COMPUTERS & SECURITY 48 (2015) 267–280

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Measuring user satisfaction with information security practices

Gustavo Percio Zimmermann Montesdioca [*], *Antônio Carlos Gastaud Maçada* [1]

Universidade Federal do Rio Grande do Sul (UFRGS-Brazil), Rua Washington Luiz, 855, Porto Alegre, RS 90010-460, Brazil

ARTICLE INFO

Article history:
Received 27 July 2013
Received in revised form
2 October 2014
Accepted 23 October 2014
Available online 4 November 2014

Keywords:
User satisfaction
Security practices
Information security
Measurement
Expectation disconfirmation theory
Needs theory
Equity theory

ABSTRACT

Information security is a major concern of organizational management. Security solutions based on technical aspects alone are insufficient to protect corporate data. Successful information security depends on appropriate user behavior while using information systems. User satisfaction is widely used to measure the success of information systems. The objective of this research is to develop a model to measure user satisfaction with information security practices. An instrument was developed based on this model. A survey was conducted, and 173 valid responses were obtained. Structural equation modeling was used for the data analysis. The results indicated that users understand the benefits of information security practices, but the use of information systems with security controls is considered a complex matter, which reduces information systems productivity. The measurement of the user satisfaction with information security practices is a starting point to diagnose the behavior of users in relation to information security, providing metrics to management evaluate the investment in information security training and awareness program.

1. Introduction

Information security is a major concern of organizational management. Security solutions based on technical aspects alone are insufficient to protect corporate data. Studies indicate that successful information security can be achieved through a combination of technical and socio-organizational investments that consider the user as an active agent (Bulgurcu et al., 2010; Dhillon, 1999; Spears and Bakri, 2010; Stanton et al., 2004). One of the most relevant variables used to assess the success of information systems is user satisfaction (Delone and Mclean, 1992). Studies using this variable are important because they suggest that user satisfaction results in the use of the information system itself and simultaneously provides data for the investment decision-making process (Doll and Torkzadeh, 1988; Delone and Mclean, 1992).

Information systems produce significant benefits to organizations when the users learn and use all of the system capabilities. However, one risk of corporate system and data protection is the difficulty users may experience in understanding and executing the information security practices that are regulated by corporate security policies (Goel and

* *Corresponding author*. Tel.: +55 51 9328 4131.
E-mail addresses: gustavo.percio@ufrgs.br (G.P.Z. Montesdioca), acgmacada@ea.ufrgs.br (A.C.G. Maçada).
[1] Tel.: +55 51 9996 7657.
http://dx.doi.org/10.1016/j.cose.2014.10.015
0167-4048/

Chengalur-Smith, 2010). Users face pressures to increase productivity at work. Security practices may limit daily activities, forcing users to a choice between system functionality and information security practices (Besnard and Arief, 2004). Understanding the factors that measure user satisfaction with information security practices can help organizations improve information systems functionality, while keeping them safe.

The success of information security depends on appropriate user behavior while interacting with information systems. Investigating the cognitive factors that influence such behavior is important in designing an effective information security policy (Rhee et al., 2009). User satisfaction is widely used to evaluate the cognitive aspects behind the user's utilization of information systems (Au et al., 2008). User satisfaction can provide the data required to align information security policies with user information system needs.

The purpose of this paper is to develop a model to address this gap and measure user satisfaction with information security procedures while using information systems. This study can help security professionals and management with the design of information security policies that leverage the user experience with the information systems and provide data to aid decision making about information security investments. The measurement of the user satisfaction with information security practices is a starting point to diagnose the behavior of users in relation to information security, providing metrics to management evaluate the investment in information security training and awareness program.

This research began with a review of the literature on information security and user satisfaction. The information security review identified the information security management concepts, practices and behavioral factors used to integrate information security and user satisfaction. The user satisfaction review generated three theories of motivation that use satisfaction as an exogenous variable (expectancy disconfirmation theory, needs theory, and equity theory) and as user satisfaction constructs and measurement items. The research model, hypotheses, and instrument[2] were validated with data gathered from academics, information security specialists, researchers, and information systems corporate users. An instrument was developed based on this model. A survey was conducted, and 173 valid responses were obtained. Structural equation modeling was used for the data analysis. The results indicated that users understand the benefits of information security practices, but the use of information systems with security controls is considered a complex matter, which reduces information systems productivity.

Section 2 of this paper presents the conceptual background of user satisfaction and information security. Section 3 presents the research model and hypotheses. The research methods are presented in Section 4. Section 5 presents the results of the structural equation modeling. In Section 6, discussion, implications, and future work are presented. Section 7 presents the conclusion for the paper.

2. Background

2.1. *Information security*

Solutions based only on technology are not sufficient to guarantee the protection of organizational assets. Information security involves human beings that do not always act as they are supposed to while interacting with information systems (Aytes and Connolly, 2004). Therefore, understanding which factors motivate users to adopt security practices is fundamental to solving information security problems (Bulgurcu et al., 2010). Social rules and interactions in the workplace influence an individual's understanding of information security (Albrechtsen, 2007).

Successful implementation of information security practices requires support and leadership from management. Managers have the responsibility to formulate the strategy for protecting information assets, defining a budget that optimizes corporate information security, and minimizing damage caused by possible attacks (Anderson and Choobineh, 2008). Management uses information security policy to guide and control users' behavior, expressing the values and sets of instructions users must follow (Hedström et al., 2011). Information security management involves implementing policies, processes, and procedures to secure the organization, including the development of the soft skills necessary to manage the personal and social identities of users to meet business objective (Ashenden, 2008). Management efforts aim to teach users the importance of adopting information security practices that are aligned with information security policies (Thomson and Solms, 2005).

One dimension of information security practices is related to user behavior while utilizing information systems and, consequently, corporate data. Such practices involve conscious security behavior while using the information systems (Rhee et al., 2009). User attention to information security is associated with a combination of personal and organizational factors, such as satisfaction with support services, satisfaction with salary, satisfaction with colleagues, organizational commitment, technical knowledge, and emotional events (Stanton et al., 2004). Security practices do not always require technology; preventive behavior can protect information systems, such as choosing safe passwords, backing-up data regularly, and carefully handling files (Ng et al., 2009).

Aytes and Connolly (2004) considered the intention for adopting a secure behavior as a rational choice based on individual perceptions of the usability of security practices and the consequences for not using such practices. Users develop attitudes about information security through interlocking organizational, technological, and individual factors. These factors influence user behavior, affect motivations about work with information security practices, create conflict of interests between information system functionality and information security practices, and influence the effect of documentation and awareness campaigns on security behavior (Albrechtsen, 2007). User behavior is also explained through the concept of

[2] Research instruments are measurement tools designed to produce quantitative descriptions of some aspects of the study population by asking people structured and predefined questions. The measurement tool is a form of survey conducted to advance scientific knowledge (Pinsonneault and Kraemer, 1993).

bounded rationality, which involves the dilemma between maximizing information systems performance and following security practices. Users face security and usability trade-offs daily. Understanding where trade-offs exist can help in the design of information security policies that are compatible with the intuitive actions users perform during information system usage (Besnard and Arief, 2004).

