Assimilation of Security-Related Policies in U.S. Firms: An Empirical Study of Web Assimilation and Related Knowledge as Antecedents

Kevin P. Gallagher  
Northern Kentucky University  
Gallagherk2@nku.edu

Xiaoni Zhang  
Northern Kentucky University  
zhangx@nku.edu

Vickie Coleman Gallagher  
Cleveland State University  
v.c.gallagher@csuohio.edu

Abstract

Security-related policies can help organizations safeguard against breaches and other threats and plan for how to respond to events. However, adoption of security, privacy and acceptable use policies, audit processes and disaster recovery, and business continuance planning may lag behind an organization’s efforts to leverage the benefits of web-based technologies.

This paper presents findings from a study of security-related policy assimilation. Assimilation is designed to measure the level of adoption. We examine the antecedents of assimilation—e.g., an organization’s web strategy, business activities conducted on the web, and the existence of security related knowledge as predictors of assimilation.

1. Introduction

Information technology (IT) continues to offer tremendous benefits to organizations, as they leverage the internet to advance their business strategy and automate their business processes. Yet information and system security issues related to IT pose tremendous threats. A number of studies have been conducted in recent years that try to understand the types of threats that companies experience and their efforts to address these problems [1]. Yet, as the measures that organizations undertake continue to evolve, so too do the nature of threats they must address. The evolving and dynamic set of threats, and subsequent responses, often highlights how today’s solutions are ineffective in combating tomorrow’s threats.

The approach undertaken in this study is to understand the degree to which organizations have assimilated policies related to securing their information, systems and business processes. Such policies should then allow organizations to more effectively plan and institute security-related measures. Effective policies and procedures give organizations the means to not only adopt and use effective IT security measures, but to also effectively diffuse newly adopted or adapted measures, in order to respond to emerging threats.

Building on prior research in the area of assimilation [2, 3] we surveyed organizations with regard to their assimilation of IT security policies. The respondents were asked about their assimilation of an acceptable use policy, an IT security policy, a privacy policy, a business continuance plan, a disaster recovery plan, and an IT risk assessment. The responses offered in the survey measure of assimilation were very similar to those utilized in prior assimilation studies, yet, as with other assimilation studies, we adapted our instrument in order to insure our respondents understood the question within the specific context [2, 3].

This paper reports results based on responses to an online survey from over 500 organizations across the United States. The sample includes small and medium sized firms, as well as many large organizations, and also includes a wide range of industry sectors, such as government, non-profit and education, to name a few.

Our analysis tests hypotheses with regard to the antecedent conditions predicted to lead to greater assimilation of security policies: The conditions include the organization’s perceived level of related knowledge, the degree to which they have deployed the web-related technologies to advance their business strategies, and the degree to which they have deployed web-related technologies to conduct their business activities. The study contributes to our understanding of IT security policy adoption, web technology experiences, and the importance of related knowledge.

2. Background

The importance of security policies, and the role that these policies play in protecting information resources, has received increased attention from academic researchers [4]. Policies represent important planning and control devices that help organizations to define acceptable behavior, establish access protocols, establish system standards, and document appropriate actions, all with the intended outcome of protecting the
information, business processes, and computer and communication systems of an organization [5].

We study the deployment and use of these policies rather than specific technologies. We see policies as a more enduring organizational means toward preventing security breaches and controlling the negative impact of security breaches. Information technology adoption, the nature of security threats, and the development of technology-related safeguards, all continue to rapidly evolve. This evolution is especially rapid for technologies related to internet communications and commerce. While surveys that track specific technologies and applications offer insights, those insights have limited time horizons, especially given the time required to collect and report the findings of a large study such as this.

Effective IT security measures must go beyond the adoption and use of security-related technologies and applications if organizations are to safeguard their information and systems against security breaches. For example, vulnerabilities related to social engineering and other internal threats in organizations highlight the need for more comprehensive approaches that include managing human behavior and providing greater education and training [6]. Effective IT security requires careful design, documentation, training, execution and monitoring of policies and the related response procedures [7].

