Issues in Information Systems
Volume 22, Issue 3, pp. 255-263, 2021

DOI: https://doi.org/10.48009/3_iis_2021_255-263

How does it security affect the fit of remote collaboration technology?

Linwu Gu, *Indiana University of Pennsylvania ,lgu@iup.edu*
Jianfeng Wang, *Independent Consultant, wangufa3@gmail.com*

Abstract

Working remotely during the pandemic may become long-term work type. Information technology and security are considered as keys to remote collaboration; however, few previous studies have explored the technology identification and security on the collaboration technology fit. Data of 107 subjects were collected from the online questionnaire. The results show that the information security coordination and policy compliance positively impact the remote collaboration technology fit. The implications and conclusions are discussed at the end.

Keywords: Technology Fit, Remote Collaboration, Information Security

Introduction

The information technologies have influenced remote team performance significantly. Since the outbreak of the pandemic, lots of discussions about mental and psychological health of human beings. Despite the fact that cyberattacks actually are more active than before, there are not so many discussions of preventing cyberattacks and how cyberattack may affect remote work or collaboration. According to the threatmap data from Checkpoint Inc on June 1, 2021, the past year there have been record-breaking numbers of cyberattacks daily. Number of daily cyberattacks has averaged from 60 million to 80 million with peak attacks close to 300 million daily in early April 2021 while 10 years ago checkpoint Inc. only recorded about 2-4 million attacks a day.

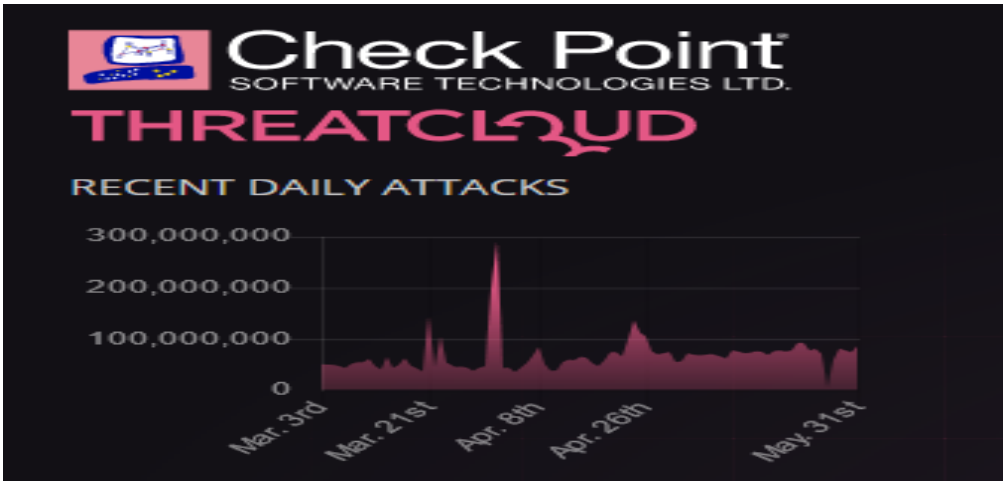

Figure 1: Daily Cyberattacks

Security technology cannot completely or automatically assure security for data transmission necessary for remote working environments. Although the IS security literature has often mentioned users as the weak link for information system security due to user errors, the group knowledge of security is widely believed to be essential to effective collaboration (Siponen et al. 2014; Whitman & Mattord 2018). The security knowledge coordination refers to the sharing of security knowledge for the information assets of remote teamwork (Spears et al. 2010). Information security technologies should protect remote group data, and successful teamwork information sharing improves better collaboration. Information security policy is the safeguard of information from a wide range of threats and vulnerabilities. Therefore, security policy and regulation compliance may strengthen the IT-based coordination (Duncan 1995; Yoo et al. 2020; Moody et al. 2018). It is important to assess how individual users view their knowledge sufficiency in information security for team collaboration. IT identity is defined as the extent to which an individual views the use of an IT as integral to his or her sense of self (Carter & Grover 2015). The importance of IT identity value is evident in previous research. Carter et al. (2020) provides sufficient evidence that IT identity is more likely to encourage IT-enabled task collaboration. Collaboration technology fit evaluates risk factors and assesses the effectiveness of IT identity. Remote collaboration technologies fit examine how the collaboration technology can achieve task accomplishment and can fit the teamwork (Maruping and Magni 2012). Additionally, collaboration technology encourages IT-based groupwork, and its functions are recognized in teamwork performance progress. (Maruping and Magni 2012; Carter and Grover 2015).

