7-1-2023

Examining the Effects of Virtual Work on Cybersecurity Behavior

Amitava Dutta

Pallab Sanyal

EXAMINING THE EFFECTS OF VIRTUAL WORK ON CYBERSECURITY BEHAVIOR

Amitava Dutta
George Mason University
adutta@gmu.edu

Pallab Sanyal
George Mason University
psanyal@gmu.edu

ABSTRACT

The Science of Security (SoS) initiative at the NSA identifies Five Hard Problems, one of which is understanding human behavior. Our study focuses on behavioral aspects of cybersecurity and is motivated by the changes brought about by the pandemic. Even though COVID is now under control, the work from home (WFH) component of organizational activity will remain significant. We propose a theoretical model that incorporates WFH factors into existing models of cybersecurity behavior. We characterize WFH based on Herzberg's motivation-hygiene theory of job satisfaction. A survey instrument is being developed to test the model. While the literature has viewed WFH as a negative force in cybersecurity, our job satisfaction conceptualization of WFH reveals that WFH also provides flexibilities that improve job satisfaction, which in turn have a positive impact on cybersecurity behavior. We develop testable hypotheses, and the managerial implication of our theoretical model is also discussed.

Keywords

Cybersecurity, conceptual model, work from home, behavioral intention

INTRODUCTION

The science of security initiative of the National Security Agency organizes its research around five "hard problems" (Scala et al 2019). The first four (i) scale and composability (ii) policy governed secure collaboration (iii) security metrics driven evaluation, design, and development (iv) resilient architecture, are technical in nature. The fifth is *understanding and accounting for human behavior* and aims to develop models of human behavior that enable the design, modeling, and analysis of systems with specified security properties. While much of past research on cybersecurity has focused on the technical dimension, the importance of the behavioral dimension, and the challenges associated with understanding it, are being increasingly recognized (Pfleeger 2012). This 'human factor' has often been recognized as being the weakest and most obscure link in creating safe and secure digital environments (Jeong et al 2019). Our research focuses on behavioral aspects of cybersecurity and is motivated by the work from home (WFH) setting forced on organizations by the COVID-19 pandemic. The scope and scale of activities that were forced online was unprecedented and organizations were ill prepared for the shift. There are two dimensions to this 'forced' move: (i) people who were not comfortable in an online environment, even for simple tasks, were forced to go online, and (ii) people who were otherwise comfortable in an online environment, found themselves expanding the scope of online activity to domains that had been mostly in-person (e.g., doctor visits). In short, COVID-19 has caused a shift from predominantly in-person ecosystems to a virtual workplace for employees. More importantly, there is widespread agreement that, even after the pandemic has been brought under control, the WFH footprint will remain extensive in most organizations (Bartik et al. 2020). There is already a robust body of literature on theoretical models which associate threat appraisal and threat coping latent variables with some manifestation of actual cybersecurity behavior or intent. However, the predominant context of these studies is in-person work settings in organizational facilities where devices, physical surroundings, and procedures are subject to organizational control, and which are designed to facilitate work. As will be discussed shortly, WFH surroundings differ from formal work settings in significant ways. This motivates us to ask the following research question: How can existing theoretical models of cybersecurity behavior be augmented to incorporate WFH characteristics and can the implications of such a modified model be used to adjust cybersecurity policies to improve cybersecurity resilience?

The paper is organized as follows. In the next section we will review characteristics of WFH that are relevant from a cybersecurity standpoint. Following that, we will briefly review the common characteristics of current theoretical models of cybersecurity behavior. We will then introduce our theoretical conceptualization of WFH and develop a theoretical model of cybersecurity behavior that incorporates WFH. A survey instrument is being prepared to test our model and sample question items are presented. This survey will be administered to a subject pool in the next phase of the study. Possible findings from the survey and their managerial implications will be discussed in conclusion.