More so, development of policies and procedures can ensure that the appropriate technologies and applications are adopted on a timely basis and used in informed and effective ways. Effective policies and procedures can also insure that personnel are aware, trained and guided to evaluate security related situations, and act with the utmost insight, caution and speed [8]. Thus, the planning and management of security policies (e.g., policies that outline the appropriate evaluation, acquisition, deployment and use of technologies, processes and procedures) will go much further to protect an organization against security threats than simply relying on investments in the latest technologies. Similarly, policies that include the necessary education, training, and maintenance will help protect organizations.

To understand the adoption of security policies, and the antecedent conditions that lead to greater adoption, we conducted a nation-wide survey in the U.S. among organizations large and small, and across a large cross section of industries. We attempt to answer the following questions:

Do organizations that have assimilated the internet into their business practices and processes, and accumulated related knowledge, report greater assimilation of security-related policies?

Our paper is outlined as follows. The following section reviews the literature on information security breaches and the importance of security-related policies in helping organizations safeguard and respond to threats. We also discuss information security policies and the challenges organizations face in adopting and deploying such policies. We also explore the concept of assimilation in the management and information systems literatures and its importance in understanding the varying degree to which organizations adopt complex organizational innovations.

We then outline the research model and develop hypothesis based on the relationships between constructs. The methods, analysis and results sections subsequently outline details of our data collection, statistical analyses and findings. The discussion offers insights from our results and limitations of our study. We conclude the paper by discussing our contributions to the literature and opportunities for future research.

3. Literature review

3.1. Role of policy in information security

Security policy has gained increasing attention from researchers in recent years (see special issues of EJIS 2009). This marks a shift in focus for researchers, given that much of their attention to date has been focused on the development of technical solutions rather than more strategic approaches, such as the creation of policies and procedures. This technical focus is argued to have created a “strategy gap” [9]. Technologies are quickly evolving and coevolving with increased threats, making management of technology a growing challenge.

Policies are needed to lay the foundation for more managerial approaches to evaluating risks. This includes items such as regular assessments, safeguarding and securing information assets with preemptive measures, and formulating contingency plans to respond to disasters and thereby insure continuance of essential business processes [9]. Therefore, security goes beyond preventative measures; thus, we refer to security-related policies collectively.

Formulation of a security policy requires first the assessment of risk by evaluating threats and vulnerabilities to assets [10]. Once established, an organization can then consider how investments should be made [11]. Clearly the next steps require creation of documented policies for security, privacy and acceptable use for an organization’s systems. In
addition, plans to respond to and recover from disasters, and to insure business continuity, must be included in a comprehensive security strategy [12].

The increased dependence of organizations on the internet in order to communicate with constituents and conduct commerce should drive organizations toward adoption of security-related policies [13]. However, implementation of web-based applications in organizations may out-pace the development of security policies. Many surveys offer evidence that adoption levels for security policies are shockingly low [14, 15, 4].

There are many challenges to the comprehensive creation and implementation of security policies. The first is an organization’s awareness of what the policy should contain and how it should be developed. Thus, both the product and process of a policy strategy are important. Even with recognition of its importance, an organization’s management and its structure can enable or constrain the progress of policy development and implementation [16].

Ultimately, a policy may be implemented, but as with any innovation, it may not be fully utilized. Passive resistance by employees can undermine the efforts to institute policies. Thus, training and governance structures often accompany the creation of protocols and procedures [16]. Yet laziness, sloppiness and lack of motivation may still create problems at the user-end of the systems; thus, an ‘endpoint problem’ may persist [17]. Even if compliance exists, interpretation of policies can become an obstacle to their effective implementation [18].

Feedback is necessary to improve an organization’s policies and procedures [19]. Audits thereby become a necessary means for organizations to evaluate adherence to policies and to surface the need to update policies based on emerging problems and evolving needs.

Furthermore, ensuring security requires compliance with policies. As a result current research has explored approaches to compliance, with focus on intent of the individual; however, individuals tend to underestimate security threats [10]. Thus, ongoing effort and vigilance are required throughout the process of creating, adopting and instituting these policies organizations.

3.2. Assimilation of complex organizational innovations

In this research we conceptualize the adoption of security-related policies as a complex organizational undertaking. The complexity of this undertaking is evident in that it requires an extensive understanding of information and technology that exists within a specific organizational context and the necessary means by which an innovation can be introduced and leveraged. The difficulties of adopting security-related policies are informed by understanding that acquisition on an innovation alone may not insure its full deployment or use [2]. Therefore, a more important measure of an organization’s deployment of such innovations is the degree to which it is assimilated [2].

