Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2016 Proceedings

Midwest (MWAIS)

Spring 5-19-2016

Effects of a Comprehensive Computer Security Policy on Computer Security Culture

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

Effects of a Comprehensive Computer Security Policy on Computer Security Culture

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

ABSTRACT

It is well known that humans are the weakest link in computer security, and that developing and maintaining a culture of computer security is essential for managing the human aspect of computer security. It is less well known how a *comprehensive* computer security policy incorporating both information technology computer security, and operational technology computer security, impacts a culture of computer security. While a literature review of this domain includes research on the impact of various aspects of a computer security policy on computer security culture, no peer reviewed research was found that explained the impact of a comprehensive computer security policy on computer security culture through an understanding of its direct or indirect effects. Thus, it is the thesis of this study that a comprehensive computer security policy has a direct effect on computer security culture, which can be further explained through indirect effects.

Keywords

Comprehensive computer security policy, effectiveness, avoidability, self-efficacy, research-in-progress.

INTRODUCTION

That humans are the weakest link in computer security is well known (Bulgurcu, Cavusoglu, & Benbasat, 2010; D'Arcy & Hovav, 2007; Sasse, Brostoff, & Weirich, 2001). 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. As a counter measure to the vulnerability of human error in computer security, it has been posited that developing and maintaining a culture of computer security is essential for managing the human aspect of computer security (Da Veiga & Eloff, 2007; Dhillon, Syed, & Pedron, 2016; Van Niekerk & Von Solms, 2010).

It is less well known how a *comprehensive* computer security policy impacts a culture of computer security, comprehensive being defined as incorporating both information technology computer security (IT computer security) and operational technology computer security (OT computer security). While the extant literature for this peer reviewed research domain includes mention of the impact of various aspects of a computer security policy on computer security culture (Chen, Ramamurthy, & Wen, 2012; Safa, Von Solms, & Furnell, 2016; Vance, Lowry, & Eggett, 2013), no peer reviewed research was found that explained the impact of a comprehensive computer security policy on computer security culture through an understanding of its direct or indirect effects.

Thus, it is the thesis of this study that a comprehensive computer security policy has a direct effect on computer security culture, which can be further explained through indirect effects. To support this statement, this study explores the direct effect that a comprehensive computer security policy has on computer security culture and on a computer security program, as well as the indirect effects derived therefrom. Specifically, this study seeks to answer the following questions:

1. Is there a direct relationship between a comprehensive computer security policy and computer security culture?
2. Are there indirect relationships between a comprehensive computer security policy and computer security culture?
    a. Is governance a mediating factor between a comprehensive computer security policy and computer security culture?
    b. Is training & awareness a mediating factor between a comprehensive computer security policy and computer security culture?
    c. Are sanctions a mediating factor between a comprehensive computer security policy and computer security culture?
3. Are there other variables that impact the relationship between a comprehensive computer security policy and computer security culture?

MOTIVATION

Key to the premise of this study is the scope and ownership of the computer security policy. This study contends that a computer security policy must be comprehensive in scope in order to have a meaningful impact on enterprise computer security culture, as a comprehensive computer security policy represents a policy that spans all aspects of enterprise computer security (von Solms, 2001). This study defines a comprehensive computer security policy as a top-level policy incorporating enterprise ownership of both IT computer security and OT computer security. A practical reference to this viewpoint 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).

The premise of this study holds that a comprehensive scope is necessary for a computer security policy to have a meaningful impact on computer security culture, and that it is the comprehensive nature of the computer security policy that separates this study from other studies in this domain. A comprehensive computer security policy sets the tone for clear ownership of enterprise computer security by recognizing the difference between IT and OT, which in turn sets the tone for developing and maintaining a culture of computer security across an enterprise. Every human in the enterprise is responsible for computer security regardless of whether their assigned role aligns more closely with IT computer security than OT computer security, and vice versa, and this distinction must be recognized by a top-level policy for persistence of a meaningful computer security culture.

The premise of this study is both novel and timely in its intent to better understand the factors that influence a culture of computer security, given that computer security culture is posited as an effective control for managing the human aspect of computer security. The premise is novel in that no peer reviewed research was found that explained the direct effect of a comprehensive computer security policy on computer security culture through an understanding of its indirect effects. The premise is timely in that 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). Therefore, research that contributes to a better understanding of the factors that impact computer security culture represents research that is important to any organization that relies on humans for computer security.

