International Journal of Cyber Criminology
Vol 14 Issue 1 January – June 2020

Effective Information Security Strategies for Small Business

Lisa Lee Bryan[1]
Colorado State University – Global, United States of America

Abstract

The purpose of this quantitative ex-post facto study was to evaluate a small business information security system composed of a computer-use policy, information security training, and virus and malware protection. The DeLone and McLean Updated Success Model provided the foundation for the small business information security system model and constructs measured in the survey. The population consisted of small businesses with less than 100 employees and independent (non-franchise) in North Carolina, South Carolina, Georgia, Florida, Alabama, and Tennessee. The model contained four relationships incorporated into four research questions and four hypotheses including four null hypotheses. Each of the three components indicated a positive relationship with the variable of positive use experience. Recommendations include small businesses using the small business information security system as a comprehensive system to protect their business from security incidents. Information technology consultants should implement this comprehensive security system for small business clients to prevent security incidents.

Keywords: Delone Mclean, Small Business Security, Information Security System, Security Incidents.

Introduction

With the introduction of computers more than 50 years ago, the task of securing the electronic data contained in each system continues to trouble small businesses (Wirth, 2017). The days of confidential information in locked drawers and rooms are past. Small businesses lack internal information technology (IT) staff and appear most vulnerable to attack (Nguyen, Newby, & Macaulay, 2015).

The result of this lack of preparation in small businesses is a reactive approach to information security (Barton, Tejay, Lane, & Terrell, 2016). In small business, investment in successful information security strategies is essential. Small businesses need effective tools to protect their information assets.

Multiple Internet threats face small businesses. Hackers use email, phishing, and malicious software to gain control of computers (Clapper & Richmond, 2016). Viruses and spyware open doorways on a computer to hackers and malicious programs. Trojan

[1] Program Chair, BSMISBA and MSDA, Colorado State University - Global, Aurora, CO, USA. Email: drlisabryan@outlook.com

viruses invade computers and hide until activated (Lin, 2018). The security of a small business depends on users. The users provide the weakest area in the security plan creating potential doorways to attack (Caldwell, 2016). Internal security must address the vulnerabilities created by computer-users.

This quantitative ex-post facto study used the DeLone and McLean Updated Information Systems Success Model to measure the success of an information security system in small business (DeLone & McLean, 2003). The DeLone and McLean model began in 1992 as a search for a way to measure the dependent variable of success in information systems research (DeLone & McLean, 1992). The updated model in 2003 included areas researched over the 10 previous years. The dependent variable of individual and organizational impact becomes net benefits when combined in the 2003 model (DeLone & McLean, 2003). The addition of the service quality factor to evaluate information systems specifically applies to the performance of information-system service providers, usually IT departments (DeLone & McLean, 2003). Small businesses often replace internal IT with external consultants or educated users.

Small businesses face conflict as business requirements force employees to use the Internet and email while they unintentionally open doorways of the business to cybercrime and attacks (Caldwell, 2016). This quantitative ex post factor study sought to evaluate security information system components used by small businesses. The three components evaluated require minimal business resources allowing small businesses with limited resources to implement.

1. Research Questions and Hypotheses

Using the DeLone and McLean updated model of IS success, computer-use policies, information security training, and virus and malware protection combined are components of a small business information security system that requires measurement (DeLone & McLean, 2003). The information, system, and service quality of these components can encourage a positive user experience, according to the model shown in Figure 1 (DeLone & McLean, 2003). A positive use experience toward the information system can create net benefits (DeLone & McLean, 2003). These net benefits for small businesses should reduce harm from security incidents.

The use of an information system when required by the business is not a valid measurement according to the model (DeLone & McLean, 1992). When required, user satisfaction is the appropriate measurement of the information system (DeLone & McLean, 1992). The question of positive use experience measured this component of the model. The small-business information security system measured includes three commonly used security strategies used in many small businesses. These three strategies included a computer-use policy, information security training, and virus and malware protection.

Research Question 1.

What is the relationship between a computer-use policy and a positive use experience of the small business information security system?

Research Question 2.

What is the relationship between information security training and a positive use experience of the small business information security system?

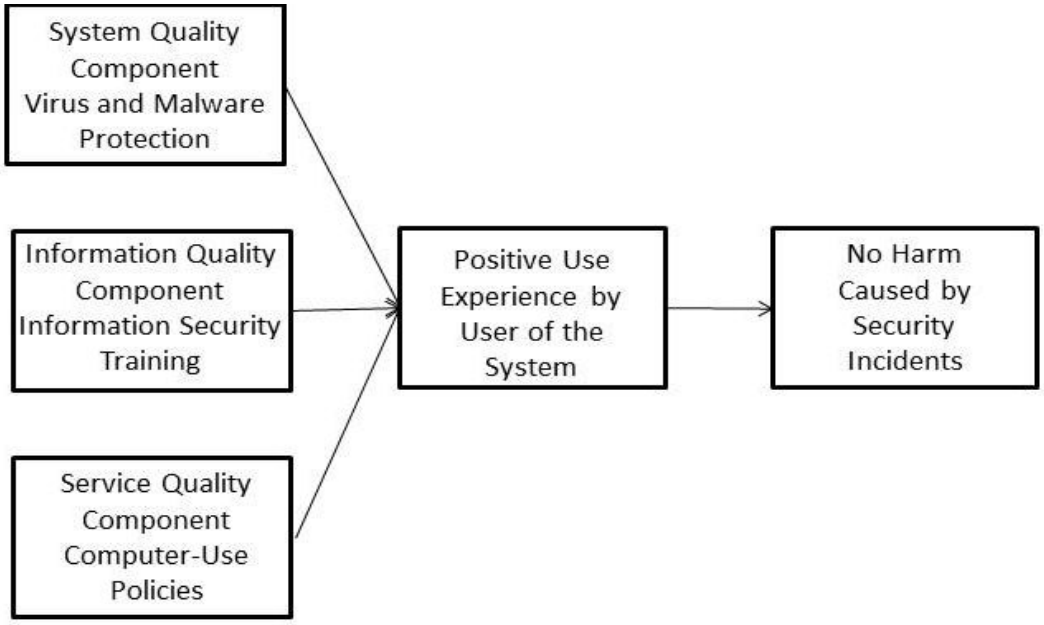
Research Question 3.

What is the relationship between virus and malware protection and a positive use experience of the small business information security system?

Research Question 4.

What is the relationship between a positive use experience of the small business information security system and no harm caused by security incidents?

Figure 1. Model of Small Business Information Security System



Adapted from "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," by W. H. DeLone and E.R. McLean, 2003, *Journal of Management Information Systems, 19*(4), p. 24. Reprinted with permission.

