JISTEM - Journal of Information Systems and Technology Management
Revista de Gestão da Tecnologia e Sistemas de Informação
Vol. 13, No. 3, Set/Dez., 2016 pp. 479-496
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752016000300007

WHAT INFLUENCES INFORMATION SECURITY BEHAVIOR? A STUDY WITH BRAZILIAN USERS

Rodrigo Hickmann Klein
Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, Brasil
Edimara Mezzomo Luciano
Programa de Pós-Graduação em Administração Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, Brasil

ABSTRACT

The popularization of software to mitigate Information Security threats can produce an exaggerated notion about its full effectiveness in the elimination of any threat. This situation can result reckless users behavior, increasing vulnerability. Based on behavioral theories, a theoretical model and hypotheses were developed to understand the extent to which human perception of threat, control and disgruntlement can induce responsible behavior. A self-administered questionnaire was created and validated. The data were collected in Brazil, and complementary results regarding similar studies conducted in USA were found. The results show that there is an influence of information security orientations provided by organizations in the perception about severity of the threat. The relationship between threat, effort, control and disgruntlement, and the responsible behavior towards information security was verified through linear regression. The results also point out the significant influence of the analyzed construct on Safe Behavior. The contributions involve relatively new concepts in the field and a new research instrument as well. For the practitioners, this study highlights the importance of Perceived Severity and Perceived Susceptibility in the formulation of the content of Information Security awareness guidelines within organizations. Moreover, users' disgruntlement with the organization, colleagues or superiors is a factor to be considered in the awareness programs.

Keywords: Information Security; Safe Behavior; Users' behavior; Brazilian users; threats

Manuscript first received/Recebido em: 26/07/2015 Manuscript accepted/Aprovado em: 07/12/2016
Address for correspondence / Endereço para correspondência

Rodrigo Hickmann Klein, Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, Brasil Mestre e Doutorando em Administração, Programa de Pós-Graduação em Administração Pontifícia Universidade Católica do Rio Grande do Sul E-mail: rodrigo.hickmann@acad.pucrs.br

Edimara Mezzomo Luciano, Programa de Pós-Graduação em Administração Pontifícia Universidade Católica do Rio Grande do Sul, Rio Grande do Sul, Brasil , Professora Titular da Faculdade de Administração, Contabilidade e Economia, Membro Permanente do Programa de Pós-Graduação em Administração E-mail: eluciano@pucrs.br

Published by/ Publicado por: TECSI FEA USP – 2016 All rights reserved

1. INTRODUCTION

The popularization of software intended to mitigate threats to Information Security has given users a sensation that software and hardware are enough to reduce Information Security breaches and suppress threats. This mistaken sensation may have originated from obtaining partial information on the subject or from the lack of adequate awareness (Liang and Xue, 2009) and also negligence, apathy, mischief, and resistance (Safa, Von Solms and Furnell, 2015), This is a human factor that might increase vulnerabilities provided it could influence Information Systems (IS) users to behave recklessly (Liginlal, Sim and Khansa, 2009). Human aspects of information security remain a critical and challenging component of a safe and secure information environment

However, this misconception alone does not explain breaches in Information Security caused by human factors. Another important insight is the efforts perceived as necessary to achieve the responsible behavior, which added to aspects such as indifference to the guidelines and human error may also induce vulnerability and breaches. Information Security refers to the protection of organizational assets from loss, undue exposure and damage (Dazazi et al., 2009). This concern has been gaining ground and popularity in recent decades due to IT artifacts that have gradually enabled the generation, processing and ubiquity of unprecedented information and have also fostered the possibility of threats (King and Raja, 2012).This article investigates the impact of user behavior on Information Security vulnerabilities. The study is grounded in user perceptions related to threats, control, and the effort to behave responsibly. Vance, Siponen and Pahnila (2012) conceptualize the vulnerability as the probability of an unwanted incident occurring if no measures are taken to prevent it. Roratto and Dias (2014) define vulnerability as a weakness in the computer system or its surroundings, which can become a security risk.

According to Kjell (2015), the organizations choose optimal defense, which is costly and consists in investing in Information Technology Security to protect their assets. Simultaneously, hackers collect information in various manners, and attempt to gain access to organizations' information security breaches, collected by the organizations themselves.

Albrechtsen and Hovden (2009) consider the users to be a liability when they do not possess the necessary skills and knowledge, thereby causing the reckless use of network connections and information or practicing unsafe acts within the organization. User perceptions may be enhanced through Security Education, Training, and Awareness (SETA) programs, which explain potential threats facing the organization and provide methods for users to improve information security practices (D'Arcy et al. 2009).

However the perception of threat is not the only thing that encourages responsible behavior provided the threat imminence perception varies from individual to individual. The effort required for responsible behavior and the relative perception of control in addition to the mitigating factors of responsible behavior that result from the context experienced by the individual are also based on individual perception. When threats are not perceived as eminent, the efforts to follow rules and best practices in Information Security may be considered unnecessary unproductive and merely a regulatory formality (Herath and Rao 2009a). In this circumstance the procedures that provide Information Security may be unsuccessful or circumvented depending on the individual perception about the balance of control/punishment and benefits. Furthermore, the disgruntlement of a user with organizations or people who set standards may produce actions that circumvent security either as a means of demonstrating their discontent (Willisom and Warkentin 2013) or simply through low motivation to comply with them (Kelloway et al. 2010).