Assimilation is a way to measure the development and evolution of an organization’s adoption decision, from its lacking in awareness of the innovation to its initial interest, then acquisition through to full deployment [20, 21]. Examining an organization’s assimilation of an innovation allows for evaluating adoption not just as a decision, but as an ongoing challenge faced by the management. In fact, management may require convincing in order to insure its use. In the case of a security-related policy, it might take some education, experience and perhaps mandatory rules in order to insure that the policy’s guidelines are understood and procedures are followed.

The concept of assimilation was first introduced in the management literature by Fichman and Kemerer [2] as a way to explore what they described as the illusory experience of organizations with innovation adoption. The process they examined was the adoption of object oriented programming methods, which presents a complex organizational challenge, as it requires not just new technology, but new knowledge, changes in work processes, and changes in organizational procedures. The authors found that organizations that had a broader range and depth of experience related to information technologies experienced greater levels of assimilating. They also found that greater related knowledge in the organization lead to higher levels of assimilation, as workers had access to the experience and expertise they needed to help them through the learning process.

The assimilation scale employed in Fichman and Kemerer’s [2] study was devised specifically to measure the deployment of an innovation in question. Recognizing that innovations differ, the authors noted that future studies of assimilation should adapt the measure to represent the characteristics of the particular innovation under study. Thus, Reardon and Davidson [3], building on the work or Fichman and Kemerer [2], recently adapted the scale to study a very different problem. The authors devised an assimilation scale to measure the adoption and use of electronic medical records in small physician practices. The challenges of this innovation and the existing context of the organizations were very different from those examined in the prior study; thus, an alteration of the measures of the level of adoption was required. Similarly, the measures examining the antecedent
conditions that might predict higher levels of assimilating the innovation in question, such as the related knowledge in the organization, may also require alteration based on the context.

To date assimilation has been employed as a dependent variable, extending research and providing an informative measure of an organization’s adoption of innovations.

4. Research model and hypothesis development

In this study we conceptualize security-related policies as a complex organizational undertaking, that to be effective requires more than its simple adoption; it requires its full deployment, or assimilation of policies. The security-related policies that can ultimately help organizations to reduce the impact of security breaches are those related to both ongoing procedures and those related to an organization’s response to adverse events. Thus, our interest was in measuring assimilation of multiple policies. These policies were devised to create a multi-item measure consisting of six separate conceptualizations of security-related policies and plans: security, privacy, acceptable use, risk assessment, business continuity, and disaster recovery. Our research model is illustrated in Figure 1 below.

Figure 1. Research model

As with the study by Reardon and Davidson [3] we undertook a conceptual translation of the assimilation measure put forth by Fichman and Kemerer [2] in order to study a different, yet still very complex innovation, and its adoption into a different, in fact more expansive organizational context. To do so we created a multi-item scale composed of the six policies and plans outlined above. We also recognized that the implementation of a policy might have limited effect on the organization. Without the procedures and policies being continually audited and routinely improved, the organization’s policies could become just another set of documentation. Thus, we also adapted the scale by extending it to include responses beyond full deployment of the policy, offering the responses of deployed and audited, and deployed, audited and routinely improved (as evidence of greater degrees of a policy’s assimilation).

The responses offered in the survey questions were very similar to those utilized in prior assimilation studies. Furthermore, as with other assimilation studies, we adapted our instrument to address the specific context [3]. In accordance with prior research, responses ranged on a scale of 1 to 9 as follow: 1) Unaware, 2) Aware, 3) Interested, 4) Evaluating, 5) Piloting, 6) Implementing, 7) Fully deployed, 8) Deployed and audited, 9) Deployed, audited and routinely improved.

The concept of assimilation recognizes the difficulties organizations have in not just adopting, but then using and gaining the benefits of an innovation. Fichman and Kemerer [2] stated that organizations were more likely to assimilate such complex organizational innovations when there was a greater scale of activities over which the learning could be spread. Conceptually, a greater scale of activities benefits from economies of scale [22]. Furthermore, they state that greater diversity of technical knowledge and activities would also lead to greater assimilation. Theoretically, a greater diversity of activities benefits from an organization having greater absorptive capacity [23].