H10.

There is no statistically significant relationship between computer-use policies and a positive use experience of the small business information security system.

H1a.

There is a statistically significant relationship between computer-use policies and a positive use experience of the small business information security system.

H20.

There is no statistically significant relationship between information security training and a positive use experience of the small business information security system.

H2a.

There is a statistically significant relationship between information security training and a positive use experience of the small business information security system.

H30.

There is no statistically significant relationship between virus and malware protection and a positive use experience of the small business information security system.

H3a.

There is a statistically significant relationship between virus and malware protection and a positive use experience of the small business information security system.

H40.

There is no statistically significant relationship between a positive use experience of the small business information security system and no harm caused by security incidents.

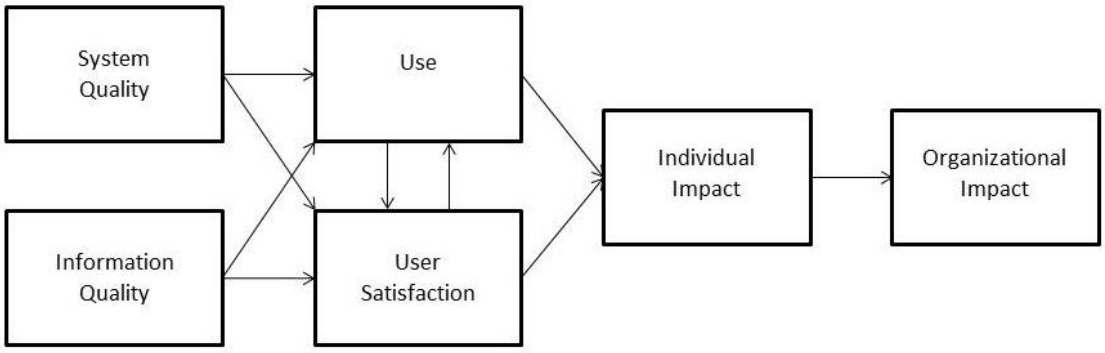
H4a.

There is a statistically significant relationship between a positive use experience of the small business information security system and no harm caused by security incidents.

2. Theoretical Framework

The study's purpose was to explore the possible relationship of information, system, and service quality to positive use experiences of computer-use policies, information security training, and virus and malware protection. The use of these systems encouraged by positive use experiences creates a system that can provide net benefits. The need for a measurement of information system success is the foundation of the original DeLone and McLean Information Systems Success Model shown in Figure 2 (DeLone & McLean, 1992). The dependent variable for information systems is successful use; therefore, creating benefits for the user and the organization (DeLone & McLean, 1992).

Figure 2. DeLone and McLean Model of IS Success



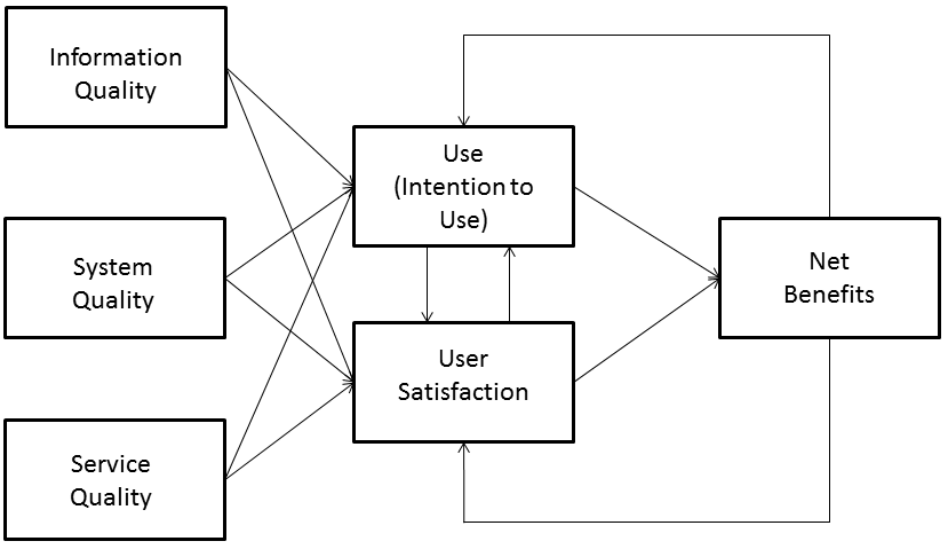
Adapted from "Information System Success: The Quest for the Dependent Variable," by W. H. DeLone and E.R. McLean, 1992, *Information Systems Research, 3*(1), p. 87. Reprinted with permission.

After 10 years of studies including the DeLone and McLean IS Success Model, the researchers explored the possibility that the model needed revision as shown in Figure 3 (DeLone & McLean, 2003). After study, the dependent variable of service quality becomes a part of the updated model to address information system departments and IT staff support (DeLone & McLean, 2003). The results of individual and organizational impacts become net benefits in the model (DeLone & McLean, 2003). The additional cyclical effect of net benefits to use and user satisfaction supports the common theory that systems that work encourage use.

This study focused on small businesses using a model to explore an information security system. Past studies focus on leadership only. The DeLone and McLean model finds the influence of leadership unrelated directly to the dependent variable of net benefits (DeLone & McLean, 2003). To extend this model, leadership encouragement and support

for a system adds to the quality of the system. This addition can apply to the other dependent variables of information, system, and service quality.

Figure 3. DeLone and McLean (2003) updated IS Success Model



Adapted from "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," by W. H. DeLone and E.R. McLean, 2003, *Journal of Management Information Systems, 19*(4), p. 24. Reprinted with permission.

3. Components of the DeLone and McLean updated IS Success Model

The original DeLone and McLean Model (1992) of success developed from previous studies on information system success. The DeLone and McLean Updated IS Success Model (2003), derived from the original model, determines the success of an information system. The components of the DeLone and McLean Updated IS Success Model (2003) include system quality, information quality, service quality, use of the system, intent to use the system, user satisfaction, and net benefits. The model determines the dependent variable of success (DeLone & McLean, 2003).

3.1. Information Systems

In the DeLone and McLean model, an information system is the independent variable introduced into an organization (DeLone & McLean, 2003). The information system requires measurement to see if it is successful and creates net benefits in the organization (DeLone & McLean, 2003).

3.2. System Quality

In the DeLone and McLean model, system quality began as a measurement in research studies of the information system process itself (DeLone & McLean, 1992). In the updated research model, system quality is the factors: functionality, data quality, portability, importance, flexibility, ease-of-use, reliability, and integration (DeLone & McLean, 2003).

