compliance have been limited to measuring respondents' intentions (Sommestad et al., 2015). The studies that did measure security policy compliance have generally relied on self-reports. The only study which measured PMT constructs and actual behaviors did so measuring behaviors first and PMT constructs second, thus undermining the interpretation of the results on the effects of PMT constructs in motivating the behaviors (Boss et al., 2015). A summary of security policy compliance studies that include compliance behavior measures is presented in Appendix A1. Prior research has shown that self-reports can be unreliable in security (Sonnenschein, Loske, & Buxmann, 2016) and privacy-related (Barnes, 2006) contexts. Hence, the question of whether fear appeals can be effective in promoting actual user compliance with the organizational security policies remains open. Technology-mediated personal information disclosure also exposes the users to privacy risks. Self-disclosure has similarly been extensively studied in Information Systems, yet the vast majority of studies have relied on self-reports to assess individual self-disclosure. Li, Lin, and Wang (2015) exemplify a parallel approach to evaluating self-disclosure which relies on the analysis of secondary data, e.g. information that people share in social networking sites. There has been little in the way of experimental evidence on factors that may affect self-disclosure. A summary of recent studies involving evaluation of different factors that affect self-disclosure is provided in Appendix A2. In the present study, we seek to address the relative lack of knowledge about actual security and privacy-related user behaviors by examining automatic responses that occur following the exposure to information about the potential threats. To this end, we apply the IP framework proposed by Beck and Clark (1997) to lay the theoretical foundation for our study. The IP framework posits that the behavioral response to a threat often precedes cognitive assessment of the potential hazard. These predictions have been confirmed in individual psychology (Zajonc, 1980) and in marketing (Obermiller & Spangenberg, 1989). This framework is suitable to evaluate users' actions from a pragmatic perspective. Due to the time pressures of modern life, people are often motivated to make split-second decisions that simply do not leave much room for cognitive evaluation. This may occur, for example, when a user is requested to specify a new password or is prompted with a request for personal information online.

The IP framework posits that threat-related information processing consists of three stages: automatic threat detection, focusing of attentional resources towards goal-directed activities,

and secondary elaboration. The first stage, termed *automatic processing*, consists of automatic identification of threatening stimuli. Threat detection is involuntary and it occurs without conscious awareness. The second stage in the IP framework emphasizes that finding a solution to the detected threat is the primary response to a threat. This second stage is characterized by *autonomic arousal*, narrowing of cognitive focus on the threat and behavioral mobilization in response to the threat. Recent functional magnetic resonance studies have shown that exposure to a threating stimulus is strongly associated with increasing activity in the problem-solving areas of the brain, supporting the propositions of the IP framework (Bishop, Duncan, Brett, & Lawrence, 2004) and these results have been confirmed in the computer security domain (Warkentin et al., 2016). The third stage in the framework is termed *secondary elaboration* and it encompasses strategic information processing, which includes assessment of one's ability to cope with similar threats in the future. This stage is characterized as a slow and effortful process, which is affected by a person's prior knowledge and mental schemas. In other words, the IP framework posits that the cognitive assessment of one's vulnerability to a threat and individual response self-efficacy commonly occurs after the actual mitigation of the threat. While threats in the environment often require immediate action, threat mitigation does not require cognitive assessment of individual vulnerability or efficacy.

While the IP framework is well suited for studying actual user behavior in response to the immediate privacy and security threats, it is important to highlight the key differences between the IP framework and PMT. PMT sheds light on which attitudes and perceptions can affect the intent to protect one's privacy and security and it may help in motivating employee compliance with the organizational computer security policies. In contrast, the IP framework helps us understand how technology users *actually react* to the immediate perceived security and privacy threats. PMT presumes that behaviors are affected by the behavioral intentions which in turn can be affected by perceptions of threat severity, individual vulnerability, general self-efficacy and the specific response self-efficacy (Maddux & Rogers, 1983; Rippetoe & Rogers, 1987). The IP framework is relevant in understanding how users respond to immediate threats that require immediate mitigation (Beck & Clark, 1997). The framework posits that in the contexts that require immediate threat mitigation cognitive assessment (secondary elaboration) does not occur until after the threat is mitigated, i.e. user takes action before perceptions and attitudes are reassessed. By experimentally manipulating the presence (or absence) of a potential threat, we will investigate its potential effect on actual user behavior. The study is thus focused on the second stage of the IP framework, which encompasses automatic threat mitigation. In particular, to assess the predictions of the IP framework in the context of technology users' reactions to security and privacy threats, we examine two key user behaviors: the strength of newly chosen passwords and the reluctance to disclose personal information. The strength of passwords provides an indication of a reaction to a perceived immediate security threat, whereas the disclosure of personal information (or lack thereof) provides evidence of a reaction to a perceived immediate privacy threat. Next, we provide a brief overview of the role of passwords in information security.

Information confidentiality along with integrity and availability are the core objectives of information security measures (Bishop, 2004). Confidentiality refers to keeping data secret. Secrecy of information is commonly accomplished by implementing user authentication and establishing access controls that restrict who has access to what. User authentication can be accomplished through a combination of techniques that are either knowledge-based ("what you know"), possession-based ("what you have") or biometric-based ("who you are"). The highest level of protection is afforded by biometric authentication (Burrows, Abadi, & Needham, 1989). While multi-factor authentication is widely recommended, most e-commerce systems in place today rely on a single-factor authentication, mainly passwords. Creating secure passwords presents a common challenge. For passwords to be effective, the users have to be able to remember them, yet the passwords have to be difficult to guess. Strong passwords, based on unusual combinations of letters, numbers and symbols, are often difficult to remember (Nelson & Vu, 2010; Yan, 2004). Consequently, studies have repeatedly shown that technology users often rely on weak passwords for authentication online (Dell'Amico, Antipolis, Michiardi, & Roudier, 2010) and password breaches stemming from brute-force password-guessing attacks are a common phenomenon in practice (Bright, 2014; Hill, 2014).

Drawing on the IP framework, we expect that exposure to information highlighting recent computer security breaches will trigger automatic processing which will identify the stories as a source of potential threat to individual computer security. The automatic threat identification will trigger mobilization of cognitive efforts to address the apparent threats and consequently the users exposed to the stories about computer security breaches will choose stronger passwords compared to the users exposed to general technology-related news stories.

H1. Awareness of information security threats has a positive effect on the strength of newly chosen passwords.

Another form of threat mitigation is the refusal to disclose information. Self-disclosure is defined as the act of revealing personal information to others (Jourard, 1971). Self-disclosure is an important part of self-expression (Livingstone, 2008) and it plays a key role in the development of social relationships (Cozby, 1973). Reciprocated self-disclosure helps to identify common ground and build trust in relationships (Wheeless & Grotz, 1977). In addition to serving individual goals, self-disclosure can have an impact that goes beyond the individual. For example, a study of online product reviews on Amazon.com found that disclosure of personal information within product reviews influences review evaluation and subsequent self-disclosure by other reviewers (Forman, Ghose, & Wiesenfeld, 2008).

Early research on computer-mediated communication suggested that technical restrictions, which preclude transmission of non-verbal cues, may lead users to increase self-disclosure in technology-mediated contexts in order to overcome technology limitations (Joinson, 2001). Perhaps few social phenomena capture apparent willingness among people to disclose personal information, as do social networking sites and social media. Estimates suggest that users share nearly 3 million bits of information through Facebook every minute (Wishpond, 2015). Facebook has announced plans to commercialize the wealth of information shared by users through the service (Don Mathis, 2014), suggesting that much of the information shared by the users through the service reveals something personal about them.