This paper is organized as follows. In the next section the research method is described, presents the results of the literature review, and all the constructs in the research model are addressed. The hypotheses and research design are then constructed and explained, followed by data analysis and discussion of the findings from our studies. We discuss the theoretical and practical implications of the findings, limitations, and suggestions for future research.

Literature Review and Research Model

Task technology fit theory explains how technology characteristics and task characteristics impacts task technology fit (Goodhue & Thompson 1995). Goodhue & Thompson (1995) argue that for an IT to have a positive impact on individual performance, the technology must be a good fit with tasks it supports.

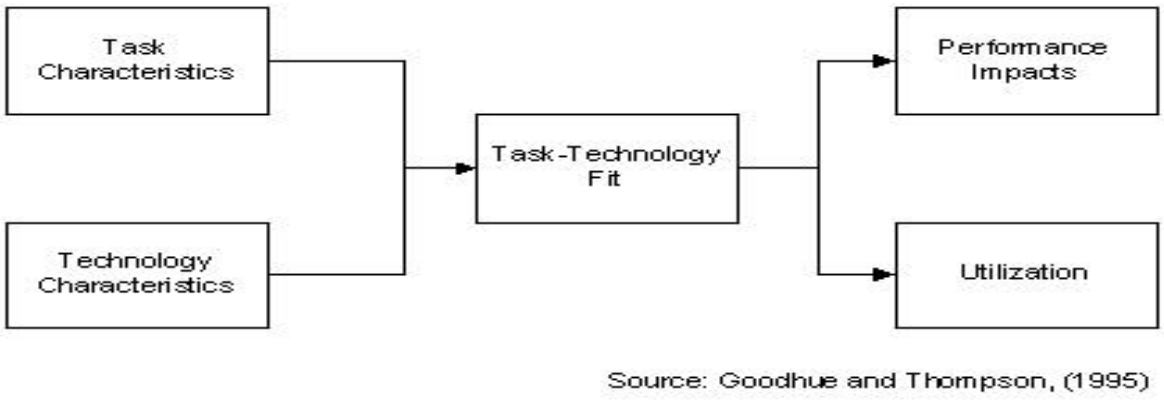

Figure 2: Task Technology Fit Model

In this research, we explore the impact from IT security on the fit of remote collaboration technologies. Work-from-home presents challenges to the data security management when employees exchange data between their home computers and their corporate servers. To assure data security, employers extend their onsite/cloud security policies and controls to the home computers of their employees. The enhanced security controls on home computers create some nuances to the stay-at-home workers. How does the enhanced security controls affect individual performance of the stay-at-home workers? Or as our research tries to explore, how does IT security affect the fit of the remote collaboration technology?

IT-enabled task collaboration fit measures how well the team coordinates their activities using collaboration technology (Bala 2017; Kudaravalli, et al 2017). In this study, the construct of remote collaboration fit is adapted and defined as the perceived fit to the degree to which the remote collaboration technology functions in teamwork. Remote collaboration fit is suited to the collaboration technology fit for remote group (Kankanhalli, et al 2003). The literature has illustrated that collaboration technology fit is not only about technology capabilities, but also about how the individual members interact to fit the technology and do well (Barrick et al. 2007).

