RAUSP Management Journal
ISSN: 2531-0488
rausp@usp.br
Universidade de São Paulo
Brasil

Received 3 February 2021
Revised 27 April 2021
24 August 2021
Accepted 11 September 2021

Antecedent factors of violation of information security rules

Alexandre Cappellozza
Universidade Presbiteriana Mackenzie, Centro de Ciências Sociais e Aplicadas, Sao Paulo, Brazil

Gustavo Hermínio Salati Marcondes de Moraes
Universidade Estadual de Campinas, Faculdade de Ciências Aplicadas, Limeira, Brazil

Gilberto Perez
Universidade Presbiteriana Mackenzie, Centro de Ciências Sociais e Aplicadas, Sao Paulo, Brazil, and

Alessandra Lourenço Simões
Universidade Metodista de São Paulo, São Bernardo do Campo, Brazil

Abstract

Purpose – This paper aims to investigate the influence of moral disengagement, perceived penalty, negative experiences and turnover intention on the intention to violate the established security rules.

Design/methodology/approach – The method used involves two stages of analysis, using techniques of structural equation modeling and artificial intelligence with neural networks, based on information collected from 318 workers of organizational information systems.

Findings – The model provides a reasonable prediction regarding the intention to violate information security policies (ISP). The results revealed that the relationships of moral disengagement and perceived penalty significantly influence such an intention.

Research limitations/implications – This research presents a multi-analytical approach that expands the robustness of the results by the complementarity of each analysis technique. In addition, it offers scientific evidence of the factors that reinforce the cognitive processes that involve workers' decision-making in security breaches.

Practical implications – The practical recommendation is to improve organizational communication to mitigate information security vulnerabilities in several ways, namely, training actions that simulate daily work routines; exposing the consequences of policy violations; disseminating internal newsletters with examples of inappropriate behavior.

Social implications – Results indicate that information security does not depend on the employees' commitment to the organization; system vulnerabilities can be explored even by employees committed to the companies.

RAUSP Management Journal
Vol. 57 No. 1, 2022
pp. 84-101
Emerald Publishing Limited
2531-0488
DOI 10.1108/RAUSP-02-2021-0022

Originality/value – The study expands the knowledge about the individual factors that make information security in companies vulnerable, one of the few in the literature which aims to offer an in-depth perspective on which individual antecedent factors affect the violation of ISP.

Keywords Security, Technology, Violation of information security, Moral disengagement, Information, Structural equation modeling, Neural networks, Violation of information security

Paper type Research paper

1. Introduction

Cyber-attacks and information leaks resulting from failures in the control of information systems are recurrent news in the daily lives of organizations. Financial data, production information, suppliers and customers are targeted by people with bad intentions who seek to take advantage of the absence of efficient security controls (Sen, Verma, & Heim, 2020).

In its annual report on cybercrimes, research firm cybersecurity ventures estimates that losses from digital crimes will reach US$6tn in 2021 (Morgan, 2019). To illustrate the impacts of these problems, one can mention some attacks suffered by large companies in the first quarter of 2020 (McCandless, Evans, Barton, Starling, & Geere, 2020), such as the online exposure of 250 million customer support records of Microsoft, payment data of 300,000 Nintendo accounts, and improper access to the registration of five million guests of the Marriott hotel chain.

Organizational information is considered a company asset, and because of its importance to the business, it must be protected by everyone involved in the processes that make up organizations. In an attempt to avoid cyber-attacks, fraud, information leakage and other risks inherent to information, applying effective Information Security controls in organizations' processes has become fundamental. Likewise, employees' knowledge and skills are critical to mitigating risks and managing the overall effectiveness of organizational information security (Yoo, Goo, & Rao, 2020). In addition to tools, controls and training, many companies have guidelines established in their information security policies (ISP), which all employees must follow according to good practice standards defined in the Information Systems literature (International Organization for Standardization [ISO], 2013, 2013).

Although ISP have rules that companies and employees must follow, it is known that the violations occur both due to external attacks and to internal factors, including reasons that involve the employees who work in these companies.

Information security literature studies show that the employee's failure to follow ISP increases the possibility of invasions to information assets, although losses and damages to organizational assets are highly undesirable (D'Arcy, Herath, & Shoss, 2014; Dhillon, Talib, & Picoto, 2020). However, studies exploring intrinsic factors related to ISP are still scarce (Dhillon *et al.*, 2020) and information security at the working group level cannot be separated from the individual level because individual security is a necessary condition for processes to occur in the desired way (Yoo *et al.*, 2020).

The moral disengagement of individuals that is linked to their inappropriate behaviors, as a rule, results in a penalty for them through disciplinary processes. In addition, this disengagement can lead the employee to practice harmful acts to violate the established safety rules. Thus, this study aims to answer the following research question:

RQ1. What impacts do individual factors have in decisions to violate ISP?

More specifically, it seeks to examine the influence of moral disengagement, perceived penalty, negative experiences of invasion and privacy and the effect of turnover intention on the intention to violate the established security rules.

The following chapters address the theoretical basis to formulate hypotheses about the factors that may involve violations of organizational ISP, the method used for data acquisition and analysis, the discussion of results and, finally, the research conclusions.

2. Theoretical framework

2.1 Moral disengagement

The literature recommends that the subjective mechanisms that support unwanted actions must be addressed to understand the cognitive processes that promote counterproductive behaviors in the workplace (Fida, Tramontano, Paciello, Ghezzi, & Barbaranelli, 2018).

The theory of moral disengagement (Bandura, Barbaranelli, Caprara, & Pastorelli, 1996) has been used to explain why individuals misbehave, for example, in their professional lives (Moore, Detert, Trevino, Baker, & Mayer, 2012). Based on this theory, moral disengagement is a mechanism through which individuals subjectively mitigate the consequences of unwanted behaviors from their own moral values (Bandura *et al.*, 1996). For instance, research shows that employees may rationalize their undesirable behavior based on work stressors (D'Arcy *et al.*, 2014).

Khan, Dapeng, Adnan Muhammad, and Ullah (2018) confirmed the interaction between moral disengagement, ethical leadership and unethical behavior in the context of sales competition. Furthermore, the study showed a positive relationship between employees' moral disengagement and anticompetitive behavior and presents ethical leadership as a factor to mitigate counterproductive behaviors during work activities (Khan *et al.*, 2018).

As a recommendation to mitigate the development of attitudes that support moral disengagement, it is recommended that employees take part in planning organizational goals with their leaders, thus promoting greater assertiveness of management expectations by employees (Barsky, 2011).