Perceptions of a privacy threat associated with computer security breaches will trigger an automatic response to the threat and action to address the risk to individual private information. It is important to note that while security breaches and privacy violations are conceptually distinct, in practice these threats often occur together. A security breach takes place when there is an instance of unauthorized computer access, regardless of the purpose of the access or whether actual data was compromised. In contrast, a privacy violation occurs when personally identifiable information collected for one purpose is used for another purpose without the individual's consent (Mamonov & Benbunan-Fich, 2015; Mamonov & Koufaris, 2014). Since personal data is increasingly collected and stored in databases and it commands high resale value in secondary markets, security breaches are often accompanied by privacy violations (Lord,

2016). For individuals concerned about privacy, withholding information (non-disclosure) presents one potential coping action in the face of a privacy threat (Joinson, Reips, Buchanan, & Schofield, 2010). Consequently, we expect that users exposed to stories about computer security breaches will disclose less information than users exposed to general technology-related news.

H2. Awareness of information security threats has a positive effect on the refusal to disclose personal information (non-disclosure).

How people react to different threats is in part determined by individual characteristics. Self-efficacy, the belief that one has the ability to perform a particular behavior, is among the key individual attributes which affect human activity across different domains (Bandura, 1977). Domain-specific self-efficacy is generally a better predictor of individual behaviors and computer self-efficacy has emerged as an important factor that predicts anxiety associated with computer use and system usage intention (Compeau & Higgins, 1995). Self-efficacy has also been shown to play a role in e-commerce use (McElroy, Hendrickson, & Townsend, 2007) and contributions to corporate knowledge management systems (Kankanhalli, Tan, & Wei, 2005). In the domain of computer security and privacy, self-efficacy has been shown to be positively related to self-reported protective behaviors, e.g. removal of cookies from the computer (Milne, Labrecque, & Cromer, 2009).

The Information Processing framework suggests that individual self-efficacy assessment occurs after the automatic threat mitigation, as a long-term process aimed at evaluating and adjusting one's level of self-efficacy. However, extensive research in management and information systems suggests that self-efficacy reflects one's experience in a specific domain, and therefore it could influence the speed and efficacy of automatic behaviors (Tiffany, 1990). While much of the research on the role of self-efficacy in general human behavior has focused on the direct effect of self-efficacy on the behavioral intention, computer security-related studies (Anderson & Agarwal, 2010; Johnston et al., 2015), have emphasized that self-efficacy not only has the direct effects, but it also moderates the response to specific threats (Maddux & Rogers, 1983). This effect has been confirmed in an experimental study which showed that security related self-efficacy moderates the computer security prevention intention in response to a security threat (LaRose, Rifon, & Enbody, 2008). Drawing on these theoretical roots and empirical findings, we expect that privacy self-efficacy, i.e. one's assessment of his or her ability to protect privacy online, will moderate the effects of exposure to security-related breach stories on both the strength of passwords that people use to protect their responses and the degree of non-disclosure to personal questions.

H3a. Privacy self-efficacy will positively moderate the effect of awareness of information security threats on the strength of passwords.

H3b. Privacy self-efficacy will positively moderate the effect of awareness of information security threats on the refusal to disclose personal information.

Threat mitigation responses include securing information with protection mechanisms such as passwords, and evaluating the disclosure risks of new information. Passwords can provide a degree of control over personal information. Greater perceived control over information has been linked with greater wiliness to disclose private information in research (Taddei & Contena, 2013) and in practice (Cavusoglu, Phan, Cavusoglu, & Airoldi, 2016). When a new protection mechanism is used to secure information, users may perceive higher levels of safety and lower risks of privacy breaches. A meta-analysis of self-disclosure in computer-mediated contexts shows that perceived safety is positively related to disclosure of personal information (Weisband & Kiesler, 1996). Therefore, we expect that selecting a stronger password would lead to lower levels of withholding personal information.

H4. The strength of newly chosen passwords will be negatively related to the refusal to disclose personal information.

The research model is summarized in Fig. 1 below.

3. Methodology

We conducted a between-groups online experiment to evaluate the hypotheses in our study.

3.1. Participants

We recruited the participants from Amazon Mechanical Turk (AMT). AMT is an online labor market for micro tasks. AMT *requesters* post tasks and offer compensation for task completion. AMT *workers* elect to work on the tasks and receive compensation upon task completion. AMT represents a readily accessible pool of over 500,000 workers that affords a more representative participant pool for research studies compared to student samples commonly used in research. AMT has been actively used for marketing and psychology studies (Buhrmester, Kwang, & Gosling, 2011; Whitla, 2009) and it has also been recommended as a source of participants for user behavior research (Steelman, Hammer, & Limayem, 2014), and for studies that focus on extra-organizational behaviors (Lowry, D'Arcy, Hammer, & Moody, 2016).

We required potential participants to be based in the United States to avoid potential cultural effects in our samples. We recruited 400 participants for our study and we paid $0.75 per participant. This level of compensation was on par with other similar tasks available on AMT. We included several trap questions in the demographic survey to assure that the participants were actually reading the survey questions. We excluded 10 participants from the analysis due to automatic response bias (same answers for all questions) or leaving most of the questions blank.

We used random assignment to assign participants to one of two experimental conditions. 191 participants were assigned to the control group and 199 participants were assigned to the treatment condition. The average age for control and the treatment groups was 37.2 ± 12.9 and 35.4 ± 11.4 respectively. 52% and 54% of the participants were male in the control and the treatment groups respectively. In terms of education, 36% of the control group and 39.4% of the treatment group had completed their undergraduate education and further 27.5% and 30.6% of the control and treatment groups respectively had taken college courses, but had not yet completed their undergraduate degree programs.

4. Materials

Each study participant was exposed to four stories. The control group was exposed to four general technology-related stories. The treatment group was exposed to four stories describing instances of corporate computer security breaches. The stories were presented in the same order to the participants in each group. Sample stories are provided in Appendix B. We validated the expected treatment effects of the exposure to the news stories in a pilot study in which

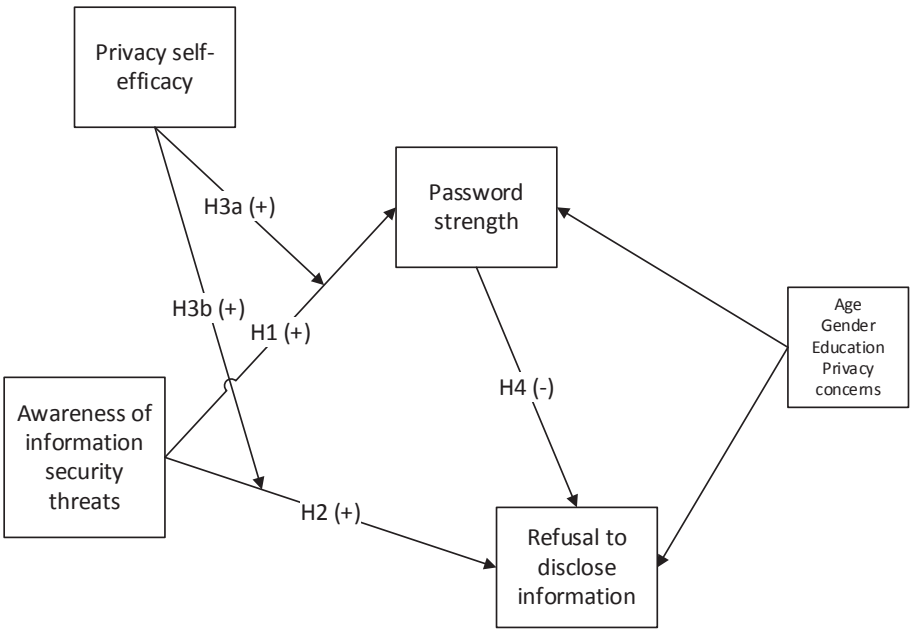

Fig. 1. Research model.

we exposed the participants to either of the two sets of news stories and surveyed the responses to the questions concerning the extent of privacy and security risks posed by online information sharing.