Da Veiga and Eloff (2010) argue that the Information Security approach in an organization should be focused on employee behavior, provided that success or failure on protecting information depends on what employees do or don't do. So the way users behave may stem from perceptions about perceived threats, controls and punishments and about perceived effort as well as environmental factors such as work overload, fatigue (Kraemer and Carayon, 2007) and disgruntlement (Willison and Warkentin, 2013; Kelloway et al., 2010). These factors may contribute to behaviors that generate vulnerability and breaches, compromising all the Information Security principles and turning information into useless pieces of data due to their loss of reliability.

Based on the concepts addressed, this article aims to identify the influence of the user's perception of the threat, control, effort and disgruntlement in safe behavior regarding Information Security.

This introduction shows the subject, research problem and goal. The theoretical basis is presented in Section 2, followed by the research model and hypotheses (Section 3). The methodological aspects are presented in Section 4, followed by the results (Section 5) and the discussion of the findings (Section 6).

2. THEORETICAL BACKGROUND

According to Liang and Xue (2010) the perceived threat is defined by the degree in which an individual perceives a malicious IT attack as dangerous or harmful. IT users develop threat perception, monitoring their computing environment and detecting potential dangers. Based on health psychology and risk analysis, the authors suggest that the perception of threat is formed by perceived susceptibility and perceived severity.

Perceived susceptibility is defined by Liang and Xue (2010) as the subjective probability of an individual that a malicious IT attack (*malware*) will adversely affect it. On the other hand, the perceived severity is defined as the degree to which an individual perceives that adverse effects caused by *malware* will be severe. According to the authors, previous studies on health protection behavior have provided a theoretical and empirical foundation on careful behavior among patients, influenced by perceptions related to the threat, which can be adapted to Information Security. The authors argue that the perceived likelihood and the negative consequences of the severity of a disease may result in the perception of a health threat, which motivates people to take measures to protect their health.

The threat assessment may cover the perceived severity of a violation (Herath and Rao (2009a) or the perceived likelihood of a security breach (2009b). The severity is the level of potential impact the threat and damage may cause, i.e., the severity of a security breach and the possibility of an adverse event caused by such (Vance, Siponen and Pahnila, 2012). Herath and Rao (2009b) found that the perception of the severity of the breach does not impact on the compliance of regulations or security policies. In contrast, Workman, Bommer and Straub (2008) found that the perceived severity was significant for compliance, as well as the likelihood of a security breach. Johnston and Warkentin (2010) found indications that perceptions regarding the severity of a threat negatively influence the perceptions regarding the response effectiveness and also regarding the perceptions of the self-efficacy related to the threat.

Several authors have studied the perception of susceptibility. Ng, Kankanhalli and Xu (2009) have demonstrated that perceived susceptibility affects users' behavior regarding emails. According to the authors, when users are aware of the likelihood of threats (perceived susceptibility) and of the effectiveness of security controls (perceived benefits), they may make a conscious decision to behave appropriately. However, perceived severity was not decisive in influencing the users' safe behavior. The research of Johnston and Warkentin (2010) was not able to demonstrate that perceived susceptibility of threats negatively influences the perceived efficacy of response, or that the perceived susceptibility of threats negatively influences the perception of self-efficacy. However, they demonstrated that perceived severity of the threat negatively influences perceived efficacy of response and the perceptions of self-efficacy.

According to Herath and Rao (2009a), gaps are security breaches. Moreover employee negligence and non-compliance with the rules often causes damage to organizations. However the behavior of the users can help to reduce these gaps by following better practices, such as protecting data with suitable passwords or logging off when leaving the computer that is being used. Workman, Bommer and Straub (2008) show that perceived vulnerability and severity have an effect on users Information Security behavior.

Herath and Rao (2009b) suggest that perceptions regarding the severity of the breaches, the effectiveness of the response and self-efficacy are likely to have a positive effect on attitudes towards security policies, whilst the cost of response negatively influences favorable attitudes. They also suggest that social influence has a significant impact on intentions to comply with Information Security policies. The availability of resources is a significant factor in the increase of self-efficacy, which in turn is important to predict the intention to comply with Information Security policies. Moreover, organizational commitment plays a dual role, having a direct impact on intentions, as well as on promoting the belief that the actions of employees have a global effect on the Information Security of an organization.

Despite the difference between the results, the consensus among researchers is that users assess the susceptibility and the severity of negative consequences in order to determine the threat they are facing.

Apart from the use of technologies that aim to guarantee the organizational Information Security these technologies are not enough to avoid gaps because Information Security cannot be defined or understood as a pure technical problem (Kearney and Kruger, 2016). Based on that, studies about the Information Security users' behavior are obtaining more attention (Herath e Rao 2009b).

3. MODEL AND HYPOTHESES

The model (Figure 1) was developed based on the theoretical background exposed previously.

According to Ng, Kankanhalli and Xu (2009), the risks and damages perception in Information Security and its possibility of occurrence depend on the measurement capacity of individuals.

