Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2017 Proceedings | Midwest (MWAIS)

6-2017

Effects of a Comprehensive Computer Security Policy on Human Computer Security Policy Compliance

Dennis C. Acuña
Dakota State University, dcacuna@bright.net

Effects of a Comprehensive Computer Security Policy on Human Computer Security Policy Compliance

Dennis C. Acuña
Dakota State University
dcacuna@dsu.edu

ABSTRACT

Several studies contend that humans are the weakest link in computer security, as humans often engage in non-secure computer practices with non-malicious intent. As a countermeasure to the vulnerability of human error in computer security, some studies posit that developing and maintaining a culture of computer security is essential for managing the human or behavioral aspect of computer security. One aspect of computer security culture is human compliance with computer security policy. However it is not well known how a *comprehensive* computer security policy effects human compliance with computer security policy, as a literature review resulted in no studies found on this topic. For purpose of this study, *comprehensive* computer security is defined as the enterprise level convergence of information technology (IT) computer security and operational technology (OT) computer security. This finding represents a gap in IS literature. Therefore, it is the thesis of this study 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.

Keywords
Comprehensive computer security policy, TPB, SEM, LISREL, research-in-progress.

INTRODUCTION

Literature Review

Several studies contend that humans are the weakest link in computer security, given that humans often engage in non-secure computer practices with non-malicious intentions. (Bulgurcu, Cavusoglu, & Benbasat, 2010; Chen, Ramamurthy, & Wen, 2012; D'Arcy & Hovav, 2007; Sasse, Brostoff, & Weirich, 2001). A non-malicious security violation (NMSV) such as failure to recognize phishing emails, use of weak passwords, development of non-secure program code, or failure to comply with computer security policies, poses a threat to computer security in the form of human error (Guo, Yuan, Archer, & Connelly, 2011; Willison & Warkentin, 2013). A recent report by IBM (2014) contends that more than 95% of computer security incidents include some aspect of human error, while a recent report by PwC (2015) states that human error contributed to 50% of the single worst data breaches in 2015, an increase of 31% over the previous year. NMSVs are acknowledged to represent human behavior separate from that predicated by malicious intent, with individuals engaged in malicious human behavior sometimes referred to as hackers, bad actors or malicious insiders (Wang, Gupta, & Rao, 2015), Given the modern day need for organizations to maintain uninterrupted access to information systems (IS) to achieve organizational objectives, human error represents a reverse salient within computer security defense-in-depth architectures due to the vulnerability it creates (Acuña, 2016; Dedehayir & Mäkinen, 2011; Guo et al., 2011; Hughes, 1983).

As a countermeasure to the vulnerability of human error in computer security, some studies contend that developing and maintaining a culture of computer security is essential for managing the human, or behavioral aspect of computer security (Da Veiga & Eloff, 2007; Dhillon, Syed, & Pedron, 2016; van Niekerk & von Solms, 2010; B. von Solms, 2000). Schein (2004) confirms this contention by stating that culture is an abstraction, and that organizations need to understand the forces that result from social and organizational situations lest they fall victim to them. One aspect of computer security culture is human compliance with computer security policy (Thomson & von Solms, 2005). Several studies have published findings on the effects of a computer security policy on computer security culture and compliance with computer security policy (D'Arcy & Hovav, 2007; Da Veiga & Eloff, 2007).

Thus, it is a premise of this study that human compliance with computer security policy is an element of computer security culture that contributes to managing the human aspect of computer security (S. H. von Solms, 2005). For this to be true, it is posited that an enterprise must have an overarching computer security policy that is *comprehensive* in scope and ownership, against which all impacted humans can be held compliant. However, no studies were found that explain the impact of a

comprehensive computer security policy on human computer security compliance through an understanding of its direct or indirect effects.

For purpose of this study, a *comprehensive* computer security policy is defined as a top-level enterprise policy incorporating all aspects of enterprise computer security encompassing information technology (IT) computer security and operational technology (OT) computer security, as opposed to only one domain or the other. The concept of merging IT computer security which is focused on information systems security with that of OT computer security which is focused on industrial control systems security is sometimes referred to as IT/OT convergence, and reflects a holistic approach to the practical management of enterprise computer security (ISACA, 2016; US-CERT Publications, 2015).

