Advances in Social Science, Education and Humanities Research, volume 542
Proceedings of the 2nd Annual Conference on Social Science and Humanities (ANCOSH 2020)

Information Systems Behavior on System Security in the Perspective of "Theory of Reasoned Action"

Benih Hartanti*, Anas Romadon, Nur Anisah, Langgeng Prayitno Utomo
Study Program of Accounting
STIE PGRI Dewantara
Jombang, Indonesia
*benih@stiedewantara.ac.id, anasromadhon1984@gmail.com, nur.anisah.stie.dw@gmail.com, lan99en9.pu36@gmail.com

***Abstract*—The increasing number of Cooperatives and MSMEs in Jombang, East Java is accompanied by the main challenges that arise generally from internal organizations, especially human resources for supervisors and administrators in supporting an operating system that is fast, easy, transparent, and has high accountability so as to build member trust by the use of information technology in business management. The aim of the research is to find users' behavioral aspects in information system security to support the accountability of organization's charter and budgeting. This study uses Theory of Reasoned Action (TRA) to analyze the relationship between attitudes towards information systems, subjective norms on information systems, intention in information system security behavior, and information system security behavior. SEM-PLS (Partial Least Square) with SmartPLS 3.0 was used as a data analysis tool. four hypotheses are accepted and only one hypothesis is rejected which is subjective norms of information systems on information system security behavior. This research emphasizes the solid factor of intention to bridge the subjective norm and attitude toward information system behavior and underline the importance of security policy and standard to stimulate the integrated behavior impact in accountability and governance.**

Keywords—cooperative, information system behavior, TRA

I. INTRODUCTION

Within the increasing number of cooperative in Jombang, East Java, Indonesia [1] and its prominent role to stabilize the economy [2], cooperatives' administrators and supervisors have to face the emergence of issues and challenges inside the organization. They are mostly related with the competence of the administrator and/or employees [3] and the managerial system [4]. Additionally, recent attention also occurs in the term of the low transparency and accountability inside the organization and the needs of digital development to support good corporate governance [5]. Therefore, in accordance with the achievement of government targets in the Industrial Age 4.0, the transformation strategies that cooperatives can undertake include re-engineering organizations based on operating systems that are fast, easy, transparent, and have high accountability so that they can build member trust, increase the use of information technology in application systems-based business management [6].

The existence of an information system and technology has proved to contribute in firm's performance [7] and has significant effect on both productivity and profitability [8]. Despite the profound impact in organization's performance, the attention of IS implementation recently focuses on the system security as the part of IT governance to comply the corporate governance. Tools and techniques have been acknowledged and applied to prevent IS assets from misuse, abuse and destruction [9], however, several studies suggest to consider socio-organizational imperatives as its equally important to organization to safeguard their resources [10-13]. The weakest link in supporting information security is correlated with employees as the insider threat inside the organization [10,11,14], therefore it is essential to conduct beneficial approach for organizations to focus on their own employees' intentions and behaviors [15].

One specific best-known theoretical model about intentions and behaviors is theory of reasoned action (TRA). TRA proposes that one's intention to perform or not to perform an action (behavioral intention) is the immediate precursor to the actual behavior [16]. That is, how and why people's beliefs change the way they act. Behavior can either be verbal or non-verbal such as body language, signals, signs, or vocally expressed [17]. Therefore, TRA puts forth three general constructs namely: (1) behavioral intention, (2) attitude, and (3) subjective norm [18]. The aim of the TRA is to investigate the relationship between attitude and behavior based on two major concepts : principles of compatibility and behavioral intention [19].

Many studies used TRA in explaining the intention and behavior within variety of topics, especially for information system and accounting information system in particular. Most of the studies used TRA in a setting of developed IT governance [20] with stated security policy [15] and compliance standard [21], however, studies of information system security in cooperatives with the low level of accountability and transparency have not yet found. Therefore, this research tries to fill the gap, in term of type of organization

and the general issues of accountability and governance in cooperatives.