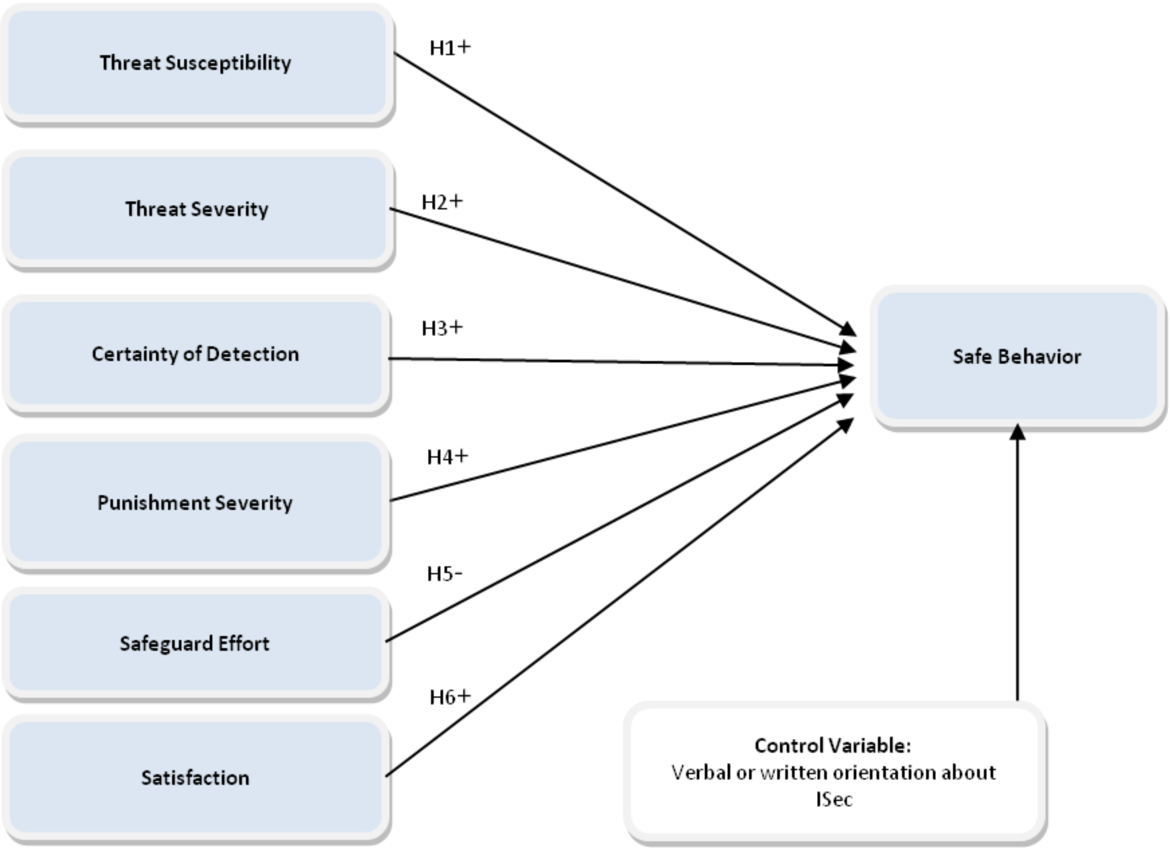

Figure 1 - Theoretical model and hypotheses

It covers the perception of susceptibility to the threat and the severity of the threat, because when individuals perceive a greater susceptibility to security incidents, they are likely to exhibit a higher level of safe behavior. Based on these concepts, the following hypothesis was formulated:

H1: The perceived susceptibility of the threat to Information Security positively influences safe behavior regarding Information Security.

Workman, Bommer and Straub (2008) found that the perceived severity was significant for compliance with Information Security Policy guidelines and for the likelihood of a security breach. For Liang and Xue (2009), the perceived severity is defined as the degree to which an individual perceives that negative consequences caused by *malware* will be severe. According to Ng, Kankanhalli and Xu (2009), when users are aware of the susceptibility and severity of the threats, they can make informed decisions to exercise adequate preventive behavior. Bearing these concepts in mind, the following hypothesis was formulated:

H2: The perceived severity of the threat to Information Security positively influences safe behavior regarding Information Security.

Herath and Rao (2009b), in their research on the effects of deterrence, found that the certainty of detection has a positive impact on the intentions to comply with the Security Policy guidelines. When employees perceive a high probability of being discovered violating the guidelines, they will be more likely to follow them. This concept produced the following hypothesis:

H3: The perception of the certainty of detection of not following the guidelines on Information Security positively influences safe behavior regarding Information Security.

Sanctions are defined as punishments, material or otherwise, incurred by an employee for failure to comply with information security policies (Bulgurcu, Cavusoglu and Benbasat, 2010). Examples of sanctions include demotions, loss of reputation, reprimands, financial or non-financial penalties, and unfavorable evaluations. The perception of these sanctions regarding non-compliance with the rules influences the user to behave responsibly, in accordance with the certainty of detection of non-compliance with the security standards, the severity and the swiftness of punishment (Herath and Rao, 2009a and 2009b). From the combination of these concepts the following hypothesis was formulated:

H4: The perception of the Punishment Severity for not following the guidelines regarding Information Security positively influences safe behavior in terms of Information Security.

According to Liang and Xue, 2009, the safeguard effort refers to physical and cognitive efforts - such as time, money, inconvenience and understanding - necessary for the safeguarding action. These efforts tend to create behavioral barriers and reduce the motivation for Safe Behavior regarding Information Security, due to the cost-benefit analysis. The authors cite the example of people's behavior regarding their health, when comparing the costs and benefits of a particular healthy behavior before deciding to practice it. If the costs are considered high when compared to the benefits, people are not likely to adopt the behavior recommended by health professionals. Thus, the user's motivation to avoid any Information Security threat may be mitigated by the potential cost to safeguard (Liang and Xue, 2010). According to these concepts the following hypothesis was developed:

H5: The perception of effort to safeguard when following the Information Security guidelines negatively influences safe behavior related to Information Security.

