Revista Argentina de Clínica Psicológica
2020, Vol. XXIX, N°1, 442-452
DOI: 10.24205/03276716.2020.60

RELATIONSHIP BETWEEN INFORMATION SECURITY BEHAVIOR AND SATISFACTION DEGREE OF PSYCHOLOGICAL NEEDS AND THE MEDIATION EFFECT OF TEAM EFFECTIVENESS AND ORGANIZATIONAL COMMITMENT

Jie Zhen[1], Zongxiao Xie[2], Kunxiang Dong[3]*

Abstract

Considering the importance of corporate information security management, this paper explores how employee's information security behavior is influenced by the satisfaction degree of their psychological needs, based on self-determination theory (SDT) and hierarchical regression. During the exploration, the employees' psychological needs were divided into three types: autonomy needs, competence needs and relatedness needs. Next, the authors discussed how that influence is mediated by team effectiveness and organizational commitment. The results show that, the satisfaction degrees of autonomy needs, competence needs and relatedness needs all have a positive influence on the information security behavior; the influence of the satisfaction degree of autonomy needs over the information security behavior is positively regulated by team effectiveness, while the influence of the satisfaction degree of autonomy needs and relatedness needs is positively regulated by organizational commitment. The research findings lay the basis for improving corporate information security management and preventing information security violations by employees.

Key words: *Self-Determination Theory (SDT), Team Effectiveness, Organizational Commitment, Information Security Behavior.*

Received: 29-01-19 | Accepted: 04-05-19

INTRODUCTION

With the wide application of information technology and information systems, information has become a key resource for the survival and development of enterprises. However, frequent information security incidents often cause economic losses to enterprises. In fact, about 80% of information security risks are induced by the employees' information security violations, which has become a major threat to corporate information security (Anderson, Baskervill, & Kaul, 2017). Therefore, if the information security violation behavior of employees cannot be effectively reduced, or the employees' protection of information resources cannot be motivated, it will be difficult to guarantee the information security of the companies (Lee, Lee, & Kim, 2016).

There are three types of unfavorable factors in information security management: (1) Employees' information security awareness is weak, they lack of initiative for corporate information security risks, and some employees even have negative emotions toward information security (D'Arcy, Herath, & Shoss, 2014); (2) The employees lack of knowledge for effective information security risk control, which directly reduces their decision-making ability

[1]School of Business Planning, Chongqing Technology and Business University, Chongqing 400067, China. [2]China Financial Certification Authority, Beijing 100054, China. [3]School of Management Science & Engineering, Shandong University of Finance and Economics, Jinan 250014, China. E-Mail: zhenjie@vip.126.com

when facing information security risks, and this may lead to serious information security violations (Flores, Antonsen, & Ekstedt, 2014); (3) Enterprises have not given sufficient support, resulting in it's difficult for employees to receive information security related trainings (Liu, Ji, & Mookerjee, 2011). It can be seen that how to formulate practical and feasible information security management strategies to improve employees' information security behavior has not received sufficient attention in organizational management.

At the same time, there are also limitations in the research on the employees' information security behavior: (1) there're more analysis of the influence of external environmental factors on employees' information security violations, but there're few discussions on the influence of employees' internal self-management and self-control on their information security behavior. (2) The research perspective is relatively simple. Most of the discussions on the employees' information security violations are based on the perspective of "the evil of human nature", applying the deterrence theory, moral disengagement theory and the techniques of neutralization theory (Cram, Proudfoot, & D'Arcy, 2017), these researches analyze the control strategies of employees' information security violations. Based on this, this paper starts from the perspective of "the goodness of human nature", and applies the self-determination theory (SDT) to discuss how the satisfaction of individual employee's psychological needs affects their information security behavior, and analyze the mediating role of team effectiveness and organizational commitment in this process to reveal the formation mechanism of the employees' information security behavior.

THEORETICAL BASIS AND RESEARCH HYPOTHESES

Satisfaction degree of autonomy needs, competence needs and relatedness needs and the information security behavior

Self-determination theory (SDT) believes that only external motivations that have satisfied the inner psychological needs will improve the internal motivation of the individual, while external incentives that have harmed the basic psychological needs will reduce the internal motivation of the individual. The internal psychological needs of the individual mainly include three aspects: autonomy needs, competence needs and relatedness needs (Deci & Ryan, 2008).