2.2. User satisfaction

User satisfaction is possibly the most widely used measurement to evaluate the success of an information system. It has a high degree of face validity with reliable measurement instruments, and strong conceptual appeal compared to other success measures (Delone and Mclean, 1992). Bailey and Pearson (1983) noted that user satisfaction has its origins in psychology studies and involves the sum of feelings and attitudes toward several factors that affect users in their workplace. User satisfaction is defined as the extent to which the user believes the system satisfies their information needs, suggesting that information systems that attend to user needs reinforce their satisfaction (Ives et al., 1983). Au et al. (2008) defined user satisfaction as the affective and cognitive evaluation the user develops from a pleasant experience using an information system. This approach aims to understand the psychological processes surrounding information system performance and translate them into different levels of satisfaction or dissatisfaction for the user.

One weakness of user satisfaction research is the lack of theories to explain their relations (Khalifa and Liu, 2003). Landy and Becker (1987), Woodroof and Kasper (1998), and Au et al. (2008) noted the theories that use satisfaction as a dependent variable: 1) expectation disconfirmation theory, 2) needs theory, and 3) equity theory.

1) Oliver (1980) developed the expectation disconfirmation theory, which uses the disconfirmation paradigm to evaluate satisfaction. This theory suggests that the expectation creates a reference frame in which the individual makes a comparative judgment about product performance. Performance worse than the expected is classified as "below" in this reference frame, leading to a negative disconfirmation. Performance better than the expected is classified as "above" in this reference frame, which generates positive disconfirmation. Expectation and performance variables, therefore, influence user satisfaction (Oliver, 1980). Information systems research used this theory to evaluate user satisfaction in studies performed by Kettinger and Lee (2005), Venkatesh and Goyal (2010), Bhattacherjee (2001) and Liao et al. (2007).
2) The needs theory used in this paper is based on studies developed by Alderfer (1969), also known as the ERG theory. It states there are three basic needs that a human being seeks to fulfill: existence, relatedness, and growth (ERG) (Alderfer, 1969). Existence is related to all types of material and physiological needs, relatedness is about relationships with significant others, and growth involves creative and meaningful individual development. Research related to satisfaction employed this theory. For example, Scherf (1974) applied the needs theory to measure the relation between consumer satisfaction and relationship frustration. Chen et al. (2012) used this theory to verify the motivational mechanisms that assess job satisfaction. Chang and Yuan (2008) applied variables of this theory to develop a model for predicting customer behavior and anticipating system development.
3) The equity theory studies the perception of injustice and dissatisfaction in work environments. A relation of equity or inequity occurs when one part, the input, has an attribute and another part receives this attribute and returns an outcome. The perception of inequality, or injustice, appears when the individual perceives that the ratio of outcomes to inputs, compared to the ratio of another's outcomes and inputs, is unequal (Adams, 1965). The equity theory is used in the information system area in studies about software piracy (Douglas et al., 2007; Morton, 2004), information sharing (Ibragimova, 2006), adoption of technology (Hess et al., 2007), and user satisfaction with the information system (Joshi, 1992; Hess and Hightower, 2002).

The integration of these theories and their variables on user satisfaction research may provide more insights to explain the cognitive and psychological aspects that affect satisfaction. Table 1 shows the variables provided by each theory. These variables, used in the research model in Fig. 1, are explained in detail in the next section.

3. Research model and hypotheses development

Fig. 1 presents the model with the variables integrated. The model and research instrument are based on studies from Bailey and Pearson (1983), Doll and Torkzadeh (1988), Delone and Mclean (1992, 2002), Ives et al. (1983), Myers et al. (1997), Tafti (1995), Baroudi and Orlikowski (1988), Landy and Becker (1987), Woodroof and Kasper (1998), and Au et al. (2008). The research instrument is available in the Appendix.

Information system performance is defined as the perceived outcome from information systems use. Performance is one of the first attributes used for assessing user satisfaction (Au et al., 2008). The expectation disconfirmation theory provided this construct. Myers et al. (1997), Tafti (1995), and Au et al. (2008) found that information system performance is an antecedent of user satisfaction.

To formulate the first hypothesis and to integrate information system performance with information security, the trade-off concept of usability and security was used. Besnard and Arief (2004) and Albrechtsen (2007) proposed the dilemma of usability versus information security. The user

Table 1 – Variables provided by theories.

Theory	Author	Variables
Expectation disconfirmation theory	Oliver (1980)	Expectation Performance
Needs theory	Alderfer (1969)	Existence Relatedness Growth
Equity theory	Adams (1965)	Input–outcome ratio

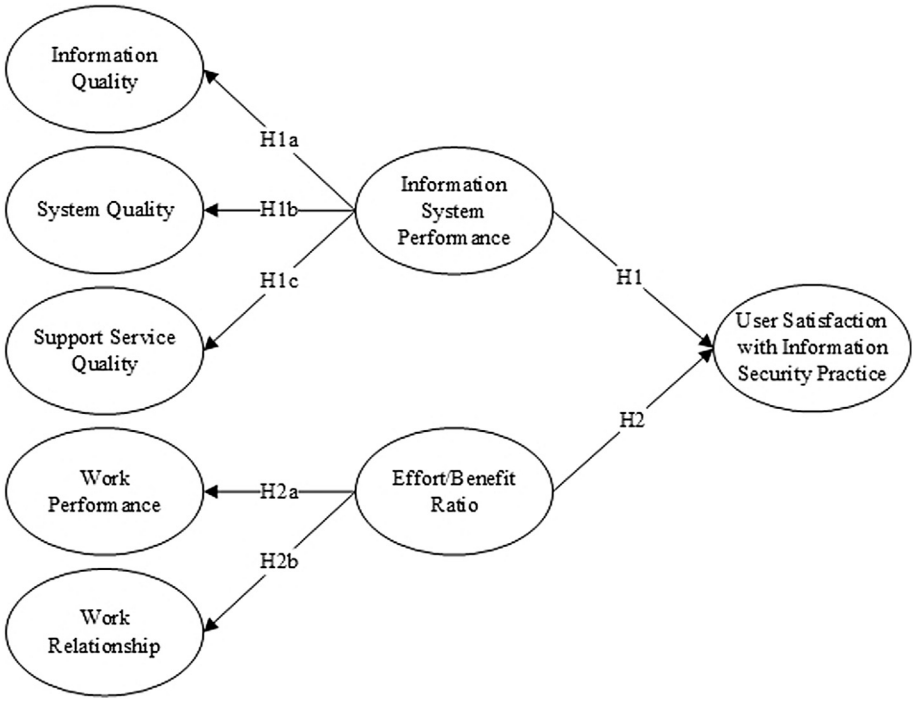

Fig. 1 – Research model.

intuitively tends to execute tasks with the best effort/benefit ratio. Considering that satisfaction is a cognitive process, if information security practices are complex, the user will encounter difficulties when using the information system. Such difficulties lead users to prioritize usability and functionality of the information system. Complex information security practices will be perceived as barriers and, consequently, will reduce user satisfaction with security practices. The following hypothesis is thus proposed:

H1: Information system performance is negatively related to user satisfaction with information security practices.