There is the possibility of breaches occurring due to lack of motivation to follow the safety guidelines (Kelloway et al., 2010), disgruntlement with the organization or colleagues (Willison and Warkentin, 2013; Spector et al, 2006), or as a form of protest resulting from an unsatisfactory situation (Spector et al., 2006). According to this possibility the following hypothesis was formulated:

H6: Satisfaction with colleagues, superiors or organization positively influences Safe Behavior regarding Information Security.

The control variable presented on the theoretical model indicates that the data analysis will be performed on the sample of respondents who received verbal or written guidance on Information Security from the organization for which they worked at the data collection time. This selection allows us to obtain the perceptions of respondents who already have some insight into the threats such as the level of control and monitoring and the punishment for not following the guidelines received. It also allows the comparison of the results with the group of respondents who did not receive the same kind of guidance.

4. METHODOLOGY

The research used an exploratory approach by conducting a survey through a self-administered questionnaire for quantitative cross-sectional data collection.

The population of this survey was composed of Information Systems users in an organizational environment from organizations of any size, industry or field of activity. However, the respondents had to have received in writing or oral Information Security guidance, by the organization they worked for by the time they completed the questionnaire. The sampling process was not probabilistic for convenience (HAIR et al., 2005).

The survey instrument was developed from consolidated instruments on the subject, as shown in the Appendix. The instrument used a Likert type scale ranging across five categories, from 1 (strongly disagree) to 5 (strongly agree), based on the instruments used in the three original surveys used as a reference for the theoretical model.

During pre-tests, a set of previous validations was conducted in order to have a suitable measuring instrument. This is the recommendation of Malhotra (2009) when the instrument is formed by others previously used in other researches.

The first part of the instrument validation was carried out by face and content validation and involved a group of professors in MIS. As a result, some questions were amended in terms of their content and order. The most significant change was the alteration of the construct of Disgruntlement, originated in Willison and Warkentin (2013), which were reversed: after this step of validation it went on to validate the disgruntlement from the perspective of the lack of contentment.

The validation of the instrument was performed by applying the instrument to a sample of 229 Brazilian IT users (non-probability sample for convenience). After the exclusion of incomplete questionnaires, 216 valid respondents remained. However, after applying the filter keeping only those respondents who received some guidance on Information Security, 135 respondents remained valid in the pre-test sample.

After the adaptation of the questionnaire, data collection was conducted through a printed form and simultaneously through an electronic survey in order to increase the amount of respondents. A number of 171 valid questionnaires were obtained (completely filled in and without errors). Among them, 112 received some Information Security guidance and with work experience from 1 to 30 years. This sample was used in the final data analysis. When considering 112 respondents and 15 questions in the final data analysis, the rate of respondents per question was 7.46, which is higher than the rate of five recommended by Malhotra (2009). As indicated by Hair et al. (2011) the T-Test was conducted to ascertain whether there were differences between the responses of the samples collected on paper compared to the responses obtained from the online survey, which did not occur.

All the analyses were performed using the SPSS Statistics version 20 software.

5. RESULTS

In order to validate the reliability of the survey instrument in the pre-test phase, Cronbach's alpha was used. At this stage of validation, a multivariate analysis was also performed in order to verify the structure of the factors that make up the scales. In order to do this, a principal component analysis with varimax rotation was used, following the recommendations of Hair et al. (2009).

The research sample (final collection) consisted of 112 respondents. Figure 2 shows respondents education profile.

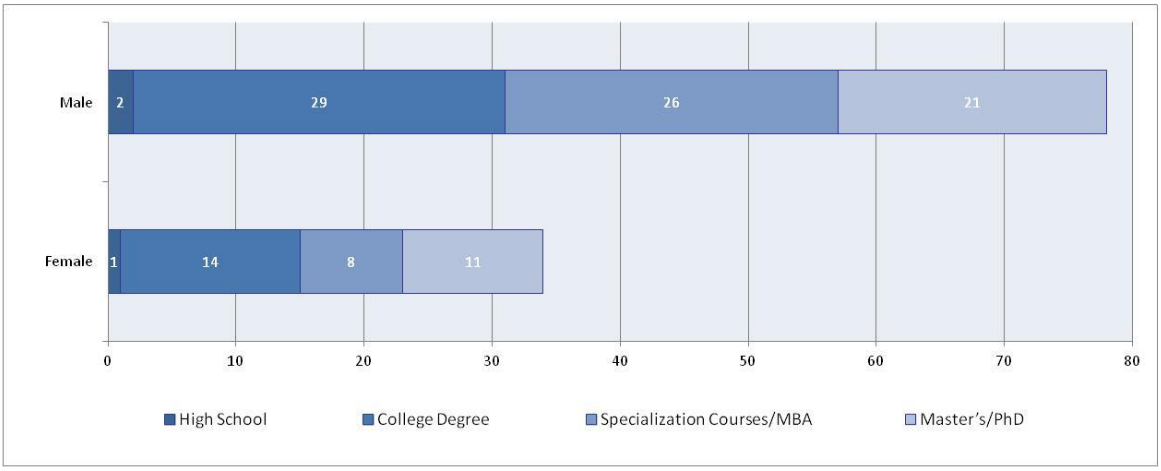

Figure 2 – Respondents Gender and Education Profiles

Figure 3 shows gender versus years of work experience.

