Issues in Information Systems
Volume 24, Issue 1, pp. 305-315, 2023

DOI: https://doi.org/10.48009/1_iis_2023_126

An exploratory study of moderators in remote group security effectiveness

Linwu Gu, *Slippery Rock University, linwu.gu@sru.edu*
Jianfeng Wang, *Kutztown University, jwang@kutztown.edu*

Abstract

Groups' technology security failure is a major concern for remote group teams. Remote workgroup research is necessary to explore group security success. Safeguarding remote workgroups from cyber-attack has become one of the top managerial priorities in many organizations. The moderation effects between cyber-attack risk and group security effectiveness are still largely unexplored. To fill this gap, this study attempts to investigate the moderation of group security risk and e-workgroup security effectiveness, examining a sample of 132 respondents using structural equation modeling. The results highlight the moderator of team empowerment on the relationship between cyber-attack risk and workgroup security effectiveness.

Keywords: cyber-attack risk, remote group security effectiveness, IT mindfulness, team empowerment

Introduction

Previous studies on IS security have highlighted several important topics such as IT security management and IS security evaluation. The widespread malicious cyber-attacks affecting IT enabled remote workgroups performance have prompted some research in remote group security (Dinev and Hu 2007). One of the key findings from the previous research is that the perceived risk of cyber-attack is negatively correlated to the IT-related workgroup security effectiveness (Hadlington and Lee 2017). Information security effectiveness is defined as the security achievement of IT enabled e-groupwork, and the intended information security usefulness (Liang et al. 2021; Zhang et al. 2011).

IT mindfulness is defined as awareness of system changes, knowledge of alternative viewpoints, and openness to new resolutions (Thatcher et al. 2018). When group members have strong IT mindfulness, they are active to recognize different perspectives and understand the current state of information security. Additionally, A more IT mindful group member might explore new suggestions that help reduce information security risk, try creative ways to prevent various security violations, and create a viable approach to managing and improving group information security effectiveness (Johnston et al. 2019).

Team empowerment represents the extent to which a team believes that it can be effective in anything it sets out to accomplish, and share significant solutions (Maruping and Magni, 2015). Higher team empowerment may enhance group security effectiveness when the cyber-attack risk is high. This is because, unlike individuals, at a group level, high team empowerment can realize the benefits of the group work, can better predict, and carry on the use of technologies that are implemented for a group of people, because

groups with high team empowerment are cooperatively responsible for team outcomes (Kritzinger and Smith 2008; Rhee et al. 2012).

Specifically, in this paper, we treat team empowerment and IT mindfulness as two moderators (Figure 1), which could rationalize the weak workgroup security effectiveness when the cyber-attack threat is high. In the next section, we review the extant literature on group security and develop a research framework for the moderation effects on workgroup security effectiveness.

