Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective

Hwee-Joo Kam
Ferris State University, kamh@ferris.edu

Pairin Katerattanakul
Western Michigan University, p.katerattanakul@wmich.edu

Greg Gogolin
Ferris State University, gogoling@ferris.edu

Soongoo Hong
Dong-A University, shong@daunet.donga.ac.kr

Follow this and additional works at: http://aisel.aisnet.org/pacis2013

Recommended Citation
http://aisel.aisnet.org/pacis2013/106

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2013 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
INFORMATION SECURITY POLICY COMPLIANCE IN HIGHER EDUCATION: A NEO-INSTITUTIONAL PERSPECTIVE

Hwee-Joo Kam, Information Security & Intelligence, Ferris State University, Big Rapids, MI, USA, kamh@ferris.edu

Pairin Katerattanakul, Computer Information Systems, Western Michigan University, Kalamazoo, MI, USA, p.katerattanakul@wmich.edu

Greg Gogolin, Information Security & Intelligence, Ferris State University, Big Rapids, MI, USA, gogoling@ferris.edu

Soongoo Hong, Management Information Systems, Dong-A University, Pusan, Korea, shong@daunet.donga.ac.kr

Abstract

External pressures could be a powerful force that drives the institution of higher education to attain information security policy compliance. Drawing on the Neo-Institutional Theory (NIT), this study examined how the three external expectations: regulative, normative, and cognitive expectations, impel the higher education of the United States to reach information security policy compliance. The research findings suggest that regulatory and social normative pressures, but not cognitive pressure, have significant effects on information security policy compliance in higher education. Based on these results, this study unfolds both the practical and research implications.

Keywords: Neo-Institutional Theory, Information Security Policy Compliance, Higher Education
1. **INTRODUCTION**

Incidents of data leakage in the higher education of the United States could harm students since the exposure of sensitive student data (e.g., social security numbers) could turn students into identity theft victims and easily jeopardize their identities. Regrettably, there have been several cases of data leakage at the higher education institutions in the United States. In the University of Texas, Austin, nearly 200,000 electronic records consisting of student’s social security numbers had been illegally accessed (Marks 2007). On March 11, 2005, a stolen laptop from the University of California, Berkeley exposed the names and social security numbers of 98,000 students (Marks 2007).

Given the criticality of student data, it has been unfortunate that there are almost no studies discussing how the external pressures drive the institution of higher education in the United States to meet information security policy compliance. These external pressures may serve as a powerful force to propel the higher education in the United States to comply. This notion is consistent with the Neo-Institutional Theory (NIT) in that organizational survival depends on securing legitimacy from the stakeholders through conformity with the stakeholder’s expectations (DiMaggio and Powell 1983). Thus, to fill in the gaps, this study draws on the Neo-Institutional Theory (NIT) to investigate how the external pressures drive information security policy compliance in the higher education of the United States.

In general, this study intends to examine how the external pressures urge universities and colleges in the United States to comply with information security laws. The research findings would serve to (1) unveil the driving force of information security policy compliance in the higher education of the United States and (2) provide suggestions to improve the implementation of information security practices across campuses.

The research framework of this study was based on the Neo-Institutional Theory (NIT). NIT postulated that organizations would conform to the external demands to secure legitimacy (i.e., what is construed as appropriate according to the social belief system) for organizational survival (DiMaggio and Powell 1983; Meyer and Rowan 1977). In the same token, we argued that higher education will obtain legitimacy through conformity to the external pressures in an attempt of achieving organizational survival. Thus, this study examined the impact of external pressures on information security policy compliance in the higher education of the United States.

The rest of this study is organized as follows. The next section presents a review of relevant literature. Then, this study proposes the hypothesized model together with its hypotheses followed by research methodology, analysis results and discussion. Finally, this study presents its conclusion with research implication and research limitation.

2. **LITERATURE REVIEW**

2.1 **Information Security Laws for Higher Education**

In the United States, the federal government mandates higher education institutions to comply with the Family Educational Rights and Privacy Act (FERPA) of 1974 to protect student information. Under FERPA, universities and colleges are allowed to disclose only directory information without student consent. Although individual institutions can designate the information that they include in directory information, the directory information generally consists of name, address, phone number, email address, dates of attendance, degree(s) awarded, enrollment status, and major field of study. On the other hand, universities and colleges are prohibited to disclose, without student consent, non-directory information including social security number, student identification number, race, ethnicity, nationality, gender, transcript, and grade reports.
Additionally, since universities and colleges are handling student’s financial aid, universities and colleges are also required to comply with the Gramm Leach Bliley Act (GLBA) for securing student’s financial records. Furthermore, universities and colleges with teaching hospitals must conform to the Health Insurance Portability and Accountability Act (HIPAA) for protecting medical records.

