Human Factors in Cybersecurity, Vol. 53, 2022, 9–18
https://doi.org/10.54941/ahfe1002196

Insider Threat: Cognitive Effects of Modern Apathy Towards Privacy, Trust, and Security

Valarie A. Yerdon[1,2] and P. A. Hancock[2]

[1]Capitol Technology University, Laurel, MD 20708, USA
[2]University of Central Florida, Orlando, FL 32826, USA

ABSTRACT

The purpose of this study was to analyze how contemporary social apathy levels towards privacy have changed over time from before the integration of computers into American society. With private information stored in a computational net of digital information, rather than in personal possession and control, there may be signals towards the increase in the "inattentive" insider Threat to cybersecurity. By using the results of sequential privacy index surveys, along with trait and state subjective questionnaires, changes, and possible shared factors in attitude towards privacy were evaluated. The results of this study suggested that privacy concern has lowered over time, there was a low level of subjective apathy, and high level of instrumental motivation, which was correlated with the level of privacy concern. This research is looking for indicators of lower concern for privacy, to mitigate the inattentive insider threat in the workplace.

Keywords: Privacy, Security, Trust, Apathy, Insider threat, Cybersecurity, Privacy attitudes, Privacy concerns

INTRODUCTION

In a recent study by Matthews and colleagues (2017), eye tracking metrics were found to suggest some evidence of deception in the information search professions in the workplace. This was established through the use of a simulated work environment in a cyber security effort to help mitigate insider-threat (IT) (Matthews et al., 2017; Yerdon, 2018). Rather than protecting secure data from the outside intruder penetrating a system, current cybersecurity efforts focus on the person in the inside trusted position. There can be either maliciously planned (hot malcontent), who chooses to release information during the workday, or is unwittingly responsible for the leaking of resources (inattentive) (Whitman, 2016; Wall, 2013; Silowash, 2012; Beer, 2012). As it is not a realistic enterprise to investigate eye tracking from an insider before, during, or after a real-world act of espionage, simulated environments must be used to examine ways to detect these acts (Hancock et al., 2008; Ortiz et al., 2017; Leschnitzer, 2013, Wall, 2013). These actions can go unnoticed for long periods of time with vast amounts of damage done from the security breach. Implicit and explicit responses to targets which are

© 2022. Published by AHFE Open Access. All rights reserved.

embedded into the simulation were monitored to find metrics to track activity in the workplace as a proactive measure for organizations as Active Indicators of Insider Threats (AIITs) (Matthews et al., 2017; Yerdon et al., 2018; Hashem et al., 2015; Neuman, Assaf, & Israeli, 2015; Twyman et al., 2014).

When the beliefs of privacy as sacred and protected in today's technologically driven society were explored, it became evident that there was a transformation occurring in such attitudes (Barbuto & Scholl, 1998; Beer, 2011). The differences in such responses may be reflective of changes in attitudes from the rapidly growing automation, which has extended human cognition into technology in many aspects of daily life. Past evaluations have suggested that what had previously has been considered private is progressively under consideration for release with the promise of increased security, health, and well-being. This process of continual trade-offs has created a paradox in the release of privacy for heightened security (Crossler & Posey, 2017; Egloff & Schmukle, 2002). The modern generation is keenly aware of this privacy paradox. With the growing use of automated aids, the lines are blurring between the physical bounds of the human body and the technological tools needed to function in modern automated environments (Hargittai & Marwich, 2016; Wilson, 2002; Frith & Frith, 2008). With the permitted increase of protective security measures, boundaries of privacy are changing rapidly, culminating in the extended cognitions of global proportions, in worldwide nets of data storage and securities (Galesic, Tourangeau, Couper, & Conrad, 2008). If the modern apathy towards privacy, security, and trust have grown, perhaps it must have contributed to "inattentive" insider-threats to organizations (Gallagher, 2014).

