Nov 14th, 10:50 AM - 11:10 AM

Towards Assessing Organizational Cybersecurity Risks via Remote Workers' Cyberslacking and Their Computer Security Posture

Ariel Luna
Nova Southeastern University, al1572@mynsu.nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Gregory Simco
Nova Southeastern University

Wei Li
Nova Southeastern University

Abstract

Cyberslacking is conducted by employees who are using their companies' equipment and network for personal purposes instead of performing their work duties during work hours. Cyberslacking has a significant adverse effect on overall employee productivity, however, recently, due to COVID19 pandemic move to remote working also pose a cybersecurity risk to organizations networks and infrastructure. In this work-in-progress research study, we are developing, validating, and will empirically test taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This study includes a three-phased developmental approach in developing the Remote Worker Cyberslacking Security Risk Taxonomy. With feedback from cybersecurity Subject Matter Experts (SMEs) on the taxonomy and measures, we then plan to use the taxonomy to assess organizational remote workers' risk level of cybersecurity threats by using actual system indicators of productivity measures to estimate their cyberslacking along with assessing the computer security posture of the remote device being used to access organizational resources. Anticipated results from 125 anonymous employees will then be assessed on the proposed novel taxonomy where recommendation to the organizational cybersecurity leadership will be provided.

Disciplines

Information Security | Management Information Systems | Technology and Innovation

Towards Assessing Organizational Cybersecurity Risks via Remote Workers' Cyberslacking and Their Computer Security Posture

Ariel Luna
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
al1572@mynsu.nova.edu
ORCID: 0000-0002-2580-0384d

Yair Levy
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
levyy@nova.edu
ORCID: 0000-0002-8994-6497

Gregory Simco
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
greg@nova.edu
ORCID: 0000-0001-5760-6933

Wei Li
College of Computing and Engineering
Nova Southeastern University
Ft. Lauderdale, FL, USA
lwei@nova.edu
ORCID: 0000-0001-5880-4640

***Abstract*— Cyberslacking is conducted by employees who are using their companies' equipment and network for personal purposes instead of performing their work duties during work hours. Cyberslacking has a significant adverse effect on overall employee productivity, however, recently, due to COVID-19 pandemic move to remote working also pose a cybersecurity risk to organizations networks and infrastructure. In this work-in-progress research study, we are developing, validating, and will empirically test taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This study includes a three-phased developmental approach in developing the Remote Worker Cyberslacking Security Risk Taxonomy. With feedback from cybersecurity Subject Matter Experts (SMEs) on the taxonomy and measures, we then plan to use the taxonomy to assess organizational remote workers' risk level of cybersecurity threats by using actual system indicators of productivity measures to estimate their cyberslacking along with assessing the computer security posture of the remote device being used to access organizational resources. Anticipated results from 125 anonymous employees will then be assessed on the proposed novel taxonomy where recommendation to the organizational cybersecurity leadership will be provided.**

Keywords—Cyberslacking, organizational cybersecurity risk, remote workers cybersecurity, employee productivity, cybersecurity posture.

I. INTRODUCTION

Cyberslacking, or cyberloafing, can be defined as an employee's use of an organizational Information Technology (IT) resources for non-work-related activities, such as surfing the web or checking personal email, which do not contribute to completion of their job function [27]. Cyberslacking is usually associated with employee productivity losses or degradation of network services and not with the increased cybersecurity risks related to cyberslacking or cyber deviant behaviors [20]. However, Vernon-Bido et al. [48] found that cyberslacking can be categorized as an expense due to the loss of productivity as well as a cybersecurity risk. Due to the COVID-19 world pandemic, organizations have increased and accelerated their adoption of remote work [35]. Working remotely has been studied extensively in terms of employee satisfaction, commitment, and productivity [2], [7], [17]. Additionally, O'Neill et al. [33] posited that many of the studies conducted on cyberslacking focused on workers who were primarily in the office environment as opposed to working remotely. Furthermore, Stitch [41] determined employees working remotely may be more suspectable to engage in activities that could be deemed cyberslacking or cyber deviance. This work-in-progress study intends to address the gap in the literature regarding cyberslacking by remote workers and the cybersecurity risks they pose to organizations. The increased adoption of working remotely provides an opportunity to investigate the impact remote workers can have on an organizational cybersecurity, specifically employees who engage in cyberslacking [35]. Thus, the main research question we propose is: How are remote workers classified in terms of the potential cybersecurity risk they pose based on the cyberslacking activities they engage in, and the cybersecurity posture of the device being used to access the organizations resources?