To measure the diversity of activities that might lead to assimilation of security-related policies, we view an organization’s assimilation of web-related strategies and activities as a way to understand their needs and motivations to protect against the adverse effects of security breaches. To measure web assimilation we adopt an existing web assimilation scale that examines both strategies and activities [24] Strategies include attracting new customers, offering value-added customer services, creating new advertising and distribution channels and enhancing the company image. Activities include receiving payments, testing and delivering products and services, providing customer support, conducting market surveys and publishing company information.

Organizations that have assimilated a broader range of strategies and activities to a greater extent via the internet are ultimately presented with a higher level of risk for security breaches, as their presence makes a larger audience aware of their website and a more extensive set of activities offers more opportunities for a breach. Thus, greater assimilation of both web-related strategies and activities could lead to greater exposure to security breaches.
Similarly, as organizations gain greater experience and knowledge of these web-related strategies and activities they should become increasingly aware of the need for security related policies in order to protect their organization, its systems data, and reputation. They should also come to understand that not having these systems available to their customers, suppliers and partners, creates a disruption in their operation that can be costly. Thus, our first and second hypotheses predict that greater assimilation of both web-related strategies and activities will lead to greater assimilation of security-related policies.

Hypothesis 1: Greater assimilation of web-related strategies will lead to greater assimilation of security-related policies.

Hypothesis 2: Greater assimilation of web-related activities will lead to greater assimilation of security-related policies.

Fichman and Kemerer [2], and Reardon and Davidson [3] also found that organizations that had greater knowledge related to the innovation in question had achieved higher levels of assimilation. This relationship fits with the overall conceptualization of innovation as a complex organizational process. Ultimately, both studies were positioned strongly on the theoretical basis that organizational learning was essential for the assimilation of their respective innovations. A related knowledge scale was created and adapted, in the former and later studies, respectively.

The scale was intended to examine the extent of abstract knowledge, know-how, and skills possessed by the organization in areas related to the innovation [2]. Thus, if an organization is staffed adequately with related knowledge it can better train and support the organization in helping it move toward higher levels of assimilation. Thus, our third hypothesis predicts that greater levels of related knowledge in the organization will lead to greater assimilation of security-related policies.

Hypothesis 3: Greater levels of related knowledge in the organization will lead to greater assimilation of security-related policies.

5. Research methods and analysis

5.1. Sample and data collection

Our approach to investigating assimilation of security-related policies was to conduct both local and nation-wide online surveys. Initial surveys were pre-tested with local and regional key constituents of the university to pilot test the overall survey and to develop some of the constructs. Development of the policy assimilation construct was conducted as a part of the local study. The pilot was conducted first with a Chief Information Officer and a Chief Security Officer, both of whom worked for financial services firms. The executives completed the survey separately while on the phone with the first author, so that the executives could provide feedback if a survey item was not stated clearly. This phase of the pilot study served to help clarify language (both wording and intent of the survey items). In the second phase of the pilot study, executives completed the survey independently, but were asked to provide feedback at the end. The intent of this phase was in part to evaluate the time it took participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.

The larger national survey data were collected from individuals in over 500 organizations using existing survey panel members solicited through a market research vendor. The panel was screened to identify participants who fit a number of requirements, including a mix of demographics such as region, industry, etc. Next, their participation was requested through an email invitation. In order to insure that our participants were qualified to respond to the questions in the survey, we used several forms of screening and validation. First, the survey panel was mined for participants to complete the survey, which is information needed for recruiting participants in a panel. Our intent was also to test the measures for face validity. The sample size from this phase of the pilot study was twenty-nine. We performed an exploratory analysis of these responses and found the items loaded as expected with the exception of one item that did not load on the expected construct. Because that particular item was one that was validated in prior studies, we checked the wording and asked for feedback from several people, but ultimately determined there was no need to alter the item. Therefore, we kept the item as originally published.
employees, and 35% have 501 or more employees. Table 1 shows the sample distribution by industry.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>4.59%</td>
</tr>
<tr>
<td>Consulting</td>
<td>3.18%</td>
</tr>
<tr>
<td>Education</td>
<td>11.48%</td>
</tr>
<tr>
<td>Financial / Investment services</td>
<td>6.54%</td>
</tr>
<tr>
<td>Government</td>
<td>8.13%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>11.66%</td>
</tr>
<tr>
<td>Insurance</td>
<td>3.00%</td>
</tr>
<tr>
<td>IT Services</td>
<td>5.12%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>8.30%</td>
</tr>
<tr>
<td>Non-profit</td>
<td>5.65%</td>
</tr>
<tr>
<td>Retail</td>
<td>8.13%</td>
</tr>
<tr>
<td>Pharmaceutical / Chemical</td>
<td>5.48%</td>
</tr>
<tr>
<td>Professional services</td>
<td>6.18%</td>
</tr>
<tr>
<td>Property &amp; construction</td>
<td>3.00%</td>
</tr>
<tr>
<td>Software</td>
<td>2.30%</td>
</tr>
<tr>
<td>Technology</td>
<td>2.83%</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>2.65%</td>
</tr>
<tr>
<td>Transportation / distribution</td>
<td>1.77%</td>
</tr>
</tbody>
</table>