Employees with higher autonomy needs will try to solve the security risks encountered in their work by themselves, and intend to obtain feedback from the management level in the process of problem solving, so as to correct or enhance their ability to resolve information security risks autonomously (Hu, West, & Smarandescu, 2015). That is, if the employees' working behavior to solve the information security risks is supported by the organization, their satisfaction of autonomy needs will be improved, which will stimulate their positive working attitude, and employees with a positive working attitude will demonstrate stronger self-confidence and resilience in information security management, making their working behavior consistent with the information security management requirements (Son, 2011). Based on this, the following hypothesis is proposed:

H1: The satisfaction degree of autonomy needs has a positive influence on the employees' information security behavior.

Employees with higher competence needs will weigh in a timely manner whether their opinions and actions are contrary to the wishes of corporate managers. Once these employees are given certain rights, their competence needs may achieve a higher degree of satisfaction, and they will have the internal motivation to take the initiative to take responsibility and face the challenges at work (Gagne & Deci, 2005). Employees with higher degree of satisfaction of competence needs can make the highest-level autonomous response within their scope of rights in information security management. At the same time, since the employees have felt the trust from the managers, their sense of responsibility will be further strengthened, and their behavior of protecting the corporate information resources will be stimulated (Posey, Roberts, Lowry et al., 2013). Based on this, the following hypothesis is proposed:

H2: The satisfaction degree of competence needs has a positive influence on the employees' information security behavior.

When a company upgrades its information technology/system, employees with a higher degree of satisfaction of relatedness needs will take the initiative to cope with the changes, and they are willing to actively learn and receive

training to improve their work behavior in order to match their working a behavior with the goal of the organization (Hsu, Shih, Yu et al., 2015). Moreover, employees with a higher degree of satisfaction of relatedness needs can also perceive that they are favored by their colleagues, and thus more actively express their own ideas and give suggestions to promote the achievement of organizational goals (Gagne & Deci, 2005). It is concluded that employees with a higher degree of satisfaction of relatedness needs are more willing to implement information security behavior. Based on this, the following hypothesis is proposed:

H3: The satisfaction degree of relatedness needs has a positive influence on the employees' information security behavior.

The mediator effect of team effectiveness

Since it's easier for the team to work under the background of rapid information technology upgrade, many organizations have adopted the form of team work. Employees with a high degree of autonomy needs tend to achieve their self-actualization, which means that compared with other team members, they like to face challenges more. With the support of team resources, these employees can generate higher degree of autonomy needs satisfaction, which will bring higher performance for the team (Posey, Roberts, Lowry et al., 2014). When employees in an efficient team face information security risks, they are more likely to form synergies within the team and actively cope with the information security problems that arise during the work. Therefore, the following hypothesis is proposed:

H4: Team effectiveness plays a mediating role in the relationship between the satisfaction of autonomy needs and the employees' information security behavior.

Employees with high competence needs will fully mobilize their psychological cognitive resources to complete the information security behavior required by the team. With the support of team resources, employees can share and integrate the information security knowledge; moreover, it also facilitates them to optimize the cognitive resources. Members in an efficient team are more sensitive to relevant environmental information, and are more likely to discover and collect knowledge for task completion, which is helpful to motivate the employees to implement the information security behavior. Therefore, the following hypothesis is proposed:

H5: Team effectiveness plays a mediating role in the relationship between the satisfaction of competence needs and the employees' information security behavior.

In team work, due to the increase of individual participation, the employees' satisfaction of interpersonal relationship is relatively high. In such case, they will implement the information security behavior that is beneficial to the organization's interests based on team goals. At the same time, employees with a higher degree of satisfaction of relatedness needs trust each other, which is helpful to improve the team effectiveness. Employees in an efficient team will adapt to the fast-changing information security requirements better. Based on this, it is concluded that team effectiveness can enhance employees' confidence in implementing information security behavior. Therefore, the following hypothesis is proposed:

H6: Team effectiveness plays a mediating role in the relationship between the satisfaction of relatedness needs and the employees' information security behavior.