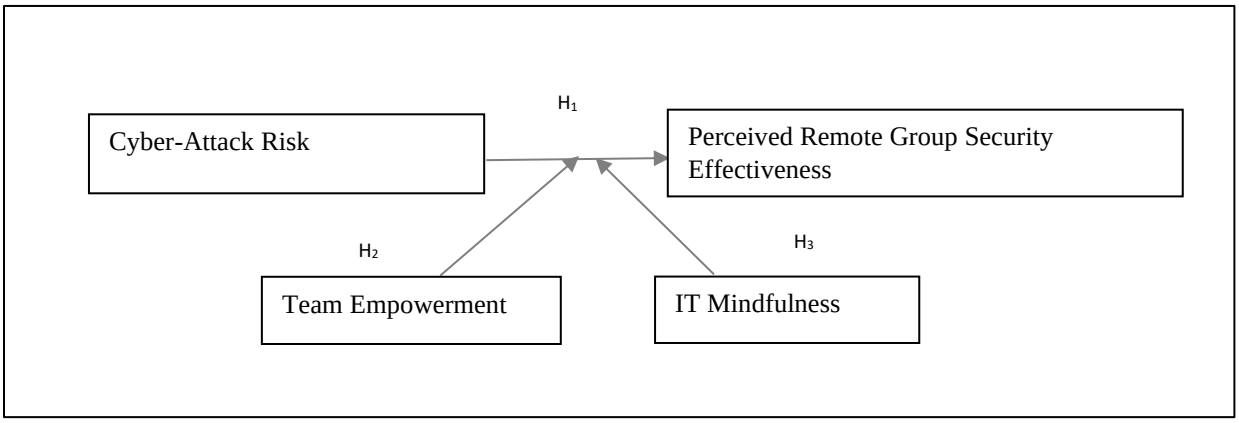

Figure 1: Proposed Research Model

Theoretical Background and Hypothesis

As it is more common for lots of companies to allow work from home, it is essential to explore how remote group workers can achieve groupwork security effectiveness. Anderson and Moore (2006) argue that the positive impact of group security effectiveness is to adopt protective technologies such as anti-virus software and firewalls. Team empowerment helps remote group members develop and share their important task experiences. According to previous studies, group members with higher level of mindfulness in IT-enabled workgroup quickly perceive differences, discover multiple resolutions, help correct flawed use of technologies, and improve group performance (Fichman 2004; Carlo et al. 2012; Bishop et al. 2004; Langer 1989).

Cyber-Attack Risk

Despite the latest technological improvements in organizational security, group security using remote systems is still an ongoing managerial challenge (Jensen et al. 2021; Siponen and Baskerville 2018). There are different types of cyber-attacks such as identity theft, social engineering, and breach of computer security (Yoo et al. 2020; Metalidou et al 2014). Cyber-attacks often result in unauthorized access to protected data. Therefore, the information system for the remote workgroup will be in danger if there is security threat in the remote working system (Hwang et al 2021; D'Arcy and Devaraj 2012; Chen et al. 2021). As such, cyber-attacks have become main impediments to remote workgroup security effectiveness. Anderson et al. (2010) explains cyber-attack is one of the issues that create a vulnerability in groupwork security. In other word, the cyber-attack is the possible main threat for IT-enabled remote group and the

whole group might experience the negative consequences associated with the threat (Sen et al. 2020; Anderson & Agarwal 2010; Zohar and Luria 2005).

IT Mindfulness

The risk assessment, security policy configuration and maintenance, regulatory compliance, and security incidence response all require mindful staff to manage these processes (Whitman and Mattord, 2021). A team of staff mindful in IT can minimize possible negative influence from a security breach or unexpected event. Thatcher et al. (2018) define "IT mindfulness as a dynamic IT-specific trait, evident when working with IT, whereby the user focuses on the present, pays attention to detail, exhibits a willingness to consider other uses, and expresses genuine interest in investigating IT features and failures". Specifically, a more IT mindful user will be faster to keep system updated or adopt new technology; a more IT mindful user will identify possible alternative ways to improve group performance; a more IT mindful user will have more capabilities to differentiate technologies, assess multiple technologies, and be open minded to new solutions (Line and Moe 2015; Langer 1989; Dennis et al. 2008). Moreover, for group members with IT mindfulness, the inclination to boost group security effectiveness might be important because they are, more open, flexible, and active. In contrast, less IT mindful people ignore alternatives, favor a fixed pattern of working procedures, and are less concerned about new solutions (Dane, E. 2011; Langer et al. 1989; Sternberg 2000). When team members overall are more updated about emergence of new threats, changes in security technologies, regulatory compliance, corporate security policies, and more open to learn new technologies, they can better manage their group work security.

Team Empowerment

The management of work group security involves detection of possible new threats, timely updates of security setting of technologies used, and monitoring integration of new technologies into the work process. Team members should also be aware of new security technologies and security patches and be trained to follow new security compliances from state and federal regulations. In the case of a security incidence or disaster, the members should be able to respond as the first responder, follow the due processes in security control, and minimize the negative impacts from the security incidence or disaster (Whitman and Mattord, 2021). Capable and qualified team members should be empowered with the necessary privileges to respond to the incidence or disaster.