THEORETICAL MODELS OF CYBERSECURITY BEHAVIOR

There is a rich body of literature on theoretical models of cybersecurity behavior. While they differ in the specific latent variables used, the general structure of these models can be summarized as shown in Figure 1. There is usually a component of the model that captures threat appraisal by the individual, another component that captures the individual's perception of coping with the threat, and then these two components are associated with some form of cybersecurity behavior. These models draw on the Theory of Planned Behavior, General Deterrence Theory, Protection Motivation Theory and Organizational Commitment theory in creating their specific latent variables.

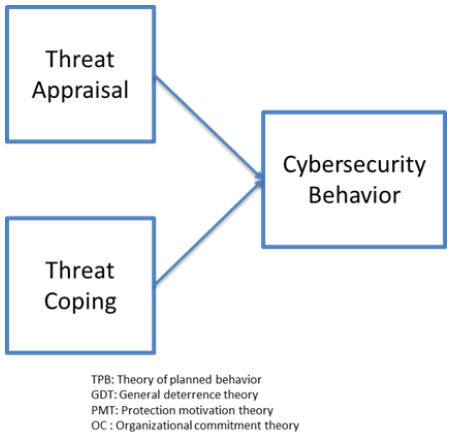

Figure 1. Generic Theoretical Model of Cybersecurity Behavior

For instance, Anderson and Agarwal (2010) use 'Intention to perform cybersecurity related behavior on the internet and one's own computer' as their dependent variables. They use 'perceived security behavior self-efficacy' as one of the threat coping variables, and 'concern regarding security threats' as one of the threat appraisal variables. A collection of hypotheses linking these latents to the dependent variable are established and then tested empirically. Li et al. (2019) investigate the impact of organizational security policy awareness on cybersecurity behavior. They have security protection behavior as the dependent variable. They, too, have self-efficacy and perceived barriers among the coping variables, perceived severity, and vulnerability among the threat appraisal latent variables. Their survey and subsequent analysis find that when employees are aware of their company's information security policy and procedures, they are more competent to manage cybersecurity tasks than those who are not aware. They also find that an organizational information security environment positively influences employees' threat appraisal and coping appraisal abilities, which in turn, positively contributes to their cybersecurity compliance behavior. Herath and Rao (2009) develop a protection motivation and deterrence model for security policy compliance intention using latent variables based on the theories mentioned earlier. Behavioral intent is the dependent variable, self-efficacy and response efficacy are examples of coping variables, and perceived probability and severity of breach are examples of the threat appraisal variables. Among other findings, they find that resource availability, organizational commitment and social influence have a significant impact on compliance intentions. In an interesting take on cybersecurity behavior, Liang and Xue (2009) examine threat avoidance behavior of individuals as the dependent variable, driven by threat appraisal and coping variables. While the authors do not conduct any empirical test, their model leads to hypotheses which hold that users are motivated to avoid malicious IT when they perceive a threat and believe that the threat is avoidable by taking safeguarding measures. If users believe that the threat cannot be fully avoided by taking safeguarding measures, they will engage in emotion-focused coping. These are a few examples of the kinds of theoretical models of cybersecurity behavior developed in the literature. Apart from the common general structure mentioned in Figure 1, these models also have another characteristic in common. They almost exclusively focus on in-person organizational settings. Oftentimes, as in the case of Herath and Rao (2009) or Liang and Xue (2009), the assumption is implicit in that the models do not have specific variables about the work environment. For the few theoretical models that do consider home computer users, as in Anderson and Agarwal (2010), the model does not conceptualize WFH characteristics or incorporate them into the model. In the following sections we discuss characteristics of WFH and then proceed to conceptualize it using some well-established theoretical constructs from organizational behavior theory. This conceptualization is then used to integrate WFH into the current theoretical model structure.

WORK FROM HOME AND CYBERSECURITY

Maintaining a good cybersecurity posture is an ongoing challenge for all organizations and the prevailing view is that WFH only makes it more difficult to maintain that posture. Figure 2 shows some of the reasons for that view (Pratt 2022).