This definition of a *comprehensive* computer security policy differs from the traditional definition of a computer security policy that only includes aspects of a computer security program from the IT domain, as this definition also includes all aspects of a computer security program from the OT domain. As such, a *comprehensive* computer security policy encompasses all enterprise aspects of computer security thereby incorporating enterprise scope and ownership of computer security into a single, overarching policy that binds all humans in the enterprise to a common cause. In doing so, the issue of human error is addressed through human compliance with a shared, *comprehensive* computer security policy which in turn is aligned with Schein's (2004) formal definition of organizational culture; "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."

Thesis

It is the *comprehensive* nature of the computer security policy that separates this study from similar studies in this research domain. Therefore, it is the thesis of this study 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.

MOTIVATION

Comprehensive Computer Security Policy

It is not well known how a *comprehensive* computer security policy effects human compliance with computer security policy, as a literature review resulted in no studies found on this topic. This finding represents a gap in IS literature and the motivation for this study, as any computer security policy to which humans are held accountable should be explainable in regard to the factors that influence human compliance with that policy. It is a premise of this study that human compliance with computer security policy is an element of computer security culture that contributes to managing the human, or behavioral aspect of computer security. In addition, it is posited that such a policy must be overarching and *comprehensive* in terms of scope and ownership, against which all impacted humans can be held compliant. As defined by this study, a computer security policy must be *comprehensive* in scope and ownership in order to have a meaningful effect on human compliance with computer security policy.

This study defines a *comprehensive* computer security policy as a top-level policy incorporating all aspects of computer security including research, control selection, tool selection, monitoring, incident response, and training and awareness practices from both the IT and OT domains. A logical reference to the distinction between the IT domain and the OT domain is that described by the Reference Model for Computer Integrated Manufacturing (CIM), wherein the separation between the IT domain and the OT domain can be paraphrased as the point of demarcation between computer decision support systems leveraged by humans (IT), and computer industrial control systems that make control decisions autonomously (OT) (CIM Reference Model Committee International Purdue Workshop on Industrial Computer Systems, 1989). Recognition of this distinction and the effect of joining both domains into a *comprehensive* computer security policy are critical to understanding the premise of this thesis.

Thus, this research is both novel and timely in its intent to better understand the factors that influence human compliance with a *comprehensive* computer security policy. This research is novel in that no peer reviewed research was found that explained the direct effect of a *comprehensive* computer security policy on human computer security compliance through an understanding of its indirect effects. This research is timely in that modern computer threats and computer vulnerabilities, sometimes referred to as cybersecurity, are evolving rapidly and are capable of introducing significant computer risk to an organization (D'Arcy & Hovav, 2007; National Intelligence Council, 2008; U.S. Government, 2011; U.S. PPD-41, 2016; UK Government, 2016). These beliefs are grounded in the thesis of this study 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. As this paper represents research-in-progress, the following content includes sections comprising the research model, research methodology, expected results and contribution, findings and publication, and other documentation necessary to support this thesis.

RESEARCH MODEL

Theory of Planned Behavior

The theory of planned behavior (TPB) seeks to predict and understand motivational influences on human behavior. Defined by Ajzen (1991), TPB states that human behavior is determined by factors that influence the intention to perform a specific behavior. TPB consists of five constructs; subjective norms, attitude toward the behavior, perceived behavioral control, intention, and behavior. Rather than model specific human behavior, TPB models human behavioral intention. The stronger the intention to perform the behavior, the more likely it is that the specific behavior will be performed. Perceived behavioral control varies across situations and actions, and in some cases can be used directly to predict a successful behavioral attempt.