The mediator effect of organizational commitment

The process of information security management affecting the employees is the process of the employees' experience from recognition to acceptance, and it is also the formation process of organizational commitment. On the one hand, when employees' autonomy needs are met, they are more likely to recognize the requirements of the organization, and they are more willing to implement the information security behavior; on the other hand, when the employees' autonomy needs are met, they won't have a compulsive feeling towards the execution of the information security management, this will increase the level of organizational commitment, and the organizational commitment has a positive influence on the information security behavior (Aurigmma & Leonard, 2015). Based on this, the following hypothesis is proposed:

H7: Organizational commitment plays a mediating role in the relationship between the satisfaction of autonomy needs and the employees' information security behavior.

The satisfaction of competence needs is the overall feeling of employees towards their

works, and it is the employee's subjective evaluation of the trust of the organization in the process of social exchange between the employee and the organization. When the employee perceives that the company is willing to believe and authorize him/her to perform certain behaviors, he/she will continue to gain and enhance his/her recognition of the organization. The increase in the level of organizational commitment will enable employees to better understand the organization's security requirements and increase their acceptance and compliance with the information security behavior (Aurigmma & Leonard, 2015). Based on this, the following hypothesis is proposed:

H8: Organizational commitment plays a mediating role in the relationship between the satisfaction of competence needs and the employees' information security behavior.

The satisfaction of the employees' relatedness needs is helpful to the internalization of the organization's behavior requirement and to enhance the employee's recognition of the organization. At the same time, good relations within the organization can enhance employees' recognition of the organization's goal and their sense of responsibility to the organization, which is also a concrete manifestation of organizational commitment. Employees with a high level of organizational commitment hope that their information security behavior is aligned with the expectation of the organization and is beneficial to the goal of the organization, and they are willing to reward the company with persistent information security behavior (Posey, Roberts, & Lowry, 2015). Based on this, the following hypothesis is proposed:

H9: Organizational commitment plays a mediating role in the relationship between the satisfaction of relatedness needs and the employees' information security behavior.

In summary, this study proposes a research model as shown in Figure 1.

RESEARCH METHODS

Sample selection and data collection

This research collected data through questionnaires. With the help of relevant industry associations and third-party certification authorities, from June 1, 2018 to July 30, 2018, the research team sent out 300 electronic questionnaires through emails to employees in companies that had clearly carried out information security management. At last, 215 valid questionnaires were returned. The descriptive statistics of the respondents are shown in Table 1.

Variables and measurement

In order to ensure the reliability and validity of the measuring tools, this study adopted the widely used research scales, combining with the research scenarios, several measurements items of individual variables had been modified. The questionnaire is a five-point Likert scale, with 1 point being strongly disagree and 5 points being strongly agree.