Background

Across multiple years of research into the effects of computers on society, and especially on privacy, Westin inquired whether prior generations, by tracking social, political, and economic dimensions of privacy (Westin, 1967; Westin, 2003; Karamaguru & Cranor, 2005). Westin studied how privacy concerns were affected by the rise in technology during the arrival of the World Wide Web. Westin was concerned that computer-based systems and online technologies were beginning to transform how business and personal matters were being handled. This change was evident through repercussions to corporate and individual privacy of information (Westin, 1967; Gallagher, 2013; Greenwald & Banaji, 1995).

Westin used pertinent questions about attitudes towards trust, social, political, and consumer dimensions of privacy. He created a classification system for groups that was based on levels of privacy concern (Westin, 2003; Kumaraguru & Cranor, 2005). He found that he could categorize the individuals into three privacy concern groups. The percentages found in each category: 1. High level of concern as Privacy Fundamentalists; 2. Medium level of concern as Privacy Pragmatists; and 3. Low level of concern as Privacy Unconcerned (Kumaraguru & Cranor, 2005; Westin, 2003). The "fundamentalist" group was defined as being distrustful of organizations' abilities to store and secure their information safely, securely, and accurately. They supported new privacy

controls and privacy rights, enforcement laws, and regulations. The "pragmatic" group emphasized the benefits and losses to the sharing of private information and the rules guiding the use, with an eye on government regulations as restricting, unless necessary to protect. This group believed that the government should not be trusted without consideration of their intent and actions by the public, wanting the option to be on the consumer to decide how what information was shared and how it could be handled. The "unconcerned" group was generally trusting of the government and organizations to handle their private information. Members of this group showed more concern for the greater good of society, supporting the benefits of having a digital record base and not in favor of new laws and regulations which could slow the progress of this effort.

In creating these categorizations during the 1990s, Westin used subcategorized surveys with questions based on domains of societal experiences with privacy, security, and trust. Some of these were the Consumer Privacy Concern Index, Medical Sensitivity Index, Distrust Scale, Computer Fear Index, and Privacy Concern Index. After a decade of administering these surveys, Westin concluded that the Privacy Concern Index was a valid indicator. The earliest of these surveys was the Harris-Equifax Consumer Privacy Survey (1990, 1991). This questionnaire posed four questions regarding whether participants were concerned about threats to their privacy, businesses as well as the Federal government gaining access to their own information, and their sense of control over that information.

In 1993, Westin added questions specifically about health information privacy such as prescriptions, health care providers, employer, insurer, and family member concerns. This line of questioning gave rise to his Medical Sensitivity Index first inquired about concerns with the health organizations beyond the doctors seeing their medical information and the assignment of medical identification numbers for patients. The next phase of this index touched upon the use of computers in medical offices and laboratories for patient records and their worry over the management and monitoring of medical record operations. These two combined efforts were found to correlate to an overall Medical Sensitivity in Westin's work. They illustrated the participant's privacy orientation towards one of his three categorizations of privacy concerns. The Computer Fear Index was then used to tap into attitudes towards the effects of computers on privacy and whether they should continue to be used or not. The Distrust Index was then developed in 1994 as an indicator of the distrust in technology, government involvement, control over these issues through voting, and business practices that may be meant to help the consumer may be harming them. This contrariness between helping and hindering touches on the Privacy Paradox mentioned earlier wherein a bartering system is in effect the trade of privacy security. In 1996 Westin added questions about consumer information sharing concerns and whether the participant felt they had been a victim of the invasion of their privacy, asking for opinions of the best path forward for our government. In this Consumer attitude survey, he asked about whether the participant believed if consumer privacy would get better, the tracking of internet usage by online services, and the use of medical records for research needs without consent.

1998 brought further questions about concerns for personal privacy in America, and 2001 brought queries about how laws and organizational practices affected the collection of personal data. The tests for the internal validity of these surveys were not reported and has been part of the criticism of Westin's work. The present study used the current data to determine internal validity with an evaluation of Cronbach's Alpha results. Validation of privacy scales is essential for their intended purposes of privacy assessment and to test whether these are states as opposed to trait characteristics in future work.