IT Identity

Carter & Grover (2015) define IT identity as the extent to which an individual views the use of an IT as integral to his or her sense of self. They operationalize IT identity as a person's positive self-connection to the use of computer system components. Although the existing research recognizes how individuals relate to technology within team situations is important, few studies focus on characteristics of an individual that evaluate himself about using security technology. At the individual level, IT identity defined as employees' knowledge about the capabilities of organizational IT (Stephan et al. 2017). Pan et al. (2017) explained technological self-identity as a cognitive construct of the individual self that answers the question related

to the use of technology. While people connect to IT usage may rely on their personal identity. As people become more experienced with IT, they interact with technology more efficiently. People with strong IT capabilities are most likely to encourage IT identity (Carter et al 2020; Boxa and Pottasa 2014). Security awareness and knowledge in collaboration technology for work-from-home should be incorporated into IT identity as corporates extend their security policies and controls to work from home. Thus we argue that IT identity with necessary security awareness and security knowledge should positively influence the fit of remote collaboration technology.

Perceived Information Security Policy Compliance

Information security has become main concern for remote teamwork. Information security policy safeguards the working quality and work-from-home coordination (Kankanhalli et al ,2003). The compliance with security policy and regulation is defined as obedience in the protection of an information system (Siponen and Vance, 2010). Ahlan et al. (2015) suggest that people can only help in preventing security violations if they are willing to secure information system. However, a common security impediment is security policy ignorance (Hadlington, 2017). The high level of compliance with information security policies may result in fewer security hazards to collaboration technologies (Hadlington, 2017). In sum, the use of protocols for securing information systems against cyberattacks is fundamental for remote teamwork, and effective compliance with the information security policies are primarily related to IT based collaboration (Spears and Barki, 2010; Bulgurcu et al 2010). Assurance of data security is not just an operational, tactical but also strategic issue. Compliance of corporate security policies, standards, guidelines, and procedures is necessary for the success of using collaboration technology for work from home. Thus we argue that perceived compliance of information security policy should positively influence the fit of remote collaboration technology.

Perceived Security Knowledge Coordination

The security knowledge coordination ensures a workable group knowledge sharing for information security (Malimage et al 2020). Thus, it is convincing to understand the role of security coordination positively affect task technology fit at a workgroup level (Kwon and Johnson, 2014). In addition, task technology collaboration fit requires group coordination for sharing information security knowledge, where the individuals' IT identities play an important role. As such, creating adequate information security coordination becomes essential in task collaboration capability (Srivastava et al. 2005; Siponen, et al 2014). Knowledge sharing of security policies, protocols and controls is very important part of security management in general, same in using remote collaboration technology to work from home. All work-from-home employees must have a thorough understanding of related security policies, protocols and controls in using remote collaboration technology, to assure that all the operations they do at home meet the requirements of security policies, standards, guidelines and procedures. Therefore we argue that perceived security knowledge coordination should positively affect the remote collaboration technology fit.

Remote Collaboration Technology Fit

Kang et al. (2012) define collaboration technologies as computer-based systems that support teamwork and share information. Remote collaboration technology fit examines how the collaboration technology can achieve task accomplishment and can fit the teamwork (Maruping and Magni 2012). In identifying the link from the individual use of collaboration technology to the assessment of group collaboration technology, Maruping and Magni (2015) find that members' individual exploration of group collaboration technology and their adoption of such technology into their work practice are essential for the successful

implementation of such collaboration technology, more so with individual members' continued efforts of exploring features of the collaboration technology. It is claimed that group collaboration technologies are more likely to be affected by individual's identification of technology use (Kraut and Streeter 1995; Maruping and Magni 2015; Stephan et al. 2017). The lack of remote group security knowledge coordination, and risky behaviors in information security lessen the collaboration technology fit (Bala et al. 2017).