Figure 1. **Diagrammatic sketch of research method**

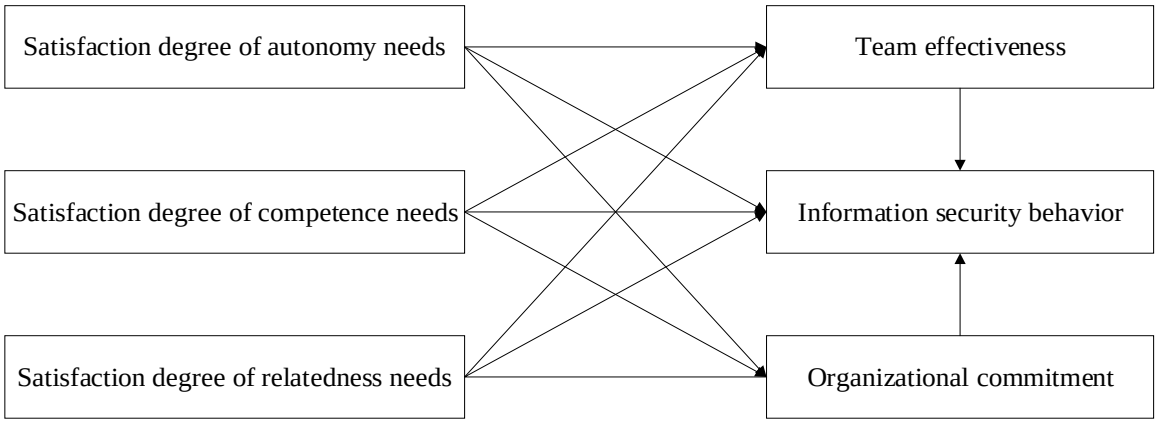

Table 1. **Descriptive statistics of the samples**

Employee characteristics	Categories	Frequency	Percentage (N=215)
Gender	Male	124	57.7%
	Female	91	42.3%
Age	20-30	99	46.1%
	31–40	79	36.7%
	>40	37	17.2%
Education level	Polytechnic and below	17	7.9%
	Bachelor	110	51.2%
	Master's and PhD	88	40.9%
Industry type	Software	57	26.5%
	Financial services	76	35.4%
	Manufacturing	49	22.8%
	Telecommunications	33	15.3%
Firm size	<100	31	14.4%
	100–199	60	27.9%
	200–300	83	38.6%
	>300	41	19.1%

(1) Independent variables-satisfaction degree of autonomy needs, satisfaction degree of competence needs, and satisfaction degree of relatedness needs. Measurements of the independent variables were modified according to the scale proposed by Chen, Vansteenkiste, Beyers et al. (2015).

(2) Dependent variable – information security behavior. The measurement of employees' information security behavior was modified according to the scales proposed by Cheng, Li, Li et al. (2013) and Posey, Roberts, & Lowry (2015), and the scales were applied to measure the employees' behavior in information security compliance, information security protection and information security participation.

(3) Mediator variables – team effectiveness and organizational commitment. The measurement of team effectiveness was modified according to the scale proposed by Lester, Meglino, & Korsgaard (2017), it was used to measure the team performance and teamwork satisfaction, respectively; the measurement of organizational commitment was measured by the scale which combined the scales of Posey, Roberts, & Lowry, (2015) and Aurigemma & Leonard (2015), it was used to measure contents of three aspects: the emotion commitment, the norm commitment and the persistence commitment.

(4) Control variables – gender, age, education level, industry type, and firm size. For employees of different genders, their attitudes toward work risks are different; older employees generally have richer work experience; and the education level has an impact on the employees' cognitive ability. Therefore, the gender, age, and education level of employees may influence their information security behavior. In addition, different industries have different degrees of dependence on information technology and information systems, which in turn leads to differences in the information security behavior of employees in different industries. Different firm sizes mean that the management level and IT department size are different, which also has an impact on the employees' information security behavior.

EMPIRICAL RESULTS AND ANALYSIS

Common method biases

In the empirical study based on questionnaires, if the observed variables are answered by the same subject, it is easy to cause the problem of common method biases. In order to eliminate the influence of common method biases, this study adopted the Harman single factor test in the control link of the statistics. The test results show that the variance of the first factor is 34.047%<40%, which indicates that there is no obvious common method bias problem in the research data.

Reliability and validity test

In this study, Composite Reliability (CR) and factor load were used to evaluate the reliability of the scale; the confirmatory factor analysis was applied to check the structural validity of the scale, whether the square root of the latent variable AVE is greater than the correlation value between the latent variables or not was used to test the validity of the scale, and the AVE was used to evaluate the convergent validity of the

scale. Relevant indicators are shown in Table 2.

It can be seen from Table 2 that the CR values of the six latent variables are 0.923, 0.915, 0.918, 0.941, 0.948, and 0.901, respectively, which are greater than 0.5; the Cronbach's α values of the six latent variables are 0.873, 0.861, 0.858, 0.916, 0.919 and 0.906, respectively, all greater than 0.7, indicating that the scale has a higher level of reliability. At the same time, the AVE values of the six latent variables are 0.800, 0.783, 0.790, 0.800, 0.859 and 0.842, respectively, which are all greater than 0.5; the factor load values of the six latent variable measurement items are all above 0.7, indicating that the scale is of high validity level.