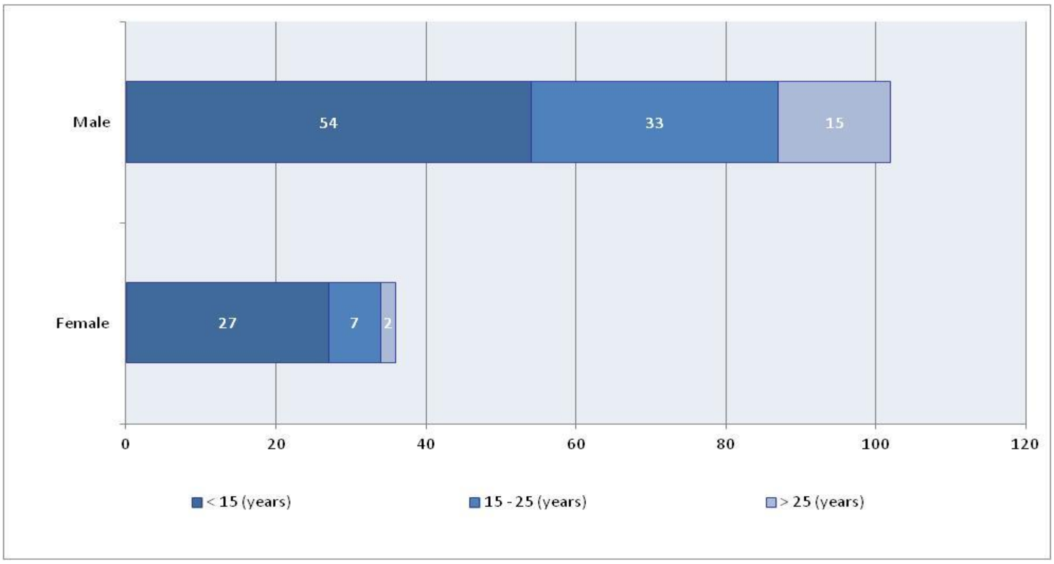

Figure 3 – Respondents' Gender and Work Experience

The normality of the collected data was verified with the Descriptive Univariate Analysis. Verification of normality was performed through the analysis of symmetry and of kurtosis.

The reliability of the scales was assessed by Cronbach's Alpha coefficient. A Cronbach's Alpha of 0.767 was obtained for the set of all 15 mandatory variables, which measured the constructs of the models. Cronbach alphas for each construct are shown in Table 1.

Construct	Variables	Cronbach's Alpha
Threat Susceptibility	SUS1, SUS2, SUS3	0.857
Disgruntlement	DESC1, DESC2, DESC3	0.819
Punishment Severity	PUNSEV2, PUNSEV3	0.852
Safe Behavior	BEH1, BEH2, BEH3	0.725
Certainty of detection	DETCERT1, DETCERT2	0.684
Threat Severity	SEV1 SEV3	0.615
Effort in Safeguarding	PSC2 PSC3 and PSC4*	0.591

* Optional questions

Table 1 – Cronbach's Alpha for each construct

The optional questions of the variables obtained a low coefficient of Cronbach's Alpha due to the low number of respondents who answered these questions (N=35). Thus the construct Effort in Safeguarding and respective variables (based on LIANG and XUE 2010) were not used in the survey resulting in the absence of support for the H5 hypothesis. Other statistical indicators were also taken into account in that decision, such as the difference in the T-Test and the lack of convergence for the respective factor in the Convergent Factor Analysis, shown in Table 2.

Variables	Factors*				
	1 (SUS)	2 (DESC)	3 (PUNSEV)	4 (DECERT)	5 (SEV)
SUS1	**0.894**	-0.031	-0.148	0.080	0.146
SUS2	**0.868**	-0.085	-0.092	-0.003	0.060
SUS3	**0.854**	0.056	-0.003	-0.081	0.046
DESC1	0.015	**0.875**	0.023	0.054	-0.106
DESC2	-0.102	**0.861**	-0.133	-0.095	0.115
DESC3	0.029	**0.819**	0.168	0.091	0.175
PUNSEV3	-0083	0025	**0899**	0108	0203
PUNSEV2	-0.142	0.011	**0.890**	0.208	0.111
DETCERT1	0.077	-0.105	0.121	**0.900**	0.002
DETCERT2	-0.121	0.212	0.220	**0.774**	0.285
SEV1	0.223	-0.005	0.052	0.153	**0.821**
SEV3	0.022	0.152	0.282	0.052	**0.792**

* Rotation converged in 5 iterations; Extraction Method: Principal Components Analysis; Rotation Method: Varimax with Kaiser Normalization

Table 2 – Convergent Factor Analysis

In order to increase the consistency and the potential to generalize the results,, a Convergent Factor Analysis was conducted. The dependent factor in the theoretical model (BEH) was obtained from three dependent variables (BEH1, BEH2 and BEH3). The five independent factors that were obtained by Factor Analysis from the independent variables explained 79.371% of the variance.

During the Factor Analysis, the Kaiser-Meyer-Olkin index (KMO) was verified. The index obtained was 0.677 for the independent constructs and 0.646 for the dependent constructs, and the sphericity test indicates that the result is valid ($p<0.001$). In the Convergent Factor Analysis, the commonalities showed satisfactory results. The commonalities were extracted by the *Principal Component Analysis* method, with no variable indicating a rate below 0.5.

The multicollinearity was verified by calculating values of tolerance and the Variance Inflation Factor (VIF).

In the analysis of the scatter plots, there was symmetrical dispersion of data values, indicating that there was homoscedasticity. Linearity was assessed by inspection of the bivariate scatter plots. All dimensions of the model studied showed linear relationships with no curvilinear relationships emerging (quadratic or cubic).

In order to confirm the relationship between the constructs from the factors of the Factor Analysis, a Multiple Linear Regression Analysis was conducted between the independent factors and the dependent factor and was used to predict the Safe Behavior from the Susceptibility to the Threat, Severity of the Threat, Certainty of Detection, Punishment Severity and Disgruntlement.

