Unlocking the Mixed Results of the Effect of Self-Efficacy in Information Security on Compliance.

Emergent Research Forum (ERF)

Dinesh S Reddy
Texas A&M University - Central Texas
dreddy@tamuct.edu

Glenn Dietrich
The University of Texas at San Antonio
glenn.dietrich@utsa.edu

Abstract

The outcome of the effect of Self-efficacy in information security (SEIS) on compliance to secure behavior has been positive to most extent. However, in some studies, the relationship between SEIS and compliance has shown a negative effect, thus signaling mixed results. The importance of unlocking this mixed result is significant since any proven deviation in results (about the effect of SEIS on compliance) will challenge the past empirical findings. Past research has ignored to explain why the results of the effect of SEIS on compliance are mixed. In this article, we explore the multi level nature of SEIS, measurement process involved, and context specific conceptualizations of SEIS as possible reasons that explain the reversal of security behavior. This research will guide future research on what could cause people with high SEIS to not exhibit secure compliance behavior, where SEIS and compliance are more often modeled in behavioral security research.

Keywords

Self-efficacy in information security, cybersecurity compliance, overconfidence.

Introduction

According to US Census 83.8 percent of U.S. households own a computer with about 74.4 percent of all households connected to internet (US Census 2013). There is heavy dependence on computers and internet for performing online transactions related to both work and personal tasks. This warrants safe and secure cybersecurity compliance behavior from end users.

Past research has very well established results on what factors will improve end user cybersecurity compliance behavior. For example: subjective norm, self-efficacy in information security (SEIS), perceived severity of sanctions, response efficacy, response cost, etc. (Sommestad et al. 2014), threat severity, threat vulnerability, safety habit strength, personal responsibility, perceived security support (Tsai et al. 2016), and big five personality factors (Johnston et al. 2016). Applying research outcomes from the past, if online transactions are to be secure all the time, the established results of the impact of various factors on compliance behavior should also be consistent. If the effect of any factor on compliance behavior is mixed, then it is difficult to predict what leads to security compliance behavior.

In this research, we consider the case of self-efficacy as a factor that is well established in past research to impact cybersecurity compliance behavior (Sommestad et al. 2014). SEIS is defined as a belief in an individual's capability to protect information and information systems from unauthorized disclosure, loss, modification, destruction and lack of availability (Rhee et al. 2009). Theoretically, SEIS should have a positive effect in increasing compliance and improving the cybersecurity behavior. The outcome of the effect of SEIS on compliance has been positive to most extent in empirical research (E.g.: Bulgurcu et al. 2010). However, there is evidence in literature that highlights a deviation in the expected outcome of the effect of SEIS on compliance, thus making the overall results fairly inconsistent.

The purpose of this paper is to explain why the results of the effect of SEIS on compliance are mixed using meta-anlysis. This is significantly important since any proven deviation in results (such as SEIS negatively affecting compliance when applied to certain situations) will challenge the validity of past empirical research where SEIS consistently has a positive impact on compliance. It is expected that computer end users who possess high SEIS should also exhibit safe compliance behavior. If not, then there might be specific situations where security of online transactions is compromised in spite of end user performing the online transactions possessing high SEIS. Hence the current research has an implication that can help guide future research on what could cause people with high SEIS to exhibit unsafe compliance behavior.

Literature Review

According to social cognitive theory, self-efficacy is concerned with how perceptions of ability to perform a task affect user's behavior. Self-efficacy is the belief in one's ability to organize and execute a particular course of action (Bandura 1986). SEIS is defined as a belief in an individual's capability to protect information and information systems from unauthorized disclosure, loss, modification, destruction and lack of availability (Rhee et al. 2009). In the same context, self-efficacy (a user's self-confidence in his/her skills or abilities in practicing computer security) is likely to increase computer security behavior (Ng et al. 2009). Research in this direction is summarized in table 1.