In addition, reminding potential offenders that their actions can harm others reduces the disconnection of acts from those people's moral values (Kish-Gephart, Detert, Treviño, Baker, & Martin, 2014). Aspects of organizational environments that discourage workers, such as situations that reduce commitment and harmony between work teams or financial losses linked to professional roles, increase the difficulties in the social relationship among employees, promote a feeling of helplessness and weaken moral values within organizations.

Thus, it is believed that moral disengagement is also linked to the emotional aspects of workers, as it positions itself as a mediating variable in the relation of negative emotions and counterproductive behaviors of professionals (Fida *et al.*, 2018). In other words, the attitudes formed by negative emotions about work can support the individual's belief that it is acceptable to harm other people for the benefits achieved by the transgressive actions.

Actions that result in fraud can be elaborated from different subjective means, such as the lack of recognition that the unethical act is a fraud, the use of rationality to mitigate the negative results that follow the negative behaviors and the development of different methods to reduce unwanted consequences (Murphy & Dacin, 2011).

It is known that personal interests reinforce human motivations in their daily actions. Therefore, situations that exhibit opportunities for gains or benefits and involve such personal interests increase individuals' possibility of disengaging morally (Kish-Gephart *et al.*, 2014). Thus, the effects of individual moral judgment are valuable for the security of information in an organization (D'Arcy & Lowry, 2019).

Attacks and violations of organizational ISP can have various motivations, but the moral disengagement of employees appears to be a significant factor, given their characteristics (D'Arcy *et al.*, 2014).

Moral disengagement is one of the explanations that support decisions involving fraud in companies, selfish acts of employees in the workplace, as well as unethical actions that weaken the security of organizational processes (Zheng, Qin, Liu, & Liao, 2019).

Furthermore, the potential of moral disengagement to increase inappropriate actions and to be an inherently individual phenomenon places organizational moral disengagement as one of the main factors managers should consider (D'Arcy *et al.*, 2014). Thus, the following hypothesis is elaborated:

H1. Moral disengagement positively influences the intention to violate ISP.

2.2 Perceived penalty

By the standard of good practices ISO/IEC 27002/2013, the management of information security includes applying disciplinary processes based on punishments or penalties, also called *sanctions*, to all those who violate the guidelines established in the ISP.

Sanctions can be seen as a disciplinary imposition by top management on wrongdoers. Guo and Yuan (2012, p. 321) address sanctions as formal controls imposed on employees to ensure compliance with established guidelines, discouraging undesirable attitudes to the organizational environment. Straub (1990) and Fajardo (2016) also state that sanctions function as a "disincentive" to commit a criminal act or to deviate from the stated guidelines.

Several studies address the issue of administrative sanctions from the general deterrence theory, the main focus of criminological theories for over 30 years (Pahnila, Siponem, & Mahmood, 2007; Santiago, Diño, & Caballero, 2017). The concept of deterrence was developed "originally to control criminal behavior," which suggests that the certainty and severity "of punishment affect people's decision to commit a crime or not."

The general deterrence theory also encompasses components such as social disapproval, which is the feeling of shame toward others for the act committed; self-disapproval, which is the shame of oneself and impulsiveness as the inability to resist, mentioned by Pahnila *et al.* (2007). Santiago *et al.* (2017) pointed out some equivalent findings in their study about violations and penalties involving plagiarism in advanced educational research.

Straub's (1990) studies also concluded that "when the risk of punishment is high" and "sanctions for violation are serious," offenders are inhibited from committing violations. Furthermore, they observed that applying sanctions "for non-compliance with the Information Security Policy increases the appropriate Information Security behavior." Therefore, the following hypothesis is proposed to assess the effect of the perceived penalty on the intention to violate security:

H2. The perceived penalty negatively influences the Intention to violate ISP.

2.3 Turnover intention

In the information age, companies that operate in knowledge-intensive sectors devote many resources to retain their talents, as turnover is expensive (Soltis, Agneessens, Sasovova, & Labianca, 2013). Furthermore, aspects related to workers' careers may also be related to turnover in companies: opportunities for career growth interact with the reduction in the turnover intention by employees.

According to Ohunakin, Adeniji, Oludayo, and Osibanjo (2018), the definition of career goals and the development of professional skills of the team, as well as the speed of promotions and the adequacy of remuneration to talented employees, are essential factors to reduce turnover, in addition to saving on hiring costs and providing the retention of high-performance professionals in companies (Ohunakin *et al.*, 2018).

Employee turnover can generate costly consequences and serious problems for companies. The People Management literature reveals a wide variety of factors that lead individuals to leave their organizations searching for a new job, either in a different organization or in a different field (Coetzee & van Dyk, 2018).

Job turnover is associated with changes in the staff of an organization, whether due to hiring or firing. On the other hand, turnover intention refers to the estimated probability, by subjective means, of employees leaving their current job in the future (Mowday, Porter, & Steers, 1982).

Motivating employees to engage in work and remain faithful in defending the organization's image has been a challenge for organizations for decades (Rafiq, Wu, Chin, & Nasir, 2019).

In general, companies must direct their resources to improve the well-being and the organizational climate among employees. Such dedication from management usually results in lower turnover rates in the staff and greater identification of employees with the organization (Tinwala & Biswas, 2020). One possible explanation for these results is that trust in top management promotes the permanence of employees in their organizations (Mölders, Brosi, Spörrle, & Welpe, 2019).

Also, there is a positive relationship between turnover intentions and workplace incivility, which may relate to many negative behaviors, such as decreased job satisfaction, absenteeism, citizenship behavior and an increase in counterproductive behavior (Manzoor, Manzoor, & Khan, 2020) which may reduce compliance with internal organizational ISP by employees.

Haque, Fernando, and Caputi (2019) indicate that workers who manifest low turnover intention tend to exhibit increased organizational commitment, promoting citizenship behavior (Katz & Kahn, 1978) and adopting internal regulations and standards to fulfill organizational activities, such as internal security policies.

Therefore, the following hypothesis is elaborated:

H3. The turnover intention positively influences the intention to violate ISP.

2.4 Negative privacy invasion experience

According to some studies, individuals may have different concerns about their privacy (Culnan & Armstrong, 1999; Smith, Milberg, & Burke, 1996). However, commonly, privacy violations caused by negative experiences, such as data leakage or theft, end up causing greater concern to individuals due to the fear that the negative experience will reoccur (Hong, Chan, & Thong, 2021; Xu, Teo, Tan, & Agarwal, 2012).