5.2. Measures

5.2.1. Web-related strategy. Web strategy measures the extent and depth to which an organization has assimilated web-based technologies in advancing its business strategy. Five items were used to measure web strategy (e.g., company website supports enhancing the company image). The five items were adapted from Chatterjee et al’s study [27]. One item was deleted after confirmatory factor analysis.

5.2.2. Web-related activities. The construct of web-related activities measures the extent and depth to which an organization has assimilated web-based technologies in conducting e-commerce activities. Seven items were used to measure web activities / e-commerce strategies (e.g., the company website is used to receive payments from customers). The seven items were adapted from Chatterjee et al. [27]. Three items were deleted after confirmatory factor analysis.

5.2.3. Related knowledge. The construct of related knowledge measures the extent of abstract knowledge, know-how, and skills possessed by an organization in areas related to the focal innovation. Four items were used to measure organizational knowledge (e.g., the company has the adequate personnel to support initiatives). The four items were adapted from Fichman & Kemerer [2].

5.2.4. Security policy assimilation. Policy assimilation measures the stage of security policy assimilation. Six items were used to measure policy assimilation (e.g., the company has a documented security policy). This measure was developed based on the studies of Fichman and Kemerer’s [2] and Reardon and Davidson’s [3].

5.3. Data analysis

AMOS 19 was used to test Figure 1. We first validated the measurement model and then proceeded to the testing of structural relationships.

5.3.1. Measurement Model. Content validity shows the extent of adequate coverage of the constructs being examined [25]. We used two methods to establish content validity: an extensive literature review and expert analysis of the items. Since policy assimilation is a new construct, we first validated this construct.

Unidimensionality illustrates that the measurement items measure a single latent construct [26, 27]. The Cronbach’s alpha for security policy is 0.94. Though prior work has used many indices to measure unidimensionality, Gefen [28] recommends confirmatory factor analysis (CFA) for the evaluation of unidimensionality. We used AMOS 19 to perform a CFA on security policy assimilation. Table 2 shows the results of the CFA. The indices for security policy assimilation are \( \chi^2/df = 3.0 \), GFI=0.99, AGFI=0.96, RMSEA=0.06, CFI=0.99. These fit indices support the unidimensionality of the security policy assimilation construct. The fit indices for other established constructs (web activity, web strategy and related knowledge) also provide evidence of unidimensionality, as noted in Table 2.

<table>
<thead>
<tr>
<th>Measure</th>
<th>Range of Standardized Loadings</th>
<th>GFI</th>
<th>AGFI</th>
<th>CFI</th>
<th>RMSEA</th>
<th>Chi squared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-Rel. Activ.</td>
<td>0.65-0.86</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
<td>0.03</td>
<td>1.43</td>
</tr>
<tr>
<td>Web-Rel. Strtg.</td>
<td>0.71-0.89</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
<td>0.06</td>
<td>3.16</td>
</tr>
<tr>
<td>Related Knowledge</td>
<td>0.71-0.90</td>
<td>0.99</td>
<td>0.97</td>
<td>0.99</td>
<td>0.05</td>
<td>2.55</td>
</tr>
<tr>
<td>Secur. Policy Assim.</td>
<td>0.67-0.92</td>
<td>0.99</td>
<td>0.96</td>
<td>0.99</td>
<td>0.06</td>
<td>3.00</td>
</tr>
</tbody>
</table>