3.3. Information Quality

In the DeLone and McLean model, information quality began as a measurement in research studies as the perceived importance and functionality of the information provided (DeLone & McLean, 1992). In the updated research model, timeliness, completeness, relevance, accuracy, and consistency are measurements of information quality (DeLone & McLean, 2003).

3.4. Service Quality

Service quality was not a component in the 1992 DeLone and McLean IS Success Model. The addition of the component to the model was the result of changes in information systems that include providing support for end users (DeLone & McLean, 2003). The measurement of service quality includes tangibles such as up-to-date hardware and software, responsiveness, reliability, assurance, and empathy with users (DeLone & McLean, 2003).

3.5. Use of the System

DeLone and McLean (1992) found in researching studies focused on IS success that use of a system was a broad category covering actual use as shown by monitoring or estimates of use. The measurement of the factor "use" is contingent on the voluntary usage of a system (DeLone & McLean, 1992). The nature of the use includes the quality, extent, and appropriateness of the system use (DeLone & McLean, 2003). A system with declining use is not successful.

3.6. Intent to Use the System

Intention to use discussed by DeLone and McLean (2003) is a possible alternative measure to use in the model for systems not implemented or actively used at the time of measurement. Since "intention to use" is an attitude not a behavior, the measurement of the factor is difficult (DeLone & McLean, 2003).

3.7. User Satisfaction

User satisfaction with a system becomes a valid measurement in information systems if usage is mandatory (DeLone & McLean, 1992). In the updated model, DeLone and McLean (2003) show the close interrelation between use and user satisfaction. "Use" in a process comes before "user satisfaction" and a positive "use" experience can lead to more "user satisfaction" (DeLone & McLean, 2003).

3.8. Net Benefits

Net benefits are a combination of individual and organizational benefits found in the DeLone and McLean IS Success Model (DeLone & McLean, 1992). The main areas of impact are task innovation, task productivity, management control, and customer satisfaction (Petter, DeLone, & McLean, 2008). The combination of individual and organizational benefits is net benefits in the updated model (DeLone & McLean, 2003).

3.9. Success

As the dependent variable in most information system studies, success is difficult to define and challenging to measure (DeLone & McLean, 1992). The introduction of an information system requires measurement of the success to justify expenses and continued

use (DeLone & McLean, 2003). The purpose of the DeLone and McLean Model (2003) is to analyze the success of an information system. In the model, a relationship of the other variables to net benefits shows success.

3.10. Computer-Use Policies

A policy is a plan that influences and seeks to direct actions and decisions (Ifindo, 2018). A computer-use policy is a guide to the behavior and the use of computers and related hardware (Ifindo, 2018).

3.11. Information Security Training

Technical controls like virus protection, firewalls, passwords, and encrypted laptops attempt to protect the business from attack from outside. Internet security normally includes a physical, procedural, and logical form of protection (Berry & Berry, 2018). User education raises security awareness often missing in small businesses (Muhirwe & White, 2016).

3.12. Virus and Malware Protection

A computer virus, much like a medical virus, seeks to spread often without the knowledge of the user (Patil & Jadhav, 2015). Malware, like viruses, are programs. The authors of these programs seek to hide destructive commands and execute without the user's knowledge (Patil & Jadhav, 2015). Spam, or junk email, is a powerful tool to pass viruses and malware (Thakur, Shan, & Pathan, 2018).

4. Method

The method needed to answer the questions defined by this study was quantitative. The research design, research variables, appropriateness of the design of the study, and the research questions provided insight into the details of the study. The hypotheses that correspond to the research questions required testing. The population studied along with a description of the sampling frame defined the group of businesses studied. A description of the nature of the study, including information on informed consent, confidentiality, and geographic location, provided additional information on the sample. The survey measured the responses from the sample and the data collected. Multiple statistical tests analyzed the data to allow internal and external validity and reliability in the study that provided confidence in the results. This research was to increase the knowledge of effective information security for small businesses.

4.1. Research Design

This research study used a quantitative method of study because of the need to have a precise and statistical finding (Rubin & Babbie, 2016). The research process in the study sought to test and define existing relationships between the variables requiring quantitative methods (Rubin & Babbie, 2016). The study was descriptive and described the relationship of the variables to the success of a small-business information security system (Rubin & Babbie, 2016).

This study used associative and multivariate research methodology that tried to determine the strength of the association between the variables studied (Rubin & Babbie, 2016). The strength of the association was not easy to see when looking at the data on paper or in a graph, but statistics provided precise values (Rubin & Babbie, 2016). The

study was multivariate research that included the study of more than one dependent variable (Salkind, 2017). The dependent variables in the DeLone and McLean model are system quality, information quality, service quality, user satisfaction, and net benefits (DeLone & McLean, 2003).

This study using online surveys focused on security incidents in the past and the performance of the security system at an earlier time. This form of study was ex post facto research. An online survey of small businesses in the chambers of commerce in the southeastern United States solicited by paper mail and email provided the data for analysis. The population of the study included independent small businesses with fewer than 100 employees.

4.2. Population

A population is a group of people who show common traits (Hoy & Adams, 2016). The population of this study included more than 10,000 small businesses found in six southeastern states in the United States. These states included North Carolina, South Carolina, Georgia, Florida, Tennessee, and Alabama. The U.S. Chamber of Commerce represents the interest of more than three million businesses with more than 96% of the small businesses having 100 or fewer employees ("About the U.S.," 2018). The U.S. Chamber of Commerce provides links to the state chambers of commerce. The state chambers provide links to the local chambers of commerce allowing an accessible list of members.

4.3. Sampling Frame

A sampling frame is a list of entities that provide selection of a sample (Rubin & Babbie, 2016). The sampling frame should reflect the study population and samples drawn and include the characteristics of the population (Rubin & Babbie, 2016). The list of small businesses for this study included mostly businesses with 100 or fewer employees with approximately 4% of the businesses larger. Using a random convenience sampling method eliminated businesses clearly over the 100 employee-level and known franchises from the sample.

The random convenience sample came from the chambers of commerce in the six southeastern states – North Carolina, South Carolina, Georgia, Florida, Tennessee, and Alabama. The six state chamber lists provided links to the local chambers. The local lists provided businesses in categories and alphabetical order. A business in each category chosen from the local chamber lists provided a sample of all types of businesses: manufacturing, physicians, lawyers, realtors, sales, and service.

The initial sample frame contained 1003 small, independent businesses gathered from the chambers of commerce in six southeastern states. These small businesses in North Carolina, South Carolina, Georgia, Florida, Alabama, and Tennessee contacted by mail and email provided a small response rate. Additional contacts by an email reminder provided a few more responses. To achieve more responses needed for a significant result, 500 more businesses from the original population of small businesses in the six southeastern states added more contacts. These businesses contacted by email provided the additional responses needed.

