A Confirmatory Analysis of Information Systems Security Success Factors

Kimberley D. Dunkerley
Nova Southeastern University
kd177@nova.edu

Gurvirender Tejay
Nova Southeastern University
tejay@nova.edu

Abstract

Information security has received a great deal of attention from a number of researchers. However, there has been little research aimed at understanding the dimensions—within the organizational context—of information security success. The current study reviews a large body of information security literature and organizes the research based on the research findings. This structure is used to develop factors composing information security success. The dimensions are tested using survey-based methodology and Confirmatory Factor Analysis. Findings indicating mixed levels of model fit are presented, with indicators above and below levels of confidence, implying a need for further iterative study.

1. Introduction

Our world has become increasingly reliant on Information Systems (IS) and their concomitant information assets. This reliance is quite tangible when presented with the facts: IS powers much of the critical infrastructure, including such modern necessities as telecommunications, power production and distribution, oil and gas distribution, and water purification and distribution. Further, the businesses, supply chains, and financial institutions that drive the global economy depend heavily on these same assets for their very survival due to their heavy utilization of IS for management of business processes, human resource records, and customer data.

While the IS assets are indeed important, the significance of the information assets themselves must also be considered; actually, the greatest damage presented by an IS security breach is often through the loss of information resources and the strategic advantages they provide.

Even with increasing attention paid to these IS and information assets, IS security incidents do occur, and with potentially deadly effects—both literally and figuratively. To combat these threats, a number of prescriptive IS security programs with varying content (e.g., U.S. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series) have been developed within both industry and academia [1]. These programs all differ in breadth and scope, but they have one common aim: securing IS and information assets. However, even after implementing one or more IS security programs, how can an organization truly know that their IS security program has achieved success? In spite of the wealth of research in IS security, there is very little understanding of what actually makes an IS security program successful within an organization. In effect, success has been treated generally as a separate entity from IS security altogether; a great deal of research has been conducted on the “means to the end”, while limited research has been focused on truly understanding what the end actually is. To date, the closest measure of IS security success is “did anything bad happen?” [2]. The research problem of this study is the lack of understanding of what factors contribute and how they interact towards IS security success within the organizational context. This lack of understanding leads IS security programs to be less effective, efficient, and enabling than would be possible were the factors and their interrelationships better explored. Without this understanding, it is difficult for organizations to accurately and consistently state the benefits the IS security program provides [3] as well as ensure optimal resource utilization for future efforts [4]. To this end, the argument of the research is that in order for the known and unknown threats to be addressed in an effective yet balanced method, a proper understanding of the factors constituting IS security success is essential.

2. Review of literature

The review of information security literature was conducted as outlined by Webster and Watson [55]. The authors examined selected papers (no time period constraint) from the information systems field using keywords capturing the definition of IS security. The reference lists of reviewed articles were also examined to expand the list of articles and journals.

2.1 Technical security

Technical means have historically been the cornerstone of IS security research and have dominated the field to date. Numerous studies have been conducted to find
solutions for insecurity through the application of technical controls. These technical streams have focused on providing technical solutions within the various levels of assets. One stream of research has dealt with controls for securing data itself, often using different types of encryption [5]. Other research has focused on the use of digital signatures to facilitate trusted transactions between parties [6]. Software controls have been considered, looking to secure infrastructures from the inside by strengthening the applications that are present on IS [7]. Finally, many studies have focused on numerous hardware solutions, including intrusion detection and firewalls [8]. Other researchers have developed models – the Bell-LaPadula model, the Biba integrity model, the Clark-Wilson model, and the Brewer-Nash model, to name a few – focusing on technical methodologies [9].