The squared correlation coefficient obtained by the final theoretical research model (R2) was 0.413, indicating that the constructs (factors) measured by the final model explained 41.3% of the Safe Behavior of the respondent users of this survey.

The research by Herath and Rao (2009a), which was used as the source for the questions regarding the constructs of the Certainty of Detection and Punishment Severity, reached a very close R2 (0.42). For Hair et al. (2011), a correlation coefficient that is in the value range of ±0.41 to ±0.7 has a force of moderate association.

The standardized Beta regression coefficients are presented, indicating the impact of the association between the dependent and the independent variable, and reflect the importance of the independent variable on the dependent (HAIR et al., 2011). The summary of the supported or unsupported associations that support the hypotheses set out in the final research model, which is shown in Figure 4. The Variance Inflation Factor obtained was 1.0 indicating that there is no multicollinearity (HAIR et al., 2011).

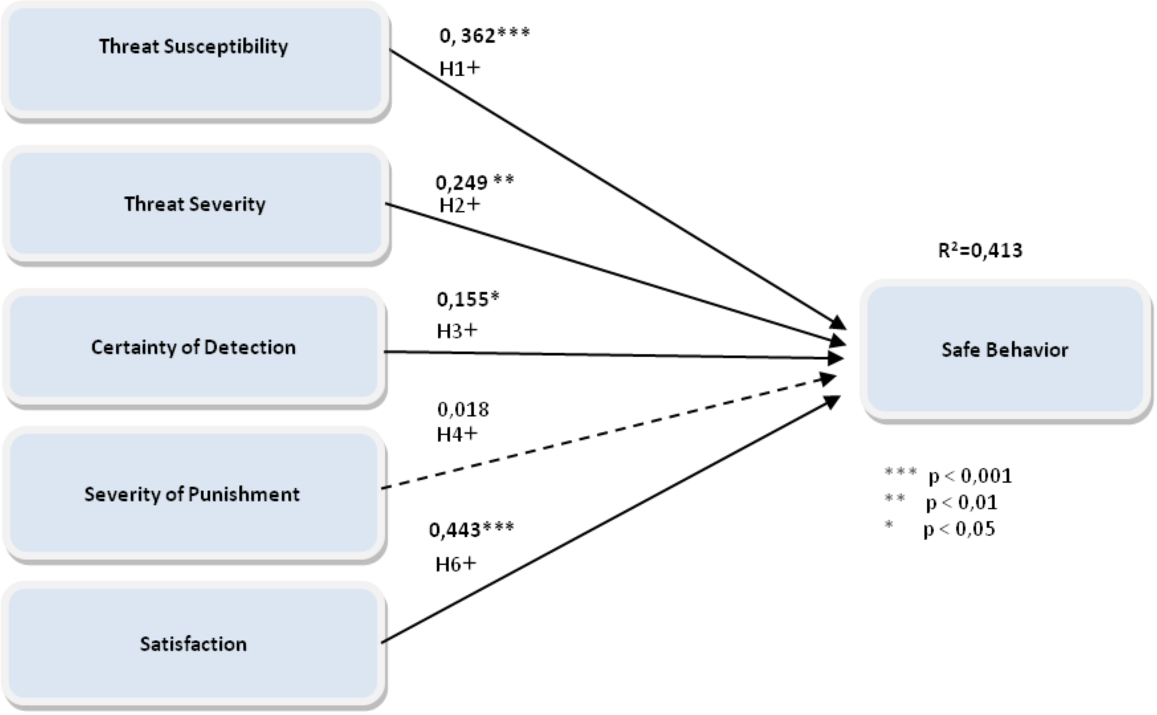

Figure 4 - Linear regression of the final model

The dashed line indicates the unsupported hypothesis and the solid lines indicate the supported hypothesis, in which the association rate between the independent variable and the dependent variable provides support to the hypothesis. The asterisks indicate statistical significance.

The results show that perceptions of Susceptibility to the Threat, Severity of the Threat and Satisfaction are determinants of Safe Behavior when it comes to care about malware in emails, providing support to hypotheses H1, H2, H6 and partially to hypothesis H3. They also show that the main effects of the perceived Punishment Severity are not significant, without providing support to the H4 hypothesis in this research.

Regarding the H5 hypothesis according to Herath and Rao (2009a) Information Security causes a greater number of procedures and tasks to be performed. As a result, a greater potential effort to carry out the additional actions may be mistakenly perceived as an unintentional hindrance, which may compromise the users' actions for the sake of safe behavior. It was not possible to determine the perception of Effort in Safeguard in this study (based on the questions of Liang and Xue, 2009) because they are optional and are based on obtaining antispyware. In the opinion of the majority of respondents (72%), antispyware software was already installed and did not need be obtained, making it impossible to measure and consequently support the H5 hypothesis.

Yet, the correlations of Certainty of Detection and Punishment Severity (hypotheses H3 and H4) with the Safe Behavior are smaller than in the research arising from these constructs (HERATH and RAO 2009a). This may indicate that the respondents did not consider, in the context of this research, the Certainty of Detection and especially the Punishment Severity as strong inducing factors to Safe Behavior. However there may be contingency effects, i.e., the effect of these factors in isolation may not be effective in indicating the practice of Safe Behavior, but the combination of these factors can lead to Information Security Safe Behavior. In other words, the Punishment Severity did not appear to be significant in its own right, but may operate alongside other factors in order to predict Information Security Safe in future researches. On the other hand, the low perception of the Certainty of Detection is consistent with the low perception of the Punishment Severity, because the users who do not believe that will be discovered, contrary to the Information Security guidelines, might consider that they will not be punished.