The study of these phenomena was based on the relation of delivering information based on the trust of a social contract, whose rules govern the behavior of the parties involved. The existence of such a contract suggests that there will be adequate management of the data entrusted to one of the parties, establishing a relationship of trust that is undone when the data subject perceives an invasion of their privacy, affecting them psychologically and generating a feeling of betrayal (Bansal, Zahedi, & Gefen, 2010).

Attacks or exploitation of flawed security controls exposes data and information that can cause harm not only to organizations but also to data subjects. This experience can leave a negative perception regarding the privacy of individuals. Some studies focus on assessing how previous negative experiences can influence the increase in concern about the privacy of information (Bansal *et al.*, 2010).

Other studies argue that the negative association between trust and breach of privacy is linked to the perception that something could have been done to decrease the likelihood of the occurrence (Ramos, Ferreira, de Freitas, & Rodrigues, 2018).

However, even with continuous efforts to protect the privacy of users, incidents of data breaches remain constant (Sen & Borle, 2015). Moreover, the negative aspects related to the breach of data privacy may even affect customer and firm performance (Martin, Borah, & Palmatier, 2017).

Attacks are less effective when administrators apply controls, but trust is reduced when the intention to share data is perceived (Bansal *et al.*, 2010). Thus, with frequent data breaches, individuals feel that they are not in control of their information online and this causes a feeling of tiredness regarding privacy issues, when individuals believe there are no effective ways to manage information on the internet (Hargittai & Marwick, 2016). In addition, individuals with previous negative experiences of hacking tend to reduce their decision-making efforts to protect information (Levav, Heitmann, Herrmann, & Iyengar, 2010).

The concern with privacy and information protection is inherent to Information Security; thus, the association between the negative experience and the security breach becomes hypothetical. Then, the following hypothesis is proposed:

H4. The negative experience of invasion of privacy negatively influences the intention to violate ISP.

3. Methodological procedures

This study was developed with a single quantitative cross-sectional approach and was carried out through a questionnaire that seeks, among other objectives, to identify opinions and the distribution of the phenomenon in the population using statistical techniques of data analysis.

Before data collection, the research project was sent to a Research Ethics Committee and applied after its approval. Then, data collection took place in person and was carried out using psychometric five-point Likert scales according to the original studies of these instruments.

We used structural equation modeling by partial least squares (PLS-SEM) with the SMARTPLS 3.0 M3 software to analyze the proposed hypotheses. The choice of PLS-SEM is justified because it is intended to test a theoretical structure from a predicting perspective and the structural model includes a considerable number of constructs and relations; therefore, it is not possible to suppose a normal data distribution (Hair, Risher, Sarstedt, & Ringle, 2019). In addition, the research's objective is to understand better antecedent factors of violation of information security rules, which makes this an exploratory research for the development of theory, which is in line with the use of the technique (Hair *et al.*, 2019).

As a form of complementary validation of the results of the hypothesis tests, a multi-analytical approach was also used, involving machine learning to study the relations between the factors and the analysis technique using neural networks.

A neural network is an artificial intelligence tool that has the ability to acquire and store knowledge and make it available for use. Furthermore, knowledge acquisition through a learning process is a characteristic of the neural network analysis technique (Haykin, 1998).

For instance, in the case of a study of the relations between variables, the shape of these relations is determined in the learning process. If a linear relationship between variables is appropriate, neural network results should approximate the linear regression models.

However, if a non-linear relationship is more appropriate, the neural network will seek other forms of relations that better fit between variables (Ripley, 1996).

Given the learning ability of this technique, studies using it can provide superior results compared to other multivariate analysis techniques, in addition to helping to verify the consistency of the results obtained by multiple regression, given that some assumptions of linear analysis techniques are not required (Lee, Hew, Leong, Tan, & Ooi, 2020). The analysis of neural networks was performed using the International Business Machines Corporation, Statistical Package for the Social Sciences v.23 software.

3.1 Operationalization of variables

Turnover Intention was measured using the instrument presented by Siqueira, Gomide, Oliveira, and Polizzi Filho (2014); negative experience of invasion of privacy belongs to the study by Santos, Cappellozza, and Albertin (2018).

To expose a situation of violation of ISP, respondents had access to a short film that exposed a hypothetical situation of password sharing at work. The film and the other indicators that deal with the perceptions of ISP were obtained from the study by D'Arcy *et al.* (2014). The measurement instrument, which is available in the Appendix (Table A1), also includes three questions to control common method bias (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003) that may influence the conclusions of this study.

3.2 Data collection and sample profile

To assess the size of the study sample and the statistical power of the analyzes, we used software G*Power 3.1 (Faul, Erdfelder, Buchner, & Lang, 2009). Considering four variables that are predictive of the intention to violate policy construct, with a 5% significance level, 0.8 statistical power (Cohen, 1988) and average effect size ($f^2 = 0.15$, which is equivalent to $r^2 = 13\%$), it was assumed that the minimum sample size is equal to 85 respondents. Data collections were carried out in person with the voluntary participation of respondents from the state of São Paulo, selected by convenience from the researchers' network of contacts.

The questionnaire was printed and applied to 338 people who worked in companies with ISP established more than a year ago to compose the final sample. After analyzing the integrity of the responses, 20 incomplete questionnaires were discarded from the final analyzes. Therefore, the final sample used to analyze the hypotheses included 318 participants.

Among the collected sample, 44% were male respondents (140 people) and 56% female respondents (178 people). Regarding the respondents' age range, the mean age is 30 years old, with a standard deviation of 10.18 years. As for the size of respondent organizations concerning the number of employees, 68.3% of respondents stated that they work in organizations with more than 50 professionals.

Approximately 95% of the respondents claim to be aware of reports of invasion of personal and organizational data, which indicates that the sample understands that data security breaches are recurrent in their daily lives and that they are subject to these discomforts if they give up measures to protect their information.

The initial treatment of the data was based on the analysis of normality, collinearity, homoscedasticity and the absence of multicollinearity in the data distribution. The results indicate that the data distribution is not normal and there are no collinearity problems, as no correlation between the dependent variables is higher than 0.60. In the analysis of homoscedasticity, the scatterplot of the residuals does not have an obvious pattern, indicating that it is adequate. In the multicollinearity analysis, the variables' variance inflation factor value was lower than 5. All values are within the established by Hair, Hult, Ringle, and Sarstedt (2017).