Descriptive statistics

It can be seen from Table 3 that the satisfaction degree of autonomy needs is positively correlated with the satisfaction degree of competence needs (r=0.695, p<0.01), the satisfaction degree of autonomy needs is positively correlated with the satisfaction degree of relatedness needs (r=0.651, p<0.01), the satisfaction degree of autonomy needs is positively correlated with team effectiveness (r=0.403, p<0.01), the satisfaction degree of autonomy needs is positively correlated with the organizational commitment (r=0.410, p<0.01), the satisfaction degree of autonomy needs is positively correlated with the information security behavior (r=0.583, p<0.01); the satisfaction degree of competence needs is positively correlated with the satisfaction degree of relatedness needs (r=0.832, p<0.01), the satisfaction degree of competence needs is positively correlated with team effectiveness (r=0.470, p<0.01), the satisfaction degree of

Table 2. **Evaluation indicators for the reliability and validity of the measurement scale**

Constructs	Measurement items	Loadings	AVE	CR	Cronbach's α
Satisfaction degree of autonomy needs	Information security management does not make me uncomfortable.	0.926	0.800	0.923	0.873
	I can accept the security requirements of my organization.	0.907			
	Following security requirements is the right thing to do.	0.848			
Satisfaction degree of competence needs	I have the ability to accomplish my security-related work.	0.905	0.783	0.915	0.861
	I have a sense of accomplishment when finishing security-related work.	0.892			
	I feel more confident when finishing security-related work.	0.857			
Satisfaction degree of relatedness needs	My organization cares about my experiences in security management.	0.921	0.790	0.918	0.858
	At security-related work, I depend on my colleagues.	0.917			
	At security-related work, I am close to my colleagues.	0.825			
Team effectiveness	Employees of my team help each other about the security policies.	0.928	0.800	0.941	0.916
	Employees of my team volunteer to do security-related behaviors.	0.908			
	Employees of my team help new colleagues adapt to security policies.	0.914			
	Employees of my team share security-related knowledge to each other.	0.824			
Organizational commitment	I am willing to put effort into my organization.	0.939	0.859	0.948	0.919
	I am willing to put effort in my security-related work.	0.925			
	Being successful in my organization is important to me.	0.916			
Information security behavior	I would follow my organization's information security policy.	0.927	0.842	0.901	0.906
	I would like to protect my organization's information resources.	0.921			
	I am involved in organizational security activities.	0.904			

Table 3. **Mean, standard deviation and correlation coefficient**

	Mean	Std.	1	2	3	4	5	6
1. Satisfaction degree of autonomy needs	4.115	0.920	1					
2. Satisfaction degree of competence needs	4.186	0.905	0.695**	1				
3. Satisfaction degree of relatedness needs	4.152	0.881	0.651**	0.832**	1			
4. Team effectiveness	3.613	1.162	0.403**	0.470**	0.435**	1		
5. Organizational commitment	3.894	0.908	0.410**	0.434**	0.461**	0.231**	1	
6. Information security behavior	4.191	1.038	0.583**	0.669**	0.705**	0.308**	0.462**	1

Note: ** indicates p<0.01.

competence needs is positively correlated with organizational commitment (r=0.434, p<0.01), the satisfaction degree of competence needs is positively correlated with information security behavior (r=0.669, p<0.01); the satisfaction degree of relatedness needs is positively correlated with team effectiveness (r=0.435, p<0.01), the satisfaction degree of relatedness needs is positively correlated with organizational commitment (r=0.461, p<0.01), the satisfaction degree of relatedness needs is positively correlated with information security behavior (r=0.705, p<0.01); team effectiveness and organizational commitment are positively correlated (r=0.231, p<0.01), team effectiveness and information security behavior is positively correlated (r=0.308, p<0.01); organizational commitment and information security behavior are positively correlated (r=0.462, p<0.01). The above results are consistent with the theoretical expectations and they provide a support for subsequent hypothesis testing.