Following the exposure to the stories, we asked the participants to set a password to protect the answers to a self-disclosure questionnaire. The instrument presented a series of 18 questions to assess their willingness to disclose personal information, based on (Joinson, Paine, Buchanan, & Reips, 2008). It includes questions asking personal information such as: *How many different sexual partners have you had?, Have you ever deliberately viewed pornography using the internet?* One of the possible answers to each of the 18 questions assessing self-disclosure was "prefer not to say". Prior research has shown that this option encourages survey participants to provide more complete and truthful information (Joinson, Woodley, & Reips, 2007). We scored non-disclosure as the number of times that each participant selected the "prefer not to say" response among the 18 questions comprising the self-disclosure measure.

4.1. Procedures

The study was posted as a task on AMT and the workers who elected to participate were provided with a link to an online survey hosted on Qualtrics, a commercial survey platform. The study received an IRB approval and the participants indicated their consent to the participation in the study at the beginning of the study. The experimental survey consisted of three parts: (1) showing technology-related stories (general for the control group or cybersecurity breaches for the treatment group); (2) asking participants to take a self-disclosure questionnaire but setting a specific password to protect their responses. We did not tell the participants that the strength of passwords and non-disclosure were the dependent variables at the beginning of the study; (3) debriefing at the conclusion of the experiment to inform participants about the objectives of the study. The participants were not limited in the time that they took to complete the study.

4.2. Measures

Password strength was measured using a methodology developed in password security research (Florencio & Herley, 2007). The methodology draws on information theory (Shannon, 1948) and it estimates how many attempts would be required to guess a password. Password strength is calculated as a function of implied character pool and password length. Character pool is a function of the different types of characters that are used in the password. If a password uses only lower case letters then there are 26 possible values (a-z) at each position within the password. If a password contains both upper and lower case letters, then the number of possible characters at each position is 52. Numbers (0–9) add 10 potential characters to the list of possible characters at each position. The use of special characters adds another 22 potential values at each position. The total number of potential passwords given the character pool and password length is calculated as: *potential combinations* = [*size of character pool*]^*password length*. Prior research on password security has adopted a log measure of password strength as a standard (Florencio & Herley, 2007):

Password strength = $\log_2(C^L)$, where C is the size of the character pool and L is the length of the password.

In evaluating the effects of the experimental manipulation, we also included age, gender, education, and privacy concerns about information collection, and about unauthorized information use as covariates. The scales for the privacy-related constructs are shown in Appendix C.

5. Data analysis and results

We employed the Partial Least Square method through SmartPLS version 3 software (Ringle, Sarstedt, & Straub, 2012). PLS has an advantage over linear regression analysis in that the method iteratively estimates item loadings on the latent factors and correlations between the factors thus providing more robust estimates of the latent construct values and the correlations among the constructs (Hair, Ringle, & Sarstedt, 2011). Further, PLS does not make any distributional assumptions and it is robust with non-normally distributed data (Hair, Hult, Ringle, & Sarstedt, 2016).

Table 1
PLS loadings and cross-loadings.

	Privacy Concerns - Information Collection	Privacy Concerns - Unauthorized Info Use	Privacy Self-Efficacy
PrC_Col1	**0.884**	0.463	−0.103
PrC_Col2	**0.701**	0.516	−0.018
PrC_Col3	**0.886**	0.540	−0.114
PrC_Col4	**0.931**	0.486	−0.215
PrC_Una1	0.464	**0.880**	−0.027
PrC_Una2	0.488	**0.817**	−0.008
PrC_Una3	0.411	**0.778**	0.028
PrC_Una4	0.478	**0.860**	−0.015
PrivSE1	−0.146	−0.029	**0.930**
PrivSE2	−0.171	−0.022	**0.934**
PrivSE3	−0.166	0.006	**0.923**

The password strength measure which is a key dependent variable in our model is not normally distributed.

As the first step in our analysis, we evaluated the convergent and discriminant validity as well as reliability of the survey instrument in the present study. We assessed convergent validity by evaluating item cross-loadings on constructs in the research model. The results are shown in Table 1. Individual survey items have loadings above 0.7 on the respective constructs. The loadings on the respective constructs exceed loadings on other constructs in the model indicating good convergent validity. Discriminant validity was assessed by comparing inter-construct correlations with the square root of average variance extracted (AVE) for the respective constructs, as shown in Table 2. The average variance extracted is above 0.7 for all constructs and the square root of AVE is greater than the correlation coefficients among the constructs, indicating appropriate discriminant validity. Construct measurement reliability was assessed using composite reliability and Cronbach's alpha scores. The data are provided in Table 2. All values for composite reliability and Cronbach's alpha are above the generally accepted threshold of 0.70.

5.1. Structural model

We used PLS bootstrapping resampling procedure with 200 subsamples to assess the statistical significance of the standardized path coefficients in our model. We found that awareness of information security threats had a significant positive impact on the strength of passwords ($\beta = 0.23$, $p < 0.01$). To ascertain the degree of the difference in the password strength between the two groups we determined the average log score for each group. The log score for the control group was 34.3, the log score for the treatment condition was 43.3. The participants in the group exposed to the news about security breaches used 500 times stronger passwords compared to the control group ($2^{43.3}/2^{34.3} = 532.4$). These results provide support for H1.

The structural path between awareness of information security threats and non-disclosure in the PLS analysis was not significant. Further examination of the results revealed that participants in both groups answered "prefer not to say" less than once on average for the 18 questions assessing self-disclosure. We also did not find evidence of statistically significant relationships between general privacy self-efficacy and either password strength or non-disclosure behavior. Privacy self-efficacy was not a statistically significant moderator of the impact of awareness of information security threats on either password strength or non-disclosure behaviors.

We hypothesized that respondents who choose stronger passwords would feel more confident in revealing personal information than those with weaker passwords. However, the relationship between the strength of passwords and the refusal to disclose personal information was not statistically significant. Hence, H4 is not supported. While participants were told that they had to set a password to protect their answers, the strength of the password (or lack thereof) did not influence the extent to which they disclose sensitive information.

Given the unexpected lack of support for a positive relationship between the exposure to security breach related stories and non-disclosure (H2) from the PLS path analysis, we examined the responses to self-disclosure questionnaire in more detail. The questionnaire includes some fairly innocuous questions, e.g. *are you right or left handed*, as well as fairly intrusive ones, e.g. information about drug use. We examined the proportion of participants responding "prefer not to say" to the individual questions. The results are shown in Appendix D.