Delone and Mclean (1992, 2002) presented a success model, largely accepted in information systems literature, in which the quality dimension has a significant effect on user satisfaction. Three variables represent quality in the Delone–Mclean model: information quality, system quality, and support service quality. Other studies also found that the information system performance construct is measured by three quality variables (Myers et al., 1997; Tafti, 1995). Hence, the following hypotheses are proposed:

H1a: Information quality is positively related to information system performance;
H1b: System quality is positively related to information system performance;
H1c: Support service quality is positively related to information system performance.

The effort/benefit ratio construct, based on the input/outcome ratio of equity theory, aims at discovering the psychological processes that generate different levels of satisfaction and dissatisfaction (Au et al., 2008). Aytes and Connolly (2004) believed that user behavior related to information security is a rational choice based on the user's perception of the usefulness of the safe behavior and the consequences of not engaging in safe behavior. Albrechtsen (2007) found that information security practices are not perceived as restrictions on information system use and that the user is aware of the importance of information security to varying degrees. Users understand the benefit of information security, even with complex security practices, or they do not adopt the security practices. Hence, the following hypothesis is proposed:

H2: The effort/benefit ratio is positively related to user satisfaction with information security practices.

Alderfer (1969) developed a needs theory with three variables based on basic human needs. These variables were measurable in their essence. Au et al.'s (2008) study found the significance of existence and relatedness variables while measuring user satisfaction. Existence represents the satisfaction of needs that originate from the use of the information system that increases work efficiency. In this research model, the work performance variable represents existence. Relatedness are the user social needs that require interaction with significant others. The work relationship variable represents relatedness in this model. These variables measure the effort/benefit ratio to determine user satisfaction. Therefore, when the perceived benefits of security practices are greater than the efforts, it is probable that the user will be satisfied with such practices while using the information system. Hence, the following hypotheses are proposed:

H2a: *Work performance is positively related to the effort/benefit ratio;*
H2b: *Work relationship is positively related to the effort/benefit ratio.*

4. Research method

4.1. Population and sample

The research population was composed of the corporate information systems users in Brazilian organizations. Invitations were sent to 1.837 people from several regions in Brazil, primarily located in the states of Rio Grande do Sul and São Paulo. The invitation to answer the questionnaire was sent by email; it included a letter explaining the purpose of the research and instructions to access the questionnaire's electronic form.

There were 221 responses received, representing 12% of the population. However, it was necessary to remove 48 questionnaires because of the selection of identical options on the answer scale and outliers.[3] The final sample was composed of 173 questionnaires. The data collection for this study occurred from November 2012 to January 2013. Table 2 shows the sample characteristics.

As 51% of users on sample were originated from Information Technology sector, Student's *t*-test was used to evaluate if there were statistical difference between the response average on IT users and non-IT users (Hair et al., 2010). The results indicated no significant difference among the groups of users.

Table 2 – Characteristics of respondents.

Category	Measure	Number of cases	Percent
Gender	Female	31	17.9%
	Male	142	82.1%
Position	Director/Manager	52	30.1%
	Employee	95	54.9%
	Consultants and others	26	15.0%
Sector	Information Technology	89	51.4%
	Consulting	13	7.5%
	Telecommunications	8	4.6%
	Banks	9	5.2%
	Other	54	31.2%
Company size (number of employees)	Less than 100	54	31.2%
	100–1000	46	26.6%
	More 1000	73	42.2%

4.2. Research instrument

The research instrument is based on the model presented in Fig. 1. This model is composed of three main constructs: information system performance, effort/benefit ratio, and user satisfaction with information security practices. The first two constructs are endogenous second-order constructs and the last one is an exogenous first-order construct.

The information system performance construct, based on the expectation disconfirmation theory, is measured by information quality, system quality, and support service quality variables. Studies by Bailey and Pearson (1983), Ives et al. (1983), and Baroudi and Orlikowski (1988) categorized measurement items into similar categories. The research instrument is composed of nine items to measure information quality, six items to measure system quality, and seven items to measure support service quality. Table 3 presents the items comprising each variable and their source.

The effort/benefit ratio construct is based on equity theory. When users' benefits exceed the efforts required, the ratio is higher and higher satisfaction results. This construct is measured by two variables from needs theory. Alderfer (1969), Scherf (1974), Au et al. (2008), and Chen et al. (2012) measured satisfaction using a similar approach. The instrument designed for this research employed work performance (existence) and work relationship (relatedness) variables. For each variable in the questionnaire, a statement represented the benefit and items represented the effort. Each variable had four measurement items. Work relationship evaluated two benefits and used an identical two items to measure each benefit. Table 4 summarizes the items measured.

Finally, the user satisfaction with information system practices construct acts as an exogenous variable in the model. It is represented by four measurement items in the instrument. Table 5 presents the items measured.

The instrument had close-ended questions, and the interviewees selected answers from a seven-point Likert scale, where 1 represented the low value and 7 represented the high value.

4.3. Pretest and pilot study

The research instrument pretest was initially performed with information system professors to improve face validity. Three professors evaluated understanding, wording, and questionnaire layout in this phase. Next, three information security specialist were invited to evaluate the research instrument. As a result of these evaluations, five items were removed, seven items were reworded to increase understanding, and the questions were reordered. Finally, eleven information systems researchers were invited to access, read, and comment on the questionnaire's electronic form. The layout was then modified to improve the questionnaire's appearance.

A pilot study was performed with a group of information systems professionals. Six hundred and ninety people were invited by email to participate in the pilot study; 56 valid responses were received. The purification process employed statistical tests, such as Cronbach's alpha, Corrected Item-Total Correlation (CITC), within-block Exploratory Factor Analysis (EFA), and the KMO test, following the recommendations of Churchill (1979) and Hair et al. (2010). Table 6 presents the results.