Figure 2. Risk factors in WFH Environments

For example, most individuals use wireless networks at home and these networks are easier to compromise than the wired networks that are generally found in the office, particularly if the WFH setting is an apartment complex or condominium where units are in proximity. Some of the enabling technologies for WFH, such as Webex and Zoom have their own vulnerabilities (Borkovich and Skovira 2020). Webcams can be hacked, and the computing devices used for WFH often serve multiple purposes and are used by multiple family members. There is less oversight by organizational IT staff in WFH settings and there are many more opportunities for distraction and disruption compared to regular office settings. In short, there are a multitude of factors in WFH settings that make it more difficult, or require more effort, to engage in desirable cybersecurity behavior. From a theoretical perspective, this would lead one to conclude that WFH would lower intent to engage in desirable cybersecurity behavior. There are other challenges to WFH besides cybersecurity issues and they include distractions at home, loneliness, blurred lines between work and personal life, time zone differences and staying motivated (Toniolo-Barrios and Pitt 2021).

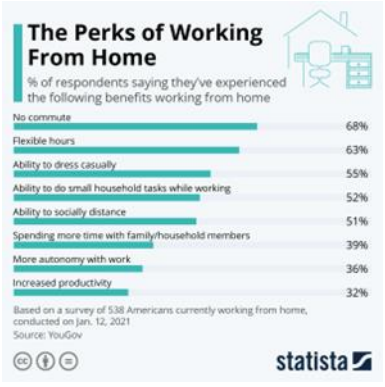

Figure 3. Benefits of WFH

	Prefer exclusively on-site %	Prefer hybrid %	Prefer exclusively remote %	Total prefer remote %
Remote workers				
Working from home exclusively	6	45	49	94
Working partially from home/partially on-site (hybrid)	15	70	15	85
Total working remotely (hybrid or exclusively)	9	54	37	91
Potential remote workers				
Working on-site, but job can be done from home	52	37	11	48

GALLUP PANEL, MAY 26–JUNE 9, 2021

Figure 4. Preferences for Continuing WFH

However, there are also benefits to WFH and all indications are that it is here to stay. Figure 3 shows the results of a survey (Richter 2021) on the perks of working from home and Figure 4 shows a recent survey (Saad and Wigert 2021) which indicates that workers overwhelmingly desire the flexibility of some remote work. This tension between the challenges and benefit of

WFH, motivates us to integrate its effects into existing cybersecurity models and test the overall impact empirically. The first step in that process is to conceptualize WFH theoretically.

Conceptualizing WFH

The benefits and challenges of WFH have been discussed in the preceding section. We have chosen to use Herzberg's two-factor theory of job satisfaction (Herzberg 2017), first published in 1959, as the lens through which to conceptualize WFH. It is well established in the organizational psychology literature that job satisfaction is closely associated with workplace behavior (Judge et al. 2020). For our purposes, cybersecurity behavior would fall in the category of workplace behavior, hence our selection of a theoretical model of job satisfaction as the lens through which to conceptualize WFH. Herzberg's two-factor theory states that job satisfaction and dissatisfaction are affected by two different sets of factors. Therefore, satisfaction and dissatisfaction cannot be measured on the same continuum. The theory was highly controversial at the time it was published, claims to be the most replicated study in this area, and provided the foundation for numerous other theories and frameworks in human resource development (Stello 2011). The two-factor theory of job satisfaction has been empirically tested in domains too numerous to list here. They include such varied settings as clinical laboratories in hospitals (Alrawahi et al. 2020), university teachers (Ghazi et al. 2013), the construction industry (Ruthankoon and Olu 2003), and army foodservice operations (Hyun and Oh 2011).