The H6 hypothesis on disgruntlement with the organization, colleagues and superiors, which after survey instrument face and content validation evaluates satisfaction, had a significant effect with an important role in influencing Safe Behavior. This was the most significant factor in predicting the Safe Behavior in the context of this research.

The results also indicate that the Information Security guidance of users is significant in determining the Safe Behavior. During the linear regression it became apparent that guidance is an important control variable influencing the correlation coefficient. When conducting the linear regression of the model factors with all 171 respondents and disregarding the Information Security guidance filter, the correlations obtained lower values (R2: 0.242). This may indicate that organizational efforts, such as awareness programs, are significant in triggering Safe Behavior. However, this does not exclude other forms of stimuli for this behavior, such as individual experience or other forms of external communications to the organization, which are not measured by this research.

Thus, the results demonstrate the importance of Information Security periodic guidance, focusing particularly on the security of the organization's information assets. The disclosure of deterrence measures, with emphasis on the monitoring carried out by the organization, and examples of rebukes for inadequate behavior should also be considered in the context of this awareness (SIPONEN and VANCE 2010).

The awareness programs should train users on the objectives and security controls (technical, physical or normative), enabling users to understand the benefits of the controls and how to reduce the risk of security threats. According to Ng, Kankanhalli and Xu (2009), when users are aware of the susceptibility to and the severity of the threats, they can make informed decisions to exercise adequate preventive behavior. Thus, awareness guidelines need to be developed to highlight the

Severity of the Threat and the Susceptibility of the Threat and should focus on educating users about the possibility of and the damage caused by threats. This can enable the user to understand the need for security, their role and their responsibility in protecting organizational data and other information assets.

6. FINAL REMARKS

This research revealed factors influencing the Safe Behavior regarding e-mail by applying a theoretical model that combined three surveys from Information Security field. The result was a new instrument, which used large, solid and repeated validation methods, hereinafter enabling the use in new application contexts and likewise in new explanatory or descriptive research.

Academically, this study contributes to understand a user's Computer Safe Behavior in an organizational context and made it possible to combine concepts from several behavioral theories. In particular, the construct of satisfaction is new to the field of Information Security and even more unusual in quantitative research in this area. Another contribution of this study is to research Brazilian users. In this country, studies on users' behavior are still far behind compared to foreign researches. Brazilian studies on Information Security are mainly focused on technical aspects, making it important to identify the local context peculiarities. As an example, Brazilian users do not show consistent privacy concerns (Britto-da-Silva, Luciano e Magnagnagno, 2015), which goes against international studies tendencies and arises concerns how far Brazilian users are from behavioral Information Security issues.

The study undertaken provides a range of managerial implications applicable to organizations that provide Information Security training and guidance. Nevertheless it addresses some more comprehensive points, which should be considered by organizations in search of greater security. The role of the lack of guidance in Information Security is highlighted and accordingly a warning is released about the risk of a lack of guidance. It also covers implications for professionals who prepare Information Security guidelines or awareness programs. In particular, the importance of Perceived Severity and Perceived Susceptibility should be highlighted in the formulation of the content of Information Security awareness guidelines within organizations. Users' disgruntlement with the organization, colleagues or superiors is a factor to be considered in the awareness programs.

According to Bulgurcu, Cavusoglu and Benbasat (2010), the strengthening of Information Security depends on employees complying with the Information Security guidelines - rules and regulations, which should be formulated according to the organizational needs (Albuquerque Junior & Santos, 2015). For Puhakainen and Siponen (2010), employees who do not comply with the Information Security policy guidelines are a serious risk to their companies. The serious consequences of breaches and vulnerabilities in Information Security and their implications for the employees and for the organization should be emphasized in the security guidelines, permitting employees to understand the gravity and serving as a driving force to practice Safe Behavior. According to Ng, Kankanhalli and Xu (2009), the security guidelines provided to employees can be even more effective when the possibility and severity of the damage to the organization information assets are explained. By emphasizing the gravity of security incidents, employees will be motivated to practice appropriate guideline behavior, provided they are not disgruntled with the organization, superiors or colleagues (WILLISON and WARKENTIN 2013).

The results show that employee behavior plays an important role in avoiding vulnerabilities and breaches in Information Security and this requires more research to study the factors that influence the decision of the individual to practice Information Security Safe Behavior.

In this study, only the practice of Information Security regarding emails was measured, which limits the generalization of the results to other practices, such as lack of software updates, access to suspicious hyperlinks, password loans or the use of weak passwords, among others. Future studies on other security practices can help uncover the common causal relationships that can strengthen a Safe Behavior or cause breaches and vulnerabilities in Information Security. It would also be useful to compare the results of those respondents who did not have previous malware incidents with those who already have.

REFERENCES

Albuquerque Junior, A. E. & Santos, E. M. (2015). Adoption of Information Security Measures in Public Research Institutes. JISTEM - Journal of Information Systems and Technology Management, 12(2), 289-315.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, *28*(6), 476-490.

Britto-Da-Silva, V. R.; Luciano, E. M.; Magnagnagno, O. A. Preocupação com a Privacidade na Internet: Uma Pesquisa Exploratória no Cenário Brasileiro. In: V Encontro de Administração da Informação (ENADI), 2015, Brasilia. Anais do V ENADI. Rio de Janeiro: ANPAD, 2015.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.