2.2 Information Security Policy Compliance

The aforementioned information security laws are a coercive force that compels higher education to abide by regulations. In the context of information security policy compliance, the traditional notion of compliance dwells on the conformity to regulations. However, contemporary compliance hinges on the requirement for organizations to meet their legal obligations according to the expected norms and values (Interligi 2010). This implies a moral dimension in contemporary compliance. Organizations conform to regulations for both obeying the regulations and fulfilling their social/moral obligations in relation to stakeholder’s expectations.

With organization-stakeholder interaction, organizations open doors to stakeholder’s influences and preferred methods for internal control (Interligi 2010). This allows stakeholders to impose pressures on organizations, urging organizations to meet stakeholder’s expectations of information security policy compliance.

2.3 Neo-Institutional Theory (NIT)

Neo-Institutional Theory (NIT) postulates that, to survive, organizations must secure legitimacy from the stakeholders by conforming to the external expectations (DiMaggio and Powell 1983). In other words, to survive, organizations must initiate internal organizational efforts to secure legitimacy by conforming to the external expectations.

Organizations are formed by phenomena in their institutional environment and gradually conform to the environment to survive. With respect to organizational survival, organizations experience institutionalization to incorporate practices that bring about legitimacy (DiMaggio and Powell 1983; Meyer and Rowan 1977). Legitimacy pertains to the assumptions of actions that are construed as appropriate based upon the social norms, values, and beliefs (Suchman 1995). In the context of NIT, institutionalization represents the process “by which social processes, obligations, or actualities come to take on a rule-like status in social thought and action” (Meyer and Rowan 1977, p. 343). That is, institutionalization embodies the social process that shapes social reality. Since institutionalization mirrors social process, organizations adopt positions, policies, procedures, or programs enforced by public opinions, laws, views of important constituents, or social prestige (Meyer and Rowan 1977).

2.4 External Expectations/Pressures

Based on the NIT, organizations will try to fulfill the external expectations to survive. These external expectations are elements of institution; for example, compliance to information security laws is one of the external expectations for the higher education. Essentially, institution consists of three external expectations that guide and restrain organizational action (Scott 1995). Each external expectation delineates its own legitimacy base to which organizations are expected to live up to (Scott 2008). The three external expectations are:

- **Regulative Expectation/Pressure** is the coercive force that compels organizations to abide by regulations such as FERPA. For information security, Regulative Expectation motivates top-down decisions to enforce security policies and procedures relative to information security safeguards (Hu, Hart, and Cooke 2007).
• **Normative Expectation/Pressure** is the social obligation or the right thing to do based on the subjective norms. For instance, mitigating identity theft by protecting student’s social security numbers represents social/moral obligation of universities and colleges.

• **Cognitive Expectation/Pressure** refers to stakeholders’ perception and ensuing expectation toward a phenomenon. The widely shared social knowledge (Markus and Zajonc 1985) affects how the overall phenomenon is categorized and interpreted (Kostova and Roth 2002), and subsequently, influences how stakeholders construct their perceptions and expectations toward the phenomenon. With regard to information security, cognitive expectation refers to how the commonly shared social knowledge shapes the stakeholder’s perception and expectation toward data leakage incidents. For example, this includes how the stakeholders perceive the data leakage caused by a stolen registrar’s laptop and what the stakeholders expect to be done to rectify this situation.

### 2.5 Organizational Efforts

Given external expectations, the organizational internal structure incorporates internal organizational efforts in handling different external expectations (Meyer and Rowan 1977). For information security, the internal organizational efforts of staying compliant entail (1) Enforcement of Policies and Procedures and (2) Information Security Awareness. Numerous previous studies suggested that these two factors affect information security policy compliance (Boss et al. 2009; Bulgurcu, Cavusoglu, and Benbasat 2010; Chan, Woon, and Kankanhalli 2005; Herath and Rao 2009).