In addition, analyzes of the common method bias (Podsakoff *et al.*, 2003) were conducted: significant correlations values between dependent variables and control variables were not found in the result (Appendix), which indicates the absence or little influence, from this bias in this study.

4. Analyzes of hypotheses

4.1 Analysis by structural models

To evaluate the measurement model, we verified convergent validity, discriminant validity and reliability of the indicators. Average variance extracted (AVE) with a value higher than 0.50 and composite reliability of each construct with a value higher than 0.70 are recommended for validation of the measurement model (Hair *et al.*, 2019). Another indicator of discriminant validity refers to the square root of the AVE from the constructs (highlighted in bold diagonal in Table 1), which must be higher than the correlation between the latent variables (Fornell & Larcker, 1981). The values of these metrics are shown in Table 1 and indicate that the results allow further analyzes.

Intention to violate ISP presented an R^2 with a high effect (Hair *et al.*, 2019), indicating that the antecedent variables are suitable for investigating the researched phenomenon.

To validate the structural model, we assessed the significance of the indicators and the student's *t*-test. Among the four relationships analyzed, we observed that the relations of moral disengagement and perceived penalty have a significant influence on the intention to violate security policies and the relation of turnover intention is a little above the limit value (*p*-value equal to 0.06) of what is usually considered significant in a relation between variables (Table 2). Conversely, the privacy invasion experience relation was not significant.

The complete model resulting from our empirical approach is presented in Figure 1.

Given the threshold significance value in the turnover intention and violation relations, in a complementary way, we decided to conduct a second analysis with artificial intelligence techniques under the neural networks approach to reassess the values obtained.

4.2 Analysis by neural networks

In general, a neural network can be composed of several layers, called the input, hidden and output layers. In this case, the neural network was designed to act in a multi-layer format

Constructs	MD	PP	TI	PI	INT
MD	0.921				
PP	−0.363	0.867			
TI	0.081	−0.117	0.943		
PI	−0.124	0.107	−0.008	0.767	
INT	0.545	−0.529	0.164	−0.073	0.965
Composite reliability	0.944	0.924	0.960	0.736	0.964
AVE	0.849	0.751	0.889	0.588	0.931
R^2	–	–	–	–	0.431

Notes: n = 318; MD: moral disengagement; PP: perceived penalty; TI: turnover intention; PI: privacy invasion; INT: intention to violate information security policies

Table 1. Composite reliability, AVE, square root of AVE and R^2

under the learning algorithm Perceptron, which adjusts the weights of the network relations to minimize the residuals (Maliki, Agbo, Maliki, Ibeh, & Agwu, 2011).

Furthermore, the three independent variables that obtained significance or threshold value, were considered in the multiple regression analysis for the composition of the input layer, namely, perceived penalty, turnover intention and moral disengagement. Finally, the output layer was composed of the dependent variable intention to violate ISP.

Until the elaboration of this study, the authors did not find a definitive recommendation on the composition of the layers that could bring better results to the research

Table 2.
Coefficients of the structural model – between construct

Path	Sample mean	SD	*t* statistics	*p* values
PI → INT	−0.002	0.048	0.367	0.714
TI → INT	0.090	0.047	1.856	0.063
MD → INT	0.404	0.051	7.962	0.000
PP → INT	−0.372	0.052	7.109	0.000

Notes: *n* = 318; MD: moral disengagement; PP: perceived penalty; TI: turnover intention; PI: privacy invasion; INT: intention to violate information security policies

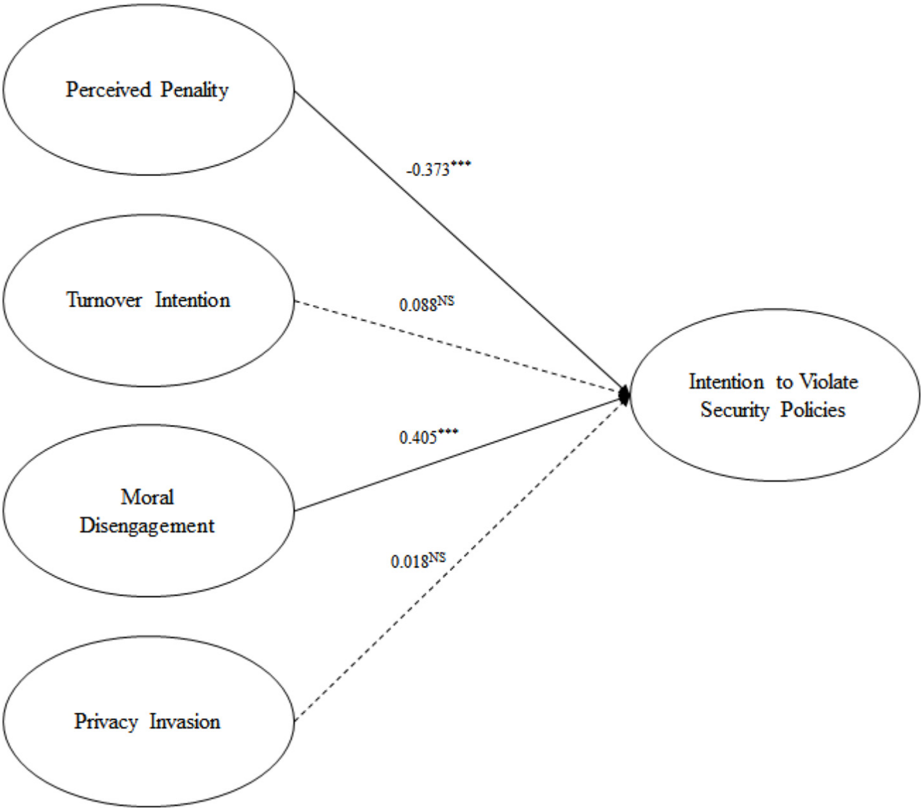

Figure 1.
Empirical model

model. Therefore, several simulations of network architectures were tested so that the results obtained could assist the selection of how to improve result performance. The analysis examined the network with 1 to 10 hidden nodes. The nodes' number in one hidden layer was set to 2 and the activation function was set to sigmoid function in both hidden and output layers. As for increasing the effectiveness of training, both inputs and outputs were normalized to the range [0,1] (Liébana-Cabanillas, Marinković, & Kalinić, 2017). Among the results, the composition of the neural network with the best performance referred to the architecture with three nodes in the second hidden layer, as shown in Figure 2.

