5-2018

Manifest Observations on a Comprehensive Computer Security Policy

Dennis C. Acuña
University of Findlay, dcacuna@bright.net

Manifest Observations on a Comprehensive Computer Security Policy

Dennis C. Acuña
University of Findlay
acunad@findlay.edu

ABSTRACT

This paper presents the summarized results of a data gathering operation, conducted as part of IRB approved research into the effects of a comprehensive computer security policy on human computer security policy compliance. For this study, a comprehensive computer security policy was defined as an enterprise policy encompassing all aspects of computer security including IT computer security and OT computer security, as opposed to only one domain or the other. The survey instrument included a questionnaire that utilized a Likert scale for belief strength measurement. In addition to questions designed as reflective indicators for latent constructs, the questionnaire included questions to authenticate participants and to gather demographic data. The empirical findings of this study suggest manifest support, regardless of domain, for human intent to comply with a comprehensive computer security policy.

Keywords

Comprehensive computer security, policy, compliance, SEM, TPB, Likert, Qualtrics.

INTRODUCTION

The data presented in this paper were gathered to support institutional review board (IRB) approved research into the effects of a comprehensive computer security policy on human computer security policy compliance (Acuña, 2017a, 2017b). For purpose of this study, a comprehensive computer security policy was defined as an enterprise policy incorporating all aspects of enterprise computer security including information technology (IT) computer security and operational technology (OT) computer security, as opposed to only one domain or the other. The separation between the IT domain and the OT domain can be paraphrased as the point of demarcation between decision support systems leveraged by humans (IT), and industrial control systems that make control decisions autonomously (OT). It is the comprehensive nature of this computer security policy that separates this study from similar studies in this research domain. Hence the thesis that a comprehensive computer security policy has a direct effect on human compliance with computer security policy, which can be further explained through indirect effects. The study used structural equation modeling (SEM) to evaluate this thesis.

The structural model leveraged social identity theory, interaction theory, deterrence theory, and the theory of planned behavior (TPB) as the foundation for building latent constructs. The measurement model included manifest variables designed as reflective indicators for the exogenous and endogenous constructs within the structural model. The majority of questions used to measure manifest variables were modeled after questions found in the extant literature for prior information systems (IS) SEM research that included TPB as a foundational theory (Bulgurcu, Cavusoglu, & Benbasat, 2010; Dinev & Hu, 2007; Flores & Ekstedt, 2016; Guo, Yuan, Archer, & Connelly, 2011; Pavlou & Fygenson, 2006; Song & Zahedi, 2005). Questions needed to fill gaps in the measurement model were designed by the principal investigator. Although terms such as information assurance, information security, and cybersecurity share similar meanings with that of computer security and tend to be used interchangeably in the literature, some researchers contend that these terms are not fully analogous (von Solms & van Niekerk, 2013; Whitman & Mattord, 2017). For purpose of this study the term comprehensive computer security was defined as encompassing all aspects of enterprise information assurance, information security, and cybersecurity, including the impact of the human factor in a security process, regardless of IT/OT domain.

RESEARCH METHODOLOGY

Survey Instrument

The survey instrument included a questionnaire consisting of 40 questions; 4 questions to explain the purpose of the research and to authenticate the participant as an authorized IT/OT user, 30 questions to measure the belief strength of reflective

indicators, and 6 questions to measure demographic variables (IT/OT identity, gender, age, education, work experience, industry sector). The survey instrument provided each participant the ability to exit, without penalty, at any time. A Likert scale (Figure 1) was used to measure reflective indicator belief strength.

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree

Figure 1. Unipolar 7-Point Likert Scale for Belief Strength Measurement

Measurement of reflective indicators in TPB based IS research is mixed, with evidence of unipolar and bipolar, 7-point and 5-point Likert scales. This study adopted the unipolar 7-point Likert scale recommended by Ajzen to measure belief strength in producing a certain outcome (Ajzen, 1991; Bulgurcu et al., 2010).

Sample Size

The SEM model for this study used maximum likelihood estimation (MLE) for parameter estimation (Diamantopoulos & Siguaw, 2000). A sample size of 200-250 participants was targeted to provide a sound basis for estimation (Hair, Black, Babin, & Anderson, 2010). The target population was experienced, authorized users located in the United States. Authorized users were defined as individuals owning credentials to access proprietary IT/OT computer systems not available to the general public. A modified three-sector theory construct (primary, secondary, tertiary, quaternary) served as the basis for industry sector categorization (Fisher, 1939).