Next we tested for convergent validity and discriminant validity. Table 3 illustrates descriptive statistics—inter-constructs correlations and AVEs. AVEs (0.77, 0.74, 0.68, and 0.71) of the four
constructs are greater than the inter-constructs correlation. Factor loadings, Cronbach’s Alpha, composite reliability are provided in Table 4. All of the loadings are above 0.5 and are statistically significant. Cronbach’s Alphas are in the range of 0.85 and 0.93 (available upon request). Composite reliabilities for web strategy, web activities, organization related knowledge, and policy assimilation are 0.91, 0.90, 0.93, and 0.94 respectively. Both Table 3 and Table 4 provide evidence of convergent and discriminant validity.

### Table 3. Correlations between Latent Constructs and means

<table>
<thead>
<tr>
<th></th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Related knowledge</td>
<td>0.77</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Security Policy assimilation</td>
<td>0.45</td>
<td>0.74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Web-Related activities</td>
<td>0.54</td>
<td>0.29</td>
<td>0.68</td>
<td></td>
</tr>
<tr>
<td>4. Web-Related strategy</td>
<td>0.49</td>
<td>0.32</td>
<td>0.65</td>
<td>0.71</td>
</tr>
</tbody>
</table>

### Table 4. Factor Loadings, Cronbach’s Alpha, and Composite Reliability

<table>
<thead>
<tr>
<th>Factors</th>
<th>Items</th>
<th>Loadings</th>
<th>Composite Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-Related Strategy</td>
<td>Enhance co. image</td>
<td>0.76</td>
<td>0.91</td>
</tr>
<tr>
<td></td>
<td>Attract cust.</td>
<td>0.83</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value-add cust. serv.</td>
<td>0.81</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New adv. channel</td>
<td>0.68</td>
<td></td>
</tr>
<tr>
<td>Web-Related Activities</td>
<td>Test prods.</td>
<td>0.67</td>
<td>0.90</td>
</tr>
<tr>
<td></td>
<td>Cust. suppt.</td>
<td>0.73</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Deliv. prods.</td>
<td>0.80</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recv. cust. pymts.</td>
<td>0.63</td>
<td></td>
</tr>
<tr>
<td>Related Knowledge</td>
<td>Adequate support</td>
<td>0.79</td>
<td>0.93</td>
</tr>
<tr>
<td></td>
<td>Training opportunities</td>
<td>0.87</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Know who can solve</td>
<td>0.83</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adequate personnel</td>
<td>0.86</td>
<td></td>
</tr>
<tr>
<td>Security Policy Assimilation</td>
<td>Annual IT risk asses.</td>
<td>0.67</td>
<td>0.94</td>
</tr>
<tr>
<td></td>
<td>Disaster recov. plan</td>
<td>0.73</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business contin. plan</td>
<td>0.91</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Docmdt. privacy pol.</td>
<td>0.92</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Docmdt. sec. policy</td>
<td>0.85</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acceptable use policy</td>
<td>0.76</td>
<td></td>
</tr>
</tbody>
</table>

5.3.2. Structural Model. We performed a CFA with AMOS. The results show the fit statistics of Chi square/df=3.31, GFI=0.92, AGFI=0.89, CFI=0.96, and RMSEA =0.064. We used multiple fit indices to evaluate model fit. Carmines and McIver [29] suggest that the x2/df ratio in the range of 2:1 or 3:1 be acceptable fit. Our result of chi square/df is 3.31 which is slightly over the recommended 3:1; however, the other fit indices (GFI, AFGI, CFI) are over 0.8 and RMSEA is less than 0.8. Therefore, we conclude that our model fits the data well. Figure 2 shows the results of SEM testing: the path coefficients, r square and significance level. The solid lines are significant paths whereas the dashed lines are insignificant. The path between web strategy and security policy assimilation is significant at the 10% level and the path between related knowledge and security policy assimilation is significant at 1% level. The R square is 20% when the three constructs (web-related strategy, web-related activities and related knowledge) are used to predict policy assimilation.