The Cronbach's alpha index value for the entire instrument was 0.935, greater than the 0.700 recommended by Hair et al. (2010). The within-block EFA analysis indicated the need to

[3] Outlier are scores that are different from the rest. Outliers present scores with unusual distribution and standard deviations above the mean of all variables. Their pattern are unusual compared to the other samples and do not represent the phenomenon (Kline, 2011).

Table 3 – Research instrument: Information System Performance items.

Construct	Item	Source
Information quality	Accuracy	Bailey and Pearson (1983), Baroudi and Orlikowski (1988), DeLone and McLean (1992), Doll and Torkzadeh (1988), Ives et al. (1983), Au et al. (2008)
	Availability	Au et al. (2008)
	Reliability	Bailey and Pearson (1983), Au et al. (2008), Baroudi and Orlikowski (1988), Delone and Mclean (1992), Ives et al. (1983)
	Updatedness	Bailey and Pearson (1983), Delone and Mclean (1992), Ives et al. (1983), Au et al. (2008)
	Relevance	Bailey and Pearson (1983), Baroudi and Orlikowski (1988), Au et al. (2008), Delone and Mclean (1992), Ives et al. (1983);
	Timeliness	Bailey and Pearson (1983), Delone and Mclean (1992), Doll and Torkzadeh (1988), Ives et al. (1983), Au et al. (2008)
	Completeness	Bailey and Pearson (1983), Baroudi and Orlikowski (1988), Doll and Torkzadeh (1988), Ives et al. (1983), Au et al. (2008)
	Presentation	Delone and Mclean (1992), Doll and Torkzadeh (1988), Au et al. (2008)
	Accessibility	Doll and Torkzadeh (1988), Ives et al. (1983), Au et al. (2008)
System quality	Response time	Bailey and Pearson (1983), Delone and Mclean (1992), Au et al. (2008)
	Reliability	Bailey and Pearson (1983), Delone and Mclean (1992), Au et al. (2008)
	Functionality	Delone and Mclean (1992), Au et al. (2008)
	Flexibility	Bailey and Pearson (1983), Delone and Mclean (1992), Ives et al. (1983)
	User friendliness	Delone and Mclean (1992), Doll and Torkzadeh (1988), Ives et al. (1983)
	Ease of integration	Bailey and Pearson (1983), Delone and Mclean (1992), Ives et al. (1983), Au et al. (2008)
Service support quality	Promptness	Bailey and Pearson (1983), Au et al. (2008)
	Reliability	Au et al. (2008)
	Responsiveness	Bailey and Pearson (1983), Au et al. (2008)
	Technical competence	Bailey and Pearson (1983), Ives et al. (1983);
	Attitude	Bailey and Pearson (1983), Baroudi and Orlikowski (1988), Ives et al. (1983), Au et al. (2008)
	Keeps accurate records	Au et al. (2002)
	Provision of training course	Bailey and Pearson (1983), Baroudi and Orlikowski (1988), Ives et al. (1983), Au et al. (2008)

Table 4 – Research instrument effort/benefits ratio items.

Construct	Item	Source
Work performance	Time to learn to use the system	Au et al. (2008)
	Intellectual skills to learn to use the system	Au et al. (2008)
	Work pressure and stress	Au et al. (2008)
	Physical strain	Au et al. (2008)
Work relationship	Time to learn to use the system	Au et al. (2008)
	Work pressure and stress	Au et al. (2008)

Table 5 – Research instrument user satisfaction with information security practices items.

Construct	Item	Source
User satisfaction with information system practices	Satisfaction with information security	Spreng et al. (1996)
	Satisfaction with security training	Petter et al. (2008), Spears and Barki (2010)
	Satisfaction with security policies	Goel and Chengalur-Smith (2010)
	Overall information security satisfaction	Kim et al. (1998), Spreng et al. (1996)

Table 6 – Pilot study results.

Factor	Number of indicators	Cronbach's alpha	CITC	Eigenvalues	% Explained variance	KMO	Bartlett's test
General satisfaction	4	0.950	0.809–0.941	3.485	87.1%	0.841	0.000
Information quality	9	0.967	0.816–0.904	7.173	79.7%	0.919	0.000
Quality of the system	5 (after removal of 1 item)	0.888	0.584–0.798	3.470	69.4%	0.803	0.000
Support service quality	7	0.954	0.750–0.913	5.508	78.7%	0.901	0.000
Performance at work	4	0.828	0.567–0.739	2.658	66.5%	0.729	0.000
Relationship at work	4	0.931	0.819–0.831	3.319	83.0%	0.744	0.000

exclude one item from the system quality variable because of the formation of two factors. After the removal of this item, the within-block EFA presented only one factor. The pilot study resulted in an instrument composed of six first-order factors and 33 indicators.

4.4. *Quantitative data analysis*

The data analysis employed covariance-based structural equation modeling (SEM) to evaluate the model unidimensionality, following Koufteros' (1999) paradigm for SEM and Koufteros et al.' (2009) paradigm for second-order models. The concepts of Hair et al. (2010), Byrne (2009), and Kline (2011) were also employed to support the SEM analysis. The statistical treatment of the data was performed with SPSS (Statistical Package for the Social Sciences) version 21.0 and AMOS (Analysis of Moment Structure) version 21.0.

5. Results

The sample analysis began with the evaluation of the influence of outliers, multicolinearity, normality, linearity, and homoscedasticity, as suggested by Kline (2011). These analyses detected the strong presence of outliers, leading to removal of these cases from the sample database. No other influences on the sample were found. The final sample for the analysis had 173 respondents.

5.1. *Measurement model*

The measurement model analysis followed Koufteros (1999) paradigm for SEM and Koufteros et al. (2009) paradigm for second-order models. Koufteros et al. (2009) recommended the evaluation of four alternative measurement models when second-order constructs exist. The first model considers all indicators tied to one first-order construct; the second model hypothesizes each first-order construct, with its own indicators, uncorrelated (orthogonal); the third model is similar to the second model, but evaluates correlated first-order constructs; and the fourth model considers complete second-order constructs. The goodness of fit indices for adequacy were calculated for each measurement model to compare them and determine the best model. Table 7 shows the results.

The selection of the best measurement model resulted from the comparison of the goodness of fit indices of each hypothesized measurement model and the theoretical specifications. The measurement model with the best goodness of fit indices is not necessarily the best alternative to represent a theoretical model (Koufteros et al., 2009). Therefore, measurement model 4 was selected because of the theoretical specification and for its indices performance compared to the other models hypothesized.

The goodness of fit indices of measurement model 4, however, indicated a low performance, which may compromise the evaluation of the research hypotheses. To improve the indices performance of the measurement model 4, standardized residual and modification indices tables were analyzed to identify problematic measurement items, as indicated by Hair et al. (2010) and Byrne (2009). Eight indicators were removed from the measurement model: three from the information quality variable, two from the system quality variable, one from the support service quality variable, one from the work performance variable, and one from the work relationship variable. Table 8 presents the goodness of fit indices and confirmatory factor analysis (CFA) of the final measurement model.