Of the 1500 invited participants, 74 participants completed the informed consent and survey process. One participant in the survey denoted in the introductory questions a value of more than 100 employees in the size of the organization demographic question.

The data for this participant required removal because of the parameters of the study. The removal of this participant left 73 usable surveys for analysis.

4.4. Sample Size

The original GPower 3.1 calculation at a 90% confidence level indicated a needed response of 112 participants. The original sampling of more than 1000 small businesses reduced the margin of error and increased the probability of significant results (Mora, 2019). The increase in the sampling to 1500 provided 73 usable survey responses after a three-month contact and completion period. Another increase in sampling showed little promise of additional valid responses in a timely extended period. A recalculation of the confidence level at 73 responses produced an 85% level in GPower 3.1. Research in areas of business security or information security created concerns for privacy and confidentiality (Nguyen, Newby, & Macaulay, 2015). Many small businesses noted these concerns in the refusal to participate in the study.

The sample sizes needed for the statistical significance varies based on the analysis type. Research into sample sizes needed by Spearman rho correlations suggested that a sample size of 73 provided a confidence level exceeding 80% (Bonett & Wright, 2000). This sample size also provided a 0.05 error probability at a medium 0.3 effect size (Bonett & Wright, 2000). PLS is a regression analysis and an additional confirmation of the Spearman correlational results.

Regression provides predictability and causality to relationships between variables (Cooper & Schindler, 2014). PLS is less restrictive and requires a smaller sample size (Goodhue, Lewis, & Thompson, 2012). Research demonstrates that the required sample size for PLS derives from the number of predictors (Goodhue et al., 2012). The research study contained four predictors requiring 10 participants per predictor (Marcoulides, Chin, & Saunders, 2009). The sample size of 73 exceeded the 40 required cases for PLS.

The smaller sample size than original calculated reduced the confidence level of the Spearman rho calculation. The reduction in the confidence level required a higher than normal result to show correlation between two variables (Bonett & Wright, 2000). The use of PLS as an additional test for relationship strength confirmed the results with the smaller sample size.

4.5. Instruments

This study relied on the theoretical framework of the DeLone and McLean Updated IS Success Model (DeLone & McLean, 2003). DeLone and McLean (2003) defined the attributes that require measurement for each dependent variable in the model. Based on these attributes, a survey consisting of a Likert scale measured agreement or disagreement with each attribute (Petter et al., 2008). The measurements, as defined by DeLone and McLean (2003), attempt to capture IS success. These measurements used in numerous surveys vary only by the information system studied shown in Table 1. In a study of knowledge-based systems, a questionnaire based on these measurements of dependent variables evaluated the success of the system (Bock, Suh, Shin, & Hu, 2009). In a study focused on an online learning system, a survey based on these measurements evaluated the success of the system (Lin, 2018).

The developed survey included the DeLone and McLean metrics shown in Table 1. The survey used with permission was from the Wixom and Todd (2005) user satisfaction and technology acceptance study. The survey measured the constructs of information

quality, system quality, service quality, system satisfaction and usefulness, ease of use, and intention to user (Wixom & Todd, 2005).

The Wixom and Todd (2005) survey modified to reflect information security provided 25 questions plus demographic questions. The questions, separated based on attribute, measured information quality, system quality, service quality, experiences of use, and results or benefits. These questions based on the attributes were similar in the areas measured to the Bock, Suh, Shin, and Hu (2009) study and the Lin (2018) study.

Table 1. Success Metrics

Systems quality
• Adaptability
• Availability
• Reliability
• Response time
• Usability
Information quality
• Completeness
• Ease of understanding
• Personalization
• Relevance
• Security
Service quality
• Assurance
• Empathy
• Responsiveness
Use
• Nature of use
• Navigation patterns
• Number of site visits
• Number of transactions executed
User satisfaction
• Repeat purchases
• Repeat visits
• User surveys
Net benefits
• Cost savings
• Expanded markets
• Incremental additional sales
• Reduced search costs
• Time savings

Adapted from "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," by W. H. DeLone and E.R. McLean, 2003, *Journal of Management Information Systems, 19*(4), p. 26. Reprinted with permission.

4.6. Data Analysis

This study used descriptive statistical analysis, factor analysis, correlation analysis, and regression analysis to examine the demographic information and the relationships between the independent and dependent variables. The use of more than one method of analysis provided a more worthy study and a basis for comparison of the results (Seddon & Kiew, 1996). The data, gathered by the online Surveymonkey.com survey, transferred by download to the local drive for analysis once the two-month time-period completed. The data provided imported to spreadsheets and other statistical software for analysis.

4.7. Scope and Limitations

The scope of this study focused on small businesses with the limitation of accurate reporting. The research study's scope provided results from the southeastern United States region. The results applied to small businesses in that area and application to other geographic areas requires further study. The survey of small businesses in this study may limit the application to larger businesses and franchises. The research study used an online survey that allows self-reporting. The study did not include validation or verification methods. The study provides for honest and accurate answers from respondents. The research study measured the potential success of an information security system composed of three information security strategies in small business. Other strategies existed but were not in this research study's scope.

4.8. Delimitations

This research study focused on small businesses in the southeastern United States. Using the DeLone and McLean (2003) Updated IS Success Model, the independent variable of the information security system and the dependent variables of computer-use policies, information security training, and virus and malware protection proceeded for evaluation as system, information, and service quality. Users of the systems by their positive use experience showed participation in the system. The reduction of the security incidents created net benefits for the business.

4.9. Reliability and Factor Analysis.

The instrument used in the study derived from the original attributes defined by DeLone and McLean (2003). The survey used with permission by Wixom and Todd (2005) measured the needed variables of information quality, system quality, service quality, use, and net benefits. The Wixom and Todd (2005) survey, modified to reflect information security, supplied 25 questions plus 4 demographic questions. The Cronbach Alpha on each construct of the Wixom and Todd (2005) instrument equaled or exceeded 0.8, implying acceptance.

A calculation of the correlation of each question in the construct to the other questions in the construct demonstrated an outlier question with a correlation of less than 0.5. This question labeled US5 with that low correlation provided an outlier that affected the variable reliability. The reliability and Cronbach Alpha increased on the Positive Use Experience (US) variable with the removal of US5.

A high Cronbach Alpha (>=0.80) demonstrated that each question for the variable captured the construct adequately (Padilla & Newton, 2011). The Cronbach Alpha demonstrates with a Likert-type scale that multiple questions measure the same variable. A Cronbach Alpha of >=0.80 on each variable demonstrated that each question measured

the corresponding variable reliably. The high Cronbach Alpha matched the expected reliability demonstrated in the Wixom and Todd (2005) instrument used. The instrument was a reliable measurement based on these results.