Operationalization

The survey instrument was operationalized in February 2017 using the Qualtrics Insight software platform, a fee based commercial service that specializes in survey based research (Qualtrics, 2016). Qualtrics distributed the survey instrument and managed the data collection. Identifiers capable of linking a response to a participant, including internet protocol (IP) address, were managed by Qualtrics and were hidden and unknown to the principal investigator. A total of 210 randomly selected participants participated in this study, consisting of 106 IT identities and 104 OT identities. This compared favorably to the targeted sample size of 200-250 participants. There were no missing or unknown responses, as the Qualtrics platform seeks to deliver fully completed surveys. The collected data was exported from Qualtrics and imported into an Excel 2010 worksheet for verification and descriptive analysis. Following these initial operations, the data was exported from Excel and imported into LISREL v9.2 for Windows for SEM analysis. Results of the LISREL SEM analysis are briefly discussed in the findings section of this paper.

DATA ANALYSIS

Participant Demographics

As shown in Table 1, the full dataset of 210 participants, denoted as Σ, is evenly distributed between IT identities, (n=106, 50.48%), and OT identities (n=104, 49.52%). This relative equality of identity is important in regard to the generalization of findings from each domain to the target population. Gender is not as evenly distributed, with 70.48% of the participants identifying as male, and 29.52% identifying as female. Age is more evenly distributed with 48.57% of the participants being age 34 years or younger and 51.43% of the participants being age 35 years or older. 43.81% of the participants reported having a bachelor's degree, with 18.10% reporting some level of graduate work. Work experience reflects a young workforce, with 60.95% having 10 years or less of work experience, and 39.05% having 11 years or more of work experience. Engagement within industry sector is split between 46.67% of the participants working with the extraction or transformation of natural resources, and 53.33% of the participants being a provider of physical services or knowledge based services. A comparison of domains however, reveals demographic differences between authenticated IT participants and authenticated OT participants.

The IT domain reflects a younger, more educated workforce in regard to undergraduate and graduate accomplishment, working primarily as physical and knowledge based service providers. The OT domain reflects an older male workforce actively engaged with industrial control systems in the heavy industries of natural resource extraction and transformation.

Only the OT domain reported work experience of 31 years or more. While the OT domain is represented across the education demographic, the dominant educational categories are an earned associate's degree or less. The IT domain reflects educational dominance in the categories of an earned bachelor's degree and higher.

Demographic	Category	Frequency Σ (n=210)	Percent Σ (n=210)	Frequency IT (n=106)	Frequency OT (n=104)
Identity	Information Technology (IT)	106	50.48%	106	0
	Operational Technology (OT)	104	49.52%	0	104
Gender	Male	148	70.48%	71	77
	Female	62	29.52%	35	27
Age	Less than 18 years old	0	0.00%	0	0
	18 to 24 years old	20	9.52%	12	8
	25 to 34 years old	82	39.05%	42	40
	35 to 44 years old	45	21.43%	24	21
	45 to 54 years old	43	20.48%	25	18
	55 to 64 years old	19	9.05%	3	16
	65 years or older	1	0.48%	0	1
Education	Some high school, but no diploma	2	0.95%	0	2
	High school diploma or equivalent (GED)	18	8.57%	7	11
	Some college credit, but no degree	32	15.24%	14	18
	Trade/technical/vocational certificate	8	3.81%	4	4
	Associate's degree	20	9.52%	9	11
	Bachelor's degree	92	43.81%	49	43
	Some graduate school work, but no graduate degree	5	2.38%	3	2
	Master's degree	25	11.90%	16	9
	Doctorate degree	8	3.81%	4	4
Work Experience	Less than 1 year	5	2.38%	3	2
	1 to 5 years	50	23.81%	21	29
	6 to 10 years	73	34.76%	37	36
	11 to 15 years	34	16.19%	22	12
	16 to 20 years	24	11.43%	13	11
	21 to 25 years	12	5.71%	6	6
	26 to 30 years	8	3.81%	4	4
	31 to 35 years	3	1.43%	0	3
	36 years or more	1	0.48%	0	1
Industry Sector	Extraction of natural resources	12	5.71%	9	3
	Transformation of natural resources	86	40.95%	19	67
	Physical service provider	20	9.52%	8	12
	Knowledge based service provider	92	43.81%	70	22