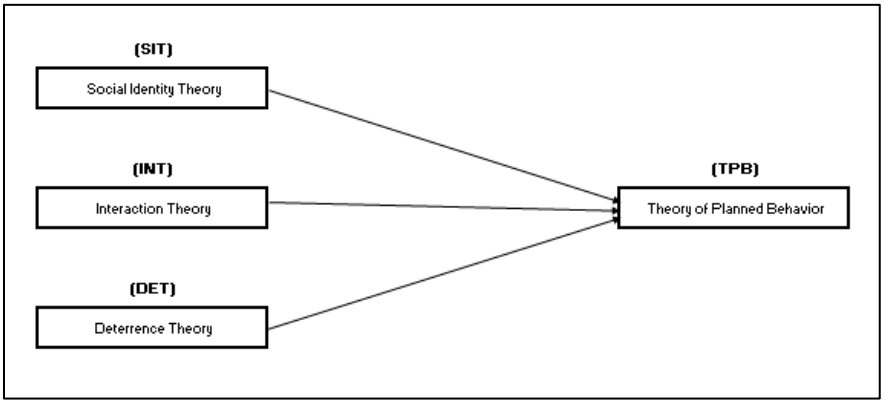

Figure 1. Theoretical Foundation

Social Identity Theory

Hogg, Terry, & White (1995) contend that social identity theory (SIT) is an accepted perspective on the social constructs of self-concept and normative behavior. The authors also contend that SIT shares the same perspective as identity theory, with the primary distinction being that SIT is a proven psychology theory used to explain group processes and intergroup relations. SIT is used to explain behavioral tendencies that cause people to classify themselves and others into various social categories such as religious affiliation, organizational recognition, gender, and age. Ashforth & Mael (1989) posit that this classification gives a person the ability to segment and order the social environment into a meaningful structure, and then locate and define themselves in that social environment. By socially identifying with a group, the individual is viewed as sharing in the group's success and status. Cheung & Lee (2010) contend that social identity helps to determine collective intention to perform a behavior. The authors also contend that if an end user exhibits strong social identity toward a group behavior, then intention will increase.

Interaction Theory

Change is often met with resistance, and the introduction of change will encounter resistance from those who are held accountable to the change. Markus (1983) contends that interaction theory (INT) provides a framework against which the introduction of change can be better managed. INT is posited to be useful with decentralized systems when a centralized system is desired, and with systems that alter the balance of power in regard to those who lose power and those who gain power. Kling (1980) posits that people and groups resist change introduced by system implementation due to the interaction between characteristics in people and characteristics related to the system. From this perspective the greater the implied change, the more likely the resistance to the change. Markus (1983) posits that INT represents a superior method for developing IS implementation strategies for managing beliefs about resistance during IS implementation.

Deterrence Theory

IS studies leverage deterrence theory (DET) to explain unethical human behavior involving the use of technology in organizations. DET suggests that the perceived certainty and severity of formal sanctions serves as a deterrent to committing an illicit act (D'Arcy & Devaraj, 2012). D'Arcy & Devaraj contend that the threat of formal sanctions has both direct and

indirect influences on the intentional misuse of technology. Hu, Xu, Dinev, & Ling (2011) report findings that contradict the accepted view of DET and information security by stating that behavior is influenced more by an individual's personal ethics or moral compass, than the ramifications of a deterrent alone. This aligns with Siponen & Vance (2010) who contend that deterrence is less effective when neutralization techniques that minimize perceived harm are detected.

Theoretical Foundation

Given the perceived influence of social identity, interaction with others, and the effect of sanction rhetoric in positively effecting intention to comply with a *comprehensive* computer security policy, the theoretical concepts of SIT, INT, and DET are incorporated into the theoretical foundation as antecedent theories to TPB (Figure 1). This theoretical foundation contributes to a better understanding of human behavior and NMSVs. This theoretical foundation also aligns with Schein's formal definition of organizational culture; "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."

Hypotheses Development

This study draws on TPB to predict human intent to comply with a *comprehensive* computer security policy. The use of TPB in IS literature to predict human intent is well documented (Bulgurcu et al., 2010; Dinev & Hu, 2007; Flores & Ekstedt, 2016; Guo et al., 2011; Pavlou & Fygenson, 2006; Song & Zahedi, 2005). Based on the documented use of TPB in IS research, hypotheses drawn against the TPB constructs of subjective norms, attitude, and perceived behavioral control are included in the research model but have been modified to support this study. These hypotheses are included for completeness, as the research model cannot be tested without these paths.

This study also incorporates constructs drawn from SIT, INT, and DET as antecedent constructs to TPB constructs to better understand the indirect factors that predict human intent to comply with a *comprehensive* computer security policy. In doing so, this study makes a unique contribution to IS literature by incorporating TPB with other behavioral theories through the use of antecedent constructs.