After selecting the composition, we calculated the results with compositions ranging from one to 10 nodes in the first hidden layer and three nodes in the output layer. To obtain the neural network results, we considered 90% of the total sample for the training stage and 10% for the test of the final model, as suggested by Hew, Leong, Tan, Ooi, and Lee (2019). This can be seen in Tables 3 and 4.

The calculated Root Mean Squared Error values indicate that the neural network can provide good accuracy in predicting the results of the research model relations (Leong, Hew, Wei-Han, & Ooi, 2013; Ooi, Hew, & Lin, 2018).

Table 4 presents the results of the sensitivity analysis calculated for all compositions of neural networks and one can observe that the values obtained from the coefficients of determination (R^2) can also be considered high and associated with good quality of prediction of the observed values of intention to violate security policies.

Table 4 also demonstrates that the sensitivity analysis shows the importance of each of the variables prior to predicting the observed values of intention to violate. Thus, moral disengagement was considered the most critical factor in the intention to violate, followed by the perceived penalty and turnover intention.

The results obtained with moral disengagement are similar to other studies (Fida *et al.*, 2018; Valle, Kacmar, & Zivnuska, 2019) designed to assess unethical behavior and confirm that this factor interferes in cognitive processes as an element that promotes the execution of unwanted actions in the workplace.

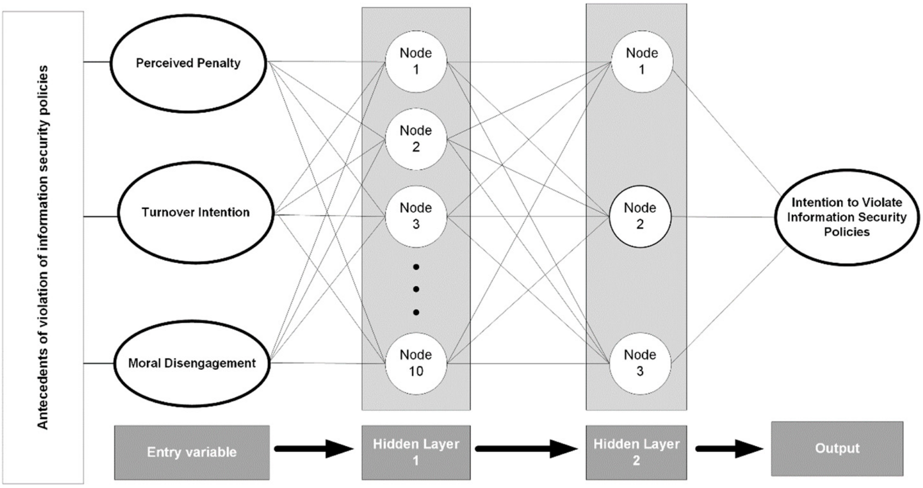

Figure 2. Neural network architecture

Table 3.
Neural network residues – model training and test steps

Neural network	Nodes Layer 1	Layer 2	Training n	RMSE	Test n	RMSE
1	1	3	281	0.18	37	0.22
2	2	3	288	0.20	30	0.14
3	3	3	288	0.19	30	0.17
4	4	3	283	0.19	35	0.19
5	5	3	277	0.19	41	0.16
6	6	3	287	0.21	31	0.19
7	7	3	278	0.21	40	0.17
8	8	3	287	0.19	31	0.17
9	9	3	280	0.18	38	0.20
10	10	3	222	0.17	64	0.22
Mean				0.19		0.18
SD				0.01		0.03

Note: n = 318

Table 4.
Sensitivity analysis

Neural network	Nodes Layer 1	Layer 2	Normalized importance (%) MD	PP	TI	R^2 (%)
1	1	3	100.00	94.80	9.20	43.00
2	2	3	100.00	97.10	33.50	36.00
3	3	3	100.00	83.30	13.40	42.00
4	4	3	100.00	95.30	16.90	43.00
5	5	3	100.00	93.40	13.90	43.00
6	6	3	93.00	100.00	6.30	32.00
7	7	3	100.00	99.40	33.50	31.00
8	8	3	100.00	91.30	14.90	44.00
9	9	3	100.00	85.60	19.20	44.00
10	10	3	100.00	86.30	18.60	42.00
Mean			99.30	92.65	17.94	40.00
SD			2.21	5.88	9.10	5.03

Notes: n = 318; MD: moral disengagement; PP: perceived penalty; TI: turnover intention

Perceived penalty, on the other hand, reinforces the need for organizational governance to develop the rules and policies that must be established to protect technological information assets but also to emphasize that, in addition to complying with the rules, the due consequences must be prescribed to members who infringe the responsibilities established by the company's management. These results are also similar to other studies (D'Arcy *et al.*, 2014) that relate this factor to unwanted behaviors of workers.

Considering the order of magnitude of the calculated magnitudes of the values of normalized amounts for each independent variable, turnover intention has an influence about five times lower than the influence of moral disengagement and perceived penalty.

Given the similarities in the interpretation of results of the SEM and the analysis of neural networks, the authors understand that it is not possible to confirm the hypothesis that turnover intention influences the intention to violate ISP. However, the additional usage of the analysis of neural networks provided methodological contributions, as it enabled additional verification of the results obtained by the SEM analysis (Sternad Zabukovšek, Kalinic, Bobek, & Tominc, 2019).

5. Research conclusion

Information security must be a factor to be considered by company leaders. Currently, the protection of users' information has become not only a competitive differential but an essential factor in the economic and a risk-mitigating development of organizations (Kauspadiene, Ramanauskaite, & Cenys, 2019), which leads to the orientation that the implementation of controls that promote information security is not a matter of choice, but survival in the organizational market.

This study sought to answer the following question:

Q1. What impacts do individual factors have in decisions to violate ISP?

The answer presents and tests a research model that weighs four potential predictive variables on behavioral intent in the perspective of violation of ISP. Therefore, it provides theoretical and managerial implications for the management of information systems and organizational policies.

Thus, the study expands the knowledge about the individual factors that make information security in companies vulnerable under a research model that contemplates dimensions that are associated with the organization's governance, such as perceived penalty, as well as factors that are associated with ethical decision-making, potential job transition and individual experiences related to privacy.

The research results emphasize that the certainty and the severity of the punishment significantly affect employees' decisions in their intention to commit a crime. Other aspects linked to the general theory of deterrence also consider some components, such as the social disapproval of the other employees of the company for the infraction committed, shame and impulsiveness as the inability to resist, which is in line with the propositions of Pahnila *et al.* (2007).

A relevant contribution of this study is the fact that until the end of the elaboration of this article, no studies were found presenting a similar research model in the information systems management literature, which adds a theoretical contribution to the studies in this research area.