METHOD

Participants

The data from total of ninety-five (n = 95) university students (54 males, 41 females, Mage = 20, SD = 2) who participated was evaluated in this study. The surveys were administered in an in-person setting at a computer workstation. The session took approximately one and one-half hours to complete, including instruction, consent, and dismissal. One researcher was present in the experimental room, sitting at another desk behind a partition. They were available for questions, but out of sight of the participant entries on the computer. This study was approved by the International Review Board (IRB) and adhered to APA ethical guidelines during every step of this research. Each participant was given an IRB approved consent form to read, with verbal consent before taking part in this study. The following surveys were administered: *(1) Demographics Questionnaire* (US Census); (2) *Personality Individual Differences* (e.g. Jonason et al.; Li & Brewer, 2004); (3) *40 Mini-Marker Personality Scale* (general personality) (Saucier,2010); (4) *Apathy Evaluation Scale (AES-S)* (Marin, 1990; Marin, Biedrzycki, & Firinciogullari, 1991); (5) *Motivation Sources Inventory Scale (MSI)* (Barbuto & Scholl, 1998); (6) *Automation-Induced Complacency Potential Rating Scale* (Singh,Molloy, & Parasuraman, 1993); (7) *Inherent Privacy Concern and Desire for Privacy* (Morton, 2009); (8) *Privacy Index Questionnaire*. (Westin, 2003; Kumaraguru & Cranor, 2005). Westin studies on Privacy attitudes of citizens in the United States in the late 1990's and early 2000's, which consists of 44 items, using several Likert -type of scales for rating (Importance, Agreement, Concern, and Accessibility): (a) *The Harris-Equifax Consumer Privacy Survey* (1990, 1991); (b) *Consumer Privacy Survey* (1993); (c) *Medical Sensitivity Index* (1993; (d) *The Computer Fear Index* (1993); (e) *The Distrust Index* (1994); and (f) *Privacy Concern Index* (1996).

Design

This experiment involved a comparison between groups (i.e., past vs. current) with the measures derived from the Privacy Index Criteria. The dependent variables are these surveys and independent variable is time. One-way Analysis of Variance (ANOVA) was used to calculate the change over time in the Westin Privacy Index surveys and correlations with apathy and aspects of this state. T-tests were used to distinguish differences between group means. Z-scores were calculated to standardize the results for analysis. Levene's test

Table 1. Significance of changes in privacy concern levels.

Westin's Privacy Level Concern Groups	Westin Consumer Privacy Concern	Westin Medical Sensitivity Index	Westin Distrust Scale	Westin Computer Fear Index	Westin Privacy Concern Index
Unconcerned (U)	*(i)* .819	*(d)* .12	*(i)* .039*	*(d)* .000***	*(i)* .000***
Pragmatic (P)	*(i)* .001***	*(i)* .44	*(i)* .429	*(i)* .154	*(d)* .000***
Fundamentalist (F)	*(d)* .000***	*(i)* .256	*(d)* .004**	*(i)* .007**	*(d)* .521

Note: (i) increase; *(d)* decrease; $*p < .05$; $**p < .01$; $***p < .001$.

for homogeneity of variance and Games-Howell test compared the possible combinations of group differences when assumptions of normal variance were violated. The present sample (n = 95) was determined by the need to obtain adequate statistical power for testing the significance of the bivariate correlations relative to a population correlation of $\rho = 0.03$. With this sample size, power for a moderate effect size of r = 0.35 is 0.95 ($\alpha = 0.05$, two-tailed).

RESULTS

Westin Privacy Concern Index

The results of Westin's surveys were compared to the answers to the identical questions collected here. Through a two-sample test of proportions of the results from those reported for Westin and those found for the current data, the hypothesis that there was a statistically significant difference, specifically a decrease in privacy concern was tested. In this effort, data was collected on the four subscales of Consumer Privacy Concern, Medical Privacy Concern, Medical Sensitivity, Computer Fear, and Distrust, and Computer Fear, which was used to calculate the Privacy Concern Index according to Westin's questions and processes (see Table 1).