As shown in Figure 2, and in support of Hypothesis 1, the path coefficient is 0.15 \( (p < 0.05) \) from web-related strategy to policy assimilation suggesting that greater assimilation of web-related strategies will lead to greater assimilation of security-related policies. However, Hypothesis 2 was not supported (as indicated by the dotted line) such that web-related activities are not significantly related to assimilation of security-related policies. Finally, in support of Hypothesis 3, the path coefficient is .036 \( (p < 0.001) \) from related knowledge, suggesting that greater levels of related knowledge in the organization will lead to greater assimilation of security-related policies.

6. Discussion

Despite the fact that a number of studies have explored various types of security threats [1, 30], research shows that the nature of such threats are dynamic and evolving. As such, our research addresses an important aspect of information security policies: the assimilation of such policies. Policies are a vital tool in planning and control in order to protect valued resources against security threats. An important contribution of our research is that we study policies rather than specific technologies, given that technologies (as well as the threats that they are designed to protect against) are constantly changing. Alternatively, policies are systemic and designed to
address emerging threats over time, regardless of the technology or technique used in the breach.

Although a number of factors are likely to contribute to the adoption and assimilation of policies, we hypothesized that three in particular would serve as indicators of policy assimilation: the extent and depth to which an organization has assimilated web-based technologies in advancing its business strategy (e.g., web-related strategy), the extent and depth to which an organization has assimilated web-based technologies in conducting ecommerce activities (e.g., web-related activities), and the extent of abstract knowledge, know-how, and skills possessed by an organization in areas related to the focal innovation (e.g., related knowledge).

Interestingly, while web-related strategy and related knowledge were positively and directly related to policy-assimilation, web-related activities were not. As discussed, companies who utilize a wide array of web-strategies utilize a greater range of internet-related approaches to the competitive environment (such as enhancing their company image, advertising, and attracting customers). This strategic approach and presence on the internet is perhaps more likely to lead to an overall strategic focus and to greater attention to planning and implementing procedures, thus greater thought and planning may lead to adoption and implementation of security policies. Perhaps companies that adopt web-related strategies cast a wider net and approach the use of the internet more broadly. These companies may therefore (by choice or by necessity) think more systemically about the risks that they may encounter.

Alternatively, when implementing web-related activities (such as customer payments) the relationship is perceived as less risky, given that it is a targeted relationship with an existing customer. This may be perceived as transactional rather than strategic. We might also hypothesize that companies may be implementing activities at a faster pace than they are able to develop and implement the policies needed to secure them. Thus, use of technology (and the artifact) is once again outpacing the management of technology and the development of security strategies and policies.

Our most important finding is that organizational knowledge and support (in the form of support, training and personnel) for security, is a strong prerequisite and predictor of successful security policy assimilation. This concurs with earlier research that found that related knowledge was critical and predictive of adoption of other complex organizational innovations [2, 3]. We therefore concur that the organizational learning perspective as first proposed by Fichman and Kemerer [2], to inform the process of assimilation, continues to hold in this new context.

Our paper has a number of strengths, such as the adaptation of existing measures that allows security research to move forward beyond consideration of the artifact of technology. Antecedents of security policy assimilation have not been investigated in this manner and our research is grounded in the literature and in theory. We employed a number of techniques to validate our measures and tested our model with an adequate sample size.

However, our research is not without limitations. Our model is parsimonious, unable to explain other potential contributors to assimilation, such as industry regulations, resources and budgets available to the institutions, etc. Finally, assimilation alone is not a guarantee that breaches will be avoided. Therefore, future research should determine the actual or reported level of breaches or the subsequent impact of said breaches. In fact, it may be assumed that organizations would be hesitant to admit to actual breaches. Perhaps a more comprehensive and less sensitive outcome measure is necessary in order to advance theory and practice. Furthermore, a major premise of our research is that technology is ahead of policies. Future research should explore this perception and measure the prevalence of this among organizations.

In addition, future research should explore differences in assimilation based on industry or size of organization. For example, perhaps organizations in the financial services industry have more regulatory or institutional pressures that implore them to implement security policies and procedures. Furthermore, organizational size may allow for more resources to dedicate to IT security, particularly since larger organizations may also have the most to lose.

7. Conclusion

This study contributes to our understanding of the extent to which organizations have instituted IT security-related policies, the antecedent conditions that contribute to policy assimilation, and the degree to which policies are effective in reducing the impact that security breaches have on an organization. By security-related we mean security, privacy, acceptable use policies, as well as policies for disaster recovery, business continuity and risk assessment.

8. References