II. LITERATURE REVIEW

A. Remote Workers and Cyberslacking

Cyberslacking is defined as "the act of employees using their companies' Internet access for personal purposes during work hours" [27]. Recent research has begun the examination of cyberslacking as it pertains to the remote workforce, those who may spend their entire work shift in front of a computer remotely and not in the physical view of a supervisor [33], [34]. O'Neill et al. [34] used a survey instrument that was distributed to 148 working adults in the United States (U.S.) who worked remotely a minimum of one day per week. The intent of their survey instrument was to collect data to measure key personality factors, self-management techniques, and engagement in work activities to determine if cyberslacking by remote workers affected job effectiveness. Their study found that direct implications of frequent cyberslacking by remote workers impacted their overall engagement in work activities [34]. Additionally, a literature review and analysis conducted by Stich [41] on workplace stress in a virtual office uncovered a common theme with respect to deviant behaviors occurring when employees were outside of the traditional office setting. These behaviors included using the Internet for non-work-related activities such as personal email, gambling, and surfing the web. Similarly, a longitudinal study conducted by Russo et al. [35] to investigate predictors of well-being and productivity

during the COVID-19 pandemic concluded that remote workers were more frequently distracted and engaged in cyberslacking activities, which suggests that further study is warranted." However, these studies have used self-reported survey instruments rather than actual assessment provided from the systems or network, which is what this work-in-progress study is attempting to do to ensure validity of the results.

B. *Employee Productivity*

Employee productivity is focused on the efficiency of an employee or employees and can be evaluated by measuring their respective output within a given time period [21]. Hanaysha [21] used a 5-point Likert scale survey instrument that was distributed online to 870 administrative and academic staff at public universities in Malaysia. Hanaysha [21] analyzed the data using structural equation modelling with several tests performed for validity, such as Cronbach's alpha reliability, convergent validity, face validity, and factor analysis. His results demonstrated that employee engagement had a significant positive effect on employee productivity. This finding supports the study conducted by Markos and Sridevi [28] that found employees who were not engaged in the workplace tended to focus on tasks of lower priority or those not essential to their job function. Ferreira and Du Plessis [16] suggested measuring employee productivity by using time spent executing required tasks to achieve the desired outcome according to job function. Similarly, Syed et al. [43] utilized the amount of work completed within a respective period of time as the measurement for productivity. In addition, Gibbs et al. [19] measured productivity using an employee's completed tasks per month divided by the number of hours worked. Thus, time on task can be an effective measure of employee productivity and will be used in this work-in-progress study.

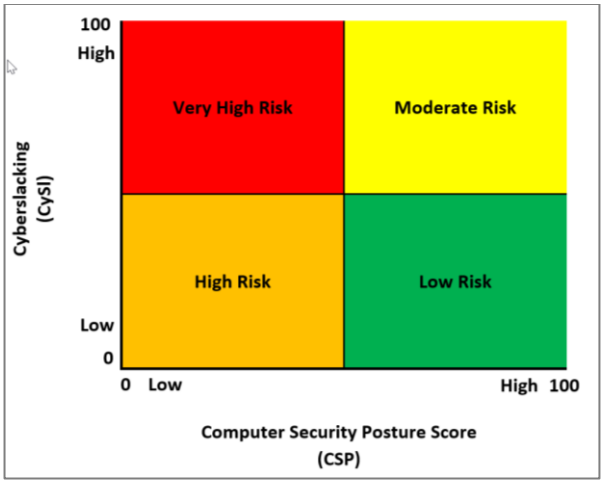
C. *Computer Cybersecurity Posture*

Cybersecurity threats were estimated to have cost about $6 trillion in 2021, and the increase in the number of cybersecurity attacks after COVID-19 is five times the rate before the pandemic [5]. The pandemic has accelerated adoption of work from home options for many organizations and has strained their respective IT departments by forcing the use of new methodologies to secure supporting infrastructure such as home computers, home routers, and Wi-Fi access points [5]. This rapid acceleration led to the March 2020 release of a bulletin outlining and reinforcing the standards for teleworking by the National Institute of Standards and Technology [31]. The bulletin detailed five key items for securing remote workers, including the use of Virtual Private Network (VPN) connections, enhancing the security of devices with the latest operating system patches, and enabling device encryption. These items are components that make up the cybersecurity posture of a device. Adel et al. [1] described cybersecurity posture as the overall security status and ability to manage an organizational technology stack such as software, hardware, networks, and data. Another term used in the literature to describe the security posture of a device as it pertains to the user is cyber hygiene. Vishwanath et al. [49] defined cyber hygiene as those practices users should adhere to in order to protect their Internet-accessible devices from being compromised in a cyber-attack. Proper cyber hygiene includes various cybersecurity controls that should be followed, such as proper patch management for all software on the device, antivirus and malware protection, firewall configuration, as well as VPNs for accessing corporate resources [12], [42], [49].