Study	SEIS increases compliance behavior?	Context of study	Antecedents of SEIS with +ve effect	Antecedents of SEIS with -ve effect	Antecedents of SEIS (not supported in the study
Bulgurcu et al. 2010	yes	org	None	None	None
Herath and Rao 2009	yes	org	Resource availability	None	None
Siponen et al. 2010	yes	org	None	None	None
Ifinedo 2012	yes	org	None	None	None
Son 2011	yes	org	None	None	None
Johnston and Warkentin 2010	yes	University	None	Perceived threat severity	Perceived threat susceptibility
Rhee et al. 2009	yes	university	computer/internet experience General controllability	Security breach incidents	None
Liang & Xue 2010	yes	university	None	None	None
Ng et al. 2009	yes	org	None	None	None
Chou &Chou 2016	yes	University	None	None	None
Tsai et al. 2016	**No**	**Home**	**None**	**None**	**None**
Sun et al. 2016	yes	University	Internet self-efficacy	None	None
Johnston et al. 2016	yes	org	None	None	None
Hanus & Wu 2016	yes	University	Countermeasures awareness	None	None

Table 1: Summary of Self-Efficacy in Information Security related literature.

From table 1, it can be observed that while most studies report that SEIS positively impacts compliance behavior, it is not always true. Tsai et al. (2016) found that coping self-efficacy negatively influenced safety intentions. This mixed result is against the theoretical concept offered by protection

motivation theory. The possible reason for this mixed result offered by Tsai et al. (2016) states that users with high self-efficacy are so well-versed with performing security tasks on a daily basis that they tend to ignore safety intentions. However the mixed result needs further investigation.

Hypotheses Development

The Role of Overconfidence

There could be multiple reasons why the relationship between SEIS and compliance is mixed. To begin with, we explore the multi level nature of self-efficacy in information security. Self-efficacy is the confidence and belief in performing a certain task. Low self-efficacy indicates low confidence and high self-efficacy indicates high confidence. However there is a breakeven point at which high confidence can turn into overconfidence. Overconfidence in general is the total certainty or greater certainty than circumstances warrant. On a logical argument basis, overconfidence works against the expected behavior. Psychological studies have experimented this construct in greater depth to negatively impact behavior (Camerer & Lovallo 1999; Moore & Healy 2008). Overconfidence creates a bias that leads to inaccurate decision making and judgment (Zacharakis & Shepherd 2001).

The point at which the individual breaks even from being sufficiently confident to overconfident will be used to test and answer why the results are mixed. Figure 1 depicts the multi level representation of self-efficacy (confidence) and its effect on compliance behavior at various levels of confidence. Hence we propose the following:

H1: *Self-efficacy in information security levels ranging from low confidence to high confidence will positively affect cybersecurity compliance behavior.*

H2: *Self-efficacy in information security levels ranging from high confidence to overconfidence will negatively affect cybersecurity compliance behavior.*

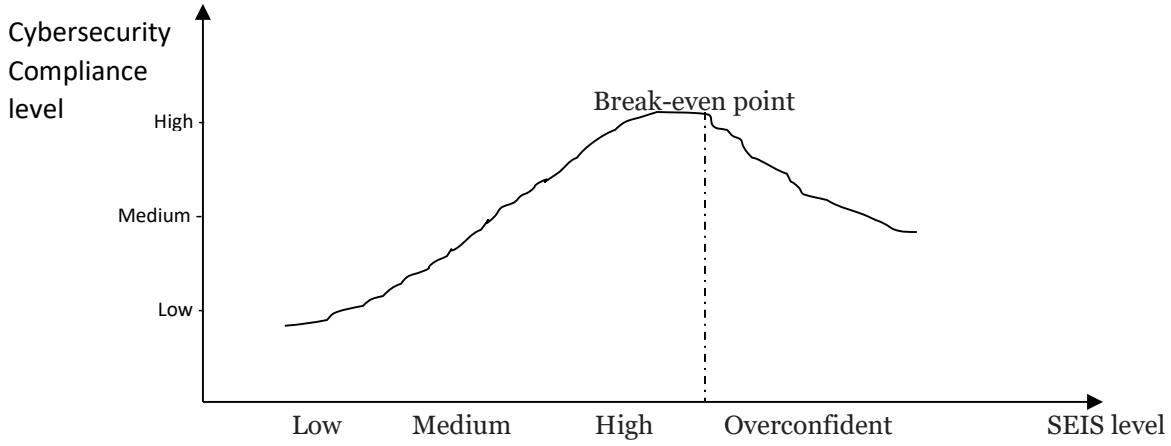

Figure 1. Multi level representation of self-efficacy (confidence)

Context specific conceptualizations of self-efficacy construct.