4.10. Data Analysis Methods.

The DeLone and McLean (2003) Updated Success Model, developed to measure the dependent variables in information system success, created the foundation for this research model. The measurement of success of an information system by five dependent variables in the DeLone and McLean (2003) Model depends on relationships. In the quantitative measurement of ranked data relationships, Spearman rho and Partial Least Squares (PLS) provide reliable measurements (Cooper & Schindler, 2014). The Spearman rho correlation results close to +1 or -1 show relationships (Christmann & Badgett, 2008). PLS, a type of regression analysis, provides an extension of the relationship to causality (Poelmans et al., 2008). PLS provides path modeling that reveals cause-effect relationships even with small sample sizes (Henseler, Ringle, & Sinkovics, 2009).

5. Results

5.1. Demographics

The demographic section of the survey was brief consisting of four questions. The first two questions allowed the confirmation of the study guidelines. The first question on the number of employees allowed exclusion of data for businesses more than 100 employees. The results allowed the exclusion of the data for one business with more than 100 employees. The record of data excluded also indicated a non-independent business. The other businesses (73) responded as independent businesses or non-franchise. The third demographic question focused on if the business had an internal information technology employee. The responses of the small businesses indicated most (73%) do not have an internal information technology employee. The small businesses indicated that 59% of the businesses used an outsourced information technology person. These findings support the lack of financial resources caused small businesses to limit internal information technology employees.

5.2. Descriptive Statistics

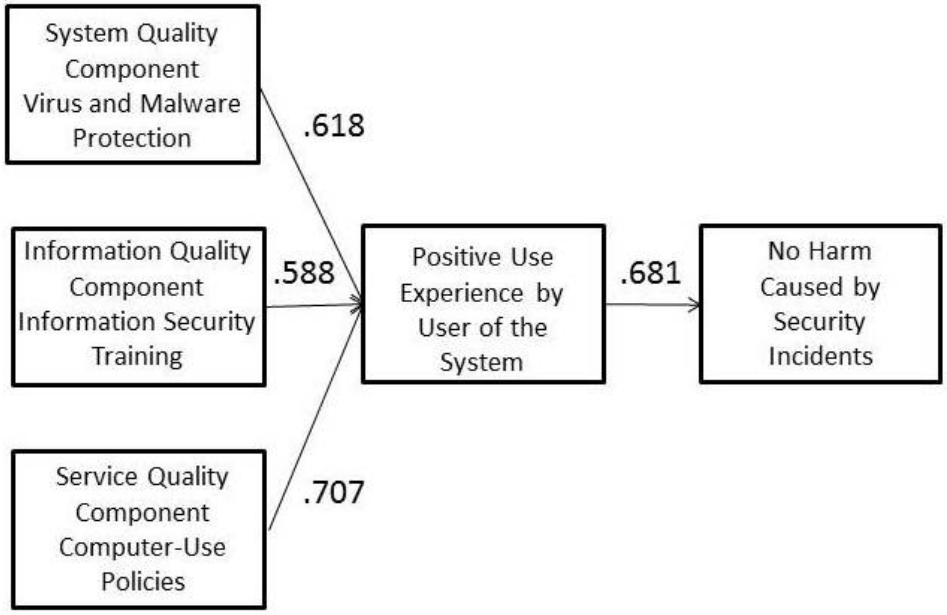
Descriptive statistics of the 73 responses provided some basic distribution and dispersion information. This information included the central tendency measures of mean, median, and mode for each variable. The standard deviation scores ranged from 0.676 to 1.128 and indicated in a range of 1 to 5 that most responses fell near the mean of the variable.

A higher standard deviation in questions IQ1, US3, and US4 signifies lower levels of agreement in responses from participants. The difference in the median and mode in question US4 signified that the respondents answered "4" most often but half of the answers were under or equal to "3". The question US4 also had the highest mean showing most respondents answered above "3", a neutral or disagree with the question response.

5.3. Testing of the Hypotheses

The results of the Spearman rho calculations in demonstrated significant relationships between the informational, system, and service quality and the positive use experience. The Spearman rho calculations demonstrated a significant relationship between positive use experience and the no harm caused by security incidents. The Spearman rho calculation used the mean of the variable responses as a summary of the questions asked in the survey for the variable. One data point per participant for each variable provided the correlation coefficients for each relationship. The relationships varied in strength from moderate to strong comparing to the strengths defined by Christmann and Badgett (2008). The relationship between computer-use policies (SV) and positive use experience (US) was strong with a correlation coefficient above 0.700. The model, with the relationships included, showed the direction and strength see Figure 4.

Figure 4. Spearman Coefficients on the Model of Small Business Information Security System

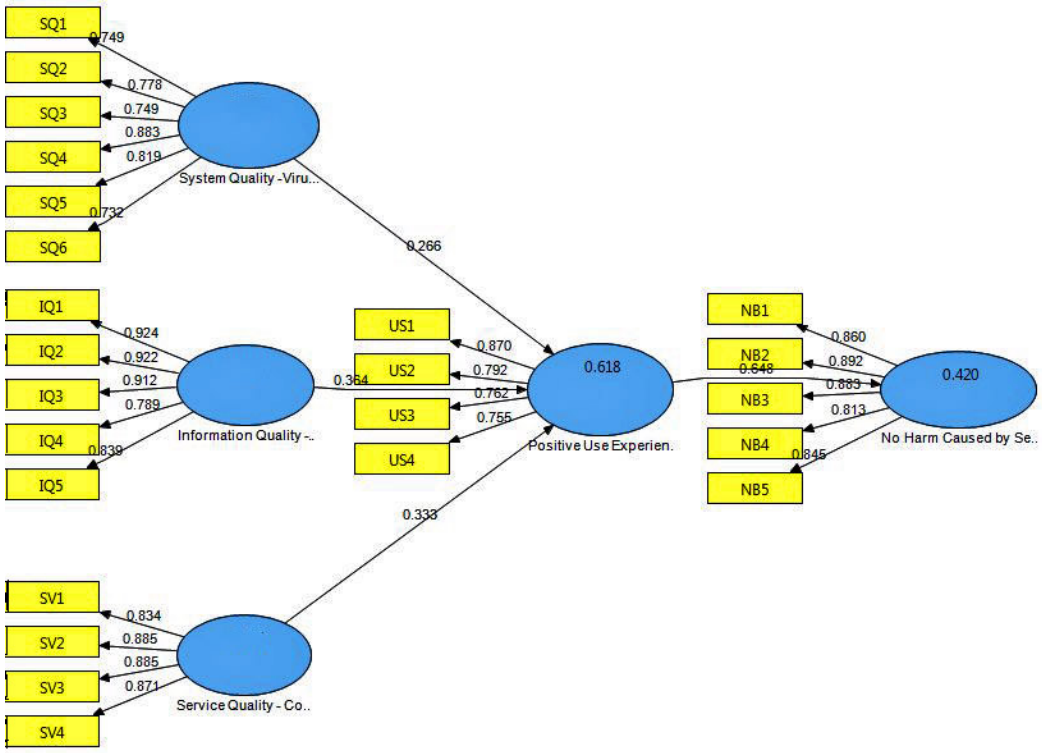


Adapted from "The DeLone and McLean Model of Information Systems Success: A Ten-Year Update," by W. H. DeLone and E. R. McLean, 2003, *Journal of Management Information Systems, 19*(4). p. 24. Reprinted with permission.