Figure 5. Herzberg Two-Factor Theory

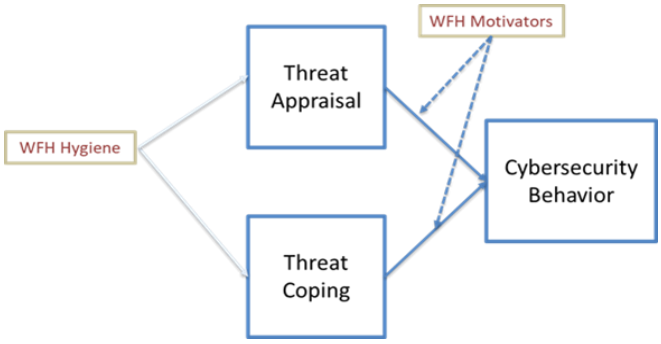

Figure 6. Integrated Cybersecurity Behavior Model with WFH

As shown in Figure 5 (Lumen 2023), Hygiene factors include work ecosystem characteristics such as working conditions, supervisor quality, salary, policies and rules etc. Motivator factors include such things as recognition, advancement, work itself, personal growth etc. There is also a temporal dimension to the two-factor model in that the influence of motivators is a long-term phenomenon while the hygiene factors tend to influence more immediately (Stello 2011). To map the two-factor model to our cybersecurity behavior context, two issues need to be addressed. Since the theory distinguishes between hygiene and motivation factors, we first need to hypothesize how these two distinct drivers would influence the generic cybersecurity model of Figure 1. We posit that hygiene factors will directly affect the threat appraisal and threat coping latent variables in Figure 1, while the motivator factors will have a moderating effect on the relationship between threat coping and threat appraisal with behavior. This results in the integrated behavior model shown in Figure 6. Hygiene factors include variables such as working conditions and policies and these would directly affect an individual's perception of threat and of their ability to cope with cyberthreats. Examples of working conditions include, for instance, distractions in a WFH setting, vulnerabilities of WFH WiFi connections, weak security configurations of personal computers, susceptibility to unauthorized viewing of content. Examples of policies and rules include such things as mandatory use of VPN for remote connections, administrative rights on WFH computers to install new software, password change rules and these too would have a direct effect on perceptions of threat appraisal and threat coping. Motivator variables, on the other hand, are what Herzberg referred to as 'intrinsic' in nature and their influence is more long term in nature. Moreover, these are variables that affect satisfaction, which in turn will influence the inclination of an individual to engage in desirable work behavior, which includes cybersecurity behavior. Therefore, we posit that Motivators will play a moderating role as shown in Figure 6. A survey instrument has been developed to test the model shown in Figure 7 and will be administered in the next phase of the study. A sample of the questionnaire items are shown in Figure 7.

LATENT	ITEMS
Perceived severity of threat	• I believe that information stored on organization computers is vulnerable to security incidents • I believe the productivity of organization and its employees is threatened by security incidents • I believe the profitability of organizations is threatened by security incidents.
Perceived Likelihood of threat	• How likely is it that a security violation will cause a significant outage that will result in loss of productivity? • How likely is it that a security violation will cause a significant outage to the Internet that results in financial losses to organizations? • How likely is it that organization will lose sensitive data due to a security violation?
Perceived response efficacy	• Every employee can make a difference when it comes to helping to secure the organization's IS. • There is not much that any one individual can do to help secure the organization's IS. • If I follow the organization IS security policies, I can make a difference in helping to secure my organization's IS.
Attitude towards Cybersecurity	• Adopting security technologies and practices is important • Adopting security technologies and practices is beneficial • Adopting security technologies and practices is helpful.
Punishment severity Detection certainty	• The organisation disciplines employees who break information security rules. • My organisation terminates employees who repeatedly break security rules. • If I were caught violating organisation information security policies, I would be severely punished • Employee computer practices are properly monitored for policy violations • If I violate organisation security policies, I would probably be caught

Figure 7. Sample Items for Cybersecurity Behavior Survey

Testable Hypotheses and Managerial Implications

Several testable hypotheses emerge from the integrated model of Figure 7, a subset of which are listed below

H1: Distractions in WFH environment will increase the perceived likelihood of threats

H2: Increased WFH resources will increase the perceived ability to cope with threats

H3: Work time flexibility will moderate the relationship between threat appraisal and cybersecurity behavior.

Since we do not yet have the results of the survey, it is not possible to draw managerial implications now. However, we surmise that the empirical findings about the influence WFH factors included in the questionnaire will guide us in suggesting managerial policies and interventions that would improve cybersecurity behavior and organizational resilience.