Drawing from the use of SIT in IS studies, Cheung & Lee (2010) leveraged SIT to measure group intention to use a social networking site by measuring subjective norms and social identity. The authors contend that subjective norms reflect social pressure from significant others to perform a behavior, as a user tends to rely on subjective norms to decide whether or not to use a new technology. The authors posit that if an end user exhibits strong social identity toward a group behavior, then intention will increase. Song & Kim (2006) synthesized the progenitor of TPB, the theory of reasoned action (TRA), and SIT to predict behavioral intention to use a service. Specifically, the authors leveraged SIT, TRA, and relationships between the constructs of social identity and subjective norms to predict user intention.

Drawing from the use of INT in IS studies, Markus (1983) posits that INT represents a superior method for managing beliefs about resistance to change, and that INT offers a superior theory for managing the resistance encountered during information system implementation. INT is posited to be useful with decentralized systems when a centralized system is desired, and with systems that alter the balance of power in regard to those who lose power and those who gain power.

Drawing from the use of DET in IS studies yields mixed results. While several studies contend that enforcement activities are an important part of any information security culture, IS studies incorporating DET have revealed positive and negative influences on intention. D'Arcy & Devaraj (2012) contend that the threat of formal sanctions has direct and indirect influences on an individual's intention to misuse information assets. Herath & Rao (2009) posit that sanctions are an effective mechanism in reducing negative behavior and exhibit a positive influence on social behavior. Johnston, Warkentin, & Siponen (2015) contend sanction rhetoric that emphasizes the impact of both personal relevance and IS relevance provides a positive influence on intention to comply with information security policy, confirming that sanction rhetoric influences human intention.

Path Diagram

Therefore, based on the usage pattern of TPB, SIT, INT, and DET in IS research, the research model for this study leverages a modified version of TPB to measure the factors that influence human intention to comply with a *comprehensive* computer security policy. The traditional TPB constructs of subjective norms, attitude, and perceived behavioral control are modeled in expected form as independent variables against a construct of intention as the dependent variable. New constructs of *comprehensive* computer security policy, social identity with organizational others, resistance to policy compliance, and perceived effect of sanctions for non-compliance are incorporated as antecedent constructs to TPB to further measure the

predictability of human intent to comply with a *comprehensive* computer security policy. The path diagram shown in Figure 2 models the inclusion of TPB constructs, new SIT, INT, DET, and *comprehensive* computer security policy antecedent constructs, 3 indirect (mediating) paths, 1 direct path, 6 control (moderating) variables, 10 research hypotheses, 1 dependent variable (intention to comply), several independent variables, 1 exogenous construct (*comprehensive* computer security policy), and several endogenous constructs.