II. METHODS

The research used a quantitative descriptive approach. The population of this research was determined from the number of cooperatives in Jombang regency [1] times the average number of cooperatives' managers/administrator and supervisors at one cooperative which is 9 persons. Therefore, within 7,056 cooperative managers/administrator and supervisors, sample was determined through the Sloven formula and resulted in 100 respondents and selected with the Non-Probability sampling technique. Questionnaire as the instrument of the research is a closed ended questions as the respondents only chose available answers in the form of a checklist with Lickert Scale (1 to 5) to indicate their agreement or unagreement. Questionnaire was developed by combining the indicator in each elements of TRA [16,18] and previous research in information system behavior [13,15,19]. The data analysis technique uses the Partial Least Square (PLS) method, which is a multivariate statistical technique that performs comparisons between multiple dependent variables. This analysis was carried out through five stages of testing, namely path coefficient (ß) testing, coefficient of determination (R^2), t-test using the bootstrapping method, effect size (f2).

III. RESULTS AND DISCUSSION

The descriptive statistic of the respondent is depicted in the following table 1.

TABLE I. RESPONDENTS' DESCRIPTION

Respondents' Descriptor	Indicators	Percentage	Total Percentage
Year of Work	< 4 Years	46%	100%
	4 - 6 Years	18%	
	> 6 Years	36%	
Job Position	Supervisors	19%	100%
	Administrators	81%	
Educational Background	Master Degree	1%	100%
	Bachelor Degree	50%	
	Diploma	9%	
	Senior High School	40%	

The results of five stages testing is shown in the following table.

Based on the Table 2, from the 5 hypotheses tested, almost all hypotheses are accepted and only one hypothesis is rejected. The rejected hypothesis is subjective norms of information systems on information system security behavior. Additionally, there is also intermediate correlation between subjective norm on information system security behavior.

TABLE II. MODEL STRUCTURE ANALYSIS RESULTS

Hypothesis		β	t-test	*f2*	Analysis			
No.	*Path*				*β*	*t-test*	R^2	f^2
H1	A >> I	0.49	5,572	0.44	Sign	Acc	Strong	Big
H2	S >> I	0.46	5,598	0.39	Sign	Acc	Strong	Big
H3	A >> B	0.25	2,367	0.11	Sign	Acc	Strong	Intermediate
H4	S >> B	0.05	0.51	0.004	Insign	Rej	Strong	Small
H5	I >> B	0.69	5,569	0.63	Sign	Acc	Strong	Big

A : Attitude to Information Systems
S : Subjective Norms on Information Systems
I : Intention on Information Systems Security Behavior
B : Information System Security Behavior

The analysis of the model structure (IE) shows the value of the path coefficient (ß) a stance on the information and intention in the behavior of information systems have significant value, and for the value of the coefficient of determination (R2), the attitude of the information systems and intention in the behavior of information systems have strong influence and on the f2 test also has a big influence. As well as the t-test attitudes towards information systems and intention in information systems behavior shows that attitudes towards information systems have an influence on intention in information systems behavior.

The result depicted in the table explains that the attitude towards information systems which is the affection that someone feels to accept or reject a certain system greatly influences the respondent's decision to increase intention in information system security behavior, because the attitude of a person who feels or assesses an information system according to them can feel the benefits and they tend to use it.

Moreover, the results of the analysis of the model structure, IE in particular the value of the path coefficient (ß) subjective norms on information systems and intention in the behavior of information systems have significant value, and for the value of the coefficient of determination (R2), subjective norms on information systems and intention in behavior information systems have a strong influence and on the f 2 test also has a big influence. As well as on subjective norm t- testing of information systems and intention in information system behavior, it shows that subjective norms on information systems have an influence on intention in information system behavior.