We understand that the article makes a significant methodological contribution by using two multivariate techniques to analyze the collected data. This research presents a multi-analytical approach that integrates statistical analysis techniques of SEM and neural networks, expanding the results' robustness. We did not identify any article that combined the two techniques used in this field of study.

As noted by many scholars, these techniques complement each other, and therefore, provide a more rigorous data analysis (Lee *et al.*, 2020). This is because neural network analysis can compensate for SEM analysis's weaknesses by capturing linear and complex non-linear relations between variables (Leong, Hew, Lee, & Ooi, 2015).

Although PLS-SEM has often been used to verify hypothesized relations in social and behavioral science (Hair *et al.*, 2017), there are few studies on integrating it with other artificial intelligence algorithms (Xu, Zhang, Bao, Zhang, & Xiang, 2019) and even fewer on information security studies.

We understood that one of the contributions of this study is the scientific evidence of the factors that reinforce the cognitive processes that involve workers' decision-making in security breaches within organizations. We also consider that our results may bring opportunities to deepen the general deterrence theory in studies related to information security and cybercrimes, for example, by adopting new dimensions related to the future consequences of a previous penalty. The introduction of such new dimensions could serve as an opportunity to transform potential non-compliance into potential compliance behaviors, as suggested in the theoretical study by Ali, Dominic, Ali, Rehman, and Sohail (2021).

Comparing the factors analyzed in this study, the results confirmed moral disengagement as the primary influence in the decision to violate ISP, followed by the perceived penalty. Based on this evidence, the first practical recommendation of this study is to improve organizational communication aimed at mitigating information security vulnerabilities.

Such communication improvement can be implemented in several ways, for example, with training actions that simulate daily work routines and situations that offer opportunities for violating organizational policies, so that professionals can have a real sense of the susceptibility of failures to data protection and mitigate individual tendencies that may favor unwanted behavior.

In addition, given the significant influence of the perceived penalty of violating actions as a force that reduces the intention to violate policies, it is suggested that training also expose the consequences of policy violations as a way of broadening the notion of penalties that employees will be subject to if they behave contrary to internal guidelines.

Another possible way to reduce moral disengagement is the dissemination of internal newsletters that can expose examples of misbehavior to increase the understanding of employees about the internal policies and rules established by the company's governance.

According to the results obtained, it also deserves attention from the information system managers that one cannot affirm that employees who plan to leave their current job tend to violate the safety rules established compared to other employees.

Even though there are studies (Silva & Cappellozza, 2014) that negatively relate affective commitment to turnover intention, our results indicate that information security does not depend on the employees' commitment to the organization; in other words, system vulnerabilities can be initiated by any employee, including those committed to the companies in which they work.

Consequently, the saying "scalded cat fears cold water" also does not apply to the results of this study: the negative experiences that workers have suffered in the context of loss of privacy do not necessarily result in attitudes that qualitatively protect organizational systems.

Thus, the fact that workers have previously had experiences with invasions or loss of private information does not exempt them from the need for training on the security of organizational information systems, given the possibility of committing acts that weaken the protections of the adopted technologies in the company.

In analytical terms, the research model analyzed provides a reasonable prediction regarding the intention to violate ISP, keeping in mind its limitations, as data collection associates a hypothetical situation with the manifestation of a behavioral intention and not, appropriately, the observation of actual security breach behavior.

Future research can adapt the measurement instrument provided in this study with the insertion of actual observations of violations of security policies to compare results and improve collection methods.

Although this study uses a neural network architecture with acceptable statistical values on the residuals and plausible results of the coefficient of determination, it is presumable that the results obtained vary under different samples and network configurations.

Another limitation of the study is the cross-sectional approach of data collection, which, although convenient, has limitations in establishing greater control over the causality of relations. Data collected over extended periods with a longitudinal approach may reveal behavioral patterns over time and shed more light on the phenomenon studied.

As another possibility for future research, after an extensive investigation of the relevant literature and the identification of the adopted constructs, it may be interesting to evaluate the effect of other factors adding to this research model (for example, the perceived complexity of the established security policies) to obtain a more comprehensive view regarding decision-making on this topic.

References

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383. doi: https://doi.org/10.3390/app11083383.

Bandura, A., Barbaranelli, C., Caprara, G. V., & Pastorelli, C. (1996). Mechanisms of moral disengagement in the exercise of moral agency. *Journal of Personality and Social Psychology*, 71(2), 364–374. doi: https://doi.org/10.1037/0022-3514.71.2.364.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, 49(2), 138–150. doi: https://doi.org/10.1016/j.dss.2010.01.010.

Barsky, A. (2011). Investigating the effects of moral disengagement and participation on unethical work behavior. *Journal of Business Ethics*, 104(1), 59–75. doi: https://doi.org/10.1007/s10551-011-0889-7.

Cohen, J. (1988). *Statistical power analysis*, 2nd ed., Hillsdale, NJ: Erlbaum.

Coetzee, M. and van Dyk, J. (2018). Workplace bullying and turnover intention: exploring work engagement as a potential mediator. *Psychological Reports*, 121(2), 375–392. doi: https://doi.org/10.1177/0033294117725073.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedure fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. doi: https://doi.org/10.1287/orsc.10.1.104.

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43–69. doi: https://doi.org/10.1111/isj.12173.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, 31(2), 285–318. doi: https://doi.org/10.2753/MIS0742-1222310210.

Dhillon, G., Talib, Y. Y. A., & Picoto, W. N. (2020). The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems*, 21(1), 152–174. doi: https://doi.org/10.17705/1jais.00595.

Fajardo, J. (2016). Optimal insider strategy with law penalties. *Revista Brasileira de Economia*, 70(1), 31–40. doi: https://doi.org/10.5935/0034-7140.20160002.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, 41(4), 41 doi: https://doi.org/10.3758/BRM.41.4.1149.

Fida, R., Tramontano, C., Paciello, M., Ghezzi, V., & Barbaranelli, C. (2018). Understanding the interplay among regulatory self-efficacy, moral disengagement, and academic cheating behaviour during vocational education: A three-wave study. *Journal of Business Ethics*, 153(3), 725–740. doi: https://doi.org/10.1007/s10551-016-3373-6.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(3). doi: https://doi.org/10.2307/3151312.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management*, 49(6), 320–326. doi: https://doi.org/10.1016/j.im.2012.08.001.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*, 2nd ed., Thousand Oaks, CA: SAGE Publications.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. doi: https://doi.org/10.1108/EBR-11-2018-0203.