Team empowerment has been identified as an important foundation to the group members' ability and willingness to integrate technology creatively and correctly into their teamwork (Maruping and Magni, 2015). Team empowerment consists of four dimensions: potency, meaningfulness, autonomy, and impact. Team empowerment potency means team can carry out a task effectively; if a team has high team potency, the team can accomplish a task more successfully; team meaningfulness suggests team members' ability to build up and share their knowledge of significant tasks (Kirkman and Rosen 1999).

In other words, team members with meaningful team empowerment from IT enabled remote groups are skilled of associating with the various technology assessments to improve the team's achievement (Kirkman et al. 2004; Ahuja and Thatcher 2005). Moreover, team empowerment with high autonomy means that the team is good at self-management by figuring out technology solutions. Consequently, it was found team members in remote workgroup with high interaction would be more willing to explore the group influences (Klaus and Changchit 2019; Taylor and Todd 1995).

Remote Group Security Effectiveness

In a remote work setting, team members should be familiar with the security controls and safe practice to work collaboratively and effectively. Remote group security effectiveness refers to the extent to which a given group level effectively accomplishes its information security effectiveness goals (Line and Moe 2015). There should be no uninvited access, no interference or interruption, no unintended modification of data, and no unauthorized access. There are a few information access models proposed and implemented to govern the rules of information sharing, read and write privileges. Necessary encryption system should be implemented for data in transit and stored (Whitman and Mattord 2021).

The perceived group security effectiveness is defined as work goals and evaluation, where the individuals' shared beliefs and efforts in pursuit of security achievement (Yoo et al. 2020). As evidenced in the previous research, IT enabled remote teamwork security effectiveness is likely to be influenced by IT enabled group empowerment (Thomas and Velthouse 1990).

IT enabled e-workgroup information security effectiveness involves technology-oriented information security goals and performance; thus, it requires a shift of focus from individual security awareness to group security usefulness (Ahuja and Thatcher 2005; Dinev and Hu 2007; Oliveira and Martins 2010). Each group pursues its security goals by completing task using remote collaborative technologies safely without data breach (Anderson and Moore 2006; Venkatesh et al. 2011). Therefore, it is significant to understand the factors, which can affect the effectiveness of information security management at a workgroup level using remote collaboration technologies (Kang et al. 2012).

In summary, at group level, IT-enabled remote workgroup with high team empowerment can be ambitious, confident, communicable, and powerful in completing tasks that make better group level decision (Kirkman and Rosen 1999). At individual level, individual group member with more IT mindfulness might be more innovative, perceptible, and openminded for any new anti-cyberattack IT adoptions or new information security trainings that are more likely to enhance group security effectiveness (Hu and Liden 2011; Yu et al. 2021; Kraemer et al. 2009). Extending from the previous research, we propose the following hypotheses:

H_1: *Cyber-attack risks negatively influence perceived remote group security effectiveness.*

H_2: *Team empowerment positively moderates the relationship between cyber-attack risks and perceived remote group security effectiveness.*

H_3: *IT mindfulness positively moderates the relationship between cyber-attack risk and perceived remote group security effectiveness.*

Data Analysis and Results

Our sample was collected from work-from-home IT group workers and students with group online projects. In the past year, lots of employees still worked at home. We used the google form to create online questionnaire to collect sample data. Data collection was performed between September 2021 and April 2022. The google-doc based online questionnaire was posted on the D2L course webpages at the end of the semester; we also sent the questionnaire link to our WeChat contacts who worked from home, asking them to share the link with their group members. The 151 responses collected were about respondents' actual remote group experience. 19 responses are not complete and had to be removed, so we used 132

questionnaire responses at the end. The average age of the respondents were 33.5 years old. In addition, 72 respondents (54.5%) were male, and 60 respondents (45.5%) were female (Table 1).

Table 1: Demographic and User Characteristics of Respondents.