Three of the eighteen individual questions on the self-disclosure survey show significantly higher non-disclosure for the group exposed to security breach related news. Following the recommendations of Gefen, Rigdon, and Straub (2011) to evaluate alternate models as a way of building stronger theoretical arguments, we defined two new constructs: sensitive information non-disclosure and non-sensitive information non-disclosure. These constructs will enable us to examine whether people treat potentially sensitive information differently. The sensitive information non-disclosure was measured as the number of times the participants responded "prefer not to say" to the three potentially sensitive questions: 1) Have you ever driven whilst you suspected you may be over the legal alcohol limit? 2) As an adult, have you ever tried any drugs (other than alcohol and nicotine, e.g. marijuana, cocaine, ecstasy, heroin)? 3) Do you agree with the death penalty?

We used the number of "prefer not to say" responses to the remaining questions on the self-disclosure survey as the measure of non-sensitive information non-disclosure and we evaluated the structural relationships in this model. We found that the exposure to potential privacy and security threat had a positive effect on the strength of passwords ($\beta = 0.23$, $p < 0.01$) and refusal to disclose sensitive information ($\beta = 0.12$, $p < 0.01$). There was no significant effect on the refusal to disclose non-sensitive information. These results provide support for H2. For the remaining hypotheses, we

Table 2
Descriptive statistics, measurement reliability, inter-construct correlations and square root of AVEs (in the diagonal).

	Mean	Standard Deviation	Composite reliability	Cronbach's alpha	Privacy Concerns - Information Collection	Privacy Concerns - Unauthorized Info Use	Privacy Self-Efficacy
Privacy Concerns - Information Collection	5.75	1.10	0.91	0.90	0.85		
Privacy Concerns - Unauthorized Info Use	6.32	0.82	0.90	0.87	0.54	0.83	
Privacy Self-Efficacy	4.33	1.51	0.95	0.92	−0.17	−0.01	0.93

followed the recommendations in Hair et al. (2016) to assess the moderating effects of privacy self-efficacy on password strength and information disclosure. Neither the direct, nor the moderating effects of privacy self-efficacy was significant. We also followed Hair et al. (2016) recommendations on mediation testing in PLS models in evaluating the mediating effects of password strength on information disclosure. Neither the direct, nor the mediating effect of password strength on sensitive information disclosure was significant.

Common method bias is not a significant concern in the evaluation of the direct effects of awareness of information security threats because the awareness is experimentally manipulated. Common method bias could be a concern if the relationship between the password strength and refusal to disclose sensitive information was significant, but the relationship was not supported by the data. To further assess the predictive quality of our model, we examined the Stone-Geisser's Q^2 for both the password strength and sensitive information non-disclosure. The Q^2 values for both constructs are positive, indicating that the model has predictive value for the respective constructs (Hair et al., 2016). We also examined potential inner-model collinearity effects by examining VIFs (Variance Inflation Factors), but found no evidence of significant multicollinearity. The results of the alternate model evaluation are summarized in Fig. 2.

5.2. Post-Hoc tests on password strength

Our operationalization of password strength was based on a mathematical formula to determine the entropy of the password given the number of character sets and the length. This entropy-based measure is known to have limitations (Bonneau, 2012; Kelley et al., 2012; Weir, Aggarwal, Collins, & Stern, 2010). For example, the measure does not account for some commonly used passwords that may receive reasonable entropy scores, e.g. “abc123” and “trustno1”, but can be easily defeated in brute-force password guessing attacks utilizing known weak password lists. The latest research on the assessment of password effectiveness suggests that subjecting passwords to brute-force attacks provides a better measure of password strength (Ur et al., 2015).

To further evaluate the effects of the exposure to security breach related stories on the strength of passwords in our study, we conducted follow up tests to assess password guessability using four different password guessing algorithms: probabilistic context-free grammar (PCFG), Markov model password guesser, John the Ripper and Hashcat. The full details of each algorithm are beyond the scope of this manuscript. Here we only provide the basic details of the password guessing strategies associated with each of the methods. We refer the reader to Ur et al. (2015) for a more detailed discussion of each method. The PCFG algorithm generates password guesses based on the frequency of different characters in a training dataset. The Markov model based algorithm follows the implementation described in Ma et al. (Ma, Yang, Luo, & Li, 2014). John the Ripper and Hashcat are wordlist based password attack tools that are commonly used by both hackers and system administrators conducting audits of user passwords (Ur et al., 2015).

The results of the four password guessing tests, summarized in Table 3, were consistent.

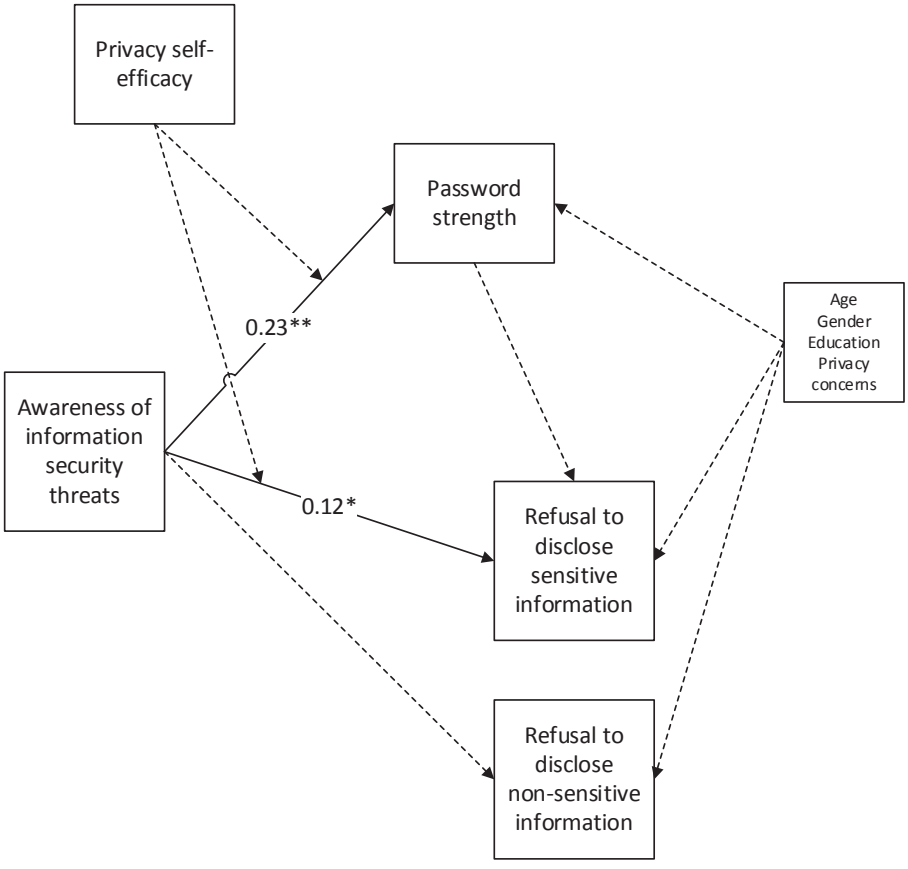

Fig. 2. Structural model results.

Table 3
Logistic regression tests of exposure to security breach related news stories on the guessability of passwords.