Hypothesis testing

This study used hierarchical regression to test the direct effects between variables. The results of regression analysis are shown in Table 4. Wherein, Model 1 takes the control variables as the independent variables, and takes the information security behavior as the dependent variable; Model 2 takes the control variables, the satisfaction degree of autonomy needs, the satisfaction degree of competence needs, and the satisfaction degree of relatedness needs as the independent variables, and takes the information security behavior as the dependent variable; Model 3 takes the control variables, the satisfaction degree of autonomy needs, the satisfaction degree of competence needs, the satisfaction degree of relatedness needs, the team effectiveness and the organizational commitment as independent variables, and takes the information security behavior as the dependent variable; Model 4 takes the control variables, the satisfaction degree of autonomy needs, the satisfaction degree of competence needs, and the satisfaction degree of relatedness needs as the independent variables, and takes the team effectiveness as the dependent variable; Model 5 takes the control variables, the satisfaction degree of autonomy needs, the satisfaction degree of competence needs, and the satisfaction degree of relatedness needs as the independent variables, and takes the organizational commitment as the dependent variable.

The results of Model 1 show that the regression coefficients of all control variables are not significant, indicating that the control variables are not sufficient to explain the information security behavior; the results of Model 2 show that the satisfaction degree of autonomy needs has a significant positive impact on information security behavior (β=0.180, p<0.5), the satisfaction degree of competence needs has a significant positive impact on information security behavior (β=0.211, p<0.5), the satisfaction degree of relatedness needs has a significant positive impact on information security behavior (β=0.525 , p<0.001). Therefore, H1, H2, and H3 have been verified.

The results of Model 3 show that team effectiveness has a significant positive influence on information security behavior (β=0.181, p<0.01), and organizational commitment has a significant positive influence on information security behavior (β=0.473, p<0.05); the results of Model 4 show that the satisfaction degree of autonomy needs has a significant positive influence on team effectiveness (β=0.290, p<0.05), the influence of the satisfaction degree of competence needs on the team effectiveness

Table 4. **Results of regression analysis**

	Dependent variable			*Mediator variable*	
	Information security behavior			Team effectiveness	Organizational commitment
	M1	***M2***	***M3***	***M4***	***M5***
Control variables					
Gender	0.148	0.105	0.128	0.153	-0.108
Age	-0.039	-0.064	-0.070	0.023	0.044
Education level	0.036	0.034	0.036	0.043	-0.036
Industry type	0.064	0.017	0.039	-0.001	0.011
Firm size	0.012	0.022	0.022	0.003	-0.016
Independent variables					
Satisfaction degree of autonomy needs		0.180*		0.290*	0.175*
Satisfaction degree of competence needs		0.211*		0.088	0.074
Satisfaction degree of relatedness needs		0.525***		0.449**	0.300**
Mediator variables					
Team effectiveness			0.181**		
Organizational commitment			0.473***		
R^2	0.023	0.539	0.271	0.220	0.240
Adjust R^2	0.001	0.521	0.246	0.190	0.211

Note: * indicates p<0.05, ** indicates p<0.01, *** indicates p<0.001, the same below.

Table 5. **Analysis of the mediator effect of team effectiveness and organizational commitment**

	Point estimation	**Correlation coefficient**		**95% confidence interval**		**Deviation correlation (95%)**		**Deviation correlation and enhancement (95%)**	
		SE	*z*	Lower	Upper	Lower	Upper	Lower	Upper
Indirect effect (Satisfaction degree of autonomy needs)									
Team effectiveness	0.040	0.030	1.984*	0.018	0.085	0.015	0.089	0.016	0.089
Organizational commitment	0.124	0.038	3.278**	0.062	0.210	0.060	0.197	0.053	0.182
Total	0.164	0.419		0.077	0.246	0.075	0.230	0.068	0.214
Indirect effect (Satisfaction degree of relatedness needs)									
Team effectiveness	0.006	0.031	0.019	-0.055	0.069	-0.049	0.065	-0.056	0.068
Organizational commitment	0.095	0.041	2.154*	0.028	0.181	0.028	0.180	0.025	0.160
Total	0.101	0.055		0.007	0.197	0.004	0.184	0.007	0.163

is not significant (β=0.088, p>0.05), the satisfaction degree of relatedness needs has a significant positive influence on team effectiveness (β=0.449, p<0.01); the results of Model 5 show that the satisfaction degree of autonomy needs has a significant positive influence on organizational commitment (β=0.175, p<0.05), the influence of the satisfaction degree of competence needs on the organizational commitment is not significant (β=0.074, p>0.05), the satisfaction degree of relatedness needs has a significant positive influence on organizational commitment (β=0.300, p<0.01). Therefore, the hypotheses H5 and H8 have been rejected.