RESEARCH MODELS

Extant research incorporating Technology Threat Avoidance Theory (TTAT), deterrence theory, and the constructs of perceived effectiveness, perceived avoidability, and self-efficacy were referenced to help develop the conceptual research model shown in Figure 1 (Chen, Ramamurthy, & Wen, 2015; Compeau & Higgins, 1995; Herath & Rao, 2009; Hu, Xu, Dinev, & Ling, 2011; Liang & Xue, 2009).

Liang & Xue (2009) contend that perceived effectiveness results from human outcome judgement regarding behavior that will lead to a specific outcome when performed (Bandura, 1982). Liang & Xue also contend that perceived effectiveness within TTAT measures the usefulness of the safeguard in terms of its ability to avoid a malicious threat. Liang & Xue further contend that perceived avoidability results from the human perception of the effectiveness of the safeguarding action that is performed, and that a coping mechanism attends to the evaluation and assessment of each available safeguarding measure. The self-efficacy component of TTAT suggests that the safeguarding measure with the highest perceived avoidability, as perceived by the user, is then selected and performed to avoid the perceived threat. The authors also posit that self-efficacy reflects human perception of the benefit of a safeguarding action.

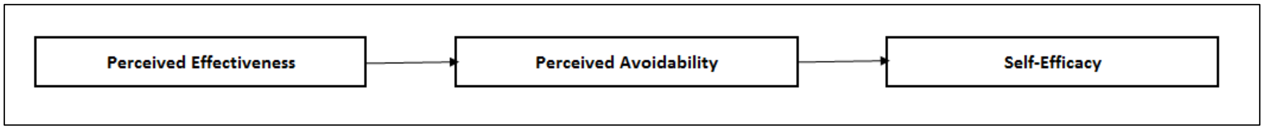

Figure 1. Conceptual Research Model

Self-efficacy is a central theme of TTAT, in the belief that human behavior is influenced by the perceived efficacy of the available safeguarding actions. TTAT theory contends that humans will adopt a safeguarding action if they perceive the threat will be mitigated by the safeguarding measure. If the safeguarding measure is perceived to be ineffective, humans will avoid the safeguarding action and instead resort to an emotion based coping behavior in the belief that the threat is unavoidable (Bandura, 1982; Compeau & Higgins, 1995; Maddux & Rogers, 1983).

D'Arcy & Devaraj (2012) contend that the threat of sanctions, or punishment, has a direct and indirect effect on influencing human behavior toward information technology threats. The threat of sanctions is drawn from deterrence theory, based on the belief that humans are deterred from certain behaviors given the perceived certainty and perceived severity of a resulting sanction (Gibbs, 1975). As with TTAT, self-efficacy plays a role in deterrence theory given a user's perception that the threat of sanctions are able to deter unwanted behavior.

Following development of the conceptual research model, each of the constructs shown in Figure 1 was operationalized into latent variables and observable variables as shown in Figure 2. Each of the variables shown in Figure 2 is measurable using a survey instrument.