Partial Least Squares (PLS) provided confirmation of the Spearman rho relationship results. The SmartPLS 2.0 software provided a variable path model and coefficients for each relationship see Figure 5. The analysis of the data provided path coefficients with positive correlations between variables. The SmartPLS 2.0 analysis provided factor analysis on each survey item for each variable confirming earlier factor results. Each survey item resulted in factor loadings over 0.700 and confirmed the reliability of the overall instrument (Padilla & Newton, 2011). Bootstrapping in SmartPLS 2.0 confirmed the significance of the path coefficients with each T-statistic > 1.96. Bootstrapping in SmartPLS 2.0 determined the strength of the relationships between the variables within the model as recommended by Wixom and Watson (2001).

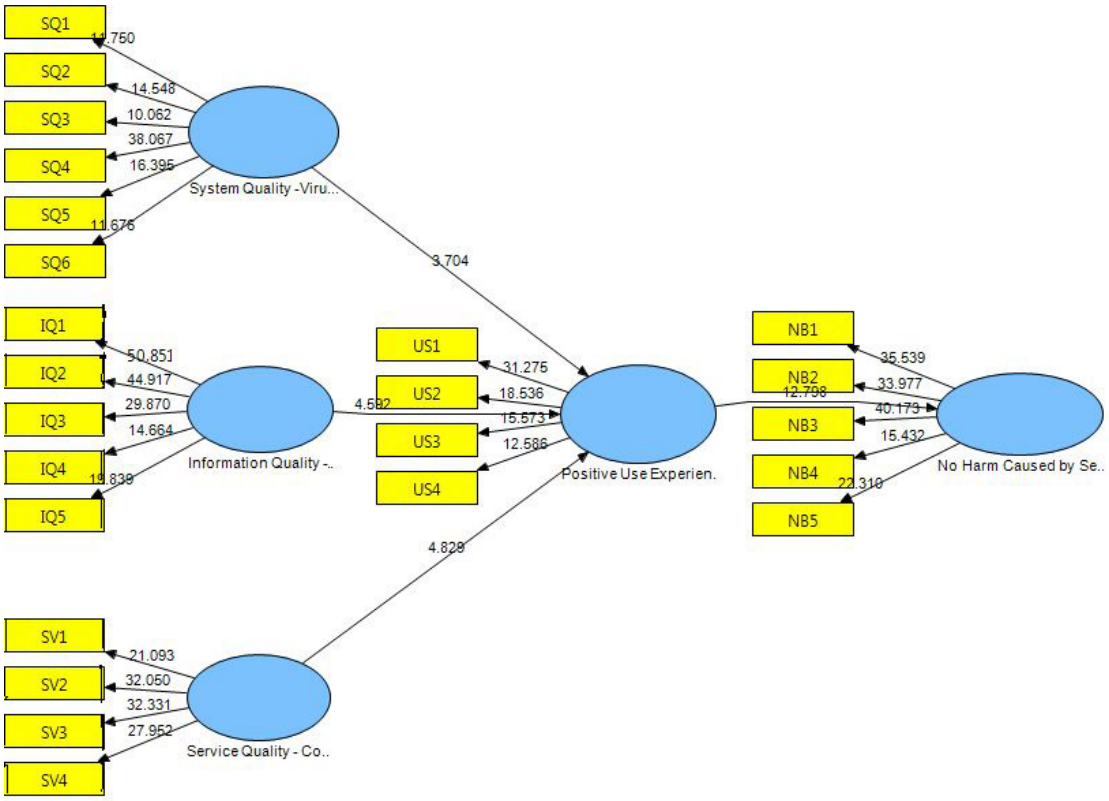
SmartPLS 2.0 describes the influence of the variables on the other variables. The resulting R2 or coefficient of determination in the positive use experience signified that 62% of the variable resulted from the influence of the variables of computer-use policies, information security training, and virus and malware protection. The variable, not harm caused by security incidents, had an R2 signifying 42% of the influence was a result of a positive use experience. The results were not 100% leaving discussion of other influences.

Figure 5. SmartPLS Path Modeling



The T-statistic produced by the bootstrapping process in SmartPLS 2.0 provided the relative strength of predictability by applying the probability of error and the application of the findings in a larger sample see Figure 6. The T-statistic of greater than 1.96 with the confidence level at 95% demonstrated the construct was a predictor of the dependent variable or construct within the sample and beyond to a larger sample (Seddon, 1997). A larger T-statistic of 12.798 demonstrated a greater predictor and influence on the dependent variable as seen in the results of the Positive Use Experience and No Harm Caused By relationship. The smaller but significant (> 1.96) positive results of the T-statistic in the System Quality, Information Quality, and Service Quality constructs to Positive Use Experience demonstrated the influence of these variables in this sample and beyond to larger samples.

Figure 6. SmartPLS 2.0 Bootstrap Path Modeling



5.4. Evaluation of the Hypotheses

Hypothesis H1a proposed a significant relationship existed between computer-use policies (SV) and a positive use experience (US). The data analysis finding rejected the null hypothesis of H10. The results of the Spearman rho and PLS analysis showed a relationship with a strong correlation of .707 and a significant PLS coefficient of .333. These findings implied the computer-use policy positively influenced the positive use experience of the small business information security system.

Hypothesis H2a proposed a significant relationship existed between information security training (IQ) and a positive use experience (US). The data analysis finding rejected the null hypothesis of H20. The results of the Spearman rho and PLS analysis showed a relationship with a moderate correlation of .588 and a significant PLS coefficient of .364. These finding implied information security training positively influenced the positive use experience of the small business information security system.

Hypothesis H3a proposed a significant relationship existed between virus and malware protection (SQ) and a positive use experience (US). The data analysis finding rejected the null hypothesis of H20. The results of the Spearman rho and PLS analysis showed a relationship with a moderate correlation of .618 and a significant PLS coefficient of .266. These findings implied that virus and malware protection positively influenced the positive use experience of the small business information security system.