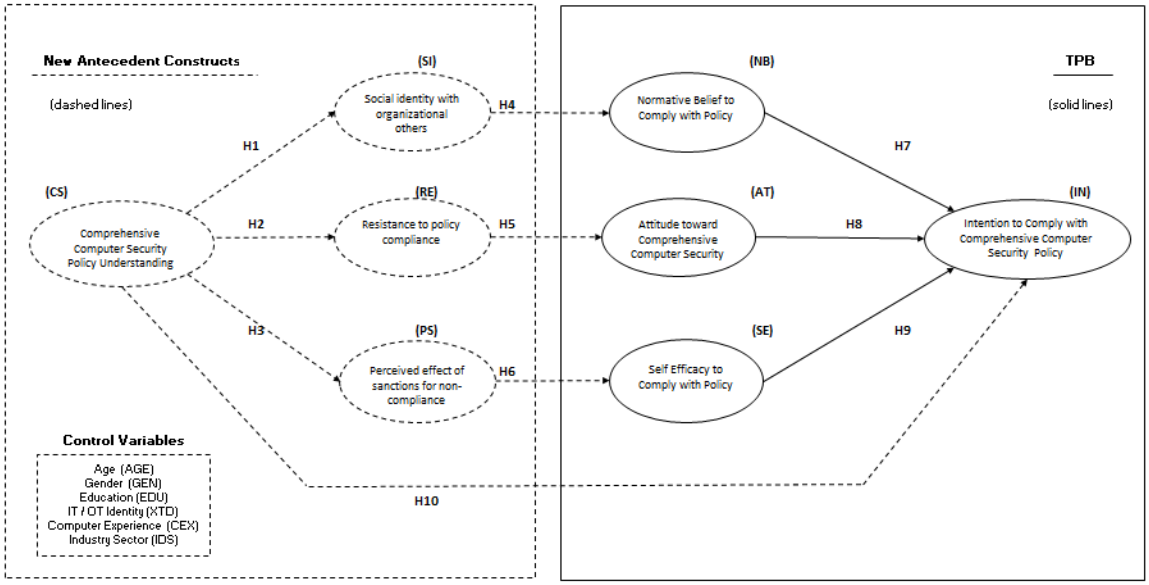

Figure 2. TPB Base Research Model with Antecedent Constructs (Path Diagram)

RESEARCH METHODOLOGY

Survey Instrument and Data Collection

The research methodology for this study includes the collection of data using a survey instrument, and analysis of the collected data using multivariate data analysis techniques (Hair, Black, Babin, & Anderson, 2009; Kumar, 2005; Trochim & Donnelly, 2008). The survey instrument will utilize a unipolar 7-point Likert scale for measurement (Ajzen, 1991). Where possible, use case scenarios and questions for the survey instrument will be drawn from previous studies conducted in this research domain (Flores & Ekstedt, 2016; Guo et al., 2011; Pavlou & Fygenson, 2006). Six control variables are planned for this study; age, gender, education, IT/OT identity, years of professional computer experience, and industry sector.

Questionnaire distribution and data collection will be performed by Qualtrics (2016), a commercial Internet service that specializes in survey based research. Although the survey instrument will be modeled after IS studies that leveraged TPB survey research, a pilot survey will be conducted prior to the primary data survey to ensure robustness. The target population for this study is authorized users located in the United States, randomly selected from defined industry sectors. It is the intention of this study that all identifiers capable of linking a response to a participant, including Internet Protocol (IP) address, will be hidden and unknown to the principal investigator.

Sample Size

Hair et al. (2009) recommend a sample size of 100 to 400 observations for SEM studies. The most common SEM estimation procedure is maximum likelihood estimation (MLE) which supports a minimum sample size of 50, but recommends a sample size of 200 to provide a sound basis for estimation. Sample sizes greater than 400 become sensitive to meaningless differences resulting in goodness-of-fit (GOF) measures that suggest a poor fit. Therefore, based on MLE recommendations, a sample size of 200 (minimum) to 250 (maximum) responses is targeted for this study. A maximum of 250 responses compares favorably to MLE recommendations, and provides a small buffer should a less than reasonably high response rate be realized.

Data Analysis

Multivariate data analysis techniques to be performed on the collected data include confirmatory factor analysis (CFA) and structural equation modeling (SEM). CFA and SEM are often used together to measure the validity of a research model, to

determine whether or not the estimated model fits the observed model. CFA is a statistical test used to determine how well the factors described by the theoretical model match the reality of data gathered by the study observations. SEM is a family of statistical models used to explain relationship strength between the multiple variables that are linked together in a path diagram (Figure 2). SEM performs this task by examining relationships between the independent variables and the dependent variable in a path diagram as a series of equations similar to a series of multiple regression equations.

SEM and CFA analyses can be performed using one of several computer software packages. This study will use the LISREL (LInear Structural RELations) computer programming language to perform CFA and SEM analyses. While SEM models such as the TPB Base Research Model with Antecedent Constructs depicted in Figure 2 are often drawn using simplified path diagrams to describe dependence relationships between independent (exogenous) and dependent (endogenous) variables, SEM models can also be drawn using a lexicon known as LISREL notation. Although LISREL refers specifically to a widely used computer program for SEM modeling, the LISREL platform includes a unique lexicon known as LISREL notation to depict and describe SEM models (Hair et al., 2009).