Algorithm	The effect of exposure to security breach related news
Hashcat	Model chi-square = 18.866, df = 4, p < 0.001 Treatment effect B = −0.929, Wald statistic = 12.176, p < 0.001,
John the Ripper	Model chi-square = 16.478, df = 4, p < 0.01 Treatment effect B = −0.527, Wald statistic = 5.525, p < 0.02
Markov	Model chi-square = 15.480, df = 4, p < 0.01 Treatment effect B = −0.564, Wald statistic = 4.854, p < 0.05
CPFG	Model chi-square = 17.356, df = 4, p < 0.001 Treatment effect B = −0.528, Wald statistic = 6.26, p < 0.02

The logistic regression tests using the successful password guesses as the dependent variable (1 − guessed successfully, 0 − could not be guessed), showed that participants exposed to security breach related news stories used significantly harder to guess passwords after controlling for age, gender and education. These results provide further support for H1.

6. Discussion

The goal of our study was to gain insight into automatic reactions of technology users to potential security and privacy threats, from the perspective of the Information Processing framework (Beck & Clark, 1997). We conducted an experimental study and evaluated the differences in the password strength and non-disclosure between two groups. The control group was exposed to general technology news and the treatment group was exposed to news stories about security breaches involving private information. Based on the premises of the Information Processing framework, we expected that exposure to the news about security breaches would trigger an automatic response reflected in stronger passwords being used to protect participants' responses in our study, and an increase in non-disclosure on a survey involving personal questions. Because self-efficacy generally reflects a person's experience and expertise (Bandura, 1982, 1997; Compeau & Higgins, 1995), we expected that individual privacy self-efficacy would positively moderate the effects of exposure to security breach related stories on both the password strength and non-disclosure. We found support for the positive effects of the exposure on the password strength and a nuanced effect on the refusal to disclose information. The treatment group exposed to the security breach news used much stronger (500×) passwords, using the entropy measure, and almost impossible to guess passwords, using a set of password cracking algorithms commonly used in practice. The treatment group also selectively chose to limit disclosure to particularly sensitive questions, e.g. the questions concerning drinking and driving, drug use and support for the death penalty. There was no effect on the refusal to disclose non-sensitive information, for example, whether the person was right or left handed.

Our hypotheses regarding the moderating role of privacy self-efficacy in privacy-protective behaviors were not supported by the empirical results. The lack of support for the role of self-efficacy is not without precedent. Self-efficacy is commonly assumed to play a role in reactions to threats; however empirical evidence has not always supported theoretical models. For example, a study of how people react to health threats showed that self-efficacy was not a significant moderator of responses to health threats (Ruiter, Verplanken, Kok, & Werrij, 2003). Experimental studies have shown that different factors besides self-efficacy may play a role in the behavioral response. For example, a study of people's reactions to health threats found that avoidant thinking can be responsible for the lack of an adaptive response to threat (Rippetoe & Rogers, 1987). Habits often exert influence over how people act (Umeh, 2004) and stress can also affect consideration of options and lead to sub-optimal decisions (Keinan, Friedland, & Ben-Porath, 1987). The results of our study suggest that self-efficacy does not interact with any of the behavioral threat mitigation strategies (password selection and self-disclosure). Future research should examine if the role of self-efficacy is more prominent in the secondary elaboration stage of the Information Processing framework.

Our study makes a number of contributions to theory and practice. First, while our study also applies cognitive models to understand technology user behavior, its distinctive characteristic is the focus on the immediate user responses to the potential security and privacy threats through the Information Processing framework lens. From this perspective, we were able to examine automatic responses as a result of a threatening stimulus that was empirically manipulated. Thus, the application of the IP framework in the information security and privacy research expands the theoretical foundation for understanding user behaviors across different contexts. The IP perspective is particularly relevant in the many situations that require the users to make split-second decisions, e.g. clicking on a link in a phishing email message and entering authentication credentials. These contexts simply do not afford sufficient time for slow cognitive processing and the IP framework will likely prove useful in understanding user behaviors in time-constrained situations.

Our second contribution is that this is one of the first studies to examine objectively measured actual technology user behaviors in response to security/privacy threats. While much of prior security and privacy-related research focused on perceptions and intentions in cross-sectional studies, we experimentally evaluate actual technology user behaviors in response to a potential security/privacy threat. Our findings are consistent with the predictions of the Information Processing framework which emphasizes that threat detection occurs automatically and it motivates a rapid response, while the process of sense-making involving assessment of individual susceptibility and self-efficacy is secondary and often occurs after the threat is mitigated. The non-significant effects of computer security self-efficacy in our study are also consistent with the predictions of the Information Processing framework and highlight the importance of understanding the automatic responses to information security and privacy threats. Whereas much of the previous research on computer security related intentions has noted the predictive value of self-efficacy in relation to the intention (Johnston & Warkentin, 2010, 2015; Liang & Xue, 2010), we find that privacy related self-efficacy does not predict actual behaviors in automatic user behaviors in our study.

Our third contribution is to the previously proposed taxonomy of privacy protective behaviors (Son & Kim, 2008). The original taxonomy offered three general types of reactions to potential privacy threats: information provisioning (withholding and misrepresentation), complaints to the offending party, and complaints to third parties. User authentication and information access control are key aspects of information security measures focusing on information confidentiality. Our results demonstrate that authentication and access control are additional measures that need to be included in the typology of potential responses. Further, we also empirically validate the prediction made by the taxonomy that non-disclosure can be one of the actions that allow technology

users to counter privacy-related threats. Most importantly, our results also reveal that users do not summarily stop self-disclosure altogether in response to potential privacy threats, but instead become very selective about what information they choose to disclose.

Our fourth contribution is to the stream of literature on how to encourage technology users to follow security guidelines and protect their information privacy and security (Arachchilage & Love, 2014; Ben-Asher & Gonzalez, 2015; Guo & Yuan, 2012). While a variety of technical solutions to promoting strong password use have been proposed (Chun-Li, Hung-Min, & Hwang, 2001; Cipresso, Gaggioli, Serino, Cipresso, & Riva, 2012; Sasse, Brostoff, & Weirich, 2001), the use of weak passwords remains commonplace in practice (Bright, 2014; Hill, 2014). Our results suggest that presenting users with narratives highlighting computer security threats may be an effective way to stimulate adherence to using strong passwords. Embedding messages within narratives has proven to be an effective technique in marketing (Dahlén, Lange, & Smith, 2010) and it may prove effective in promoting best security practices as well. This approach could be useful in non-organizational contexts, or in those without explicit compliance guidelines for password selection and maintenance.

Lastly, we would like to note that no research study is without limitations. While the experimental methodology allowed us to evaluate the causal effects of an exposure to information about potential security/privacy threats on password strength and non-disclosure, the experimental environment does not necessarily replicate real-world conditions. We aimed to create a realistic environment by exposing the participants to representative news excerpts which the study participants may have encountered in major media outlets, but the experimental manipulation does not necessarily replicate a workplace context where employees may have certain expectations of security measures or privacy protections. Our experimental setting resembles a voluntary or a home computer use context, where users interact directly with sites of their choosing. Further research is needed to examine the extent to which different contexts play a role in the perceptions of security and privacy threats. Our study also lays the foundation for future research on the most effective way to present computer privacy and security messages with the goal of eliciting stronger behavioral responses. For example, research on priming has suggested that the text color may interact with the narratives and produce stronger behavioral response to textual messages (Gerend & Sias, 2009). There is also an opportunity to better understand the mental processes that underlie the behavioral effects observed in our study. It would be of interest to examine different primes and different mental processes in relation to privacy and security related computer user communications.