Hypothesis H4a proposed a significant relationship existed between a positive use experience (US) of the small business information security system and no harm caused by

security incidents (NB). The data analysis finding rejected the null hypothesis of H40. The results of the Spearman rho and PLS analysis showed a relationship with a moderate correlation of .681 and a significant coefficient of .648. These findings implied that a positive use experience of the small business information security system positively influenced no harm caused by security incidents.

5.5. Reliability and Validity

This study used the DeLone and McLean (2003) Updated Success Model as the foundation to determine the success of a small business information security system. The model, used in more than 150 quantitative empirical studies, provided a history of studies evaluating various information systems (Petter & McLean, 2009). The results of these studies provided analysis on the four relationships found in this study. Previous research and the results of this study provided validity and reliability in the results (Petter & McLean, 2009).

5.5.a. Validity.

Validity in this study included the survey (construct) validity. The construct validity derived from the instrument and the metrics developed by Wixom and Todd (2005) and DeLone and McLean (2003). The correlation of the metrics in the Wixom and Todd (2005) instrument demonstrated validity. The correlation in the survey in this study demonstrated the metrics measured separate variables by using multiple questions. The use of the same constructs in this study provided similar results to the Wixom and Todd (2005) study. The constructs were valid in this study because individual variable measurements do not overlap. Each attribute measured in this study was unique.

External validity allows the causal relationships to generalize to other settings and populations (Salkind, 2017). This study's external validity needs verification with further research to confirm scientific validity. The use of bootstrapping in SmartPLS 2.0 demonstrated the application to a larger sample. The results of bootstrapping showed significant results on all relationships in the small business information security model. The ability to generalize to a different population like an enterprise business or a franchise would require further research. Generalizations to other small businesses in other areas of the country and in different specializations is applicable given the SmartPLS 2.0 bootstrapping results (>1.96). Generalizations to other information systems or security systems require further study.

5.5.b. Reliability.

Reliability of this study focused on the use of the DeLone and McLean (2003) Model and the Wixom and Todd (2005) metrics and instrument. The measurement metrics of the DeLone and McLean (2003) Success Model requires multiple questions for each variable. The multiple questions and the use of factor analysis ensure reliable results (Seddon & Kiew, 1996). The Wixom and Todd (2005) instrument used to develop the survey provided a Cronbach Alpha of equal to or greater than 0.8 on each construct. The survey in this study provided similar results with the Cronbach Alpha of equal to or over 0.8. The factor coefficients provided by the previous survey by Wixom and Todd (2005) and the survey in this study showed repeatability of results and accuracy of the measurement.

6. Discussion and Conclusion

The purpose of this ex post facto study was to evaluate an information security system for small business using the DeLone and McLean (2003) Updated Success Model. The model uses variable relationships to show success of an information system. Four relationships defined those variable pathways. Quantitative methods evaluated the four possible pathways defined by the DeLone and McLean (2003) Model.

6.1. Study Description and Scope

The study included several limiting factors. The first factor was the number of participants. In a total population of small businesses in six states, 73 participants were a small representation. The response rate of less than 5% was below the expected levels. The use of PLS regression attempted to overcome this limitation because only small samples sizes are necessary. The study design limited the ability to manipulate variables. The non-experimental ex post facto methodology required users to remember experiences. Depending on timing, memories of security incidents, training, policies, and system usage may diminish. The focus on the small businesses in six southeastern states may limit the application of the results to the other 44 states. The instrument developed for broad use based on the DeLone and McLean (2003) model constructs should apply to any business in the United States. The small business information security system contains three widely used security methods applicable to small businesses throughout the United States.

The Small Business Information Security System. The PLS results reflected significant results on all pathway relationships within the model. The acceptance of all four hypotheses and the rejection of all four null hypotheses implied success of the information system in the DeLone and McLean (2003) Updated Success Model. The PLS R2 results demonstrated that computer-use policies, information security training, and virus and malware protection account for 62% of the influence on a positive use experience. The PLS R2 results demonstrated that a positive use experience accounts for 42% of the influence on no harm caused by security incidents. The PLS R2 results demonstrated influences outside the bounds of the study by other variables. The PLS R2 results provided evidence of significant influences from the small business information security system on no harm caused by security incidents.

6.2. Implications for Small Business

Small businesses need computers and the Internet to do simple tasks. These tasks include banking, ordering, sales, shipping, invoicing, payroll, and communications. Viruses, malware, hackers, spyware, and phishing are some of the security incidents that can bring business to a halt (Simmonds, 2017). The numbers and types of security vulnerabilities leave small businesses unprepared with outdated or ineffective protection (Simmonds, 2017). Often the small business responds only after the security incident occurs.

Small businesses need to invest in security information systems that provide, in return, protection from security incidents (Simmonds, 2017). Small businesses need an information security system that is affordable, easy to implement and use, and prevents harm by security incidents. A security system not used is like a lock on a door left open. A security system that does not prevent theft provides no security from security incidents. A security system must encourage use with a positive experience for the user. The use of

that security system must provide protection from security incidents for the user and the small business.

The small business information security system in this research was a combination of three strong but separate security components. Computer-use policies, implemented by the information technology department or the computer power-user, were the service quality component. Information security training, the information quality component, was specific training for users on security awareness, security vulnerabilities, and safe computer-use practices. Virus and malware protection, the system quality component, was software that comes from many different sources and contains various options and settings. Each of the three components indicated a positive relationship with the variable of positive use experience.

The comprehensive small business information security system contains a computer-use policy, information security training, and business virus and malware protection. This comprehensive security system requires use to create no harm by security incidents. The results of the study show that a positive use experience of this information security system influences the security incidents at the small business. The DeLone and McLean (2003) Updated Success Model, applied to the small business information security system in this study, implied use may reduce the harm caused by security incidents. For small business, the information security system is a reliable and affordable starting point. The separate security system components create vulnerabilities but used together can improve the information security of a small business.

6.3. Recommendations for Future Research

The limitations defined in this study provide opportunities for future exploration and research. This study focused on the six southeastern states of North Carolina, South Carolina, Georgia, Florida, Alabama, and Tennessee. To understand the application to other geographic areas, a wider study, including the entire United States, requires exploration. The types of small businesses and concerns for security and privacy may vary in other geographic areas. A demographic question on the region or state would assist in determining the areas surveyed and differences that may result.