Goodness-of-Fit

SEM goodness-of-fit (GOF) measurement compares theory to reality by comparing the difference between the estimated covariance matrix, or theory, to the observed covariance matrix, or reality (Hair et al., 2009). If the modeled theory is perfect then a comparison of the estimated covariance matrix and the observed covariance matrix will show no difference, a perfect fit, between the two matrices. For SEM, the implied null hypothesis is that there is no difference between the estimated covariance matrix, or theory, and the observed covariance matrix, or reality, meaning that the research model is a good fit with reality. One statistic used to measure variance between the two matrices is chi-square (χ^2). Given that the value of χ^2 increases as the variance between the two matrices increases, we also reference the *p-value* associated with χ^2 to assess the equality of the estimated covariance matrix and the observed covariance matrix within a given population (Hair et al., 2009). This leads to desired critical values of a relatively small χ^2 value that approaches zero (0), and a correspondingly large *p*-value that approaches one (1).

However, due to known problems using χ^2 as a test statistic for SEM GOF, Hair et al. (2009) suggest that SEM studies report at least one absolute GOF index and one incremental GOF index in addition to χ^2. Absolute GOF indexes include χ^2, root mean square error of approximation (RMSEA), and the goodness-of-fit index (GFI). Incremental GOF indexes include the normed fit index (NFI), and the comparative fit index (CFI).

EXPECTED RESULTS AND CONTRIBUTION

Expected Results

The thesis of this study is 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. It is a premise of this study that human compliance with computer security policy is an element of computer security culture that contributes to managing the human aspect of computer security. This study is both novel and timely in its intent to better understand the factors that influence human compliance with a *comprehensive* computer security policy, and minimize the vulnerability that is human error. It is anticipated that the statistical findings of this study will support these beliefs and will benefit researchers and practitioners in several ways.

Contribution

First, this research represents a contribution to IS literature in that no peer reviewed research was found that explains the direct effect of a *comprehensive* computer security policy on human computer security compliance through an understanding of its indirect effects. This study also contributes to IS literature in that it incorporates new antecedent constructs from SIT, INT, and DET with traditional TPB constructs to better understand the factors that influence human intent to comply with a *comprehensive* computer security policy. Completion of this study will provide researchers with a descriptive understanding of the direct and indirect effects on human intention to comply with a *comprehensive* computer security policy.

Second, the prescriptive application of a shared *comprehensive* computer security policy will have a positive impact on enterprise computer security awareness and reduced human error. A better understanding of the practical benefits of compliance with a *comprehensive* computer security policy will lead to improved computer security awareness, which will help manage the resistance to change that is often encountered when change alters the perception of power in regard to those who lose power and those who gain power. Improved computer security awareness will also contribute to an increase in self-

efficacy and personal intent to comply with such a policy, resulting in the direct effect of reduced human error and fewer occurrences of NMSVs.

Third, this research is timely in that modern computer threats and computer vulnerabilities are evolving rapidly and are capable of introducing significant risk to both the IT computer domain and the OT computer domain. Publication of this study will help draw attention to the practical need for convergence of IT computer security and OT computer security. This contribution is underscored by the notion that theory is not the exclusive domain of academia, but can also be found in the experience and practice gathered through the observation of real world behavior (Hair et al., 2009; Lee, 1999).

Lastly, the practical application of these findings will benefit the enterprise by helping to develop a *comprehensive* culture of computer security by incorporating enterprise scope and ownership of computer security into a single, overarching policy that binds all humans in the enterprise to a common cause. The findings from this study will reinforce Schein's contention that culture is an abstraction, and that organizations need to understand the forces that result from social and organizational situations lest they fall victim to them. In addition, the findings will contribute to the ongoing development and persistence of organizational culture as defined by Schein; "a pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems."

FINDINGS AND PUBLICATION

There are no findings to report at this time as this paper represents research-in-progress. A research application has been filed with the Dakota State University (DSU) Institutional Review Board (IRB). The data collection phase is scheduled to begin in 1Q2017, which will be followed by the data analysis phase. Completion of this study is scheduled for 2Q2017. Final results will be presented in a public forum at DSU, and submitted for publication in an academic journal shortly thereafter.

REFERENCES

1. Acuña, D. C. (2016). Enterprise Computer Security: A Literature Review. *Journal of the Midwest Association for Information Systems (JMWAIS), 2016*(1), Article 3, 37-53.

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

3. Ashforth, B. E., & Mael, F. (1989). Social Identity Theory and the Organization. *The Academy of Management Review, 14*(1), 20-39.

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. Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29*(3), 157-188.

6. Cheung, C. M. K., & Lee, M. K. O. (2010). A theoretical model of intentional social action in online social networks. *Decision Support Systems, 49*(1), 24-30.