While technical research has occasionally interspersed external theories developed within the social, criminological, or behavioral domains, technical studies have largely focused on protecting infrastructure by facilitating the classic CIA (Confidentiality, Integrity, and Availability) triad. CIA has become a cornerstone of IS security; even while a host of other factors have been proposed, such as responsibility, privacy [10] trust, non-repudiation and authenticity [11] are mentioned alongside, the CIA triad is a mainstay. Most secure system development activities and organizational security policies have been exclusively based on the pursuit of these core principles, and many studies are based on the assumption that achieving the CIA of an organization’s assets are the essential objectives of an IS security program [12].

However, security cannot ultimately only mean CIA; in order to have a measure of security effectiveness there must be generally accepted measurements for CIA. To date, there are none. Further, Anderson urges for the establishment of metrics, not only for CIA, but also for quantifying the value of the IS security program and how the program provides a “well assured sense of assurance” to an organization.

2.2 Risk management

A key point within risk management research is the assumption that a clear analysis and understanding of risks are critical to achieving effective security within an organization. The goal of risk analysis is to help management make informed decisions about investments and to develop risk management and information security policies while fully considering the constraints in place inherent to the organization [13]. Risk analysis methodologies generally measure risk either as the probability of a negative outcome or a product of the probability of a negative outcome due to a threat and the probability that the corresponding control will fail to eliminate the threat. Within this context, many IS risk analysis methodologies have been developed within both academia and industry. These include quantitative methods (e.g., expected value (EV) analysis [14], stochastic dominance approach [15], Livermore Risk Analysis Methodology (LRAM) [16], qualitative methods (e.g., scenario analysis, questionnaire, and fuzzy metrics), and tool kits (e.g., Information Risk Analysis Methodologies (IRAM), the CCTA Risk Analysis and Management Method (CRAMM) [13], National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-37, and the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method [17]). In turn, risk analysis methodologies have evolved from more checklist-based approaches to include more sophisticated theories such as Theory of Belief Function [13] and finally, strategic conceptual modeling approaches [18].

2.4 IS security policies, standards, and checklists

While not as thoroughly studied as purely technical controls [19] it has been argued that one of the most important IS security controls that can be introduced into an organization is the IS security policy [20]. Studies have suggested that most IS security decisions within small to medium-sized organizations are directly guided by policy while large organizations institutionalize IS security in their culture through the use of policy [21]. The term “policy” itself has been argued, with research divided into two schools of thought: technical/computer security and non-technical/management security. Technical policy generally refers to the automated implementation of management policies [22]. This is confused by the term “policy” being used within technical contexts, such as group policies in a directory environment, or access control policies on a firewall. Management policy, as defined within [21], is a high-level plan embracing the organization’s general security goals and acceptable procedures. Within this perspective, there has been significant study conducted as to the role of policy within the organization.

2.5 Economic aspects of IS security

As information as an asset increases in importance, a number of researchers have discussed the organizational value of information systems and how their protection supports and furthers the business as a whole [23, 24, 25]. Since most measures – technical, personnel, procedural – involve some level of resource allocation, spending on IS security has become an important priority within organizations [24]. Understanding how to create value – investing the optimal amount in protecting assets and creating balance – is key. A good deal of research has focused on deriving the optimal amount for an organization to invest for securing their IS and related
assets [26, 27]. This research has culminated in the development of models for predicting this optimal amount [28, 29]. Finally, as large amounts of money are allotted for IS security measures, stakeholders have begun to demand results that they can see, in order to justify these expenditures. Traditional economic ideas, such as Return on Investment (ROI), have been discussed, with researchers attempting to determine if tools such as Return on Security Investment (RoSI) [24] and the Analytic Hierarchy Process (AHP) [30] would be useful for explaining IS security investments.

It is also important for stakeholders to understand the value that IS security can create within an organization; however, when attempting to explain how an IS security program creates value for an organization, one cannot focus solely on economic aspects. Research has discussed at length the socio-organizational considerations involved with IS security, such as effects on organizational culture, and their value to the organization [31].