The Koufteros (1999) paradigm was used for the CFA evaluation of the measurement model 4. The results in Table 8 suggest convergent validity, as *t*-values are greater than |2| and R^2 is greater than 0.500 (Koufteros, 1999; Hair et al., 2010). The goodness of fit indices indicate a good performance. The analysis of standardized residuals in the final measurement model suggests unidimensionality, as none of the pairs presented values greater than |2.58| (Hair et al., 2010).

The discriminant validity analysis was not performed because of the existence of second-order factors. Koufteros et al. (2009) indicated that convergent validity is more relevant than discriminant validity when models have second-order factors. The convergent reliability is assessed through analysis of composite reliability and AVE of first-order variables (Koufteros et al., 2009). The composite reliability and AVE are greater than the recommended limits of 0.700 and 0.500 (Table 8), respectively, which suggests reliability for the final measurement model.

5.2. *Structural model*

The final step in the structural equation modeling is the structural model analysis (Hair et al., 2010; Koufteros, 1999). Based on the measurement model 4, path analysis was performed to verify the hypotheses proposed for the conceptual model of this research. The structural relationships between the endogenous and exogenous variables replaced the covariance links. Fig. 2 presents the model. Table 9 shows the statistical results.

The results of the path analysis are significant for the two main constructs: information system performance ($p < 0.05$)

Table 7 – Goodness of fit indices for mensuration models.

Indices	Reference values	Model 1	Model 2	Model 3	Model 4
Chi-squared/degrees of freedom (χ^2/df)	≤3.000	4.066	3.341	2.347	2.330
Comparative fit index (CFI)	≥0.900	0.761	0.817	0.898	0.897
Normed-fit index (NFI)	a	0.708	0.758	0.835	0.834
Non-normed fit index (NNFI)	a	0.744	0.804	0.887	0.889
Standardized root mean square (SRMR)	≤0.050	0.0754	0.3218	0.0432	0.0538

[a] Values close to 1.00 indicate better adjustment.

Table 8 – Confirmatory factorial analysis and model fit.

Construct [AVE] (Composite reliability)	Indicators	Non-standardized coefficient		Standardized coefficients	t-Value[b]	R^2
		Factorial weight	Standard errors			
Information quality	IQ1	0.973	0.064	0.846	15.210	0.716
(0.788)	IQ3	1.094	0.067	0.878	16.256	0.771
[0.946]	IQ4	1.050	0.060	0.914	17.636	0.836
	IQ5	1.061	0.059	0.919	17.981	0.844
	IQ6	0.961	0.057	0.894	16.978	0.800
	IQ8	1.000	a	0.872	a	0.760
System quality	SQ1	1.111	0.084	0.882	13.212	0.777
(0.727)	SQ3	1.175	0.084	0.921	13.953	0.848
[0.886]	SQ4	1.000	0.083	0.811	12.120	0.658
	SQ5	1.000	a	0.791	a	0.626
Service support quality	SSQ1	1.187	0.094	0.894	12.665	0.798
(0.749)	SSQ2	1.220	0.099	0.869	12.268	0.754
[0.931]	SSQ3	1.230	0.093	0.922	13.174	0.850
	SSQ4	1.205	0.092	0.915	13.162	0.838
	SSQ5	1.084	0.093	0.825	11.634	0.680
	SSQ7	1.000	a	0.756	a	0.571
Work performance	WP1	1.090	0.103	0.852	10.618	0.726
[0.675]	WP2	1.015	0.094	0.858	10.750	0.736
(0.808)	WP4	1.000	a	0.750	a	0.563
Work relationship	WR11	1.072	0.076	0.888	14.149	0.788
[0.764]	WR12	1.115	0.077	0.904	14.505	0.817
(0.906)	WR22	1.000	a	0.828	a	0.685
User satisfaction with information security practices	US1	0.835	0.049	0.841	17.069	0.708
	US2	0.983	0.056	0.850	17.467	0.722
[0.764]	US3	1.021	0.046	0.926	22.122	0.857
(0.939)	US4	1.000	a	0.943	a	0.890

Goodness of fit indices: $\chi^2/df = 1.911$; CFI = 0.940; NFI = 0.883; NNFI = 0.933; SRMR = 0.0508.

[a] Factorial weight arbitrarily fixed in 1.

[b] $p < 0.01$.

and effort/benefit ratio ($p < 0.05$). Table 10 shows the research hypotheses analysis.

6. Discussion

The purpose of this paper was to develop a model to measure user satisfaction with information security practices. An instrument based on information systems literature discussing user satisfaction and information security was developed and validated with structural equation modeling. The validation of the model and the research instrument demonstrated that the significant variables for this study were information quality, system quality, support service quality, work performance, and work relationship. These variables are part of the second-order constructs of information system performance and effort/benefit ratio, and they are related to user satisfaction with information security practices, as shown in Fig. 1.

Studies of user satisfaction with information systems present a high level of maturity, which allowed the development of significant measurement items and constructs. The conceptual model of Delone and Mclean (1992, 2002), for example, provided consistency on user satisfaction research related to the information systems field, supporting the usage of quality dimension in this model. The recurrent use of measurement items and constructs of user satisfaction research provides consistency and validity. Several aspects of the information system area had been measured in previous studies, but there is a gap in research regarding information security practices.

The studies of the socio-organizational aspects of information security are recent, particularly those that use quantitative methods. The lack of measurement items and constructs that are significant for information security is an issue that becomes apparent in the information security decision-making process (Goel and Chengalur-Smith, 2010). The development and reuse of quantitative metrics that support research on information security can increase the problem evaluation and decision making accuracy level.