This study is based on the BOOTSTRAP method. Using the PROCESS plug-in in SPSS, the sample size was set to 5000, the confidence interval was set to 95%, concerning the theoretical model, the multiple mediator effect was tested, and the results are shown in Table 5.

It can be seen from Table 5 that the total indirect effect of the satisfaction degree of autonomy needs on information security behavior is 0.164, the deviation correction and enhancement of the 95% BOOTSTRAP confidence interval is [0.068, 0.214], and the confidence interval does not contain 0. Therefore, the total indirect effect of the satisfaction degree of autonomy needs is significant; the total indirect effect of the satisfaction degree of relatedness needs is 0.101, the deviation correction and enhancement of the 95% BOOTSTRAP

confidence interval is [0.007, 0.163], and the confidence interval does not contain 0. In conclusion, the total indirect effect of the satisfaction degree of autonomy needs is significant.

In the testing process of multiple mediator effect, in addition to pay attention to the total indirect effect, the single mediator effect between the variables should also be analyzed. It can be seen from Table 5 that the mediator effect of the satisfaction degree of autonomy needs through team effectiveness on information security behavior is 0.040 (z=1.984, $p<0.05$), the deviation correction and enhancement of the 95% BOOTSTRAP confidence interval is [0.016, 0.089], and the confidence interval does not contain 0. Therefore, H4 has been verified; the mediator effect of the satisfaction degree of autonomy needs through organizational commitment on information security behavior is 0.124 (z=3.278, $p<0.01$), the deviation correction and enhancement of the 95% BOOTSTRAP confidence interval is [0.053, 0.182], and the confidence interval does not contain 0. Therefore, H7 has been verified; the mediator effect of the satisfaction degree of relatedness needs through team effectiveness on information security behavior is 0.006 (z=0.019, $p>0.05$), the deviation correction and enhancement of the 95% BOOTSTRAP confidence interval is [-0.056, 0.068], and the confidence interval contains 0. Therefore, H6 has been rejected; the mediator effect of the satisfaction degree of relatedness needs through organizational commitment on information security behavior is 0.095 (z=2.154, $p<0.01$), the deviation correction and enhancement of the 95% BOOTSTRAP confidence interval is [0.025, 0.160], and the confidence interval does not contain 0. Therefore, H9 has been verified.

RESEARCH CONCLUSIONS AND MANAGEMENT IMPLICATIONS

Research conclusions

(1) The satisfaction degrees of autonomy needs, competence needs and relatedness needs all have a positive influence on the information security behavior. When the employees' needs are met, the self-motivation effect will make them continuously improve their information security behavior to meet the requirements of corporate information security management. At the same time, the theoretical research of corporate information security management should not only be based on organizational management requirements, it also needs to pay attention to the internal psychological needs of employees, and meanwhile taking into account the needs of management subjects and objects, so as to achieve the matching of information security management and the needs of the employees.

(2) Team effectiveness plays a mediator role in the relationship between the satisfaction degree of autonomy needs and information security behavior. This shows that the employees' satisfaction degree of autonomy needs not only directly affects their information security behavior, but also has an indirect influence on the information security behavior through team effectiveness. This provides a theoretical reference for studying the mediating mechanism of the employees' information security behavior.

(3) Organizational commitment plays a mediator role in the relationship between the satisfaction degree of autonomy needs, the satisfaction degree of relatedness needs, and the information security behavior. In corporate information security management, the satisfaction degree of autonomy needs and relatedness needs of the employees will affect their recognition of the organization, and the organizational commitment level of the employees will ultimately be reflected in the form of the employees' information security behavior, which also enriches the theoretical study of the mediating mechanism of the employees' information security behavior.