2.6 Behavioral aspects of IS security

Research has suggested that IS security has an almost “self-canceling” phenomenon to consider: the user [32]. Studies have shown that a lack of user compliance has been directly tied to a decrease in IS security effectiveness [33]. Since the effectiveness of controls that are put into place to protect information assets are constrained by behaviors of human agents who access, use, administer, and maintain them [34, 35], it is clear that the users and their effect on IS security must be considered. It has been argued that information insecurity is as much due to “perverse incentives” as it is to weaknesses in the technical infrastructure [23].

One line of research deals with counterproductive computer usage and malicious extremes, including insider threats [36, 37, 38] and external threats [39, 40, 28]. While firms are shown to spend more resources countering perceived threats originating from external forces [35], it has been argued that the insider threat is perhaps the most significant threat an organization should consider and that the actual number of internally-led breaches suffered cannot be known due to the vast amount of unreported and unknown breaches [41]. Much research centers around General Deterrence Theory-based approaches to solving insider threat [42] theorizing that misuse will decrease as the disincentives increase. Further, studies have shown that increasing internal knowledge of policies and other countermeasures, while not consistent, has the effect of decreasing misuse from certain internal groups [42]. Finally, criminological theories have been introduced, attempting to shed new light on internal threats using fresh perspectives to the IS domain [43].

A second subset of user behavioral research focuses on the awareness of users towards the systems—both the information system and its protective technologies—with which they interact. Research has shown that awareness of technology is central to the formation of user attitudes, and in turn, the user’s concern for IS security [44] but is difficult to characterize due to the individual nature of the variable itself [32]. For instance, awareness towards the negative consequences of spyware has been found to motivate users to develop positive attitudes towards protective technologies and their intention to use them [45]. However, research suggests that simply telling users to follow secure practices is not enough; they must be convinced of it [46].

Another research stream attempts to better understand the user’s intentions and their effect on IS security. These studies often incorporate theories such as the Theory of Planned Behavior or Theory of Reasoned Action to explain user intention and its affect on subsequent behavior. Research suggests that user intention is affected by a number of external moderators, including organizational commitment [47], codes of ethics [48], and cultural factors [45]. Further studies have discussed the link between the user’s awareness and their intentions towards IS [49] and suggest that user awareness has a direct link to their intentions, which in turn affects behavior. These findings suggest that user intention—ranging from the malicious to the beneficial—might be a key to understanding why users behave in the manner that they do, and the measures that must be taken to prevent or protect against malicious behavior.

2.7 Themes in research

The research streams within IS security differ in their nature, but there are definite themes recurring throughout the domain. Early works within IS security research were significantly technical, and highly prescriptive, with a heavy dependence on checklists and methodological-based approaches aimed at producing a “one-size-fits-all” method of protection. This mindset, while long deemed inadequate by researchers [21], does continue to persist through a number of governance and standards-based measures currently in use. However, the field as a whole is evolving with the times; researchers have begun to expand into organizational optimization, considering the concepts of balance and emergence. These concepts weave through a considerable number of studies across the IS security domain. An example is the economic research of Gordon and Loeb [24, 25] promoting the idea of a balanced IS security program as value maximization by optimal investment into the protection of assets, a highly context dependent concept. These concepts align with Anderson’s definition of IS security as risks and controls being in balance [2].

Another theme present within the IS security domain is the importance of considering the human factor present within the IS. While the IS is not solely technical in
nature, early research streams within the IS security domain focused primarily on achieving CIA and its fellow tenets through technical methods. A paradigm shift in the domain occurred when the human aspect began to be considered. Da Veiga and Eloff described IS security as having distinct phases of evolution: the first phase, purely technical in nature, heavily depended on the technological means of securing the IS [50]. The second phase began when the realization was made that the human element urgently needed to be addressed. This realization has been reflected within the body of research; the IS security domain has moved from purely technical considerations to the inclusion of a great number of studies focusing on socio-organizational areas such as culture, awareness, and user behavior. Clearly, as research has suggested a powerful mitigating effect presented by the human factor, it can be expected that the human factor will continue to be an important consideration across the IS security domain.