7. Conclusion

The present study takes the first steps towards understanding how technology users react to potential immediate security and privacy threats. We drew on the Information Processing framework which emphasizes the primacy of threat mitigation action as the theoretical lens and we conducted an experimental study in which we evaluated users' behavioral responses. Specifically, we examined the degree of self-disclosure and the strength of passwords users set to protect their answers in response to an exposure to several news stories about corporate computer security breaches. We found that participants in our study readily reacted to news stories about security and privacy breaches by using 500× stronger passwords and selectively limiting disclosure of personal information. Our study contributes to the existing research by offering a novel theoretical perspective that can guide future research on the immediate technology user reactions to potential threats. The study also provides the initial empirical evidence that privacy and security threats rapidly motivate protective behavioral responses. Our findings are useful to practice as they speak to the importance of exposing users to security-related narratives to promote the creation of stronger passwords.

Appendix A1. Behavior measures in PMT-related security research

Citation	Context/method	Security-related behavior measures
Chan, Woon, and Kankanhalli (2005)	A survey of employees	Self-report of organizational security policy compliance
Pahnila, Siponen, and Mahmood (2007)	A survey of employees	Self-report of organizational security policy compliance
Myyry, Siponen, Pahnila, Vartiainen, and Vance (2009)	A survey of employees in Finland	Self-report of organizational security policy compliance
Son (2014)	A survey of employees	Self-report of organizational security policy compliance
Arachchilage and Love (2014)	A survey of undergraduates in UK	Self-report of phishing attack avoidance
Siponen, Adam Mahmood, and Pahnila (2014)	A survey of employees	Self-report of organizational security policy compliance
Crossler, Long, Loraas, and Trinkle (2014)	Two surveys – students and employees.	Self-report of organizational security policy compliance
Boss et al. (2015)	Two experiments involving undergraduate and graduate students	Data backups Malware warning response
Posey, Roberts, and Lowry (2015)	A survey using a panel of participants	Self-report of security protective behaviors
Y. Chen and Zahedi (2016)	A survey using convenience sample of students and their contacts	Self-report of security protective behaviors
Warkentin, Johnston, Shropshire, & Barnett (2016)	A survey of undergraduate students	Self-report of continued organizational security policy compliance
Bélanger, Collignon, Enget, and Negangard (2017)	A survey of students, faculty and staff at a university.	Self-report of early organizational security policy compliance
Burns, Posey, Roberts, and Benjamin Lowry (2017)	A survey using a panel of participants	Self-report of security protective behaviors
Crossler, Belanger, and Ormond (2017)	A survey of soccer tournament participants.	Self-report of security protective behaviors
Thompson, McGill, and Wang (2017)	A survey of participants recruited through a commercial panel data provider.	Self-report of security protective behaviors

Appendix A2. Self-disclosure measures in Information Systems research

Citation	Context/method	Self-disclosure measure
Posey, Lowry, Roberts, and Ellis (2010)	A survey administered through a market research firm in the UK and France	Self-report
Zimmer, Arsal, Al-Marzouq, and Grover (2010)	A survey of undergraduate students.	Self-disclosure intention
Lowry, Cao, and Everard (2011)	A survey of information disclosure in messaging applications	Self-report
Jiang, Heng, and Choi (2013)	A survey of students in Singapore	Self-report
Yu, Hu, and Cheng (2015)	A survey of students	Self-report
Chen and Sharma (2015)	A survey of students	Self-report
Matook, Cummings, and Bala (2015)	A longitudinal survey	Self-report
Li et al. (2015)	Panel data	Secondary data, measure extracted as self-disclosure in blog posts
Bansal, Zahedi, and Gefen (2016)	Experimental study	Self-disclosure intention
Choi and Land (2016)	Experimental	Self-report, willingness to share Facebook profile data
Zhu, Ou, van den Heuvel, and Liu (2016)	A survey of students	Self-report, willingness to disclose personal information
Liu, Min, Zhai, and Smyth (2016)	A survey of micro-blogging service users in China	Self-report
Li, Luo, Zhang, and Xu (2017)	A survey of students	Self-report
James, Wallace, Warkentin, Kim, and Collignon (2017)	A survey of students	Self-report of intention to disclose information about others
Veltri and Ivchenko (2017)	An experimental study	Self-disclosure is measured using a survey
Lin and Utz (2017)	An experimental study	Subjective evaluation of others' self-disclosure
Shih, Lai, and Cheng (2017)	A consumer survey	Self-disclosure intention
Chen and Li (2017)	A survey of SNS users in Hong Kong	Self-report
Zhang (2017)	A survey of SNS users	Self-report

Appendix B. Sample News Stories

Control group	Treatment group
Story 1. Designed to transform digital marketing programs in the country, Adobe and Razorfish have outlined a joint initiative for the Indian market. Leveraging their global partnership, the two companies will develop solutions focused on digital personalization for marketers in India.	Story 1. Adobe Systems Inc. disclosed last month that hackers stole login information for some 38 million of its customers. Now Facebook Inc. and other Internet companies are worried their users might also be affected. Internet users, despite repeated warnings, often use the same password on many different websites. So, even if Facebook wasn't hit by the latest cyber-attack, the Adobe hackers still might be able to break into Facebook user accounts with recycled passwords.
Story 2. A Walmart executive recently laid out his company's strategy for the holiday shopping season as follows: "We're going to win." Other retailers say the same. Heavy discounting is predicted, and victories may prove pyrrhic in profit terms. The stock market, however, has predicted one winner: Amazon. Its shares, which had traded in line with consumer discretionary stock indices for three years, started to rally after the third-quarter report in October. Its market value has since risen by a quarter. What has changed? Maybe nothing. There is a general fever for growth companies, especially those with a technological frisson. Netflix and Facebook shares have rallied, too. There was genuine improvement in Amazon's third-quarter numbers - specifically, incremental sales in the quarter ($3.3bn) were greater than in the third quarter a year ago ($2.9bn). This is a big deal, as there had been incremental sales declines in the previous five quarters.	Story 2. Hackers stole personal information with details of up to 70 million people – a third of American adults – including phone numbers, email and home addresses, the US retail chain Target admitted on Friday. The management said that the extent of a 19-day pre-Christmas break-in to its computer systems was far greater than it had thought when in late December it estimated the number of credit and debit cards affected at 40 m. It hadn't previously said how many people were affected. Analysts reckon it will affect more people than the card-skimming operation at TJX Cos Inc in 2007, which was reckoned to affect 90 m cards over an 18-month period. "I think they still have no idea how big this is," David Kennedy, who runs the consulting firm TrustedSec told Reuters. "This is going to end up being much larger than 70 million and end up being the largest retail breach in history."

Appendix C. Survey instrument

All questions were assessed using 7-point Likert scale anchored in 1 – strongly disagree and 7 – strongly agree, except for PrivSE1, which was anchored in 1 – very difficult, 7 – very easy.

Privacy self-efficacy (based on (Compeau & Higgins, 1995))

PrivSE1	For me to control my privacy online is (1 – very difficult, 7 – very easy)
PrivSE2	If I wanted to, it would be easy for me to control my privacy online.
PrivSE3	I believe I have the ability to have privacy online.

Privacy concerns about information collection (Hong & Thong, 2013)

Priv_Col1	It usually bothers me when companies ask me for personal information.
Priv_Col2	When companies ask me for personal information, I think twice before providing it.
Priv_Col3	It bothers me to give personal information to so many companies.
Priv_Col4	I'm concerned that companies are collecting too much personal information about me.