Table 1. Participant Demographics (percentages subject to rounding error)

Manifest Observations

The summarized results of manifest observations for Σ, IT, and OT categorizations exhibited negative (left) skewness with a concentration in the 6-7 range of the Likert scale. This is exhibited in Table 2 through the use of mode as a measure of central tendency, and in Table 2a through the use of median as a measure of central tendency. With the exception of specific instances within two variables, H43 and H93 (Table 2a), all Σ, IT, and OT median scores measured 6 on the Likert scale. The data listed in Table 2 and Table 2a suggest manifest support for human intent to comply with a comprehensive computer

security policy, regardless of authorized user domain (H81, H82, H83, HA1, HA2, HA3). These findings suggest that the scope of an enterprise computer security policy should include both the IT domain and the OT domain, as opposed to only one domain or the other.

Variable ID	Manifest Observation on a Comprehensive Computer Security Policy	Mode Σ (n=210)	Mode IT (n=106)	Mode OT (n=104)
H11	My coworkers agree that I should comply with the new policy.	6	6	6
H12	My coworkers will think that I should comply with the new computer security policy.	6	6	6
H13	My supervisor will want me to comply with this new policy.	7	7	6
H21	It is important that I convince my coworkers to comply with the new computer security policy.	7	7	6
H22	My coworkers rely on my opinion.	6	7	6
H23	The new policy is important and others need to know how I feel about it.	6	7	6
H31	I will be reprimanded if my organization is aware of my non-secure actions.	7	7	6
H32	My management notices when I follow security procedures, and encourages me to keep doing a good job!	6	6	6
H33	I am encouraged when the company notices I am following security procedures.	6	7	6
H41	As a professional, I have to do certain things on my job. Strictly following computer security policies is one of them.	6	7	6
H42	Following computer security rules and policies is an important part of what I do as a professional.	7	7	6
H43	Breaking security policies hurts my image as a professional.	7	7	7
H51	This security policy helps to secure all computer systems.	7	7	6
H52	This security policy is absolutely necessary.	7	7	6
H53	This security policy is important.	7	7	6
H61	I understand the risks posed by poor security and that I may be reprimanded if I don't comply with policy.	7	7	7
H62	I am aware of the potential threats and negative consequences that are possible if I don't follow the proper security procedures.	7	7	6
H63	It is important that I follow the rules for keeping my organization secure so that I don't get into trouble.	7	7	7
H71	My co-workers and I agree that complying with the new policy is the right thing to do.	6	7	6
H72	It is important to me that my co-workers comply with the new policy.	7	7	6
H73	It is important that my co-workers know that I intend to comply with the new computer security policy.	7	7	7
H81	I believe that complying with the new security policy is a good idea.	7	7	7
H82	I think that complying with the new security policy is the right thing to do.	7	7	7
H83	By complying with the new security policy I am helping the company stay secure from computer threats.	7	7	6
H91	Complying with the new policy helps to improve my job performance.	6	7	6
H92	Complying with the new policy lets me perform my tasks more effectively.	6	6	6
H93	Complying with the new policy makes it easier for me to do my job.	6	7	6
HA1	I am confident that I will comply with the new computer security policy.	7	7	7
HA2	I understand the benefits of the new computer security policy and I intend to comply with it.	7	7	6
HA3	Regardless of how others think or act, I intend to comply with the new computer security policy.	7	7	6

Table 2. Manifest Observations (Mode) on a Comprehensive Computer Security Policy

A finding common to both domains is that while complying with a comprehensive security policy is perceived as the right thing to do, the act of being compliant may not contribute to individual job performance, performing individual tasks more

effectively, or make doing a job easier (H91, H92, H93). While authorized users may intend to comply with the comprehensive policy, management feedback mechanisms will need to be adjusted to reinforce the desired behavior (H31, H32, H33).