3. Research methodology

3.1 Theoretical framework

This research study will build upon the body of work by Shannon and Weaver [51] and Mason [52] develop a model for predicting IS security success within an organization. Shannon and Weaver identified three constructs involved in effective communications. First, the technical level of communications involves the accuracy and efficiency of the communication system that produces information. Second, the semantic level relates to the success of the information in conveying the intended meaning from sender to receiver. Finally, the effectiveness level is the result the information actually has on the user’s behavior. Mason adapted the work by Shannon and Weaver in order to relate it specifically to information systems. This study will adopt the Shannon and Weaver taxonomy of communication levels and apply it within the IS security domain.

The review of literature suggested notable findings from IS security researchers that can readily be presented within the framework of Shannon and Weaver. First, the technical streams of IS security have demonstrated the importance of securing IS assets through technical means, or ensuring that information “outputs fully and fairly reflect [inputs] and [processes] are complete, timely, authorized, and accurate” [53]. This is crucial, as information is arguably the most important asset an organization controls. However, the IS itself cannot be forgotten; the information cannot be relied upon if the “accuracy, completeness, timeliness, validity, and processing methods” of the IS itself have not been secured properly [54]. Therefore, the concepts of information security and IS security go hand-in-hand towards a common end. Further, the IS security program should not only create value to the organization through the security provided to the information and IS assets, but also through enablement of business objectives. Security controls applied in a “one-size-fits-all” manner have the ability to stifle not only the everyday mission of an organization through laborious mechanisms or heavy-handed policies, but can be a real threat to the organizational objectives. Again, considering the Anderson definition of IS security, an organization must be well-informed in regards to its strategic goals and how the IS security program must balance those goals with the quantified threats to the organization. Considering this, the IS security program operating in a balanced manner should not hinder the strategic goals of the organization; instead, the IS security program should incorporate the concepts of usability and flexibility to deal with emergent situations or exceptions. Quite simply, the IS security program should help the organization get the job done. These concepts – securing the information and IS assets and enabling operations – form the basis of the Technical Level as described by Shannon and Weaver.

As the extant literature has suggested, the user is a key factor when considering how IS security actually fits into the organizational dynamic. Stanton found that the user dimension was composed of two elements, the user’s intentions towards the IS and the user’s knowledge. In the context of organizational IS security, it becomes extremely vital to understand the user’s intentions towards IS and its protective technologies, on a spectrum from positive to negative [35]. Further, the user’s knowledge describes his or her cognition of the organizational environment, both technical and non-technical. Technical knowledge refers to the user’s technical savvy. On the other hand, non-technical knowledge involves user awareness about security policy and various controls to protect information assets and the organizational mission. The user factors form the basis of the Semantic Level, as discussed by Shannon and Weaver.

Based on the previously discussed concepts of balance, flexibility, and emergence, IS security success can – and often will – mean different things within different organizational contexts. For example, an organization that relies heavily on highly classified information assets might find success to mean zero information spillages occurring within a given time period. Another organization might determine success to mean compliance with regulatory guidance. Being well-informed provided the organizational leadership with the tools to determine what success means within the particular organizational context. Further, IS security success is not predetermined to be positive in nature; it is a realistic possibility that, based on the inputs provided, the level of success is found to be negative in nature. The success of the IS security program itself forms the basis for the Effectiveness Level as detailed by Shannon and Weaver.
Understanding these factors presented within the structure provided in Shannon and Weaver, the benefits provided through the dynamic relationship between the Technical Level factors (Information Integrity, IS Assurance, and Operations Enablement) and the Semantic Level factors (User Intention and User Knowledge) lead to the Effectiveness Level proffered upon the organization, IS Security Success.