- **Enforcement of Policies and Procedures** is the emphasis of the policies and procedures within an organization. The efforts of specifying policies and procedures augment the perceived mandatoriness of security policies among the employees (Boss et al. 2009). Subsequently, this promotes information security policy compliance.

- **Information Security Awareness** influences employee’s beliefs about the benefit of compliance and the cost of non-compliance (Bulgurcu et al. 2010). Organizations expect employees to understand the requirements and the objectives of information security (Bulgurcu et al. 2010).

### 3. Hypothesized Model

For information security in higher education, the three external expectations include regulative expectation (REG), normative expectation (NORM), and cognitive expectation (COG). Additionally, internal organizational efforts include Enforcement of Information Security Policies and Procedures (POL) and Information Security Awareness (AWA). According to the NIT, to survive, organizations must initiate internal organizational efforts to conform to the external expectations for securing legitimacy (DiMaggio and Powell 1983). That is, all the external expectations would have direct effects on the internal organizational efforts. Thus, this study proposed the hypothesized model as shown in Figure 1 and the following six hypotheses for this model.

- **H1**: Regulative expectation drives higher education to enforce information security policies and procedures
- **H2**: Normative expectation drives higher education to enforce information security policies and procedures
- **H3**: Cognitive expectation drives higher education to enforce information security policies and procedures
- **H4**: Regulative expectation drives higher education to raise information security awareness
- **H5**: Normative expectation drives higher education to raise information security awareness
- **H6**: Cognitive expectation drives higher education to raise information security awareness
4. RESEARCH METHODOLOGY AND ANALYSIS RESULTS

4.1 Questionnaire

To develop the questionnaire used in this study, we adopted some measurement items used in some of the previous studies about information security (i.e., Boss et al., 2009; Bulgurcu et al., 2010; Chan et al., 2005; Herath and Rao, 2009). Our original questionnaire had 20 items that measured the five constructs (i.e., REG, NORM, COG, POL, and AWA). Each of these 20 measurement items used the 7-point Likert scale with 1 for strongly disagree, 4 for neutral, and 7 for strongly agree.

A pilot study was conducted to enhance the original questionnaire. Overall, five college administrators (e.g., Dean, Associate Dean, Department Chair, Information Security Officer) of one higher education institution participated in this pilot study. These higher education administrators responded to and provided their feedbacks on each measurement item in the original questionnaire. Based on their responses, we computed the Cronbach’s alpha and the item-to-total score to assess the reliability for each construct. Then, hinged on this reliability assessment and the feedbacks collected from the pilot study, we adjusted the measurement items in the original questionnaire. The final version of the questionnaire used in this study comprised of 12 measurement items representing the five constructs.

4.2 Data Collection

Numerous emails were sent to the faculty members, management and administrators (e.g., Presidents, Provosts, Associate Provosts, Deans, Associate Deans, Department Chairs), and staff members (e.g., Information Security Officers, IT personnel) of the three universities and colleges in the Midwest region of the United States. The emails outlined the study objectives. Using emails, we invited the recipients to participate in this study by providing a hyperlink to the online questionnaire. We sent emails to
approximately 250 people. For the next two months, we distributed email reminders to follow up with the previous email messages we sent out. Telephone and face-to-face conversations were also used to remind the email recipients to participate in this study. After two months, we received 100 responses.

The participants in this study included 51 faculty members, 38 management and administrators, and 11 staff members. All of the three universities and colleges participating in this study were state-funded institutions. Two universities are research-focused universities and each has more than 20,000 students whereas the other university is a student-centered university with only 5000 students.

4.3 Measurement Assessment

This section presents the various tests conducted to establish construct reliability and validity of the measuring instrument. The hypothesized model consisted of five latent constructs -- REG, NORM, COG, POL, and AWA. All of these five constructs were reflective constructs. This study adopted Partial Least Square (PLS) method and used SmartPLS software for hypothesis testing.

SmartPLS software operates as a component-based path modeling application based on the PLS method (Vance, Elie-Dit-Cosaque, and Straub 2008). We went with PLS method because PLS path modeling is applicable even under a condition of a very small sample size (Chin 1998; Haenlein and Kaplan 2004; Henseler, Ringle, and Sinkovics 2009). Unlike the covariance-based Structural Equation Modeling that requires the sample size of more than 100 observations (Nasser and Wisenbaker 2003), PLS path modeling can be performed with a sample size as low as 50 observations (Chin and Newsted 1999).