Privacy concerns about unauthorized information use (Hong & Thong, 2013)

Priv_Una1	Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
Priv_Una2	Companies should devote more time and effort to preventing unauthorized access to personal information.
Priv_Una3	Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
Priv_Una4	Companies should never sell the personal information in their computer databases to other companies.

Self-disclosure survey.

Please refer to Joinson et al. (2008)for details regarding the instrument.

Appendix D. Non-disclosure response to individual survey questions.

Question	Percent non-disclosure - General tech news group	Percent non-disclosure - Security breach news group	Z test score for the difference in proportions
Which season were you born in?	2.62%	3.02%	0.24
Are you left or right handed?	1.05%	1.05%	0.00
How many different sexual partners have you had? Please include all, however brief	8.90%	10.47%	0.52
Since age 18 how many different serious relationships have you had?	4.71%	4.71%	0.00
Have your partners been opposite/same sex?	4.19%	5.24%	0.49
What are your living arrangements?	3.66%	2.62%	−0.59
Have you ever driven whilst you suspected you may be over the legal alcohol limit?	3.66%	7.85%	1.77*
Have you ever deliberately viewed pornography using the internet?	7.33%	9.42%	0.75
As an adult, have you ever tried any drugs (other than alcohol and nicotine, e.g. marijuana, cocaine, ecstasy, heroin)	3.14%	8.90%	2.38*
Are you a religious person?	5.76%	4.19%	−0.71
Have you ever passed by and ignored someone who needed help?	6.81%	5.24%	−0.65
Do you agree with the death penalty?	2.62%	7.85%	2.31*
Have you ever pretended you could not do a favor for someone, while in reality you did not want to do it?	4.19%	4.19%	0.00
As an adult, have you ever felt depressed?	3.66%	6.28%	1.19
Please estimate the number of times you have visited a doctor in the last two years?	2.09%	3.14%	0.65
Do you give to charity?	2.62%	2.62%	0.00
Please rate your health in comparison to that of your peers on the following scale	19.37%	19.37%	0.00
Have you ever been in a traffic collision that was at least partly your fault?	1.57%	3.66%	1.29

*- statistically significant one-tailed test at $p < 0.05$ level.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.

Andriotis, A., & McMillan, R. (2017). Hackers entered equifax systems in March. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122–147.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Worth Publishers.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management, 53*(1), 1–21.

Barnes, S. B. (2006). A privacy paradox: Social Networking in the United States. *First Monday, 11*(9).

Beck, A. T., & Clark, D. A. (1997). An information processing model of anxiety: Automatic and strategic processes. *Behaviour Research and Therapy, 35*(1), 49–58.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of Early

Conformance with information security policies. *Information & Management*.
Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51–61.
Bishop, M. (2004). *Introduction to Computer Security. Addison-Wesley Professional*.
Bishop, S., Duncan, J., Brett, M., & Lawrence, A. D. (2004). Prefrontal cortical function and anxiety: Controlling attention to threat-related stimuli. *Nature Neuroscience, 7*(2), 184–188.
Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Security and privacy (SP), 2012 IEEE symposium on* (pp. 538–552). IEEE.
Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protectiove security behaviors. *MIS Quarterly, 39*(4), 837–864.
Bright, P. (2014). *7 million Dropbox username/password pairs apparently leaked. Ars Technica*. Retrieved from http://arstechnica.com/security/2014/10/13/7-million-dropbox-usernamepassword-pairs-apparently-leaked/.
Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science, 6*(1), 3–5.
Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190–209.
Burrows, M., Abadi, M., & Needham, R. M. (1989). A logic of authentication. In *Proceedings of the royal society of London A: Mathematical, physical and engineering sciences* (Vol. 426, pp. 233–271). The Royal Society.
Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on facebook. *Information Systems Research: Informs* (November 4).
Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the Workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(March 2015), 18–41.
Chen, H. T., & Li, X. (2017). The contribution of mobile social media to social capital and psychological well-being: Examining the role of communicative use, friending and self-disclosure. *Computers in Human Behavior, 75*, 958–965.
Chen, R., & Sharma, S. K. (2015). Learning and self-disclosure behavior on social networking sites: The case of facebook users. *European Journal of Information Systems, 2431*(1), 93–106.
Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and Behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205–A12.
Choi, B. C. F., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information and Management, 53*(7), 868–877.
Chun-Li, L. I. N., Hung-Min, S. U. N., & Hwang, T. (2001). Attacks and solutions on strong-password authentication. *IEICE Transactions on Communications, 84*(9), 2622–2627.
Cipresso, P., Gaggioli, A., Serino, S., Cipresso, S., & Riva, G. (2012). How to create memorizable and strong passwords. *Journal of Medical Internet Research, 14*(1).
Compeau, D., & Higgins, C. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly* (June), 189–212.
Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin, 79*(2), 73.
Crossler, R. E., Belanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users??? multi-layered protection from security threats. *Information Systems Frontiers, 101*, 1–15.
Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209–226.
Dahlén, M., Lange, F., & Smith, T. (2010). *Marketing communications: A brand narrative approach*. John Wiley & Sons.
Dell'Amico, M., Antipolis, S., Michiardi, P., & Roudier, Y. (2010). Password strength: An empirical analysis. In *INFOCOM, 2010 Proceedings IEEE* (pp. 1–9).
Fernandez-Aleman, J. L., Senor, I. C., Lozoya, P. A. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562.
Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web* (pp. 657–666).
Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*.
Forman, C., Ghose, A., & Wiesenfeld, B. (2008). Examining the relationship between reviews and sales: The role of reviewer identity disclosure in electronic markets. *Information Systems Research, 19*(February 2015), 291–313.
Gefen, D., Rigdon, E. E., & Straub, D. (2011). An update and extension to SEM guidelines for administrative and social science research. *MIS Quarterly, 35*(2), iii–xiv.
Gerend, M. A., & Sias, T. (2009). Message framing and color priming: How subtle threat cues affect persuasion. *Journal of Experimental Social Psychology, 45*(4), 999–1002.
Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information and Management, 49*(6), 320–326.
Hair, J. F., Jr., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.
Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice, 19*(2), 139–152.
Hill, K. (2014). Google says not to worry about 5 million "Gmail passwords" leaked. *Forbes*.
Hirschfield Davi, J. (2015). Hacking of government computers exposed 21.5 million people. *New York Times*. Retrieved from http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0.
Hong, W., & Thong, J. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 1–3.
Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79.
James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management* (2016).
Jiang, Z. J., Heng, C. S., & Choi, B. C. F. (2013). *Behavior in Synchronous Online Social Interactions Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions* (March 2014).
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.
Johnston, A. C., & Warkentin, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134.
Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology, 31*(2), 177–192.
Joinson, A. N., Paine, C., Buchanan, T., & Reips, U.-D. (2008). Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior, 24*(5), 2158–2171.
Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-computer Interaction, 25*(1), 1–24.
Joinson, A. N., Woodley, A., & Reips, U.-D. (2007). Personalization, authentication and self-disclosure in self-administered Internet surveys. *Computers in Human Behavior, 23*(1), 275–285.
Jourard, S. M. (1971). *The transparent self. Van Nostrand Reinhold New York*.
Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan.
Kankanhalli, A., Tan, B., & Wei, K. (2005). Contributing knowledge to electronic knowledge repositories: An empirical investigation. *MIS Quarterly, 29*(1), 113–143.
Keinan, G., Friedland, N., & Ben-Porath, Y. (1987). Decision making under stress: Scanning of alternatives under controllable and uncontrollable threats. *Journal of Personality and Social Psychology, 52*(3), 639–644.
Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., et al. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE symposium on security and privacy* (pp. 523–537).
LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71–76.
Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413.
Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information and Management, 52*(7), 882–891.
Li, H., Luo, X., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management* (2016).
Lin, R., & Utz, S. (2017). Self-disclosure on SNS: Do disclosure intimacy and narrativity influence interpersonal closeness and social attraction? *Computers in Human Behavior, 70*, 426–436.
Liu, Z., Min, Q., Zhai, Q., & Smyth, R. (2016). Self-disclosure in Chinese microblogging: A social exchange theory perspective. *Information & Management, 53*(December 2015), 53–63.
Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society, 10*(3), 393–411.
Lord, B. (2016). An important message about Yahoo user security. Retrieved from https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security.
Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure Technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200.
Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including mechanical Turk and online panels. *The Journal of Strategic Information Systems, 25*(3), 232–240.
Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479.