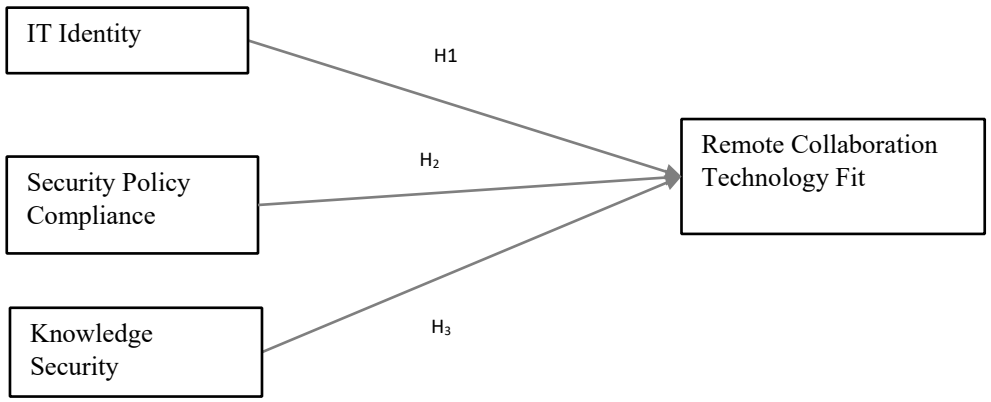

Figure-3: How IT Security Impact Remote Collaboration Technology Fit?

Based on our discussion above, we propose the following hypothesis:

H_1: IT Identity positively influences the remote collaboration technology fit.

H_2: Information security compliance positively influences the remote collaboration technology fit.

H_3: Security knowledge coordination positively influences the remote collaboration technology fit.

Data Collection and Analysis

Subjects, Procedures, and Measures

Data were collected from 107 subjects who registered our online/zoom classes of a business school in a state university. Among them, 59 students are female and 48 males; 3 students are from Asia; 7 black students; 4 Hispanic; The rest are all white students. Most of them are general business major students in finance, accounting, marketing and management. Oldest student is 28 years old, the youngest is just 19. None of them had any security problems with their phones or personal computers before. These Students were assigned to work on their group projects, due a week before the end of the semester, Spring 2021. They used D2L learning management system and zoom video conferencing system. Once they submitted their projects at the D2L system, each of them would answer the survey questionnaire as part of the project completion at D2L. There are totally 135 students from our six classes. 28 students either ignored or forgot our request for them to fill the survey questionnaire. The survey response rate is 79%. The survey items used to measure the research model variables were primarily derived and adapted from the previous studies and are listed in the Appendix. All the scales were assessed with seven-point Likert scales with anchor points of 1 = "totally disagree" and 7 = "totally agree."

Assessment of Measurement Validation

The partial least squares (PLS) approach was used to test the proposed research hypotheses. The measurement quality of constructs was assessed by examining the convergent validity, and composite reliability. First, we examined factor loadings of individual measures, as well as the average variance extracted (AVE); the square root of the AVE for each construct is stated in the diagonal of the correlation of constructs matrix (Table 1). All the measurement item loadings were greater than the minimum value of 0.7, and the AVE values for all constructs were above the minimum suggested value of 0.50, thus demonstrating that all reflective constructs exhibit good reliability and convergent validity.

Table 1: Cronbach Alpha, AVE, and Square Root of AVE

	Composite reliability	AVE	Square Root AVE
IT Identity	0.7124	0.7312	0.8551
Security Policy compliance	0.7432	0.8935	0.9453
Security Knowledge Coordination	0.8215	0.8677	0.9315
Remote Collaboration Technology Fit	0.7076	0.8203	0.9057

Results and Discussion

H_1: The effect of IT identity on the remote collaboration technology fit has path coefficient 0.13 (p=0.314), not significant. So the hypothesis 1 can be rejected.

H_2: The effect of security policy compliance on remote collaboration technology fit has path coefficient 0.622 (p=0.021), which does have significant influence, so hypothesis 2 is supported.