Construct reliability was evaluated by examining the Composite Reliability (CR) score (Fornell and Larcker 1981) and the Cronbach’s alpha of each construct. Results in the following Table 1 show CR values ranging from 0.879 to 0.930 and Cronbach’s alpha ranging from 0.728 to 0.851. These values exceed 0.70, thus asserting construct reliability (Chin 1998).

<table>
<thead>
<tr>
<th>Composite Reliability</th>
<th>AVE</th>
<th>Cronbach’s Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG</td>
<td>0.879</td>
<td>0.784</td>
</tr>
<tr>
<td>NORM</td>
<td>0.909</td>
<td>0.833</td>
</tr>
<tr>
<td>COG</td>
<td>0.905</td>
<td>0.761</td>
</tr>
<tr>
<td>POL</td>
<td>0.931</td>
<td>0.871</td>
</tr>
<tr>
<td>AWA</td>
<td>0.907</td>
<td>0.766</td>
</tr>
</tbody>
</table>

Table 1. CR, AVE, and Cronbach’s Alpha

To test convergent validity, the average variance extracted (AVE), a measure of variance explained by a latent construct for the variance observed in its measurement items, should be at least 0.5 or higher (Fornell and Larcker 1981). Results in the aforementioned Table 1 provide evidence of convergent validity. Additionally, this study applied bootstrapping with 500 random re-samples and then examined the t-values of the outer model loadings. Convergent validity is demonstrated when all the measurement items load significantly on their respective latent construct. Typically, for each factor loading, the t-value should be larger than 1.96 with its p-value significant at least at 0.05 level (Gefen and Straub 2005). The following Table 2 shows that every measurement item significantly loaded on its respective latent construct with loading > 0.8, t-value > 2.5, and p-value < 0.001.
Construct | Item | Description | Factor Loading (t-value)
--- | --- | --- | ---
REG | REG1 | Legal action from regulator as a result of data breaches | 0.860*** (20.61)
| REG2 | Realize the legal damages suffered by a different university or college as a result of data breaches | 0.911*** (40.10)
NORM | NORM1 | Stakeholder’s expectation of data protection | 0.902*** (19.23)
| NORM2 | Protect information security in order to be competitive | 0.923*** (45.88)
COG | COG1 | Negative publicity due to data breaches | 0.820*** (10.16)
| COG2 | Monetary loss due to data breaches | 0.898*** (36.20)
| COG3 | Loss of stakeholder’s trust due to data breaches | 0.898*** (24.75)
POL | POL1 | Formal security policies in the college setting | 0.935*** (37.88)
| POL2 | Formal security policies to protect computer system | 0.931*** (42.07)
AWA | AWA1 | Employees realize the potential threats to security | 0.924*** (54.56)
| AWA2 | Educating employees about the cost of security problem | 0.827*** (18.34)
| AWA3 | Inform employees of the new threats to security | 0.872*** (24.76)

***p-value < 0.001

Table 2. Factor Loading and t-value

To evaluate discriminant validity, two tests were conducted. First, in the AVE analysis, the square root of the AVE of each construct must be larger than the correlations of this construct to all the other constructs (Chin 1998). The results depicted in Table 3 demonstrate strong discriminant validity.

<table>
<thead>
<tr>
<th>Construct</th>
<th>REG</th>
<th>NORM</th>
<th>COG</th>
<th>POL</th>
<th>AWA</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG</td>
<td>0.886</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NORM</td>
<td>0.299</td>
<td>0.913</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COG</td>
<td>0.471</td>
<td>0.520</td>
<td>0.873</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POL</td>
<td>0.466</td>
<td>0.386</td>
<td>0.307</td>
<td>0.993</td>
<td></td>
</tr>
<tr>
<td>AWA</td>
<td>0.490</td>
<td>0.370</td>
<td>0.332</td>
<td>0.545</td>
<td>0.875</td>
</tr>
</tbody>
</table>

Table 3. Construct Correlations and Square Root of AVE (in shaded cells)

The second test of discriminant validity is to examine the cross-loadings of measurement items on the latent constructs. In this test, discriminant validity is proven when each measurement item loads higher on its intended construct than on any other constructs. The difference in loadings should be at least 0.10 (Gefen and Straub 2005). Results in the following Table 4 indicate that all the measurement items show excellent discriminant validity.