According to the education background, respondents aware that knowledge of information systems in an organization is essential. therefor they feel the importance of an information system in an organization where it is expected that the organization will sustain and develop more which further create the supportive environment to work and lead to their tendency in following and implementing the information system.

Other value of IE of the path coefficient (ß) at a stance on the information system and the behavior of the security of information systems have significant value, and for the value of the coefficient of determination (R2), the attitude of the information system and the behavior of the security of information systems has an influence strong and the f 2 test also has a moderate effect. As well as the t-test of attitudes towards information systems and information system security behavior shows that attitudes towards information systems have an influence on information system security behavior.

This results explains that when someone feels a system is useful, the behavior of information system security will also increase. Administrators/manager and supervisors who feel the benefits of information systems will improve their information system security behavior in their organizations.

Final IE value of the path coefficient (ß) subjective norms on information systems and the behavior of the security of information systems has a value that is not significant, and for the value of the coefficient of determination (R2), subjective norms on information systems and the behavior of system security information has a strong influence and the f 2 test also has little effect. As well as in the subjective norm t-test test for information systems and information system security behavior, subjective norms on information systems have no influence on information system security behavior

Correlating with descriptive statistic of respondent, though the education level of the respondents is 50% educated, 46% of them have not work for long (less than 4 years) while their job description is maintaining regulation, producing budgeting and maintaining them. This argues that even though they feel that information system behavior is important, the subjective norm factor came from suggestions from colleagues and higher authority don't give a significant influence to their behavior in responding the information system security.

The rejection of subjective norm and less impact of attitude directly to system security behavior indicate that there are other varied factors to stimulate system security behavior. These findings also indicate that to have an integrated intention and behavior toward information system security, the supporting factors such as subjective norms and attitude could be established in organization settings. Moreover, these also demonstrate the solid factor of intention to support the behavior in system security, even though the setting of organization is lack of security policy, standard and IT governance and the broader and overreaching role of stated procedure, standard and policy in stimulating higher attitudes and subjective norm of the cooperative's administrators.

Finally, these propose an implication in both practical and further enhancement of research. In term of practical contribution, these research findings emphasize the crucial role of system security procedure, standard and policy, higher authority in cooperatives that consists of supervisor, local government and ministry of cooperatives and SMEs could integrate in planning, organizing and communicating regulations that could be implemented as the general accepted system security standard in cooperatives. Therefore, management board is responsible for controlling and directing these activities to enhance the awareness of information security among employees [22]. Although senior management alone cannot guarantee successful risk management, it is essential for senior management individuals to execute and control information security activities [23,24]. Furthermore, the implementation of TRA could be combined with persuasion-centric theory [25] and protection motivation theory [26] to examine and extend the understanding of system security intention and system security behavior.

IV. CONCLUSION

From the results, four hypotheses are accepted and only one hypothesis is rejected which is subjective norms of information systems on information system security behavior. Combining the analysis test for the hypotheses and descriptive statistic, this research concludes that educational background and years of work might be the factors in strengthening the attitude of using information system and acknowledging the benefits, however, the role of subjective norm as one of the factors in behavior, especially in information system security is less considered. Due to supporting the whole factor in behavior of information system security in purpose to support the accountability and governance, higher authority in cooperatives that consists of supervisor, local government and ministry of cooperatives and SMEs could integrate in planning and organizing regulations that could be implemented as the general accepted system security standard in cooperatives.

ACKNOWLEDGMENT

Appreciation of contribution is addressed for Study Program of Accounting and Department of Research and Community Services of STIE PGRI Dewantara for their support in coordinating and organizing during the research process until its publication process.

REFERENCES

[1] Dinas Koperasi dan Usaha Kecil Menengah Provinsi Jawa Timur, "Data Jumlah Koperasi Se-Jawa Timur," 2019. .

[2] N.M. Sari, "Fungsi Koperasi, Jenis dan Tujuannya Sebagai Landasan Ekonomi Bangsa."