		Absolute	Percentage
Gender	F	60	45.5%
	M	72	54.5%
Age	<25	53	40.2%
	25-45	51	38.6%
	>45	28	21.2%
Remote Group Experience	1 Semester	36	27.3%
	2 Semesters	18	13.6%
	>1 year	78	59.1%
Profession	College Student	54	40.9%
	IT Engineer	78	59.1%

Measurement Constructs

Measurement constructs were taken from the previous literature and adapted to this research context. All the constructs were assessed with seven-point Likert scales with anchor points of 1 = "totally agree" and 7 = "totally disagree." As shown in Appendix A, the lowest value of Cronbach's alpha is 0.725 for the remote group security effectiveness and all greater than 0.70 (Nunnally and Bernstin 1994). To test convergent validity and reliability, we tested average variance extracted (AVE) and composite reliability (CR).

As shown in Table 2, all these scores are acceptable. Discriminant validity is evaluated by comparing the square root of average variance extracted for each construct with the correlations. The value of AVE is greater than or equal to 0.5 and the value of CR exceed 0.8, which is considered a satisfactory convergent validity for a construct (Bagozzi 1981).

Table 2: Descriptive Statistics, Correlations, and Average Variance Extracted

	Mean	SD	CR				
IT Mindfulness	5.23	1.18	0.905	**0.882**			
Team Empowerment	5.01	1.21	0.838	0.671	**0.814**		
Cyber-Attack Risk	4.08	1.33	0.861	0.383	0.506	**0.933**	
Workgroup Security Effectiveness	4.9	1.27	0.936	0.114	0.227	0.272	**0.851**

Note: Correlations between constructs (square root of AVE on diagonal).

Structural Model

We first test the H_1, which predicts that cyber-attack risk will decrease workgroup information security effectiveness. Then, the team empowerment and IT mindfulness are added to the model respectively to examine the moderation effects for H_2 and H_3. We summarize the results of structural model testing in figure 2. From the p-values of the coefficients and the coefficient of determination (R^2) (figure 2), the coefficient of cyber-attack exposure is significant (β= -0.328; p <0.001) when the moderating variables are

not added. Cyber-attack risks negatively influence perceived remote group security effectiveness. When the two moderators are added in the model, the path coefficients are significant plus the impacts from cyberattack exposure on perceived group security effectiveness is reduced. The moderating effect of team empowerment is significant (β =0.252, $p < 0.001$ for team empowerment). The coefficient (-0.156 with $p<0.001$) of cyber-attack exposure is negatively smaller (Baron & Kenny, 1986). H1 and H2 are supported. The result indicates that team empowerment moderates the causal relationships between the cyber-attack risk and remote group security effectiveness. But the p values for IT mindfulness in the path both are a lot bigger than 0.05. So IT mindfulness is not a significant moderator between cyber-attack risk and remote group security effectiveness. H_3 is not supported in this study.

Discussion

The research results are generally consistent with our assumptions regarding the moderating effects of team empowerment to support the group work security when negative cyber-attack risk effect was high. This result suggests a lot for the management of actual security control. First, there should be capable enough and qualified team members. Second, thorough security training in both security technologies, security regulation, and security policies is necessary. Third, team members should have enough privileges and authority to respond to any security incidence.

When Zoom video conference system was first available, there were lots of problems when users used Zoom to work together remotely. Zoom Inc. was able to enhance their security features and helped their clients better train their employees such as using passwords to login or using waiting room or encryption of voice data to protect communication data. The evolutionary path of security improvement in using Zoom indicates to us that both team empowerment and IT mindfulness are important for security effectiveness (Zoom Inc, 2023).