The model validation process allowed for the evaluation of the proposed research hypotheses. The hypothesis H1 demonstrated a negative relation between information system performance and user satisfaction. Existing literature lacks quantitative research addressing the effects of security practices while users are interacting with information systems; this information is important because it substantiates the need to develop security policies that facilitate the utilization of information systems. User dissatisfaction with security practices can be a risk for information systems protection and, ultimately, represents a security threat for organizations. One way to change this negative relation may be through user participation in developing security practices. Spears and Barki (2010) affirmed that user participation in

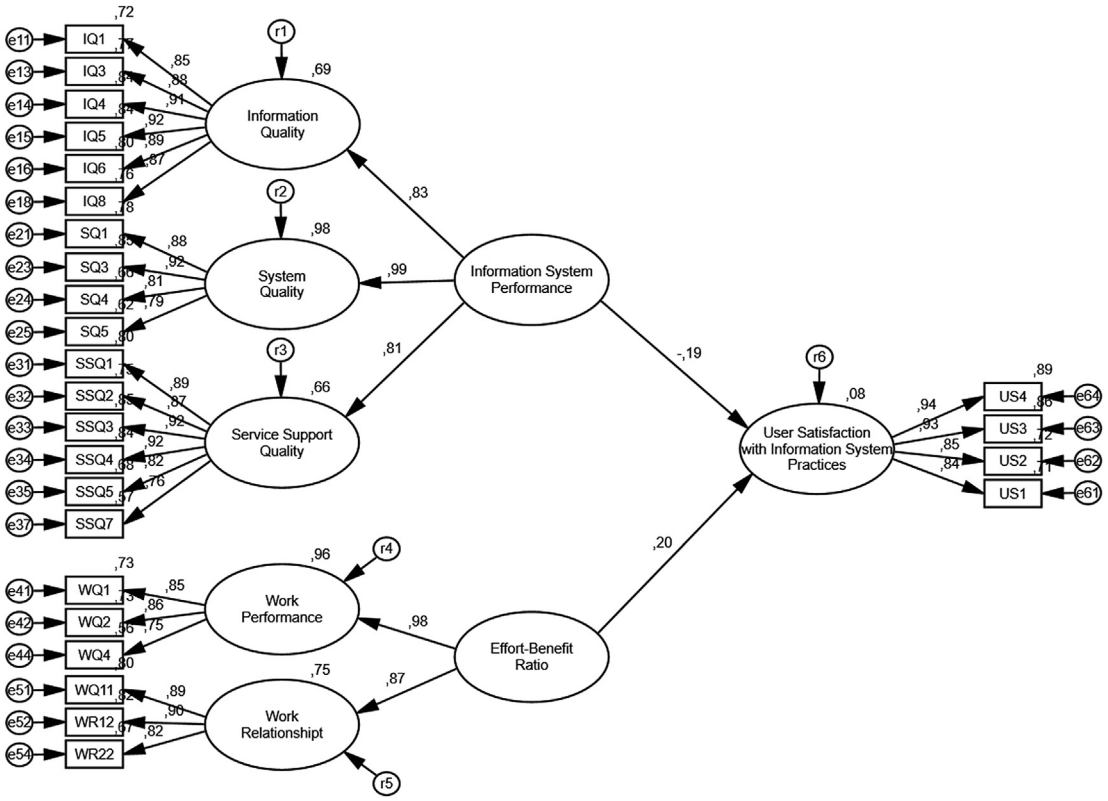

Fig. 2 – Structural model.

managing information security risks is one way to avoid security problems. The development of consistent policies, combining user and organization needs, and effectively involving the people interacting with the information systems can stimulate the adoption of security behaviors (Johnston and Warkentin, 2010). Training users on the use of information systems shortcuts can increase productivity while maintaining information security.

The hypotheses evaluating the relation of information system performance with the variables of information quality (H1a), system quality (H1b), and support service quality (H1c) were supported. This reinforces the relation of the quality dimension on user satisfaction studies and indicates validity when evaluating user satisfaction with information security practices. The importance of these variables to user satisfaction research were indicated by Myers et al. (1997), Tafti (1995), Au et al. (2008), Delone and Mclean (1992, 2002), Ives et al. (1983), and Baroudi and Orlikowski (1988), and these variables are now validated for the information security field.

The hypothesis H2, which evaluated the relation of the effort/benefit ratio with user satisfaction with information security practices, was supported. This construct evaluated the benefits received by the user compared to the necessary effort required to use the information system with security practices. Because security is viewed as inconvenient, as noted by Ng et al. (2009), this result suggests that users perceived a benefit in the information security practices,

Table 9 – Structural model statistics.

Structural relationship	Non-standardized coefficient		R^2	*t*-Values	*p*[a]
	Factorial weight	Standard errors			
IQ ← DSI	1.274	0.116	0.691	11.021	0.001
SSQ ← DSI	1.404	0.121	0.976	11.615	0.001
SQ ← DSI	1.029	0.109	0.664	9.404	0.001
WP ← REB	1.061	0.196	0.960	5.412	0.001
WR ← REB	0.963	0.172	0.748	5.608	0.001
US ← DSI	−0.291	0.12	0.037	−2.415	0.016
US ← RBE	0.306	0.124	0.041	2.469	0.014

R^2 of the SG factor = 0.08.
Goodness of fit indices: $\chi^2/df = 1.909$; CFI = 0.940; NFI = 0.883; NNFI = 0.933; SRMR = 0.0528.
[a] Significance.

Table 10 – Analysis of research hypotheses.

Hypotheses	Results
H1: Information system performance is negatively related to user satisfaction with information security practices.	$p < 0.05$ (supported)
H1a: Information quality is positively related to the information system performance.	$p < 0.01$ (supported)
H1b: System quality is positively related to the information system performance.	$p < 0.01$ (supported)
H1c: Service support quality is positively related to information system performance.	$p < 0.01$ (supported)
H2: Effort/benefit ratio is positively related to the user satisfaction with information security practices.	$p < 0.05$ (supported)
H2a: Work performance is positively related to the effort/benefit ratio.	$p < 0.01$ (supported)
H2b: Work relationship is positively related to the effort/benefit ratio.	$p < 0.01$ (supported)

leading to the conclusion that they understand the importance of such practices. The hypothesis H2a that proposed work performance is related to the effort/benefit ratio construct, and H2b, which related the work relationship with the effort/benefit ratio, were also supported.

These results are important because they provide a theoretical background to user satisfaction research, which is necessary to establish consistency in these studies. The evidence of the perceived benefits of information security practices compared to efforts supports management initiatives that increase the usage of security practices. Most of practices performed by users are not time-consuming, e.g., locking the computer when absent from it; password etiquette; safe and secure use of e-mail; cautious use of the Internet; and avoidance of software for file sharing (Albrechtsen, 2007). Management can provide training on security practices and promote effective awareness campaigns. The formation of an information security culture may reduce problems confronted by companies and losses from security problems.

6.1. *Academic and managerial contributions*

From an academic point-of-view, this research provides a conceptual model and a research instrument that relates information security and user satisfaction. The research model explains the relations between the measurement items and the constructs used in the research instrument. The variables selected to measure user satisfaction with information security practices were validated and a reliable research instrument is provided to literature.

The socio-organizational security studies are recent, particularly because of the technical nature of information security. Therefore, quantitative studies that evaluate the behavioral aspects of information security are important to enhance the understanding of this subject. Instruments that are consistent and repeatable are also an important contribution to academia, and it is expected that they will be used in future research.

From the managerial perspective, a known problem for information security decision making is the lack of measurement items that can help management. Quantitative research about user satisfaction with information security practices can help identify problems on information security practices and indicate changes necessary to increase their effectiveness. Applying this study to a specific organization can identify gaps and contribute to the formulation of security policies aligned with user and organizational security needs. Finally, the quality of investments in information security may also be evaluated through the data generated from such research.