[3] Warta Ekonomi, "Kemenkop dan UKM Ungkap Permasalahan Koperasi," 2017.

[4] E. Catriana, "Tantangan Koperasi di Indonesia, Persaingan hingga Masalah Pengelolaan".

[5] Indonesia News, "Akuntabilitas dan Transparansi Koperasi di Indonesia Masih Rendah," 2019.

[6] R. Dahuri, "Peran Koperasi dalam Pembangunan Ekonomi di Era Revolusi 4.0," 2018.

[7] N. Melville, K. Kraemer, and V. Gurbaxani, "Information Technology and Organizational Performance: An Integrative Model of IT Business Value," MIS Q., vol. 28, no. 2, pp. 283–322, 2004.

[8] T. Jacks, P. Palvia, and R. Schilhavy, "A framework for the impact of IT on organizational performance," Bus. Process Manag. J., vol. 07, no. 05, pp. 846–870, 2011.

[9] M. Workman, W.H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," Comput. Human Behav., vol. 24, no. 6, pp. 2799–2816, 2008.

[10] C. Vroom, R. Von Solms, P.E. Technikon, P. Elizabeth, and S. Africa, "Towards information security behavioural compliance," Comput. Secur., vol. 23, no. 3, pp. 191–198, 2004.

[11] J.M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," Comput. Secur., vol. 24, no. 2, pp. 124–133, 2005.

[12] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance," in Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 2007, pp. 3–6.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance : An Empirical Study of Rationality-B Ased Beliefs," MIS Q., vol. 34, no. 3, pp. 523–548, 2010.

[14] G.V. Post and A. Kagan, "Evaluating information security tradeoffs: Restricting access can interfere with user tasks," Comput. Secur., vol. 26, no. 3, pp. 229–237, 2007.

[15] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Comput. Secur., vol. 31, no. 1, pp. 83–95, 2012.

[16] I. Ajzen, "The Theory of Planned Behavior," in The Theories of Social Psychology, P. A. M. Van Lange, A. W. Kruglanski, and E. T. Higgins, Eds. Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE, 2012, p. 438.

[17] O.C. Otieno, S. Liyayla, and B.C. Odongo, "Theoretical and Practical Implications of Applying Theory of Reasoned Action in an Information Systems Study," pp. 10–14, 2015.

[18] I. Ajzen and M. Fishbein, Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs: Prentice-Hall, 1980.

[19] D. Mishra, I. Akman, and A. M. Mishra, "Theory of Reasoned Action application for Green Information Technology acceptance," Comput. Human Behav., vol. 36, pp. 29–40, 2014.

[20] M. Nicho, "A process model for implementing information systems security governance," Inf. Comput. Secur., vol. 26, no. 1, pp. 2056–4961, 2018.

[21] S. Gantman and J. F. Fedorowicz, "Communication and control in outsourced IS development projects: Mapping to COBIT domains," Int. J. Account. Inf. Syst., vol. 21, pp. 63–83, 2016.

[22] H. Stewart and J. Jürjens, "Information security management and the human aspect in organizations," Inf. Comput. Secur., vol. 25, no. 7, pp. 494–534, 2017.

[23] S.R. Boss, L.J. Kirsch, I. Angermeier, R. A. Shingler, and R. W. Boss, "'If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security,'" Eur. J. Inf. Syst., vol. 18, no. 2, pp. 151–164, 2009.

[24] E. McFadzean, J.N. Ezingeard, and D. Birchall, "Anchoring information security governance research: sociological groundings and future directions," Int. J. Inf. Secur., vol. 2, no. 3, pp. 3–48, 2006.

[25] [J.D. Wall and M. Warkentin, "Information & Management Perceived argument quality ' s effect on threat and coping appraisals in fear appeals : An experiment and exploration of realism check heuristics," Inf. Manag., vol. 56, no. 8, p. 103157, 2019.

[26] T. Herath and R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106–125, 2009.