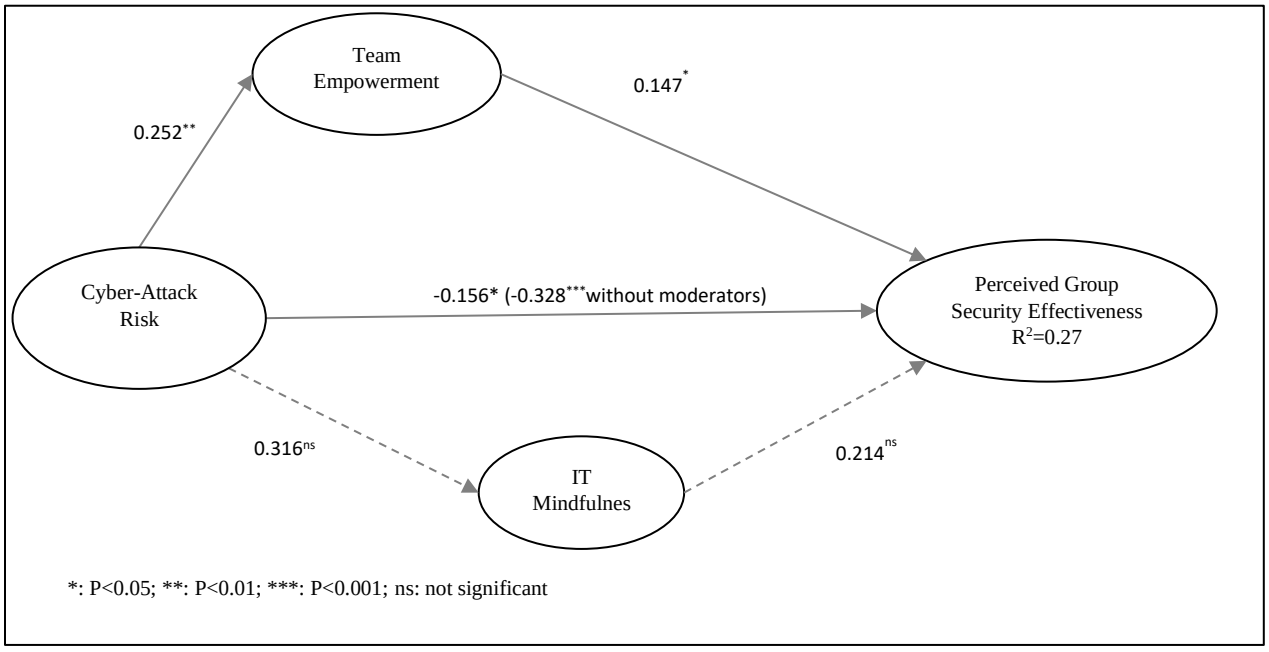

Figure 2: The Results of the Structural Model Testing

However, IT mindfulness does not show a significant moderating effect between cyber-attack risk and perceived workgroup security effectiveness, which is quite unexpected. As we know, security education and awareness are foundational to effective security management (Whitman and Mattord, 2021). Team members with enough security awareness should be quite IT-mindful. IT mindfulness should be part of the results of going through security training and education. We expected IT mindfulness to be positively related to the perceived group security effectiveness. But our data does not support it. Future research may be to replace IT mindfulness with security awareness and use security awareness as a moderator

Conclusions

Although these findings are promising and useful, like all research, our study has its limitations. First, we are not sure that our results can be generalized to all types of remote groups. Our sample consists of only online students and IT professionals (work-from-home WeChat contacts). Our sample size is not as big as we wish. This research is an exploratory study.

We might further study to check whether the current research has sampling bias. In further study, we are also interested in understanding what motivates group users to protect themselves from some of the most widespread cyber-attacks and what technology characteristics can increase the effectiveness of group security initiatives. Moreover, there is a need to further examine several group-level factors that may interact with various individual-level factors to affect remote workgroup performances, and future research should therefore explore a balanced approach between the individual and group level factors and creating a consistent set of questions to assess group security effectiveness. As discussed above, future research may use security awareness as a moderator.

References

Ahuja, M. K., & Thatcher, J. B. (2005). Moving Beyond Intention and Toward the Theory of Trying: Effects of Work Environment and Gender on Post-Adoption Information Technology Use. *MIS Quarterly*, 29(3), 427-459.

Anderson, R., and Moore, T. (2006). The Economics of Information Security. *Science*, 314 (5799), pp 610-613.

Anderson, C. & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34, 613-643.

Bagozzi, R. P. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error: A Comment. *Journal of Marketing Research*, *18*(3), 375–381.

Baron, R., & Kenny, D. (1986). The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journey of Personality and Social Psychology, 51*(6), 1173-1182.