6.2. *Limitations and future work*

This study was conducted with information systems corporate users from multiple organizations, and most respondents worked in information technology, which can limit the generalization of conclusions. The sample size was another limitation of this research. The participation index was 12%. In addition, this research was a cross-sectional study, that is, the data analysis was based on one single moment. This limitation is of importance in studies that evaluate user satisfaction because expectation, one of the variables in the expectation disconfirmation theory, cannot be evaluated.

Future work can apply this research instrument to a single company to evaluate how variables relate and analyze the data gathered. This research instrument can also be applied to larger samples, which will allow a more accurate study of the effects among model constructs.

7. Conclusion

The development of studies on information security behavior is important for increasing knowledge of this subject. The results presented in this study provide an important contribution to related information security studies. The model development aggregates concepts and theories that helps clarify the effects of security practices on user satisfaction. The application of these concepts and theories provides a strong background to build a research instrument, contributing to academic and managerial areas.

Whereas information security behavioral studies using quantitative data are only beginning, information security can generate financial losses to people and organizations. These research results indicate that users understand the benefits of information security practices, which suggests that awareness programs are important instruments to promote security practices within organization. The education of user on security practices required during information systems use can enhance corporate security and is key to reduce security incidents.

Acknowledgments

The authors are grateful for the support provided by CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brazil) and CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico – Brazil). We would like to thank the editor senior editor and to the anonymous reviewers for the contributions and feedback during the review process.

Appendix

Final Research Instrument

User Satisfaction with Information Security Practices

	Strongly Disagree ←			Neutral			→ Strongly Agree
I am satisfied with the information security practices.	1	2	3	4	5	6	7
I am satisfied with the information security training.	1	2	3	4	5	6	7
I am satisfied with the information security policy.	1	2	3	4	5	6	7
Overall, I am very satisfied with information security.	1	2	3	4	5	6	7

Information System Performance – Information Quality

Considering the information security practices, evaluate how they affect information quality of corporate information systems.							
	Very Low ←			Neutral			→ Very High
Information security practices interfere with the accuracy of the information provided by the system.	1	2	3	4	5	6	7
Information security practices interfere with the reliability of the information provided by the system.	1	2	3	4	5	6	7
Information security practices interfere with the timeliness of the information provided by the system.	1	2	3	4	5	6	7
Information security practices interfere with the relevance of the information provided by the system.	1	2	3	4	5	6	7
Information security practices interfere with the presentation of the information provided by the system.	1	2	3	4	5	6	7

Information System Performance – System Quality

Considering the information security practices, evaluate how they affect system quality of corporate information systems.							
	Very Low ←			Neutral			→ Very High
Information security practices interfere with response time of the system.	1	2	3	4	5	6	7
Information security practices interfere with functionality of the system.	1	2	3	4	5	6	7
Information security practices interfere with flexibility of the system.	1	2	3	4	5	6	7
Information security practices interfere with user friendliness of the system.	1	2	3	4	5	6	7
Information security practices interfere with ease of integration with other systems.	1	2	3	4	5	6	7

Information System Performance – Support Service Quality

Considering the information security practices, evaluate how they affect support service quality of corporate information systems.							
	Very Low ←			Neutral			→ Very High
Information security practices interfere with promptness of the system service support.	1	2	3	4	5	6	7
Information security practices interfere with the reliability of the system service support.	1	2	3	4	5	6	7
Information security practices interfere with responsiveness of the system service support.	1	2	3	4	5	6	7
Information security practices interfere with technical competence of the system service support.	1	2	3	4	5	6	7
Information security practices interfere with the attitude of the system service support.	1	2	3	4	5	6	7
Information security practices interfere with provision of training courses on the system service support.	1	2	3	4	5	6	7

Effort/Benefits Ratio – Work Performance

For each statement about BENEFIT, evaluate EFFORT required to perform the task, indicating whether BENEFIT is smaller, fair or greater than the EFFORT.							
BENEFIT - Information systems add efficiency to my work.							
	Benefits are much less than input			Fair			Benefits are much more than input
EFFORT - Amount of time required to learn to use the system with information security practices.	1	2	3	4	5	6	7
EFFORT - Level of intellectual skills required to learn to use the system with information security practices.	1	2	3	4	5	6	7
EFFORT - Amount of physical effort required to use the system with information security practices.	1	2	3	4	5	6	7

Effort/Benefits Ratio – Work Relationship

For each statement about BENEFIT, evaluate EFFORT required to perform the task, indicating whether BENEFIT is smaller, fair or greater than the EFFORT.							
BENEFIT - Knowing how to use information systems effectively allows me to establish better relationships with colleagues and customers.							
	Benefits are much less than input			Fair			Benefits are much more than input
EFFORT - Amount of time required to learn to use the system with information security practices.	1	2	3	4	5	6	7
EFFORT - Level of intellectual skills required to learn to use the system with information security practices.	1	2	3	4	5	6	7
BENEFIT – Knowing how to use information systems effectively allows me to have more influence on my coworkers.							
EFFORT – Level of intellectual skills required to learn to use the system with information security practices.	1	2	3	4	5	6	7

REFERENCES

Adams J. Injustice in social exchange in advances in experimental social psychology. In: Berkowitz L, editor. Advances in experimental social psychology. New York: Academic Press; 1965. p. 267–99.

Albrechtsen E. A qualitative study of users' view on information security. Comput Secur 2007;26(4):276–89.

Alderfer C. An empirical test of a new theory of human needs. Organ Behav Hum Perform 1969;4(2):142–75.

Anderson E, Choobineh J. Enterprise information security strategies. Comput Secur 2008;27(1/2):22–9.

Ashenden D. Information security management: a human challenge? Inf Secur Tech Rep 2008;13(4):195–201.

Au N, Ngai E, Cheng T. A critical review of end-user information system satisfaction research and a new research framework. Omega – Int J Manag Sci 2002;30(6):451–78.

Au N, Ngai E, Cheng T. Extending the understanding of end user information systems satisfaction formation: an equitable needs fulfillment model approach. MIS Q 2008;32(1):43–66.

Aytes K, Connolly T. Computer security and risky computing practices: a rational choice perspective. J Organ End User Comput 2004;16(3):22–40.

Bailey J, Pearson S. Development of a tool for measuring and analyzing computer user satisfaction. Manag Sci 1983;29(5):530–45.

Baroudi J, Orlikowski W. A short-form measure of user information satisfaction: a psychometric evaluation and notes on use. J Manag Inf Syst 1988;4(4):44–59.