D. *Proposed Remote Worker Cyberslacking-Security Risk Taxonomy*

The novelty of this work-in-progress study is in the proposed measures and the taxonomy to assess cybersecurity risk to organizations of remote workers. As many of the prior studies associated with both the remote worker cyberslacking and their computer security have used self-reported survey instrument that are questionable in their validity, this study will focus on actual measures provided from the system, application, and network activities. The main goal of this research study is to develop, validate, and empirically test a taxonomy to assess an organizational remote workers' risk level as depicted in Figure 1. This study will measure a worker's potential participation in cyberslacking and the computer security posture of the organizational-provided remote device used to access organizational resources. Venktraman et al. [47] described that despite an increase in cyberslacking and cyberdeviance research, an overall understanding of the issue by both practitioners and researchers is still limited, while further research is needed. The more time employees spend on websites and activities not related to their job function, the greater the risk to the cybersecurity posture of an organization [48]. In addition, Russo et al. [35] highlighted that the increase in adoption of working remotely facilitates the opportunity to research the impact remote workers can have on an organizational cybersecurity, specifically with employees who engage in cyberslacking

Fig. 1. Proposed Remote Worker Cyberslacking Security Risk Taxonomy



III. Methodology

This work-in-progress research study, a three-phased developmental approach as depicted in Figure 2, is intended to create the Remote Worker Cyberslacking-Security Risk Taxonomy. In collaboration with cybersecurity SMEs, the intended main goal of this research study is to develop, validate, and empirically test a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats by using

productivity measures to determine their potential engagement and the computer security posture of the remote device being used to access corporate resources. To achieve the goal of this study the following six Research Questions (RQs) are proposed:

RQ1: What are the specific elements identified by SMEs to measure cyberslacking that will enable an aggregated score to determine cybersecurity risk?

RQ2: What are the specific elements identified by SMEs to measure the computer cybersecurity posture of the device being used to access corporate resources?

RQ3: How are the employees positioned in the Remote Worker Cyberslacking Security Risk Taxonomy using the cyberslacking score and the computer security posture score?

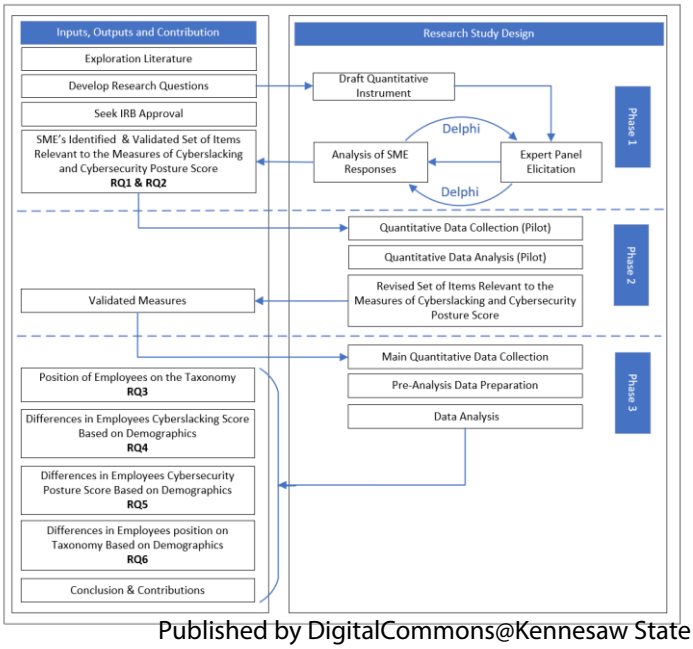
RQ4: Are there significant mean differences in the employees' cyberslacking scores based on the demographic indicators of (a) age, (b) gender, (c) education level, and (d) years of work experience

RQ5: Are there significant mean differences in the employees' computer security posture scores based on the demographic indicators of (a) age, (b) gender, (c) education level, and (d) years of work experience?

RQ6: Are there any differences in an employee's position in the Remote Worker Cyberslacking Security Risk Taxonomy based on the demographic indicators of (a) age, (b) gender, (c) education level, and (d) years of work experience?