H_3: The effect of security knowledge coordination on remote collaboration technology fit has path coefficient 0.544 (p=0.001), which does indicate significant influence. So hypothesis 3 is confirmed.

IT identity is an insignificant contributor to the remote collaboration technology fit. but security policy compliance and knowledge coordination have strong significant impacts on the remote collaboration technology fit. This finding supports what security community has advocated about the importance of general security education and security awareness (Whitman & Mattord 2018). The same thing can be claimed in the security assurance of using remote collaboration technologies. For all employees to work from home, they must accept security training and education about how to follow employers' security policies, standards, guidelines, and procedures at home. For any updates in the remote collaboration technologies, employees must be notified and trained and keep current of any changes or enhancements in security controls.

Conclusion

The present study has a few limitations. First, the student group project data lack diversity, and data is not big enough. Second, only two collaboration technologies were used in the project: D2L discussion forums and Zoom Video meeting system. It was reported that zoom video system had some security issues such as zoom bombing or uninvited attenders joining sessions. We did not experience such issues. We did

follow some general security advice from our IT support center such as using password for each session and set up waiting room so only familiar students will be admitted. We follow the general rules for access, authentication, and accountability in remote teaching.

The current study indicates the positive effects of such compliance with security policy and security knowledge coordination on remote collaboration technology fit. Our research suggests that security compliance and security knowledge sharing improve security awareness and organizational security control. The present study suggests a couple of possible valuable future research. First, an examination of IT infrastructure at an individual level of analysis would improve better collaboration; increased awareness and security compliance would be consistent outcomes associated with collaboration technology. The need for supervisory compliance may encourage more user technology identification for remote technology. Second, other security measure should also be considered as factors leading to better fit between collaboration technology and security. Such addition will make the model more complicated for future research.

References

Ahlan, A., Lubis, M., and Lubis, A. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. *Procedia Computer Science* 72, pp. 361 – 373.

Bala, H., Massey, A. & Montoya, M. (2017). The Effects of Process Orientations on Collaboration Technology Use and Outcomes in Product Development. *Journal of Management Information Systems*, 34 (2), pp. 520–559.

Barrick, M. R., Bradley, B. H., Kristof-Brown, A. L., and Colbert, A. E（2007）. "The Moderating Role of Top Management Team Interdependence: Implications for Real Teams and Working Groups," *Academy of Management Journal* (50:3), pp. 544-557

Boxa, Debra and Pottasa, D. (2014). A model for information security compliant behavior in the healthcare context. Procedia Technology 16, pp. 1462–1470.

Bulgurcu, B.; Cavusoglu, Hasan, and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34 (3), pp. 523-548.

Carter, M.; Petter, S., Grover, V., and Thatcher, J. (2020). Information Technology Identity: A Key Determinant of It Feature and Exploratory Usage. *MIS Quarterly,* 44(3), pp. 983-1021.

Carter, M., and Grover, V. (2015). Me, My Self, and I(T): Conceptualizing Information Technology Identity and its Implications," *MIS Quarterly,* 39(4), pp. 931-957.

Checkpoint. (2021). https://threatmap.checkpoint.com/, retrieved on June 1, 2021.

Duncan, N. (1995). Capturing Flexibility of Information Technology Infrastructure: A Study of Resource Characteristics and Theory Measure. *Journal of Management Information Systems,* 2(2), pp. 37-57

Goodhue, D., & Thompson, R. (1995). Task-technology fit and individual performance. *MIS Quarterly 19* (2), pp. 213–236.

Hadlington, Lee (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Hiliyon*, 48(1), pp. 45-51

Kang, S., Lim, K. H., Kim, M. S., and Yang, H.-D. (2012). A Multilevel Analysis of the Effect of Group Appropriation of Collaborative Technologies Use and Performance. *Information Systems Research*, 23(1), pp. 214-230

Kankanhalli, A., Teo, H.-H., Tan, B. C., and Wei, K.-K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 23(2), pp. 139-154.