MOTIVATION SOURCES INVENTORY SURVEY

Discussion

This study sought to investigate the change in attitudes towards privacy and the levels of concern related to subjective measures of states and traits of personality, over the past two decades since Dr. Westin and his colleagues' published study (Westin, 2003). This was enacted to address increased levels of inattentive insider threats to organizations. It was hypothesized that there would be significant evidence of 1) change over time in concern for privacy, 2) high distrust, 2) high apathy, 3) low motivation, 4) difference between privacy group membership and subjective measure factors.

The hypothesis that the Privacy Concern Index would show a lower concern for privacy across time was supported by the data. This showed a highly significant increase in privacy Unconcerned group. The privacy Pragmatic group also showed a highly significant decrease in the proportion of

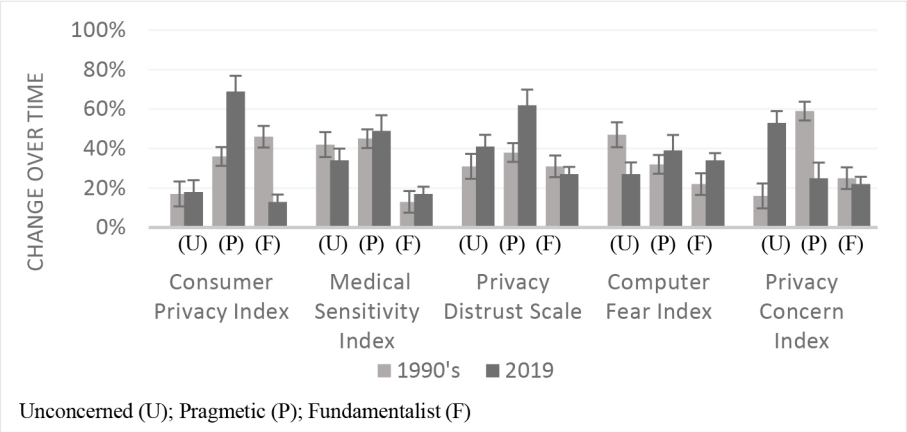

Figure 1: Change over time in privacy concern levels.

Table 2. Analysis of variance difference between privacy group & motivation source inventory.

ANOVA	Mean	Median	SD	Range	Min	Max	F(2,92)	p
Intrinsic	0.17	0.17	0.026	0.15	0.10	0.25	0.36	0.699
Instrumental	0.187	0.2	0.029	0.13	0.10	0.23	5.175	0.007**
External Self-Concept	0.196	0.2	0.024	0.13	0.11	0.24	0.723	0.488
Internal Self-Concept	0.208	0.21	0.022	0.13	0.16	0.29	2.679	0.074
Goal Internalization	0.238	0.23	0.038	0.22	0.18	0.40	1.149	0.247

Note: **$p < 0.01$.

the population with a level of concern about privacy since 2003. In addition, there was a decrease in the privacy Fundamentalist group, but this was not a significant difference in group membership over time. In the sub-scales and indexes, there is a highly significant decrease in the group Unconcerned and a highly significant increase in the Fundamentalist high level of concern with Computer Fear regarding privacy. The decrease in the unconcern group towards computer fear, along with the increase in the high level of concern may be reflective of the change in the highly digitized modern society and the awareness of how integrated our privacy is with the computerized world of today.

A second hypothesis was that there would be higher levels of distrust over time. This was supported by the present results as represented by the significant decrease in the high level of concern and the significant increase in the low level of concern group in the Distrust Scale. The Consumer Privacy Concern supports the hypothesis of a decrease in the concern regarding privacy, with a highly significant increase in the medium level of concern, a highly significant decrease in the high level of concern, with the data indicating an increase in the lowest level. However, this was not a significant

difference. It is interesting that Medical Sensitivity did not show any significant change from the 1990's. This suggests that those concerns have not been incorporated as an element of the Privacy Paradox (Crossler & Posey, 2017; Egloff & Schmukle, 2002). This may reflect an attitude in modern society that people still retain some feeling of control over their medical records. In Westin's time, the internet was in its infancy and computers were not a part of people's everyday life. The growth of automation may affect societal attitudes towards personal privacy (Hargittai & Marwich, 2016; Wilson, 2002).