Bishop, S. R., Lau, M., Shapiro, S., Carlson, L., Anderson, N. D., Carmody, J., Segal, Z. V., Abbey, S., Speca, M., Velting, D., and Devins, G. (2004). Mindfulness: A Proposed Operational Definition. *Clinical Psychology: Science and Practice*, 11(3), 230-241.

Carlo, J. L., Lyytinen, K., and Boland, R. J. (2012). Dialectics of Collective Minding: Contrary Appropriations of Information Technology in a High-Risk Project. *MIS Quarterly*, 36(4), 1081-1108.

Chen R., Kim D. J., and Rao, H.R. (2021). A study of social networking site use from a three-pronged security and privacy threat assessment perspective. *Information Management*, 58(5),

Dane, E. (2011). Paying Attention to Mindfulness and its Effects on Task Performance in the Workplace. *Journal of Management*, 37(4), 997-1018.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: testing a contemporary deterrence model. *Decision Sciences*, 43 (6): 1091–1124

Dennis, A. R., Fuller, R. M., and Valacich, J. S. (2008). Media, Tasks, and Communication Processes: A Theory of Media Synchronicity. *MIS Quarterly*, 32(3), 575-600.

Dinev T & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J Assoc Inf Syst.*, 8, 386–408.

Fichman, R. G. (2004). Going Beyond the Dominant Paradigm for Information Technology Innovation Research: Emerging Concepts and Methods. *Journal of the Association for Information Systems* 5(8), 314-355.

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

Hwang, I., Wakefield, R., Kim, S., and Kim, T. (2021). Security Awareness: The First Step in Information Security Compliance Behavior*" Journal of Computer Information Systems*, 61(4), 3 45-356

Hu, J., and Liden, R. C. (2011). "Antecedents of Team Potency and Team Effectiveness: An Examination of Goal and Process Clarity and Servant Leadership. *Journal of Applied Psychology*, 96, 851-862.

Jensen, M.L., Durcikova, A., Wright, R. T. (2021). Using susceptibility claims to motivate behavior change in IT security, *European Journal of Information Systems*, 30(1), 27-45.

Johnston, A., Di Gangi, P., Howard, J., and Worrell, J. (2019). It Takes a Village: Understanding the Collective Security Efficacy of Employee Groups, *Journal of the Association for Information Systems*, 20(3), 186-212.

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), 214-230

Kirkman, B. L., Rosen, B., Tesluk, P. E., and Gibson, C. B. (2004). The Impact of Team Empowerment on Virtual Team Performance: The Moderating Role of Face-to-Face Interaction. *Academy of Management Journal* 47(2), 175-192.

Kirkman, B. L., and Rosen, B. (1999). Beyond Self-Management: The Antecedents and Consequences of Team Empowerment. *Academy of Management Journal* (42), 58-74

Kritzinger E and Smith E (2008). Information security management: an information security retrieval and awareness model for industry. *Computer Security*. 27(5–6), 224–31.

Klaus, T. & Changchit, C. (2019) Toward an Understanding of Consumer Attitudes on Online Review Usage,"*Journal of Computer Information Systems*, 59(3), 277-286

Kraemer, S., Carayon, P., Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28 (7), 509-520.

Langer, E. J. (1989). Mindfulness, Reading, MA: Addison-Wesley

Langer, E., Hatem, M., Joss, J., and Howell, M. (1989). Conditional Teaching and Mindful Learning: The Role of Uncertainty in Education, *Creativity Research Journal*, 2(1), 140-150

Liang, T., Kohli, R., Huang, H., and Li Z (2021). What Drives the Adoption of the Blockchain Technology? A Fit-Viability Perspective. *Journal of Management Information Systems*, 38(2), 314-337

Line, M. B., & Moe, N. B. (2015). Understanding Collaborative Challenges in IT Security Preparedness Exercises. *ICT Systems Security and Privacy Protection*, edited by H. Federrath and D. Gollmann.. New York: Springer, pp. 311-324.

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

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia - Social and Behavioral Sciences*, 147, 424 – 428

Nunnally, I.C. and Bernstin, I.H. (1994). Psychometric Theory, 3rd. ed., McGraw-Hill, NY.