The data collection for this work-in-progress developmental study will utilize an experimental field study approach as described by Levy and Ellis [26]. This experimental design is appropriate when randomization of the participants is not possible, leaving the researcher to use pre-defined groups. This taxonomy will be leveraged as the artifact or "thing" that is built to address the identified research problem [15].

Fig. 2. Proposed Research Design Process



A. *Measures*

The measures for cyberslacking activity and device Computer Security Posture (CSP) are anchored in prior literature. Productivity has been used as an indicator of an organization's success, and continues to expand as a key performance measure, incorporating strategic organizational goals along with financial considerations [8], [30], [50], [51]. The studies conducted by Eldridge and Pabilonia [14], Ferreira and Du Plessis [16], and Syed et al. [43] utilized employee's engagement in work activities within a respective period of time as the measurement for productivity. Similarly, Das et al. [13] attributed a decrease in an employee's overall work performance to their engagement in non-work activities such as cyberslacking. To measure employee productivity and engagement time, this study will use an aggregate value of key indicators that have been identified from the literature and validated using feedback from SMEs. This study will expand on the work done by Yang et al. [52], Franscilla et al. [18] and Cao et al. [10] which focused on the use of major productivity tools such as Microsoft Teams, Outlook, OneDrive, and SharePoint to measure productivity and multitasking behaviors. The measure of cyberslacking activity will be comprised of the following inputs: employee engagement and productivity, total hours in the workday, and a constant measure for breaks, as depicted in Equation 1.

$$CySl = k*(WkD\ (hrs) - [(Brk\ (hrs) + EP\ (hrs))]) \quad (1)$$

As shown in Equation 1, CySl is the user-assigned value for cyberslacking opportunity in hours and WkD is the typical workday. In the U.S., a typical workday is eight hours [40], [45]. Brk is a constant value of time provided for breaks or activities that are not directly related to work but do not impact overall engagement time. The normalization coefficient is represented by k (100/7.5 or 40/3). Lastly, EP is the overall employee productivity and engagement time.

To measure the computer security posture of the device being used by remote workers to access corporate systems, the study will use an aggregate value of key indicators that have been identified from the literature, validated, and assigned proper weights using feedback from SMEs. Abdel et al. [1] referred to cybersecurity posture as overall security status and the ability to manage an organization's technology stack such as software, hardware, networks, and data. In addition, cybersecurity posture considers the organization's ability to react, mitigate, and recover from security events. Cybersecurity posture includes many areas that need to be addressed to protect an organization from potential cyber threats. This study will focus on cybersecurity posture from the endpoint device used to access corporate resources with company-provided devices and their overall cyber hygiene, which plays a large role in cybersecurity breaches [9]. The literature demonstrates that proper cyber hygiene includes various security controls that should be followed such as proper patch management for all software on the device, antivirus and malware protection, firewall configuration, and VPN for accessing organizational resources [12], [42], [49]. Thus, this study will use the indicators of proper cyber hygiene as derived from the literature to determine an aggregate score for computer security posture as depicted in Equation 2.

$$CSP = j^* (w_1^*CSP_1 + \ldots + w_8^*CSP_8) \quad (2)$$

As shown in Equation 2, CSP is the value for the computer security posture of the device being used to access organizational resources remotely. The computer security posture indicator is represented by CSP_i, the weight of the computer security posture indicator is represented by w_i, and j represents the normalization coefficient for CSP_i. The value for CSP is normalized using j coefficient (100/8), to a value between 0 and 100 for consistency representing percent of computer security posture. The CSP normalized score will be used as one of the two values to determine the employee's position in the Remote Worker Cyberslacking Security Risk Taxonomy.

The literature has demonstrated that demographics, such as age, gender, education level, and years of work experience, have been "empirically verified to have contributed to cyberloafing and often referred to as cyberloafing antecedents" [37]. Although the literature does support demographics as antecedents, inconsistent findings exist pertaining to age, gender, education, and work experience with respect to employees' cyberslacking [4], [22], [37]. Hartijasi and Fathonah [22], as well as Sheikh et al. [37] stated age, gender, education, and work experience were factors that contributed to cyberslacking activities. Conversely, Hernandez et al. [23] found that age, gender, level at the organization, and education did not show a significant difference in cyberslacking activities. Another example of varying findings pertaining to demographics is demonstrated in Ugrin et al.'s [44] study in which executives were more likely to engage in cyberslacking activities. Similarly, Aghaz and Sheikh [3] found a positive correlation between level in the organization and cyberslacking behaviors. Therefore, further research is warranted with respect to employee cyberslacking demographic factors such as age, gender, education, and level at the organization.