Based on the previous discussion, the proposed model predicting the interaction of constructs composing IS security success within the organizational context is presented in Figure 1. The model details the relationship between the technical level – Information Integrity, Information Systems Assurance, and Operations Enablement – and the semantic level – User Intention and User Knowledge. This relationship further results in the dependent variable, IS Security Success.

Figure 1. Model of IS Security Success

To correspond with the relationships depicted in Figure 1, there are 10 hypotheses.

H1: Information Integrity is positively related to User Intention.
H2: Information Integrity is positively related to User Knowledge
H3: IS Assurance is positively related to User Intention.
H4: IS Assurance is positively related to User Knowledge
H5: Operations Enablement is positively related to User Intention.
H6: Operations Enablement is positively related to User Knowledge
H7: User Intention is positively related to User Knowledge
H8: User Intention is positively related to IS Security Success
H9: User Knowledge is positively related to User Intention
H10: User Knowledge is positively related to IS Security Success

3.2 Research approach

This phase of the research is concerned with the validity of the constructs themselves. An important first step before analyzing the model and its path is ensuring that the observed variables are valid and capturing the essence of the desired latent variables. To that end, a survey instrument was developed to test the indicators chosen for measurement of the proposed latent variables. The survey instrument contained 5 items per construct; research has shown little improvement on internal consistency by using more than 5 items per construct, and keeping the number of items relatively low minimizes the potential for response bias caused by participant fatigue. Items were measured using a 5-point Likert scale consisting of “Strongly Disagree”, “Disagree”, “Neither Agree Nor Disagree”, “Agree”, and “Strongly Agree”. Survey items were constructed to capture the observed variables as listed in Appendix A.

A study was conducted on a convenience sample of 61 individuals identified as IS security experts. 61 surveys were distributed and 61 received completed by participants, for a 100% response rate. Respondents held positions identified as “technical”, “managerial”, or “professional”. Further, 94% identified as “Defense Contractors”, while 6% identified as “Manufacturing”. Further, company size identified as medium for all respondents, with 100% employed by a company with 10,000 employees or less. As the focus was the validation of the factors synthesized from literature, collected data was analyzed using Confirmatory Factor Analysis (CFA) techniques. CFA was chosen because it has proven to be ideal for testing the validity of proposed constructs. All 61 cases had complete data.

4. Findings

Based on prior evidence and theory, a six-factor model was specified in which the indicators of Information Integrity, Confidentiality and Authenticity loaded onto the latent variable of Information Integrity; IS Integrity and IS Availability loaded onto the latent variable of Information Systems Assurance; Non-Repudiation and Continuity of Operations loaded onto the latent variable of Operations Enablement, and Effectiveness, Efficiency, Enablement of Organizational Goals, and Value loaded onto the latent variable of IS Security Success. The variables User Knowledge and User Intention were measured through single indicators of User Knowledge and User Intention, respectively. All indicators were chosen through a study of IS security literature. The measurement model contained no double-loading indicators. The model was overidentified with 390 df.
A key concern when using survey-based methodology is assuring the reliability of the scale. A popular test for scale reliability is Cronbach's alpha, which determines the internal consistency of items in a survey instrument to gauge its reliability. The Cronbach's alpha of the instrument was calculated as .74, exceeding the .70 found to be an acceptable reliability coefficient.

Prior to the CFA analysis, the collected data was evaluated for univariate and multivariate outliers by examining leverage indices for each participant. An outlier was defined as a leverage score that was five times greater than the sample average leverage value. No univariate or multivariate outliers were detected. Normality of the indicators was examined using PRELIS 2.80.