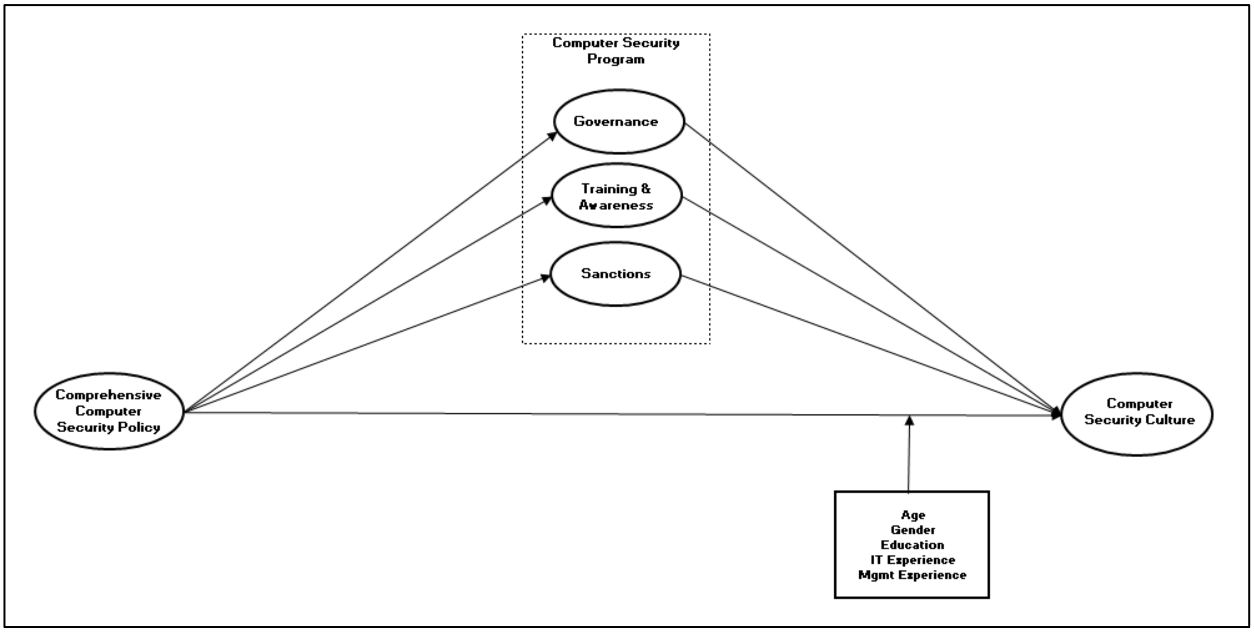
Computer Security Program
Governance
Training & Awareness
Sanctions
Comprehensive Computer Security Policy
Computer Security Culture
Age
Gender
Education
IT Experience
Mgmt Experience

Figure 2. Operationalized Research Model

RESEARCH METHODOLOGY

Data collection for this study will be performed using a survey instrument and a Likert scale for measurement. Where possible, questions for the survey instrument will be drawn from similar studies conducted in this research domain. A commercial Internet service will be used for survey instrument distribution and data collection. A pilot survey will be conducted prior to the primary data survey to ensure robustness. Target respondents are information technology practitioners located within the United States, randomly selected from the information technology workforce.

Multivariate data analysis techniques performed on the collected data will include confirmatory factor analysis (CFA) to test how well the measured variables represent model constructs. Structural equation modeling (SEM) will be used to estimate the overall fit of the model. Particular attention will be given to the indirect effect of factors, both mediating and moderating, impacting computer security culture.

DEVELOPMENT AND PUBLICATION

There are no findings to report at this time as this paper represents research-in-progress. Completion of this study is scheduled for 1Q2017. Next steps include acceptance and approval of the research proposal, initiation of the data collection process, statistical data analysis, and writing the final report. Findings resulting from this study will be submitted for publication in an academic peer reviewed journal.

CONCLUSION

It is the thesis of this study that a comprehensive computer security policy has a direct effect on computer security culture, which can be further explained through indirect effects. It is anticipated that the statistical findings of this study will support the conceptual research model. It is further anticipated that the findings of this study will benefit scholars and practitioners alike.

REFERENCES

1. Bandura, A. (1982). Self-Efficacy Mechanism in Human Agency. *American Psychologist, 37*(2), 122-147.

2. 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.

3. 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.

4. Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). IMPACTS OF COMPREHENSIVE INFORMATION SECURITY PROGRAMS ON INFORMATION SECURITY CULTURE. *The Journal of Computer Information Systems, 55*(3), 11-19.

5. 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.

6. Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly, 19*(2), 189-211.

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

8. D'Arcy, J., & Hovav, A. (2007). DETERRING INTERNAL INFORMATION SYSTEMS MISUSE. *Communications of the ACM, 50*(10), 113-117.

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

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

11. Gibbs, J. P. (1975). *Crime, Punishment, and Deterrence*. New York, NY: Elsevier North-Holland, Inc.

12. 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.

13. 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.

14. 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

15. Liang, H., & Xue, Y. (2009). AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE. *MIS Quarterly, 33*(1), 71-90.

16. 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*, 469-479.

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

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

19. Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

20. 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.

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

22. Vance, A., Lowry, P. B., & Eggett, D. (2013). Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems, 29*(4), 263-290.

23. von Solms, B. (2001). Information Security - A Multidimensional Discipline. *Computers & Security, 20*(6), 504-508.