The third major hypothesis was that there would be a higher level of apathy in the present sample. In the Subjective Apathy Evaluation Survey showed a low current level of apathy, significantly below what would be considered normal for the healthy adult according to measures used in clinical evaluations (Marin, et. al, 1991). This result supported the null hypothesis that apathy would not be significantly high. The analysis showed no significant difference in privacy group membership. However, with the low mean and median levels of apathy, significantly below the normal levels for a healthy adult from a clinical subjective evaluation measure in the results, this suggests a low level of apathy may be a significant element to be considered when looking at the changes over time of privacy concern levels. The relationship may be more linear and congruent as low levels in apathy can signal higher goal-oriented behavior, increased motivation, and lower complacency towards feelings regarding control of outcomes (Marin et al. 1991). This may be reflective of the population that was tested rather than the broader demographic in this age group, but more investigation would be important to inspect this significant difference.

The fourth hypothesis, that there would be difference between privacy group membership and subjective measure factors was supported by the results for Instrumental Motivation, which represents the type of motivation that comes from the thought of tangible rewards. This result suggests that modern society is significantly motivated by extrinsic material rewards for behaviors (Barbuto & Scholl, 1998). The results showing high instrumental motivation may help to understand of attitudes towards privacy in the workplace. In relation to the actions and attitudes of the Inattentive Insider Threat, the motivation to keep resources safe and private may not be reward-based in moment-by-moment work with protected data. Keeping records, resources, data, and information guarded may become very mundane. Any motivation to consistently follow security guidelines would not be found intrinsically. With the results showing no correlation of the intrinsic types of motivation with the privacy concern level, the evidence suggests that the empathetic and internal, unconscious acts of motivation towards protecting data may be a missing link. It may a challenge to bridge this new definition and attitude towards privacy and goals for the protection of resources leaking from the inattentive insider.

CONCLUSION

The present findings suggest a way to find metrics to use for the mitigation of the Inattentive IT. From the combination of low apathy towards privacy,

a significant correlation of instrumental motivation with the expectation of extrinsic rewards to privacy concern level was found. With data showing low concern for privacy, it is evident these attitudes are indeed indicative of the increase in the Inattentive IT in current society. The challenge of protecting resources from leaking out from the careless worker may be a sign of an incongruency between how the employer has defined privacy through standard training and security practices and how the individual in today's society views privacy and its importance in their everyday life. It becomes clear from these findings that privacy is not defined the same as it was before technology began handling, managing, and storing data streams in the financial, medical, and personal arenas. There is a plethora of services now available, which are being highly promoted as the most secure manner to protect and secure personal information. The "privacy net" of the cloud services seemingly float above the population with the lulling promise that technology will be more adept and capable of controlling and protecting this information. Keeping the personal data out of the hands of the individual from which it originated and into the databases of technology is touted to be creating a more streamlined, fluid, and secure system to protect and manage data of populations. In this, the concept of privacy has become very removed from the individual, in the name of increased and more sophisticated security and protected systems. As corporate and government entities look to secure the data within their walls from leaking out, a new approach and definition of privacy and security, concerning how their workforce views these concepts, needs to be part of their awareness. The methods to mitigate must integrate measures which more proactively protect the information as it streams to and from these new security clouds, from the unconsciously careless worker.

REFERENCES

Barbuto Jr, J. E., & Scholl, R. W. (1998). Motivation sources inventory: Development and validation of new scales to measure an integrative taxonomy of motivation. Psychological Reports, 82(3), 1011-1022.

Beer, W. (2011). Cybercrime: Protecting against the Growing Threat. Global Economic Crime Survey, retrieved February 30, 2012.

Crossler, R. E., & Posey, C. (2017). Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. Journal of the Association for Information Systems, 18(7), 487.

Egloff, B., & Schmukle, S. C. (2002). Predictive validity of an implicit association test for assessing anxiety. Journal of Personality and Social Psychology, 83(6), 1441.

Frith, C. D., & Frith, U. (2008). Implicit and explicit processes in social cognition. Neuron, 60(3), 503–510.