7. CIM Reference Model Committee International Purdue Workshop on Industrial Computer Systems. (1989). *A Reference Model for Computer Integrated Manufacturing (CIM): A Description from the Viewpoint of Industrial Automation*. Instrument Society of America, Research Triangle Park, NC.

8. D'Arcy, J., & Devaraj, S. (2012). Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. *Decision Sciences, 43*(6), 1091-1124.

9. D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM, 50*(10), 113-117.

10. Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

11. Dedehayir, O., & Mäkinen, S. J. (2011). Determining reverse salient types and evolutionary dynamics of technology systems with performance disparities. *Technology Analysis & Strategic Management, 23*(10), 1095-1114.

12. Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56*, 63-69.

13. 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.

14. 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.

15. 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.

16. Hair, J. F., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2009). *Multivariate Data Analysis* (7th ed.): Prentice Hall.

17. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

18. Hogg, M. A., Terry, D. J., & White, K. M. (1995). A Tale of Two Theories: A Critical Comparison of Identity Theories with Social Identity Theory. *Social Psychology Quarterly, 58*(4), 255-269.

19. Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

20. Hughes, T. P. (1983). *Networks of power: Electrification in Western Society, 1880–1930*. Baltimore, MD: The Johns Hopkins University Press.

21. IBM. (2014). *IBM Security Services 2014 Cyber Security Intelligence Index: Analysis of of cyber attack and incident data from IBM's worldwide security operations*. Retrieved from http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_TM_USEN_P&htmlfid=SEW03039USEN&attachment=SEW03039USEN.PDF

22. ISACA. (2016). IT/OT Convergence and Industrial Cybersecurity. Retrieved from http://www.isaca.org/Education/Online-Learning/Pages/Webinar-ITOT-Convergence-and-Industrial-Cybersecurity.aspx

23. 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-A117.

24. Kling, R. (1980). Social analyses of computing: Theoretical perspectives in recent empirical research. *ACM Computing Surveys, 12*(1), 61-110.

25. Kumar, R. (2005). *Research Methodology: A Step-by-Step Guide for Beginners* (2nd ed.). London, England: SAGE Publications.

26. Lee, A. (1999). Inaugural editor's comments. *MIS Quarterly, 23*(1), 1-1.

27. Markus, M. L. (1983). Power, politics, and MIS implementation. *Communications of the ACM, 26*(6), 430-444.

28. National Intelligence Council. (2008). *Disruptive Civil Technologies - Six Technologies with Potential Impacts on US Interests out to 2025*.

29. 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.

30. PwC. (2015). *2015 Information Security Breaches Survey*. Retrieved from http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

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

32. 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.

33. Schein, E. H. (2004). *Organizational Culture and Leadership* (3rd ed.). San Francisco, CA: Jossey-Bass.

34. Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly, 34*(3), 487-A412.

35. Song, J., & Kim, Y. (2006). Social influence process in the acceptance of a virtual community service. *Information Systems Frontiers, 8*(3), 241-252.

36. 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.

37. Thomson, K.-L., & von Solms, R. (2005). Information security obedience: a definition. *Computers & Security, 24*(1), 69-75.

38. Trochim, W. M. K., & Donnelly, J. P. (2008). *The Research Methods Knowledge Base* (3rd ed.). United States: Cengage Learning.

39. U.S. Government. (2011). *International Strategy for Cyber Space*. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

40. U.S. PPD-41. (2016). *Presidential Policy Directive -- United States Cyber Incident Coordination*. Retrieved from https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

41. UK Government. (2016). *United Kingdom National Cyber Security Strategy 2016-2021*. Retrieved from https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

42. US-CERT Publications. (2015). *Security Tip ST05-017 Cybersecurity for Electronic Devices*. https://www.us-cert.gov/ncas/tips/ST05-017: United States Computer Emergency Readiness Team.

43. van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security, 29*(4), 476-486.

44. von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security, 19*(7), 615-620.

45. von Solms, S. H. (2005). Information Security Governance – Compliance management vs operational management. *Computers & Security, 24*(6), 443-447.

46. Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS Quarterly, 39*(1), 91-A97.

47. Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly, 37*(1), 1-20.