As was observed with the demographic data, examination of belief strength data reveals differences between the IT domain and the OT domain. This finding suggests belief strength differences should be acknowledged when developing domain specific components of an enterprise computer security policy. One observation is that authorized users from the IT domain may be more likely to understand the benefits of a comprehensive computer security policy than are authorized users from the OT domain (H51, H52, H53), and may be more likely to comply with a comprehensive computer security policy than OT authorized users. This may be related to the perceived prevalence of security countermeasures within information systems (IT domain), and the perceived lack of security countermeasures within industrial control systems (OT domain). One such example being the perceived prevalence of security education, training, and awareness (SETA) programs in the IT domain, as opposed to the OT domain.

Variable ID	Manifest Observation on a Comprehensive Computer Security Policy	Median Σ (n=210)	Median IT (n=106)	Median OT (n=104)
H43	Breaking security policies hurts my image as a professional.	6	7	6
H93	Complying with the new policy makes it easier for me to do my job.	5	5	5

Table 2a. Manifest Observations (Median) on a Comprehensive Computer Security Policy

Despite observed differences, the belief strength indicators for authorized users from both domains suggest an understanding of the benefits provided by an enterprise computer security policy and human intent to comply with a comprehensive computer security policy. As posited by TPB, the stronger the intent to perform a behavior, the more likely it is for that behavior to be performed.

FINDINGS AND CONTRIBUTION

The empirical findings of this study suggest manifest support, regardless of domain, for human intent to comply with a comprehensive computer security policy. Although 9 of 10 SEM path hypotheses exhibited statistical support for human intent to comply with a comprehensive computer security policy, the LISREL model did not produce the statistical support necessary to declare SEM goodness-of-fit (GOF) due to differences between the structural (theory) model and the measurement (reality) model. Unfortunately, theory did not match reality for this study. While it was tempting to pursue solutions within the measurement model to better fit the structural model, that would have been the wrong path to follow. By design, SEM models are based on theoretical substance and poor fitting models should be reevaluated from a theoretical perspective, not a data perspective (Diamantopoulos & Siguaw, 2000).

Regardless of the SEM GOF findings, the manifest observations produced by this study are of interest to the comprehensive computer security research community as they provide insight into the human belief strength of enterprise computer security.

Research contributions include the opportunity to evaluate manifest observations from a measurement model designed to reflect human intent to comply with a comprehensive computer security policy. Systematic study of these data will result in improved structural models seeking to understand the direct and indirect effects that determine human intent to comply with a comprehensive computer security policy, and the theoretical foundations that ground these effects.

Practitioner contributions include the opportunity to evaluate empirical findings from the IT domain and the OT domain in regard to the belief strength of human intent to comply with a comprehensive computer security policy. Examination of these data will contribute to the development and adoption of comprehensive computer security policies, standards, procedures and guidelines, and the convergence of IT computer security with OT computer security. Understanding the differences in demographics and belief strength within discrete domains will benefit SETA programs in the form of bespoke curriculums, and computer security culture development.

Realization of these contributions will result in improved enterprise computer security, through the reduction of vulnerabilities associated with the human factor. Next steps include continued research into the effects of a comprehensive computer security policy on human computer security policy compliance, to build upon the findings from this study.

REFERENCES

1. Acuña, D. C. (2017a). *Effects of a Comprehensive Computer Security Policy on Human Computer Security Policy Compliance.* Paper presented at the Proceedings of the Twelfth Midwest Association for Information Systems Conference, Paper 35, University of Illinois-Springfield.

2. Acuña, D. C. (2017b). *Effects of a Comprehensive Computer Security Policy on Human Computer Security Policy Compliance*. Doctoral Dissertation Final Defense. Dakota State University. Madison, SD.

3. Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

4. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-A527.

5. Diamantopoulos, A., & Siguaw, J. A. (2000). *Introducing LISREL*. London: SAGE Publications.

6. Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems, 8*(7), 386-408.

7. Fisher, A. G. B. (1939). Production, Primary, Secondary and Tertiary. *Economic Record, 15*, 24–38.

8. Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44.

9. Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

10. Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.): Prentice Hall.

11. Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly, 30*(1), 115-143.

12. Qualtrics. (2016). Online Survey Platform. Retrieved from https://www.qualtrics.com/

13. Song, J., & Zahedi, F. M. (2005). A Theoretical Approach to Web Design in E-Commerce: A Belief Reinforcement Model. *Management Science, 51*(8), 1219-1235.

14. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

15. Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security* (Sixth ed.). United States of America: Cengage Learning.