Oliveira, T. and Martins, M.F. (2010). Understanding e-business adoption across industries in European countries. *Industrial Management & Data Systems*, 110(9), 1337–1354.

Rhee HS, Ryu YU, Kim CT (2012). Unrealistic Optimism On Information Security Management. *Computer Security*.;31(2):221–32.

Sen, Ravi, Verma, Ajay, and Heim, Gregory R. (2020). Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets. *Journal of Management Information Systems*, 37(1), 191–216

Sternberg, R. J. (2000). Images of Mindfulness. *Journal of Social Issues*, 56(1), 11-26

Siponen, M & Baskerville, R. (2018). Intervention effect rates as a path to research relevance: information systems security example. *Journal Association Information System*,19(4), 247–65.

Taylor, S., and Todd, P. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research*, 6(2), 144-176.

Thatcher, J. B., Ryan T. W., Sun, H., Zagenczyk, T. J., and Klein, R. (2018). Mindfulness In In Information Technology Use: Definitions, Distinctions, And a New Measure. *MIS Quarterly*, 42 (3)

Thomas, K. W., and Velthouse, B. A. (1990). Cognitive Elements of Empowerment: An 'Interpretive' Model of Intrinsic Task Motivation. *Academy of Management Review*, 15, 666-681

Whitman, M, and Mattord, H. (2021). Principle of Information Security, 7th edition, Cengage Learning,

Venkatesh, V., Thong, J. Y.L., Chan, F.K.Y., Hu, P.J.H, and Brown, S.A. (2011). Extending the Two-Stage Information Systems Continuance Model: Incorporating UTAUT Predictors and The Role of Context, *Information System Journal*, 21, 527

Yu, B., Vahidov, R., Kersten, G. E. (2021). Acceptance of technological agency: Beyond the Perception of Utilitarian Value. *Information & Management*, 58

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

Zhang, X., Venkatesh, V., and Brown, S. A. (2011). Designing Collaborative Systems to Enhance Team Performance, *Journal of AIS*, 12(8), 556-584.

Zohar, D., and Luria, G. (2005). A Multilevel Model of Safety Climate: Cross-level Relationships Between Organization and Group-Level Climates. *Journal of Applied Psychology*, 90, (4), 616-628

Zoom Inc. https://explore.zoom.us/en/collaboration-tools/. Retrieved on July 12, 2023

Appendix A

Scale	Item	Sources	Loading
IT Mindfulness Cronbach's Alpha=0.815	I find it easy to create new and effective ways of using technology.	*Thatcher et al. 2018*	0.842
	I make many novel contributions to my work-related tasks through using technology.		0.833
	I am very creative when using technology.		0.844
	I am often open to learning new ways of using technology.		0.831
	I have an open mind about new ways of using technology.		0.822
	I like to figure out different ways of using technology.		0.841
	I like to investigate different ways of using technology.		0.855
	I 'get involved' when using technology		0.832
Team Empowerment Cronbach's Alpha=0.803	Our team has confidence.	*Kirkman et al. 2004*	0.902
	Our team cares about what it does.		0.831
	Our team feels that its tasks are worthwhile.		0.822
	Our team can select different ways to do the team's work.		0.928
	Our team determines as a team how things are done in the team.		0.855
Cyber-Attack Risk Cronbach's Alpha=0.846	Using remote technology may expose myself to online frauds.	*Chen et al. 2021*	0.816
	Using remote technology site may expose myself to identity theft.		0.864
	Use of remote technology site may expose myself to cyber criminals.		0.928
	Using remote technology site may expose myself to malicious attacks.		0.811
Perceived Group Information Security Effectiveness Cronbach's Alpha=0.725	Our team's protection of physical facilities and compliance with security management policy	Yoo et al. 2020	0.727
	Our team's detection and report of possible breaches against the remote group information system.		0.704
	Our team's security awareness of individual member and the security culture for the remote information system.		0.713
	Our team's compliance with password management policy the remote information system.		0.651