Mamonov, S., & Benbunan-Fich, R. (2015). An empirical investigation of privacy breach perceptions among smartphone application users. *Computers in Human Behavior, 49*, 427–436.

Mamonov, S., & Koufaris, M. (2014). The impact of perceived privacy breach on smartphone user attitudes and intention to terminate the relationship with the mobile carrier. *Communications of the Association for Information Systems, 34*(1), 60.

Mathis, Don (2014). What Facebook's Atlas means for brands and agencies. Retrieved from http://adage.com/article/digitalnext/facebook-s-atlas-means-brands-agencies/295293/.

Matook, S., Cummings, J., & Bala, H. (2015). Are you feeling Lonely? The impact of relationship characteristics and online social network features on loneliness. *Journal of Management Information Systems, 31*(4), 278–310.

Ma, J., Yang, W., Luo, M., & Li, N. (2014). A study of probabilistic password models. In *Security and privacy (SP), 2014 IEEE symposium on* (pp. 689–704). IEEE.

McElroy, J., Hendrickson, A., & Townsend, A. (2007). Dispositional factors in internet use: Personality versus cognitive style. *MIS Quarterly, 31*(4), 809–820.

McMillan, R., & Knutson, R. (2017). Yahoo triples estimate of breached accounts to 3 billion. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449–473.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18*(S2), 126–139.

Nelson, D., & Vu, K.-P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior, 26*(4), 705–715.

Obermiller, C., & Spangenberg, E. (1989). Exploring the effects of country of origin labels: An information processing framework. *Advances in Consumer Research, 16*(1), 454–459.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. In *Proceedings of the annual Hawaii international conference on system sciences* (pp. 1–10).

Ponemon Institute. (2017). *2017 Cost of Data Breach Study*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the U.K. Who use online communities. *European Journal of Information Systems, 19*(2), 181–195.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 57*(November), 338–349.

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153–161.

PricewaterhouseCoopers. (2017). *Global State of Information Security Survey: 2017 results by industry*. Retrieved from https://www.pwc.com/gx/en/issues/information-security-survey/geopolitical-cyber-threats.html.

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly, 36*(1).

Rippetoe, P. a, & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*(3), 596–604.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology, 91*(1), 93–114.

Ruiter, R. A. C., Verplanken, B., Kok, G., & Werrij, M. Q. (2003). The role of coping appraisal in reactions to fear appeals: Do we need threat information? *Journal of Health Psychology, 8*(4), 465–474.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link"—a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122–131.

Shannon, C. E. (1948). Key papers in the development of information theory. *Bell Syst. Tech. J, 27*, 623–656.

Shih, H. P., Lai, K. H., & Cheng, T. C. E. (2017). Constraint-based and dedication-based mechanisms for encouraging online self-disclosure: Is personalization the only thing that matters? *European Journal of Information Systems, 26*(4), 432–450.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy, 9*(1), 26–46.

Son, J. Y. (2014). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management, 48*(7), 296–302. http://doi.org/10.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 503–529.

Sonnenschein, R., Loske, A., & Buxmann, P. (2016). *Gender differences in mobile users' it security appraisals and protective Actions: Findings from a mixed-method study*.

Steelman, Z., Hammer, B., & Limayem, M. (2014). Data collection in the digital age: Innovating alternatives to student samples. *MIS Quarterly, 38*(2), 355–378.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29*(3), 821–826.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376–391. https://doi.org/10.1016/j.cose.2017.07.003. Retrieved from.

Tiffany, S. T. (1990). A cognitive model of drug urges and drug-use behavior: Role of automatic and nonautomatic processes. *Psychological Review, 97*(2), 147.

Umeh, K. (2004). Cognitive appraisals, maladaptive coping, and past behaviour in protection motivation. *Psychology and Health, 19*(6), 719–735.

Ur, B., Segreti, S. M., Bauer, L., Christin, N., Cranor, L. F., Komanduri, S., & Shay, R. (2015). Measuring real-world accuracies and biases in modeling password guessability. In *In 24th USENIX security symposium (USENIX security 15)* (pp. 463–481).

Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity on online privacy disclosure. *Computers in Human Behavior, 73*, 238–246.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016a). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016b). Neural correlates of protection motivation for secure IT behaviors: An fMRI exploration. *Journal of the Association for Information Systems, 17*(3), 194.

Weir, M., Aggarwal, S., Collins, M., & Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 162–175) (ACM).

Weisband, S., & Kiesler, S. (1996). Self disclosure on computer forms: Meta-analysis and implications. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 3–10) (ACM).

Wheeless, L. R., & Grotz, J. (1977). The measurement of trust and its relationship to self-disclosure. *Human Communication Research, 3*(3), 250–257.

Whitla, P. (2009). Crowdsourcing and its application in marketing activities. *Contemporary Management Research, 5*(1).

Wishpond. (2015). *Up-to-Date Facebook Facts and Stats*. Retrieved from http://blog.wishpond.com/post/115675435109/40-up-to-date-facebook-facts-and-stats/.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329–349.

Yan, J. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy, 5*, 25–31.

Yang, H., & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems, 31*(2), 35–60.

Yu, J., Hu, P. J.-H., & Cheng, T.-H. (2015). Role of affect in self-disclosure on social network websites: A test of two competing models. *Journal of Management Information Systems, 32*(2), 239–277.

Zadelhoff, M. Van (2016). The biggest cybersecurity threats are inside your company. *Harvard Business Review*. Retrieved from https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

Zajonc, R. (1980). Feeling and thinking: Preferences need no inferences. *American Psychologist, 35*, 151–175.

Zeng, Y., Wang, L., Deng, X., Cao, X., & Khundker, N. (2012). Secure collaboration in global design and supply chain environment: Problem analysis and literature review. *Computers in Industry, 63*(6), 545–556.

Zephoria Digital Marketing. (2017). *The Top 20 Valuable Facebook Statistics – Updated November 2017*. Retrieved from https://zephoria.com/top-15-valuable-facebook-statistics/.

Zhang, R. (2017). The stress-buffering effect of self-disclosure on Facebook: An examination of stressful life events, social support, and mental health among college students. *Computers in Human Behavior, 75*, 527–537.

Zhu, H., Ou, C. X. J., van den Heuvel, W. J. A. M., & Liu, H. (2016). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management* (September 2000).

Zimmer, J. C., Arsal, R. E., Al-Marzouq, M., & Grover, V. (2010). Investigating online information disclosure: Effects of information relevance, trust and risk. *Information and Management, 47*(2), 115–123.