Haque, A., Fernando, M., & Caputi, P. (2019). The relationship between responsible leadership and organisational commitment and the mediating effect of employee turnover intentions: an empirical study with Australian employees. *Journal of Business Ethics*, 156(3), 759–774. doi: https://doi.org/10.1007/s10551-017-3575-6.

Hargittai, E., & Marwick, A. (2016). 'What can I really do?' explaining the privacy paradox with online apathy. *International Journal of Communication*, 10(20), 3737–3757.

Haykin, S. (1998). *Neural networks: a comprehensive foundation* (2nd ed.), New York, NY: Macmillan College Publishing.

Hew, J. J., Leong, L. Y., Tan, G. W. H., Ooi, K. B., & Lee, V. H. (2019). The age of mobile social commerce: An artificial neural network analysis on its resistances. *Technological Forecasting and Social Change*, 144, 311–324. doi: https://doi.org/10.1016/j.techfore.2017.10.007.

Hong, W., Chan, F. K. Y., & Thong, J. Y. L. (2021). Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective. *Journal of Business Ethics*, 168(3), 539–564. doi: https://doi.org/10.1007/s10551-019-04237-1.

ISO/IEC 27002:2013 (2013). Information technology – security techniques – code of practice for information security controls.

International Organization for Standardization (2013). Information technology – security techniques – code of practice for information security controls. Retrieved from www.iso.org/standard/54533.html (accessed 25 November 2020).

Katz, D., & Kahn, R. L. (1978). *The Social Psychology of Organizations*, New York, NY: Wiley.

Kauspadiene, L., Ramanauskaite, S., & Cenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*, 1–19, doi: https://doi.org/10.3846/tede.2019.10298.

Khan, S., Dapeng, L., Adnan Muhammad, S., & Ullah, R. (2018). The buffering role of ethical leadership in moral disengagement: Anticompetitive behavioral tendency link. *Proceedings of the European Conference on Management, Leadership & Governance*, pp. 345-351.

Kish-Gephart, J., Detert, J., Treviño, L., Baker, V., & Martin, S. (2014). Situational moral disengagement: Can the effects of Self-Interest be mitigated? *Journal of Business Ethics*, 125(2), 267–285. doi: https://doi.org/10.1007/s10551-013-1909-6.

Lee, V.-H., Hew, J.-J., Leong, L.-Y., Tan, G. W.-H., & Ooi, K.-B. (2020). Wearable payment: A deep learning-based dual-stage SEM-ANN analysis. *Expert Systems with Applications*, 157, 1–15. doi: https://doi.org/10.1016/j.eswa.2020.113477.

Leong, L.-Y., Hew, T.-S., Wei-Han, T. G., & Ooi, K.-B. (2013). Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach. *Expert Systems with Applications*, 40(14), 5604–5620. doi: https://doi.org/10.1016/j.eswa.2013.04.018.

Leong, L.-Y., Hew, T., Lee, V.-H., & Ooi, K. (2015). An SEM-artificial-neural-network analysis of the relationships between SERVPERF, customer satisfaction and loyalty among low-cost and fullservice airline. *Expert Systems with Applications*, 42(19), 6620–6634. doi: https://doi.org/10.1016/j.eswa.2015.04.043.

Levav, J., Heitmann, M., Herrmann, A., & Iyengar, S. S. (2010). Order in product customization decisions: Evidence from field experiments. *Journal of Political Economy*, 118(2), 274–299. doi: https://doi.org/10.1086/652463.

Liébana-Cabanillas, F., Marinković, V., & Kalinić, Z. (2017). A SEM-neural network approach for predicting antecedents of m-commerce acceptance. *International Journal of Information Management*, 37(2), 14–24. doi: https://doi.org/10.1016/j.ijinfomgt.2016.10.008.

Maliki, O. S., Agbo, A. O., Maliki, A. O., Ibeh, L. M., & Agwu, C. O. (2011). Comparison of regression model and artificial neural network model for the prediction of electrical power generated in Nigeria. *Advances in Applied Science Research*, 2(5), 329–339.

Manzoor, M. T., Manzoor, T., & Khan, M. (2020). Workplace incivility: A cynicism booster leading to turnover intentions. *DECISION*, 47(1), 91–99. doi: https://doi.org/10.1007/s40622-020-00238-6.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36–58. doi: https://doi.org/10.1509/jm.15.0497.

McCandless, D. Evans, T. Barton, P. Starling, S., & Geere, D. (2020). World¨s biggest data breaches & hacks. Retrieved from www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (accessed 23 July 2020).

Mölders, S., Brosi, P., Spörrle, M., & Welpe, I. M. (2019). The effect of top management trustworthiness on turnover intentions via negative emotions: The moderating role of gender. *Journal of Business Ethics*, 156(4), 957–969. doi: https://doi.org/10.1007/s10551-017-3600-9.

Moore, C., Detert, J. R., Trevino, L. K., Baker, V. I., & Mayer, D. M. (2012). Why employees do bad things: Moral disengagement and unethical organizational behavior. *Personnel Psychology*, 65(1), 1–48. doi: https://doi.org/10.1111/j.1744-6570.2011.01237.x.

Morgan, S. (2019). Official annual cybercrime report. Retrieved from www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (accessed 5 July 2020).

Mowday, R. T., Porter, L. W., & Steers, R. M. (1982). *Employee-organization linkages: The psychology of commitment, absenteeism, and turnover*, New York, NY: Academic Press.

Murphy, P., & Dacin, M. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics*, 101(4), 601–618. doi: https://doi.org/10.1007/s10551-011-0741-0.

Ohunakin, F., Adeniji, A., Oludayo, O., & Osibanjo, O. (2018). Perception of frontline employees towards career growth opportunities: Implications on turnover intention. *Business: Theory and Practice*, 19(0), 278–287. doi: https://doi.org/10.3846/btp.2018.28.

Ooi, K. B., Hew, J. J., & Lin, B. (2018). Unfolding the privacy paradox among mobile social commerce users: A multi-mediation approach. *Behaviour & Information Technology*, 37(6), 575–595. doi: https://doi.org/10.1080/0144929X.2018.1465997.

Pahnila, S., Siponem, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study. Paper presented at the PACIS Proceedings.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. doi: https://doi.org/10.1037/0021-9010.88.5.879.

Rafiq, M., Wu, W., Chin, T., & Nasir, M. (2019). The psychological mechanism linking employee work engagement and turnover intention: A moderated mediation study. *Work*, 62(4), 615–628. doi: https://doi.org/10.3233/WOR-192894.