Management implications

(1) In information security management, we should pay attention to the degree of satisfaction of employees' internal needs, and design humanized management measures to continuously improve employees' internal satisfaction. For example, motive the enthusiasm of employees to participate in information security through informal organizations within the company, and give feedback to their confusions in information security management; enrich the knowledge of the employees by holding information security trainings to improve their cognition and control level of the information security requirements; closer the gap between the employees and the

information security by letting the information security department to organize activities, making the employees feel the support of the organization in the information security management.

(2) Focus on improving the employees' team effectiveness perception. Provide effective resource support for employees in different business departments, establish a good communication environment and clarify information security rewards and punishments. Sufficient resource support can ensure that the employees can get right information, applicable equipment and proper work arrangements; a good communication environment can ensure the communication of employees concerning the topic of information security, enhance the possibility of cooperation, reduce the necessity of supervision; clear reward and punishment for information security can highlight the organization's emphasis on information security management, reflect the efforts and deficiencies of employees in information security, and ultimately contribute to the sustainability of information security management.

(3) Improve the organizational commitment level of the employees through effective information security management measures. Effective information security management can enhance employees' emotional dependence on the company and their loyalty in company strategy. For example, ensure employees' needs in self-expression, self-growth and relatedness in information security management so as to enhance their dependence on the organization; at the same time, pay attention to strategic layout in information security management, for example, the protection of key information infrastructures can make the employees understand the organization's strategic situation and intentions, and help them proactively implement the information security behavior.

Research limitations

(1) In order to ensure the reliability and validity of the measurement, the measurement of the satisfaction degree of the autonomy needs, competence needs and relatedness needs has adopted the question items that are widely used in existing researches. In future research, the scales should be modified after verification according to the specific scenarios in the corporate information management in Chinese companies, so that the research conclusions are more in line with the information security management practices of Chinese companies.

(2) The questionnaire survey targets are employees of companies in industries that have a relatively high level of information security management, and this has limited the industries to which the samples belong to a certain extent, resulting in the industries covered by the research samples are not extensive enough, and the subsequent research should expand the sample capacity.

Acknowledgement

This research is supported by the National Social Science Foundation of China (17CGL019).

REFERENCES

Anderson, C., Baskervill, R. L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems, 34(3),* 1082-1112.

Aurigmma, S., & Leonard, L. (2015). The influence of employee affective organizational commitment on security policy attitudes and compliance intentions. *Journal of Information System Security, 11(3),* 201-222.

Chen, B., Vansteenkiste, M., Beyers, W., Boone, L., Deci, E. L., Van der Kaap-Deeder, J., Duriez, B., Lens, W., Matos, L., Mouratidis, A., Ryan, R. M., Sheldon, K. M., Soenens, B., Van Petegem, S., & Verstuyf, J. (2015). Basic psychological need satisfaction, need frustration, and need strength across four cultures. *Motivation & Emotion, 39(2),* 216-236.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security, 39(B),* 447-459.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems, 26(6),* 605-641.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee response to stressful information security requirement: A coping perspective. *Journal of Management Information Systems, 31(2),* 285-318.

Deci, E. L., & Ryan, R. M. (2008). Facilitating optimal

motivation and psychological well-being across life's domains. *Canadian Psychology, 49(1),* 14-23.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing inorganizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43(6),* 90-110.

Gagne, M., & Deci, E. L. (2005). Self-determination theory and work motivation. *Journal of Organizational Behavior, 26(4),* 331-362.

Hsu, S. C., Shih, S. P., Yu, W. H., Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26(2),* 282-300.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems, 31(4)*, 6-48.

Lee, C., Lee, C. G., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. Computers & Security, 59(C), 60-70.

Lester, S. W., Meglino, B. M., & Korsgaard, M. A. (2017). The Antecedents and Consequences of Group Potency: A Longitudinal Investigation of Newly Formed Work Groups. *Academy of Management Journal, 45(2)*, 352-368.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems, 52(1),* 95-107.

Posey, C., Roberts, T. L., &Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems, 2015, 32(4): 179-214.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37(4),* 1189-1210.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridge the divide: A qualitative comparison security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51(5),* 551-567.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48(7),* 296-302.