Kudaravalli, S., Faraj, S., and Johnson, S. L. 2017. "A Configural Approach to Coordinating Expertise in Software Development Teams," *MIS Quarterly,* 41(1), pp. 43-64.

Kraut, R. E., and Streeter, L. A. (1995). Coordination in Software Development. *Communications of the ACM* 38(3), 69-81.

Kwon, J.; and Johnson, M.E. (2014) Proactive versus reactive security investments in the healthcare sector *MIS Quarterly*, 38(2), pp. 451–471.

Malimage, K., Raddatz, N., Trinkle, B.S. Crossler, R., and Baaske, R. (2020) Impact of Deterrence and Inertia on Information Security Policy Changes. *Journal of Information Systems American Accounting Association. 34(1),* 123–134

Maruping, L. M., and Magni, M. (2015). "Motivating Employees to Explore Collaboration Technology in Team Contexts," *MIS Quarterly*, 39(1), pp. 1-16

Moody, G. D., Siponen, M., and Pahnila, S. (2018). "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly,* 42(1), pp. 285-311.

Pan, Z., Lu, Y., Wang, B., and Chau, P. Y. 2017. "Who Do You Think You Are? Common and Differential Effects of Social Self-Identity on Social Media Usage," *Journal of Management Information Systems,* 34(1), pp. 71-101.

Siponen, M., Mahmood, M. A., and Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management* 51(2), pp. 217-224

Siponen, M., and A. Vance (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* ,34 (3), pp. 487–502

Spears, Janine L. and Barki, Henri (2010). User Participation in Information Systems Security risk Management. *MIS Quarterly*. 34(3)503-522.

Srivastava, L. 2005. "Mobile Phones and the Evolution of Social Behaviour," Behaviour & Information Technology (24:2), pp. 111-129.

Stephan, A., Kamen, M., and Bannister, C. (2017). Tech Fluency: A Foundation of Future Careers. *Deloitte Review, Issue 21.*

Whitman, M, & Mattord, H. (2018). Principles of Information Security. Cengage Learning Inc., USA.

Yoo, C. Goo, J., and Rao, R., and Raghav, H (2020). Is Cybersecurity A Team Sport? A Multilevel Examination of Workgroup of Workgroup Information Security Information Security Effectiveness. *MIS Quarterly,* 44(2), pp. 907-931.

Appendix

Remote Collaboration Technology Fit (adapted from Bala et al. 2017):

1. I would rate the collaboration technology capabilities provided by Zoom in terms of quality.
2. In general, zoom provides me with high-quality collaboration technology capabilities. Collaboration satisfaction (reflective measures)
3. I am very satisfied with the collaboration technology capability provided by Zoom functions.
4. Overall, the collaboration technology capability provided by Zoom are very satisfying.

Security Policy Compliance (adapted from Ahlan et al. 2015)
1. It is easy to understand general written IS rule of campus.
2. Quick access for related privacy protection.
3. It is necessary to arrange campus IS rule refer to corporation standard.

IT Identity (Carter et al. 2020)
1. Thinking about myself in relation to the software, I am dependent on this software.
2. Thinking about myself in relation to the software, I am reliant on this software.
3. Thinking about myself in relation to the software, I am energized
4. Thinking about myself in relation to the software, I am enthusiastic
5. Thinking about myself in relation to the software, I am linked with the software
6. Thinking about myself in relation to the software, I am concerned with the software

Security Knowledge Coordination (Yoo et al. 2020)
1. Co-workers in the workgroup share their security knowledge and skills with one another I the workgroup
2. If someone in our workgroup has relevant knowledge and skills in a certain security task, he/she is likely to help other co-workers when it is needed.
3. More knowledgeable group members freely provide other co-workers with knowledge or skills on security issues.
4. Our workgroup members know who has the relevant skills and knowledge that are relevant to certain security tasks.
5. Our workgroup co-workers know who in our workgroup needs security knowledge and skills to perform the security tasks well