The data was then loaded into LISREL 8.80. Appendix B depicts the path diagram generated by LISREL. The sample covariance matrix was analyzed using a maximum likelihood minimization function. Maximum likelihood was chosen because it allows for a statistical evaluation of how well the factor solution is able to reproduce the relationships among the indicators. Goodness of fit was evaluated using the standardized root mean square residual (SRMR), root mean square error of approximation (RMSEA) and its 90% confidence interval (90% CI), and the comparative fit index (CFI). Acceptable model fit was defined by the following criteria: RMSEA ≥ .06 with 90% CI ≤ .06, SRMR ≤ .08, and CFI ≥ .95. Multiple indices were used because they provide different information about model fit (i.e., absolute fit, fit adjusting for model parsimony, fit relative to a null model); used together, these indices provide a more conservative and reliable evaluation of the solution. The selected goodness-of-fit indices provided mixed results for model fit. The RMSEA of .082 with a 90% CI of .065 indicated good model fit. However, the SRMR of .054 and CFI of .89 were less than the defined levels of confidence.

5. Conclusion

This study produced mixed results of model fit, indicating a need for further refinement of potential constructs. While an acceptable Cronbach's Alpha and RMSEA were found, other indicators of model fit were below the level of confidence and imply a need for further iteration.

This study is the first known research conducted to determine the composition of IS security success. Thusly, this research can be considered a basic, initial step towards this better understanding of IS security success. Future research should focus on the constructs themselves; adding new constructs that are validated as worthy, removing constructs found to be weak, as well as testing the theories with a larger sample to increase assurances of validity. Also, a model should undergo analysis via Structural Equation Modeling techniques to better understand the interaction between the proposed latent variables.

6. References


Appendix A. Latent and Observed Variables within Survey Instrument

<table>
<thead>
<tr>
<th>Latent Variable</th>
<th>Observed Variable</th>
<th>Survey Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Integrity</strong></td>
<td>Data Integrity</td>
<td>II1, II3, II5</td>
</tr>
<tr>
<td><em>Definition:</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The assertion that information is</td>
<td>Confidentiality</td>
<td>II2, II4</td>
</tr>
<tr>
<td>precisely the same during transmission, receipt, and storage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information Systems Assurance</strong></td>
<td>Availability</td>
<td>ISA1, ISA2</td>
</tr>
<tr>
<td><em>Definition:</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The guarantee of the integrity and availability of the information system.</td>
<td>IS Integrity</td>
<td>ISA3, ISA4, ISA5</td>
</tr>
<tr>
<td><strong>Operations Enablement</strong></td>
<td>Enablement of Business Objectives</td>
<td>OE1</td>
</tr>
<tr>
<td><em>Definition:</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The facilitation of organizational objectives in an efficient manner.</td>
<td>Usability</td>
<td>OE2</td>
</tr>
<tr>
<td></td>
<td>Non-Repudiation</td>
<td>OE3</td>
</tr>
<tr>
<td></td>
<td>Continuity of Operations</td>
<td>OE4, OE5</td>
</tr>
<tr>
<td><strong>User Intention</strong></td>
<td>Intent</td>
<td>UI1, UI2, UI4</td>
</tr>
<tr>
<td><em>Definition:</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The intentions of the users toward protective measures of an information system.</td>
<td>User Ethics</td>
<td>UI3, UI5</td>
</tr>
<tr>
<td><strong>User Knowledge</strong></td>
<td>User Awareness</td>
<td>UK1, UK2, UK4</td>
</tr>
<tr>
<td><em>Definition:</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The users’ knowledge about protective measures of an information system.</td>
<td>User Training</td>
<td>UK3, UK5</td>
</tr>
<tr>
<td><strong>IS Security Success</strong></td>
<td>Enablement of Goals</td>
<td>ISS1</td>
</tr>
<tr>
<td><em>Definition:</em></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cumulative effect of the relationship between information systems experience and user experience.</td>
<td>Value</td>
<td>ISS2, ISS4</td>
</tr>
<tr>
<td></td>
<td>Effectiveness</td>
<td>ISS3</td>
</tr>
<tr>
<td></td>
<td>Balance</td>
<td>ISS5</td>
</tr>
</tbody>
</table>
Appendix B. IS Security Success Model Path Diagram