Ramos, F. L., Ferreira, J. B., de Freitas, A. S., & Rodrigues, J. W. (2018). The effect of trust in the intention to use m-banking. *Brazilian Business Review*, 15(2), 175–191. doi: https://doi.org/10.15728/bbr.2018.15.2.5.

Ripley, B. D. (1996). *Pattern recognition and neural networks*, Cambridge: Cambridge University Press.

Santiago, A. B. B., Diño, M. J., & Caballero, M. E. (2017). Plagiarism in advanced educational research: Reasons, extent, perceived penalty and severity. *International Journal of Business and Social Science*, 8(4), 121–124.

Santos, J. G., Cappellozza, A., & Albertin, A. L. (2018). Antecedents of perceived benefits of compliance towards organizational data protection policies. *IEEE Latin America Transactions*, 16(3), 891–896. doi: https://doi.org/10.1109/TLA.2018.8358670.

Sen, R. and Borle, S. (2015). Estimating the contextual risk of data breach: an empirical approach. *Journal of Management Information Systems*, 32(2), 314–341. doi: https://doi.org/10.1080/07421222.2015.1063315.

Sen, R., Verma, A., & Heim, G. R. (2020). Impact of cyberattacks by malicious hackers on the competition in software markets. *Journal of Management Information Systems*, 37(1), 191–216. doi: https://doi.org/10.1080/07421222.2019.1705511.

Silva, R. S., & Cappellozza, A. (2014). O impacto do suporte organizacional e do comprometimento afetivo sobre a rotatividade. *Revista de Administração IMED*, 4(3), 314–329. doi: https://doi.org/10.18256/2237-7956/raimed.v4n3p314-329.

Siqueira, M. M. M., Gomide, S. Jr., Oliveira, A. F., & Polizzi Filho, A. (2014). Intenção de rotatividade. In M. M. M. Siqueira (Ed.), *Novas medidas do comportamento organizacional: ferramentas de diagnóstico e de gestão*, Porto Alegre: Artmed.

Smith, H., Milberg, S., & Burke, S. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167–196. doi: https://doi.org/10.2307/249477.

Soltis, S. M., Agneessens, F., Sasovova, Z., & Labianca, G. (2013). A social network perspective on turnover intentions: The role of distributive justice and social support. *Human Resource Management*, 52(4), 561–584. doi: https://doi.org/10.1002/hrm.21542.

Sternad Zabukovšek, S., Kalinic, Z., Bobek, S., & Tominc, P. (2019). SEM–ANN based research of factors' impact on extended use of ERP systems. *Central European Journal of Operations Research*, 27(3), 703–735. doi: https://doi.org/10.1007/s10100-018-0592-1.

Straub, D. W. (1990). Effective is security: An empirical study. *Information Systems Research*, 1(3), 255–276. doi: https://doi.org/10.1287/isre.1.3.255.

Tinwala, R., & Biswas, U. N. (2020). Perceived sustainability practices, turnover intentions, and organizational identification in hotel industries. *Management: Journal of Sustainable Business & Management Solutions in Emerging Economies*, 25(1), 1–11, doi: https://doi.org/10.7595/management.fon.2019.0009.

Valle, M., Kacmar, K. M., & Zivnuska, S. (2019). Understanding the effects of political environments on unethical behavior in organizations. *Journal of Business Ethics*, 156(1), 173–188. doi: https://doi.org/10.1007/s10551-017-3576-5.

Xu, Y., Zhang, W., Bao, H., Zhang, S., & Xiang, Y. (2019). A SEM–neural network approach to predict customers' intention to purchase battery electric vehicles in china's Zhejiang province. *Sustainability*, 11(11). doi: https://doi.org/10.3390/su11113164.

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly*, 44(2), 907–931. doi: https://doi.org/10.25300/MISQ/2020/15477.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, 23(4), 1342–1363. doi: https://doi.org/10.1287/isre.1120.0416.

Zheng, X., Qin, X., Liu, X., & Liao, H. (2019). Will creative employees always make trouble? Investigating the roles of moral identity and moral disengagement. *Journal of Business Ethics*, 157(3), 653–672. doi: https://doi.org/10.1007/s10551-017-3683-3.

Appendix

Construct	Item
Intention to violate information security policies	How likely is it that you would have done the same as Jim in that situation? I could see myself sharing the password as Jim did
Perceived penalty	What is the likelihood that Jim would be formally punished? Jim would be reprimanded at some point for sharing the password Jim would receive harsh sanctions for sharing the password If punished, Jim's punishment would be immediate
Turnover intention	I think about leaving the company where I work I plan to leave the company where I work I want to leave the company where I work
Moral disengagement	Sharing a password really would not hurt the organization Giving a password to a coworker if he/she needs it does not really do any harm It is okay to share a password because no direct damage is done to the company
Privacy invasion	I have already been a victim of the invasion of the privacy of my personal data Recently, I have heard or read, about the misuse of personal data I see news of data leaks from companies
Common method bias	I like outside activities better than inside activities ($r = 0.08^{\text{NS}}$) I like to meet my friends at a restaurant more than at home ($r = 0.01^{\text{NS}}$) I exercise every day ($r = -0.07^{\text{NS}}$) Jim is an employee in your organization. One day while Jim is out of the office on
Information security policies	A sick day, one of his coworkers needs a file on Jim's computer. The coworker is of
Violation scenario	equal rank and performs job functions similar to Jim's. The coworker calls Jim and asks for the password. Although Jim knows that your organization has a policy that
(Vignette)	passwords must not be shared, he shares his password with the coworker

Note: NS: not significant

Table A1. Survey items and vignette

Author contributions are as follows: Alexandre Cappellozza – Corresponding Author, Conceptualization (Lead), Formal analysis (Lead), Methodology (Lead), Project administration (Lead), Supervision (Lead), Writing-original draft (Lead). Gustavo Hermínio Salati Marcondes de Moraes – Data curation (Supporting), Formal analysis (Supporting), Methodology (Supporting), Validation (Supporting), Visualization (Lead), Writing-review & editing (Lead). Gilberto Perez – Methodology (Supporting), Validation (Supporting), Visualization (Supporting), Writing-review & editing (Supporting). Alessandra Lourenço Simões – Writing-original draft (Supporting).

Corresponding author
Alexandre Cappellozza can be contacted at: alexandre.cappellozza@mackenzie.br

Associate editor: Violeta Sun