Besnard D, Arief B. Computer security impaired by legitimate users. Comput Secur 2004;23(3):253–64.
Bhattacherjee A. Understanding information systems continuance: an expectation-confirmation model. MIS Q 2001;25(3):351–70.
Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34(3):523–48.
Byrne B. Structural equation modeling with AMOS. Abingdon: Routledge Academic; 2009.
Chang L, Yuan S. Synthesized model of Markov chain and ERG theory for behavior forecast in collaborative prototyping. J Inf Technol Theory Appl 2008;9(2):45–63.
Chen Y, Park J, Park A. Existence, relatedness, or growth? Examining turnover intention of public child welfare caseworkers from a human needs approach. Child Youth Serv Rev 2012;34(10):2088–93.
Churchill G. A paradigm for developing better measures of marketing constructs. J Mark Res 1979;16(1):64–73.
Delone W, Mclean E. Information system success: the quest for the dependent variable. Inf Syst Res 1992;3(1):60–95.
Delone W, Mclean E. Information systems success revisited. In: Proceedings of the 35th Hawaii international conference on system sciences; 2002. p. 238–48.
Dhillon G. Managing and controlling computer misuse. Inf Manag Comput Secur 1999;7(4):171–5.
Doll W, Torkzadeh G. The measurement of end-user computing satisfaction. MIS Q 1988;12(2):259–74.
Douglas D, Cronan T, Behel J. Equity perceptions as a deterrent to software piracy behavior. Inf Manag 2007;44(5):503–12.
Goel S, Chengalur-Smith I. Metrics for characterizing the form of security policies. J Strateg Inf Syst 2010;19(4):281–95.
Hair J, Black W, Babin B, Anderson R. Multivariate data analysis. New Jersey: Prentice Hall; 2010.
Hedström K, Kolkowska E, Karlsson F, Allen J. Value conflicts for information security management. J Strateg Inf Syst 2011;20(4):373–85.
Hess T, Hightower R. Using equity theory to understand user satisfaction with ERP systems: extending and advancing the equity-implementation model. In: Proceeding of the 23rd international conference on information systems; 2002. p. 737–42.
Hess T, Joshi K, Mcnab A. An empirical investigation of the equity implementation model: an alternative lens for understanding technology adoption. In: Proceeding of the 13th Americas conference on information systems; 2007. p. 1–10.
Ibragimova B. The role of equity theory in knowledge sharing. In: Proceedings of the 12th Americas conference on information systems; 2006. p. 1714–9.
Ives B, Olson M, Baroudi J. The measurement of user information satisfaction. Commun ACM 1983;26(10):785–93.
Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q 2010;34(3):549–66.
Joshi K. A causal path model of the overall user attitudes toward the MIS function: the case of user information satisfaction. Inf Manag 1992;22(2):77–88.
Kettinger W, Lee C. Alternative scales for measuring information systems service quality. MIS Q 2005;29(4):607–23.
Khalifa M, Liu V. Determinants of satisfaction at different adoption stages of Internet-based services. J Assoc Inf Syst 2003;4(5):206–32.
Kim C, Suh K, Lee J. Utilization and user satisfaction in end-user computing: a task contingent model. Inf Resour Manag J 1998;11(4):11–24.
Kline R. Principles and practice of structural equation modeling. New York: Guilford; 2011.
Koufteros X, Babbar S, Kaighobadi M. A paradigm for examining second-order factor models employing structural equation modeling. Int J Prod Econ 2009;120(2):633–52.
Koufteros X. Testing a model of pull production: a paradigm for manufacturing research using structural equation modeling. J Oper Manag 1999;17(4):467–88.
Landy F, Becker W. Motivation theory reconsidered. Res Organ Behav 1987;9(1):1–38.
Liao C, Chen J, Yen D. Theory of planning behavior (TPB) and customer satisfaction in the continued use of e-service: an integrated model. Comput Hum Behav 2007;23(6):2804–22.
Morton N. Understanding attitudes toward online music piracy. In: Proceedings of the 10th Americas conference on information systems; 2004. p. 402–6.
Myers B, Kappelman L, Prybutok V. A comprehensive model for assessing the quality and productivity of the information systems functions: toward a theory for information systems assessment. Inf Resour Manag J 1997;10(1):6–25.
Ng B, Kankanhalli A, Xu Y. Studying users' computer security behavior: a health belief perspective. Decis Support Syst 2009;46(4):815–25.
Oliver R. A cognitive model of the antecedents and consequences of satisfaction decisions. J Mark Res 1980;17(4):460–9.
Petter S, Delone W, Mclean E. Measuring information systems success: models, dimensions, measures, and interrelationships. Eur J Inf Syst 2008;17(3):236–63.
Pinsonneault A, Kraemer K. Survey research methodology in management information systems: an assessment. J Manag Inf Syst 1993;10(2):75–105.
Rhee H, Kim C, Ryu Y. Self-efficacy in information security: its influence on end users' information security practice behavior. Comput Secur 2009;28(8):816–26.
Scherf G. Consumer dissatisfaction as a function of dissatisfaction with interpersonal relationships. J Appl Psychol 1974;59(4):465–71.
Spears J, Barki H. User participation in information systems security risk management. MIS Q 2010;34(3):503–22.
Spreng R, MacKenzie S, Olshavsky R. A re-examination of the determinants of consumer satisfaction. J Mark 1996;60(3):15–32.
Stanton J, Mastrangelo P, Stam K, Jolton J. Behavioral information security: two end user survey studies of motivation and security practices. In: Proceedings of the 10th Americas conference on information systems; 2004. p. 1–7.
Tafti M. User satisfaction with information systems: a research framework. In: Carey J, editor. Human factors in information systems: emerging theoretical bases. Norwood: Ablex Publishing Corporation; 1995. p. 223–35.
Thomson K, Solms R. Information security obedience: a definition. Comput Secur 2005;24(1):69–75.
Venkatesh V, Goyal S. Expectation disconfirmation and technology adoption: polynomial modeling and response surface analysis. MIS Q 2010;34(2):281–303.
Woodroof J, Kasper G. A conceptual development of process and outcome user satisfaction. Inf Resour Manag J 1998;11(2):37–43.

Gustavo Percio Zimmermann Montesdioca received the degree of M.Sc. in Management Information Systems from the Universidade Federal do Rio Grande do Sul (UFRGS) in 2013. He is currently working on his PhD at same university in MIS area. He earned CISSP certification in 2008 and PMP certification in 2010, and have been working on information security field last 10 years. His research interests include information security, human behavior, and information management.

Antônio Carlos Gastaud Maçada is a Professor of Management Information Systems in the School of Management at Universidade Federal do Rio Grande do Sul (UFRGS), Brazil. He earned his PhD in Management Information System from UFRGS in 2001. His main research fields include information management, information governance, management information system, knowledge management and supply chain management.