<table>
<thead>
<tr>
<th>Construct</th>
<th>REG</th>
<th>NORM</th>
<th>COG</th>
<th>POL</th>
<th>AWA</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG1</td>
<td>0.8602</td>
<td>0.3086</td>
<td>0.4509</td>
<td>0.3213</td>
<td>0.4280</td>
</tr>
<tr>
<td>REG2</td>
<td>0.9105</td>
<td>0.2310</td>
<td>0.3923</td>
<td>0.4884</td>
<td>0.4404</td>
</tr>
<tr>
<td>NORM1</td>
<td>0.1854</td>
<td>0.9016</td>
<td>0.4454</td>
<td>0.3693</td>
<td>0.2754</td>
</tr>
<tr>
<td>NORM2</td>
<td>0.3512</td>
<td>0.9233</td>
<td>0.5004</td>
<td>0.3364</td>
<td>0.3935</td>
</tr>
<tr>
<td>COG1</td>
<td>0.4024</td>
<td>0.4402</td>
<td>0.8201</td>
<td>0.1846</td>
<td>0.2089</td>
</tr>
<tr>
<td>COG2</td>
<td>0.4213</td>
<td>0.4037</td>
<td>0.8976</td>
<td>0.2825</td>
<td>0.3572</td>
</tr>
<tr>
<td>COG3</td>
<td>0.4145</td>
<td>0.5258</td>
<td>0.8978</td>
<td>0.3135</td>
<td>0.2763</td>
</tr>
<tr>
<td>POL1</td>
<td>0.4088</td>
<td>0.4048</td>
<td>0.2899</td>
<td>0.9352</td>
<td>0.4931</td>
</tr>
<tr>
<td>POL2</td>
<td>0.4610</td>
<td>0.3136</td>
<td>0.2833</td>
<td>0.9310</td>
<td>0.5254</td>
</tr>
<tr>
<td>AWA1</td>
<td>0.4660</td>
<td>0.3829</td>
<td>0.3134</td>
<td>0.5230</td>
<td>0.9235</td>
</tr>
<tr>
<td>AWA2</td>
<td>0.4071</td>
<td>0.2401</td>
<td>0.2771</td>
<td>0.4502</td>
<td>0.8273</td>
</tr>
<tr>
<td>AWA3</td>
<td>0.4094</td>
<td>0.3356</td>
<td>0.2799</td>
<td>0.4548</td>
<td>0.8716</td>
</tr>
</tbody>
</table>

Table 4. Cross-loadings of Measurement Items on Latent constructs
4.4 Hypothesis Testing

After assessing measurement properties of the instrument, we tested all the six hypotheses of the hypothesized model based on the PLS structural model (see Figure 1). We estimated the path coefficients ($\beta$) of the structure model using the bootstrapping technique with 500 random re-samples (Mathieson, Peacock, and Chin 2001; White, Varadarajan, and Dacin 2003). To evaluate the significance of the path coefficients, we examined the significant level of each t-value. Results in Table 5 show that H3 and H6 were not supported, indicating that cognitive expectation had no direct effect on the higher education’s efforts of staying compliant.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>$\beta$</th>
<th>t-value</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: REG $\rightarrow$ POL</td>
<td>0.393</td>
<td>4.413**</td>
<td>Yes</td>
</tr>
<tr>
<td>H2: NORM $\rightarrow$ POL</td>
<td>0.280</td>
<td>2.435*</td>
<td>Yes</td>
</tr>
<tr>
<td>H3: COG $\rightarrow$ POL</td>
<td>-0.024</td>
<td>0.193</td>
<td>No</td>
</tr>
<tr>
<td>H4: REG $\rightarrow$ AWA</td>
<td>0.412</td>
<td>5.038**</td>
<td>Yes</td>
</tr>
<tr>
<td>H5: NORM $\rightarrow$ AWA</td>
<td>0.240</td>
<td>2.647**</td>
<td>Yes</td>
</tr>
<tr>
<td>H6: COG $\rightarrow$ AWA</td>
<td>0.014</td>
<td>0.146</td>
<td>No</td>
</tr>
</tbody>
</table>

**p-value < 0.01 *p-value < 0.05

Table 5. Hypotheses Testing

5. DISCUSSION

The results of hypothesis testing suggest that both the regulative and normative expectations have significant effects on the internal organizational efforts of staying compliant. However, cognitive expectation does not show any significant impacts on organizational efforts of attaining compliance.