CONCLUSION

In this paper, we have described the development of a theoretical model to capture the effects of work from home arrangements on cybersecurity behavior. WFH, forced on organizations by the COVID pandemic, is here to stay even though the pandemic is now under control. While WFH was mostly seen as a negative influence from a cybersecurity standpoint, the COVID experience has shown that there are definite advantages to WFH, which if properly exploited in setting cybersecurity policies, can improve cybersecurity behavior and make organizations more resilient. Herzberg's two-factor theory of job satisfaction provides a theoretical lens through which to conceptualize WFH and integrate it into current theoretical models of cybersecurity behavior. This model can then be tested empirically and the findings used to develop data driven cybersecurity policies.

ACKNOWLEDGMENTS

This work was supported by Grant No. 224041 from the Commonwealth of Virginia Cybersecurity Initiative.

REFERENCES

1. Alrawahi, S., Sellgren, S. F., Altouby, S., Alwahaibi, N., & Brommels, M. (2020). The application of Herzberg's two-factor theory of motivation to job satisfaction in clinical laboratories in Omani hospitals. *Heliyon*, *6*(9), e04829.
2. Amato, F., Castiglione, A., De Santo, A., Moscato, V., Picariello, A., Persia, F., & Sperlí, G. (2018). Recognizing human behaviours in online social networks. *Computers & Security*, *74*, 355-370.
3. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS quarterly, 613-643
4. Bartik, A. W., Cullen, Z. B., Glaeser, E. L., Luca, M., & Stanton, C. T. (2020). *What jobs are being done at home during the COVID-19 crisis? Evidence from firm-level surveys* (No. w27422). National Bureau of Economic Research.
5. Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4).
6. Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97*, 101931.

7. Ghazi, S. R., Shahzada, G., & Khan, M. S. (2013). Resurrecting Herzberg's two factor theory: An implication to the university teachers. *Journal of Educational and Social Research*, *3*(2), 445.
8. Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior*, 108, 106319.
9. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*, 106-125.
10. Herzberg, F. (2017). *Motivation to work*. Routledge.
11. Hyun, S., & Oh, H. (2011). Reexamination of Herzberg's two-factor theory of motivation in the Korean army foodservice operations. *Journal of Foodservice Business Research*, *14*(2), 100-121.
12. Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019, December). Towards an improved understanding of human factors in cybersecurity. In 2019 *IEEE 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 338-345). IEEE.
13. Judge, T. A., Zhang, S. C., & Glerum, D. R. (2020). Job satisfaction. *Essentials of job attitudes and other workplace psychological constructs*, 207-241.
14. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.
15. Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.
16. Lumen Learning (2023). Reading: Herzberg's Two-Factor Theory. https://courses.lumenlearning.com/wmintrobusiness/chapter/reading-two-factor-theory/ last accessed Feb 27, 2023.
17. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, 31(4), 597-611.
18. Pratt M.K. (2022). Remote work cybersecurity: 12 risks and how to prevent them. www.techtarget.com August 2022. https://www.techtarget.com/searchsecurity/tip/Remote-work-cybersecurity-12-risks-and-how-to-prevent-them . Last accessed Feb 27, 2023.
19. Richter F. (2021). The Perks of Working From Home. https://www.statista.com/chart/25020/perceived-perks-of-working-from-home/ last accessed Feb 27, 2023.
20. Ruthankoon, R., & Olu Ogunlana, S. (2003). Testing Herzberg's two-factor theory in the Thai construction industry. *Engineering, Construction and Architectural Management*, *10*(5), 333-341.
21. Saad, L., & Wigert, B. (2021). Remote work persisting and trending permanent. *Gallup News Insights*, *13*.
22. Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, 39(10), 2119-2126.
23. Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 9(4), 475.
24. Stello, C. M. (2011). Herzberg's two-factor theory of job satisfaction: An integrative literature review. In *Unpublished paper presented at the 2011 student research conference: Exploring opportunities in research, policy, and practice, University of Minnesota Department of Organizational Leadership, Policy and Development, Minneapolis, MN*.
25. Toniolo-Barrios, M., & Pitt, L. (2021). Mindfulness and the challenges of working from home in times of crisis. *Business horizons*, *64*(2), 189-197.