D'Arcy, J., Hovav, A., and Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 20(1), 79-98.

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. Government Information Quarterly, 26(4), 584-593.

Hair, J. F., Black, W. C., Babin, B. J. & Anderson, R. E. (2009). *Multivariate Data Analysis*. Pearson.

Hair Jr, J. F., Wolfinbarger, M., Money, A. H., Samouel, P. & Page, M. J. (2011). Essentials of Business Research. Taylor & Francis.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, *34*(3), 549-566.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation?. Computers & Security, 61, 46-58.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), 143-154.

Kelloway, E. K., Francis, L., Prosser, M., & Cameron, J. E. (2010). Counterproductive work behavior as protest. *Human Resource Management Review*, *20*(1), 18-25.

Kjell, H. (2015). A Strategic Analysis Of Information Sharing Among Cyber Hackers. JISTEM - Journal of Information Systems and Technology Management, 12(2), 245-270.

King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*,*28*(3), 308-319.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS quarterly*, 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11* (7), 394-413.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, *28*(3), 215-228.

Malhotra, N. K. (2008). *Marketing research: An applied orientation, 5/e*. Pearson Education India.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*,*46*(4), 815-825.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757-778.

Roratto, R., & Dias, E. D. (2014). Security Information in Production and Operations: a Study on Audit Trails in Database Systems. JISTEM - Journal of Information Systems and Technology Management, 11(3), 717-734.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. Computers & Security, 56, 70-82.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, *34*(3), 487.

Spector, P. E., Fox, S., Penney, L. M., Bruursema, K., Goh, A., & Kessler, S. (2006). The dimensionality of counterproductivity: Are all counterproductive behaviors created equal?. *Journal of vocational behavior*,*68* (3), 446-460.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1-20.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816.

APPENDIX – Research instrument

The complete research instrument (as used to collect the data) can be obtained upon request.

Threat Susceptibility

From Strongly Disagree (1) to Strongly Agree (5).
(SUS1*) The chances of receiving an e-mail attachment with malware are high.
(SUS2*) There is a good possibility that I receive an e-mail attachment with malware.
(SUS3*) I am susceptible to receive an e-mail attachment with malware.
*Based on the questionnaire of Ng, Kankanhalli and Xu (2009).

Severity of threat

From Strongly Disagree (1) to Strongly Agree (5).
(SEV1*) Having my computer infected by malware as a result of opening a suspicious email attachment is a serious problem for me.
(SEV2*) Losing organizational data as a result of opening a suspicious email attachment is a serious problem for me.
(SEV3*) If my computer is infected by malware as a result of opening a suspicious email attachment, my work could be negatively affected.
* Based on the questionnaire of Ng, Kankanhalli and Xu (2009). The term virus was updated to malware in this research.

Certainty of detection

From Strongly Disagree (1) to Strongly Agree (5).
(DETCERT1*) In the organization where I work, the computer use is monitored.
(DETCERT2*) In the organization where I work, the inappropriate use of the computer would surely be detected.
* Based on the questionnaire of Herath and Rao (2009a)

Punishment Severity

From Strongly Disagree (1) to Strongly Agree (5).
(PUNSEV2*) The organization where I work dismisses who makes inadequate use of computer.
(PUNSEV3*) In the organization where I work, if I was caught using the computer improperly, I would be severely punished.

* Based on the questionnaire of Herath and Rao (2009a)

Efforts to safeguard

(PSC1*) In the organization where you work, does your computer have an anti-spyware? (Yes/No/Don't Know).
Note: Anti-Spyware is a software that removes or blocks spyware on a computer. Spyware is a type of malware that is secretly installed on a computer, with the objective of gathering information about users or organizations without your knowledge.

If you answered "No" or "Don't know" in the previous question, set your level of agreement with the statements below - From Strongly Disagree (1) to Strongly Agree (5).
(PSC2**) I don't know how to get anti-spyware software.

(PSC3**) Anti-spyware software may cause problems to other programs on my computer.
(PSC4**) The installation of anti-spyware software is very complicated.

* Created by the authors, based on theoretical background.
** Based on the questionnaire of Liang and Xue (2010).

Satisfaction - Disgruntlement
From Strongly Disagree (1) to Strongly Agree (5).
Considering the organization where you work:
(DESC1*) I am very happy with my co-workers.
(DESC2*) I am very happy with my superiors.
(DESC3*) I am very happy with the organization where I work.
* Based on Willison and Warkentin (2013).

Safe Behavior
From Strongly Disagree (1) to Strongly Agree (5).
(BEH1*) Before reading an email, I first check whether the subject and the sender make sense.
(BEH2*) Before opening an email attachment, I check first if the filename of the attachment makes sense.
(BEH3*) I am cautious when receiving an e-mail attachment because it may contain a malware.
(BEH4*) I do not open email attachments if the content of the email looks suspicious.
* Based on the questionnaire of Ng, Kankanhalli and Xu (2009). The term virus was updated to malware in this research.

Control Variables
(ORI1*) Does the organization where you work provide verbal or written orientation on Information Security? (Yes, but the reasons for each item highlighted are not clarified; Yes, and the reasons for each item highlighted are clarified; No).
(ORI2*) If you answered Yes to any option in the previous question, the guidelines were: Periodically, every ____ months; Once.
* Based on the questionnaire of Puhakainen and Siponen (2010).

Demographics and profile items
Gender
Age
Education (level of education and field)
Occupation
Years of professional experience
Number of people working in your company (approximately)
Professional experience in the Information Technology field (Yes, No)
Organizational segment (industry, commerce, services, government)