Because stakeholders perceive higher education as a body for education and knowledge creation, rather than for information security safeguard (Rezgui and Marks 2008), incidents of data leakage in higher education may not be judged harshly. For instance, despite the leakage of 200,000 students’ electronic records in the University of Texas, Austin (Marks 2007), the respective university has not suffered from a drop in ranking. This may help explaining the aforementioned results for higher education in that cognitive expectation does not significantly affect organizational efforts of staying compliant.

Additionally, we contend that cognitive expectation could channel the normative pressure that directly drives universities and colleges to stay compliant. That is, when stakeholders begin to understand the criticality of information security, stakeholders will reconfigure their perceptions toward information security in higher education, leading to the new resultant cognitive expectation. Then, stakeholders will ascribe information security safeguard to corporate social responsibility (CSR). Overall, corporate social responsibility (CSR) refers to the notion that organizations behave in a socially responsible way to benefit the community (Campbell 2007). Thus, CSR represents normative expectation.

In this respect, universities and colleges will try to fulfill the social obligation by taking care of the stakeholder’s interest in information security protection. Attempting to safeguard information, universities and colleges will eventually be rewarded with social acceptance and respect (Deephouse and Carter 2005), thereby securing the normative-based legitimacy from the stakeholders. In sum, cognitive expectation may have a direct effect on normative expectation rather than on the internal organizational efforts for information security policy compliance.

On the other hand, academic freedom is the essence of academic culture (Frincke 2003). Academic freedom supports research innovation and knowledge creation (Reis 1997). In this regard, universities and colleges determine the legitimacy of rules and regulations based on “their consistency with the goals of academic ideology” (Dill 1982, p. 308). That is, universities and colleges would initiate their internal
organizational efforts to comply with regulations only when the regulations meet the goals of academic ideologies. For instance, universities and colleges would not implement even common information security practices that might delay the process of knowledge creation and dissemination, resulting in the violation of academic freedom.

Consequently, we argue that, for higher education, information security regulations depend on the cognitive elements rather than the coercive force to prevail. That is, to effectively promote internal organizational efforts of information security policy compliance in higher education, information security regulations must be consistent with the cognitive expectation shaped by stakeholder’s perception. Therefore, through regulative expectation, cognitive expectation may also have an indirect effect on the internal organizational efforts of information security policy compliance.

6. CONCLUSION

NIT posited that, to survive, organizations must secure legitimacy from stakeholders by conforming to the external expectations (DiMaggio and Powell 1983). The three external expectations encompass regulative, cognitive, and normative expectations. This study examined how these three external expectations influence information security policy compliance in the higher education of the United States.

The results of hypothesis testing show that both the regulative and normative expectations significantly influence the internal organizational efforts of staying compliant. On the other hand, cognitive expectation does not have any significant impacts.

These hypothesis testing results also suggest an important practical implication of this study. That is, the institution of higher education should encourage stakeholders to understand the criticality of information security so that the stakeholders would reconfigure their perceptions toward information security safeguard, leading to new cognitive expectation in support of information security policy compliance.

Additionally, our discussion contends that, through both the normative and regulative expectations, cognitive expectation may have indirect effects on the internal organizational efforts of attaining information security policy compliance. That is, the institution of higher education encompasses cognitive expectation that harnesses the coercive force of regulatory pressure and leverages the social normative pressure of serving the community through information security safeguard.

Therefore, the major research implication of this study is to further investigate the effects of cognitive expectation on the higher education’s organizational efforts of achieving information security policy compliance. The alternative research model may depict the indirect effects of cognitive expectation on the higher education’s organizational efforts of staying compliant through the normative and regulative expectations. In addition, the alternative research model may include a construct for academic culture because academic culture is altered by stakeholder’s cognitive expectation (Feldman and Desrochers 2004) and academic culture is the major barrier to information security implementation in higher education (Kvavik 2004).

Finally, this study is not without limitations. The study had limited sample size and its data were collected from only a few universities and colleges in the Midwest region of the United States. Thus, the research findings from this study may be closely linked to these particular higher education institutions. Researchers may need to be cautious when referencing these research findings.
References


Marks, A. (2007). Exploring universities’ information systems security awareness in a changing higher education environment: A comparative case study research (Doctoral dissertation), University of Salford, Salford, United Kingdom.