Bandura (2006) pointed out that the self-efficacy scale is not a comprehensive measuring tool and that it must be tailored to specific fields in order to achieve accurate measurement. Studies have stressed the need to develop subject specific self-efficacy scales in the wider concept of self-efficacy. Some examples are, software-specific self-efficacy scale (Agarwal et al. 2000), web-specific self-efficacy scale (Hsu and Chiu 2004), system-specific computer self-efficacy scale (Hasan 2006), and mobile-specific self-efficacy scale (Wang, Chang, Chou, and Chen 2013). In some studies, self-efficacy has been classified into different forms and examined in the same study. For example, Sun et al. (2016) classified self-efficacy into

two constructs: namely internet self-efficacy and anti-phishing self-efficacy. The results of their study indicated that anti-phishing self-efficacy significantly mediated the relationship between Internet self-efficacy and anti-phishing behavior. Similarly, Wong et al. 2016 use social self-efficacy and general self-efficacy to affect perceived self-efficacy. These examples support the fact that self-efficacy in information security study is something more and different than self-efficacy studies in general. As mentioned earlier, a recent study by Tsai (2016) shows that self-efficacy in information security research results deviate from research results using general self-efficacy (Tsai 2016).

So the context of information security can be considered as a context that may result in deviations of existing relationships established in IS literature. This opens up some important research questions on why SEIS results deviate from self-efficacy results in non-security context. With respect to the research models, an important question is that how SEIS should be modeled in each context. If there are multiple constructs affecting the pathways between SEIS and compliance, then those multiple constructs should be part of the research model. These additional constructs can either be mediators or moderators. Accordingly we propose the following:

> H3: *Self-efficacy in information security when conceptualized in non-security context will positively affect cybersecurity compliance behavior.*
>
> H4: *Self-efficacy in information security when conceptualized in security context will negatively affect cybersecurity compliance behavior.*

Measurement process involved.

Measurement of psychological construct is in general difficult since most studies rely on self-reported surveys. The measurement error tends to be high especially in cases where survey methodology is followed (Bound et al. 2001; Bertrand & Mullainathan 2001). Hence we propose that:

> H5: *Self-efficacy in information security when measured with non-survey methodology will consistently positively affect cybersecurity compliance behavior.*
>
> H6: *Self-efficacy in information security when measured with survey methodology will occasionally negatively affect cybersecurity compliance behavior.*

Home computer user contrasted with organizational user.

The study by Tsai et al. (2016) uses HIT posted on Amazon MTurks to collect data from home computer users. However the actual data should be coming from cyber institutions and cyber employees. Since MTurks deals with generic population who mostly represents USA population, there could be deviation in results from home users and organizational users.

> H7: *Self-efficacy in information security when measured using organizational sample will consistently positively affect cybersecurity compliance behavior.*
>
> H8: *Self-efficacy in information security when measured using home computer sample will occasionally negatively affect cybersecurity compliance behavior.*

Conclusion

The current article reviewed the IS security literature and identified mixed results on the effect of self-efficacy in information security on compliance. We discussed how these mixed results counter the theoretical modeling and the proven empirical results of numerous studies. There is a paucity of reasoning to explain these mixed results. In this paper, we try to answer that question by providing explanations for mixed results. We framed 8 hypothesis to guide future validation using meta-analysis.

REFERENCES

Bandura, A. (1986). *Social foundations of thought and action* (pp. 5-107). Prentice Hall.: Englewood Cliffs, NJ.

Bertrand, M., & Mullainathan, S. (2001). Do people mean what they say? Implications for subjective survey data.

Bound, J., Brown, C., & Mathiowetz, N. (2001). Measurement error in survey data. *Handbook of econometrics*, *5*, 3705-3843.

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), 523-548.

Camerer, C., & Lovallo, D. (1999). Overconfidence and excess entry: An experimental approach. *The American Economic Review*, *89*(1), 306-318.

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, *65*, 334-345.

Hanus, B., & Wu, Y. A. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2-16.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.*Decision Support Systems*, *47*(2), 154-165.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. Management Information Systems, 34(3), 549-566.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231-251.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. JOURNAL OF THE ASSOCIATION FOR INFORMATION SYSTEMS, 11(7), 394-413.

Moore, D. A., & Healy, P. J. (2008). The trouble with overconfidence. *Psychological review*, *115*(2), 502.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*,*46*(4), 815-825.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816-826.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64-71.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security, 22(1), 42-75.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296-302.

Sun, J. C. Y., Yu, S. J., Lin, S. S., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249-257.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150.

Zacharakis, A. L., & Shepherd, D. A. (2001). The nature of information and overconfidence on venture capitalists' decision making. *Journal of Business Venturing*, *16*(4), 311-332.