Along with a larger target population, a larger sample would provide a stronger significance to the results. The Partial Least Squares (PLS) regression does not require a larger sample but correlation analysis does. The response rate of small businesses on security related questions may vary based on familiarity with the surveyor. A survey by a well-known group like the National Federation of Independent Businesses (NFIB) or the National Cyber Security Alliance (NCSA) could provide the trust and privacy factor that an individual surveyor lacks. Small businesses are hesitant to share information that may create risk or reveal private or confidential data.

This study focused on small businesses with under 100 employees and independent (non-franchised). The definition of small business varies with some including businesses with up to 500 employees. The larger size businesses will include more businesses with internal information technology personnel. This demographic requires measurement to determine if internal staff or an external consultant influences the success of this small business information security system in the larger diverse businesses. A study of larger corporations and global enterprises requires additional study with more demographic information.

Acknowledgements

I appreciate the UOPX College of Doctoral Studies including Mansureh Kebritchi, Ph.D., Dr. David Proudfoot, and Dr. Sandy Nunn. Their guidance and editing advice were instrumental. I appreciate the contributions of Dr. DeLone and Dr. McLean in creating the DeLone and McLean model of information systems success. The use of this model created a foundation for this study. I appreciate the contributions from Dr. Wixom and Dr. Todd in the survey foundation for this study. I appreciate the leadership of CSU Global for their support and encouragement to complete this article. I appreciate Dr. Frank Appunn who chaired my original dissertation committee. His knowledge of quantitative research provided guidance on analysis tools. He encouraged me to complete this research and finish my degree. (25-Apr-2020)

References

About the U.S. Chamber of Commerce. (2018). Retrieved from https://www.uschamber.com/about/about-the-us-chamber.

Barton, K., Tejey, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers and Security, 59*, 9-25. doi: 10.1016/j.cose.2016.02.007

Berry, C., & Berry, R. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management, 8*(1). doi: 10.1504/IJBCRM.2018.090580

Bock, G., Suh, A., Shin, K., & Hu, A. (2009). The factors affecting success of knowledge-based systems at the organizational level. *Journal of Computer Information Systems, 50*(2), 95-105.

Bonett, D., & Wright, T. (2000). Sample size requirements for estimating Pearson, Kendall and Spearman correlations. *Psychometrika, 65*(1), 23-28.

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud and Security, 2016*(6), 8-14. doi: 10.1016/S1361-3723(15)30046-4

Christmann, E., & Badgett, J. (2008). *Interpreting Assessment Data: Statistical Techniques You Can Use*. Arlington, VA: NSTA Press.

Clapper, D., & Richmond, W. (2016). Small business compliance with PCI DSS. *Journal of Management Information and Decision Sciences, 19*(1), 54-67.

Cooper, D., & Schindler, P. (2014). *Introduction to Business Research* (12th ed.). New York, NY: McGraw-Hill: Irwin.

DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems, 19*(4), 9-30.

DeLone, W., & McLean, E. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60-95.

Goodhue, D., Lewis, W., & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly, 36*(3), 981-1001.

Henseler, J., Ringle, C., & Sinkovics, R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20*, 277-319. doi: 10.1108/S1474-7979(2009)0000020014

Hoy, W., & Adam, C. (2016). *Quantitative Research in Education: A Primer* (2nd ed.). Thousand Oaks, CA: Sage Publications Inc.

Ifindo, P. (2018). Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal, 31*(1), 53-82. doi: 10.4018/IRMJ.2018010103

Lin, L. (2018). A detection and defense technology for information-stealing and deceitful trojan viruses based on behavioral features. *International Journal of Network Security, 20*(5), 983-987. doi: 10.6633/IJNS.201809 20(5).20

Marcoulides, G., Chin, W., & Saunders, C. (2009). A critical look at Partial Least Squares modeling. *MIS Quarterly, 33*(1), 171-175.

Mihirwe, J., & White, N. (2016). Cybersecurity awareness and practice of next generation corporate technology users. *Issues in Information Systems, 17*(2), 183-192. Retrieved from http://www.iacis.org/iis/2016/2_iis_2016_183-192.pdf.

Mora, M. (2019, August 12). *What is the right sample size for a survey*. Retrieved from http://relevantinsights.com/sample-size.

Nguyen, T. H., Newby, M., & Macaulay, M. J. (2015). Information Technology Adoption in Small Business: Confirmation of a Proposed Framework. *Journal of Small Business Management*, *53*(1), 207–227. doi: contentproxy.phoenix.edu/10.1111/jsbm.12058

Padilla, M., & Newton, M. (2011). *Bootstrap Reliability via Coefficient Alpha*. Washington, DC: American Psychological Association.

Patil, B. V., & Jadhav, R. J. (2015). Computer Virus and Antivirus Software –A Brief Review. *International Journal of Advancements in Management and Economics, 4*(2), 1-4. Retrieved from http://www.managementjournal.info/index.php/IJAME.

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: Models, dimensions, measures, and interrelationships. *European Journal of Information Systems, 17*, 236-263.

Petter, S., & McLean, E. (2009). A meta-analytic assessment of the DeLone and McLean IS success model: An examination of IS success at the individual level. *Information & Management, 46*, 159-166. doi: 10.1016/j.im.2008.12.006

Poelmans, S., Wessa, P., Milis, K., Bloemen, E., & Doom, C. (2008). Usability and acceptance of e-learning in statistics education, based on the compendium platform (Hogeschool-Universiteit Brussel). Retrieved from http://www.wessa.net/download/iceripaper1.pdf.

Rubin, A., & Babbie, E. (2016). *Essential research methods for social work* (4th ed.). Boston, MA: Cengage Learning.

Salkind, N. (2017). *Exploring research (9th ed.)*. Upper Saddle River, NJ: Pearson Education, Inc.

Seddon, P. (1997). A respecification and extension of the DeLone and McLean model of IS success. *Information Systems Research, 8*(3), 240-253.

Seddon, P., & Kiew, M. Y. (1996). A partial test and development of DeLone and McLean's model of success. *Australian Journal of Information Systems, 4*(1), 90-109.

Simmonds, M. (2017). How businesses can navigate the growing tide of ransomware attacks. *Computer Fraud & Security, 2017*(3), 9-12. doi: 10.1016/S1361-3723(17)30023-4.

Thakur, K., Shan, J., & Pathan, A. (2018). Innovations of phishing defense: The mechanism, measurement and defense strategies. *International Journal of Communication Networks and Information Security (IJCNIS), 10*(1), 19-27.

Wirth, A. (2017). *The economics of cybersecurity. Biomedical Instrumentation & Technology*, 52-59.

Wixom, B., & Todd, P. (2005). A theoretical integration of user satisfaction and technology acceptance. *Information Systems Research, 16*(1), 85-102.

Wixom, B., & Watson, H. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly, 25*(1), 17-41.