Galesic, M., Tourangeau, R., Couper, M. P., & Conrad, F. G. (2008). Eye-tracking data: New insights on response order effects and other cognitive shortcuts in survey responding. Public Opinion Quarterly, 72(5), 892–913.

Gallagher, S. (2013). The socially extended mind. Cognitive Systems Research, 25, 4–12.

Greenwald, A. G.; Banaji, M. R. (1995). "Implicit social cognition: Attitudes, self-esteem, and stereotypes". Psychological Review. 102: 8.

Hancock, P., Vincenzi, D., Wise, J., & Mouloua, M. (2008). Human Factors in Simulation and Training. CRC Press.

Hashem, Y., Takabi, H., GhasemiGol, M., & Dantu, R. (2015, October). Towards insider threat detection using psychophysiological signals. In Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats (pp. 71–74). ACM.

Hsu, C. L., & Lin, J. C. C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. Computers in Human Behavior, 62, 516–527.

Ikehara, C. S., & Crosby, M. E. (2005, January). Assessing cognitive load with physiological sensors. (p. 295a). IEEE.

Kumaraguru, P., & Cranor, L. F. (2005). Privacy indexes: a survey of Westin's studies. Leschnitzer, D. H. (2013). Cyber Security Lecture Series: The CERT Insider Threat Guide (No. LA-UR-13-25766). Los Alamos National Laboratory (LANL).

Lenzner, T., Kaczmirek, L., & Galesic, M. (2011). Seeing through the eyes of the respondent: An eye-tracking study on survey question comprehension. International Journal of Public Opinion Research, 23(3), 361-373.

Marin, R. S., Biedrzycki, R. C., & Firinciogullari, S. (1991). Reliability and validity of the Apathy Evaluation Scale. Psychiatry Research, 38(2), 143–162.

Matthews, G., Joyner, L., Gilliland, K., Campbell, S. E., Falconer, S., & Huggins, J. (1999). Validation of a comprehensive stress state questionnaire: Towards a state 'Big Three'? In I. Mervielde, I. J. Deary, F. De Fruyt, & F. Ostendorf (Eds.), Personality psychology in Europe (Vol. 7, pp. 335–350). Tilburg, the Netherlands: Tilburg University Press.

Matthews, G., Reinerman-Jones, L., Wohleber, R., & Ortiz, E. (2017, September). Eye Tracking Metrics for Insider Threat Detection in a Simulated Work Environment. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 61, No. 1, pp. 202–206). Sage CA: Los Angeles, CA: SAGE Publications.

Neuman, Y., Assaf, D., & Israeli, N. (2015). Identifying the location of a concealed object through unintentional eye movements. Frontiers in Psychology, 6, 381.

Ortiz, E., Reinerman-Jones, L., & Matthews, G. (2016). Developing an Insider Threat training environment. In Advances in Human Factors in Cybersecurity (pp. 267–277). Springer, Cham.

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., & Flynn, L. (2012). Common sense guide to mitigating insider threats 4th edition (No. CMU/SEI-2012-TR-012). Carnegie-Mellon University, Pittsburg, PA, Software Engineering Inst.

Sternberg, S. (1969). Memory-scanning: Mental processes revealed by reaction- time experiments. American Scientist, 57(4), 421–457.

Twyman, N. W., Lowry, P. B., Burgoon, J. K., & Nunamaker Jr, J. F. (2014). Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. Journal of Management Information Systems, 31(3), 106–137.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. Security Journal, 26(2), 107–124.

Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. Communications of the ACM, 10(9), 533–537.

Westin, A. F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), 431–453.

Whitman, R. L. (2016). Brain Betrayal: A Neuropsychological Categorization of Insider Attacks. In KSU Proceedings on Cybersecurity Education, Research and Practice. 9.

Wilson, M., (2002). Six views of embodied cognition. Psychonomic Bulletin & Review, 9(4), 625–636. 8.

Yerdon, V. A., Wohleber, R. W., Matthews, G., & Reinerman-Jones, L. E., 2018. A simulation-based approach to development of a new insider threat detection technique: Active indicators. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, July 21-25, 2018.