B. Proposed Sample

Currently there is no consensus in terms of a panel size and number of rounds for the Delphi method that will be leveraged in phase one of this study [6], [39], although Okoli and Pawlowski [32] suggested that an expert panel size should have 10 to 18 experts participating in each round. Similarly, Skinner et al. [38] posited that expert panels can range from 10 to 30 experts. For phase one of this research study, the proposal is to contact 20 experts, with a desired response rate of 15. The expert panel is to be recruited via LinkedIn and professional cybersecurity organizations. Clayton [11] defined an expert as "someone who possesses the knowledge and experience necessary to participate in a Delphi". According to Clayton's definition, members of the panel will be limited to cybersecurity professionals with the requisite knowledge, education, experience, and professional certification credentials.

For the second phase of the study, the work-in-progress research will collect demographic data, cyberslacking activity, and computer cybersecurity posture indicators in the form of a pilot study to ensure the taxonomy meets the requirements set forth. The participants for the pilot will be recruited via email and will be a subset of employees of the intended larger sample. In order to participate in the study, the employees must be information workers with technology backgrounds who work from home. Pilot users will be excluded from the main data collection to avoid adversely affecting the participants' behavior, as this can be a common drawback of using a pilot [46].

Phase three of the study will utilize a sample of the population as described by Sekran and Bougie [36] as representative of the overall population by which conclusions can be drawn, specifically a target of 125 participants. This work-in-progress study will leverage a sample of convenience from a large technology firm, specifically targeting information workers with technology backgrounds who primarily work from home. The participants will be contacted via email to participate in the study.

C. Preanalysis Data Screening

To ensure that data being collected in this work-in-progress study will not contain irregularities or present issues during the collection process, pre-analysis data screening will be utilized prior to conducting the final analysis, as recommended by Levy [25]. Mertler and Reinhart [29] posited the need to leverage screening methods that ensure the quality of data collected in terms of accuracy, completeness, and absence of outliers, as these can have adverse effects on the results and conclusions made from the analysis. Levy [25] discussed the four main reasons for ensuring pre-analysis screening is conducted on the data collected before final analysis. The first reason is data accuracy, it is imperative to ensure that the data collected is accurate to provide accurate analysis. The second reason is to mitigate the issue of response-set, whereby respondents to an instrument submit the same score for the full set of questions, as this poses a threat to the validity of the measures [24],[25]. The third reason is to validate data is not missing by ensuring the data collection methods have been designed to prevent such an occurrence. Missing data can affect not only the conclusions drawn but the validity of the dataset [24], [29]. Lastly, pre-analysis screening should address outliers, which can have an adverse effect on the results and conclusions made from the analysis.

IV. Conclusions and Discussions

This work-in-progress study will develop the Remote Worker Cyberslacking Security Risk Taxonomy to assess an organization's remote workers' risk level of cybersecurity threats when engaging in cyberslacking activities. In phase one, SMEs from the cybersecurity field will be recruited to identify and validate measures for the computer security posture score. The Delphi method will be utilized to validate the key indicators for employee cyberslacking and cybersecurity posture. Phase two will involve collaboration with the identified SMEs to define, develop, and test the novel Remote Worker Cyberslacking-Security Risk Taxonomy. Data will be collected from a pilot group of participants to verify the validity of the defined measures for device cybersecurity posture and their derived composite values. This study will utilize a t-test to check for differences based on demographic information collected and the dependent variables of cyberslacking activity score and computer security posture index. Phase three of this work-in-progress study will consist of main data collection and analysis using the defined measures for cyberslacking and

device cybersecurity posture, along with their derived composite values and demographic information. Similarly, to the process utilized with the pilot, Tukey's post hoc test will be used to check for differences based on demographic information collected and the dependent variables of cyberslacking activity score and computer security posture index. Future research will include using the taxonomy on different diverse set of organizations to see if employees from a given industry present a higher risk compared to another industry. Using the taxonomy as a benchmarking may further assist organizations mitigate the threat vector associated with remote workers.

REFERENCES

[1] Adel A., Sarwar D., & Hosseinian-Far, A. (2021). Transformation of cybersecurity posture in IT telecommunication: A case study of a telecom operator. In: Jahankhani H., Jamal A., Lawson S. (Eds.) Cybersecurity, Privacy and Freedom Protection in the Connected World. Advanced Sciences and Technologies for Security Applications (pp. 441-457). Springer. https://doi.org/10.1007/978-3-030-68534-8_28

[2] Abilash, K. M. & Siju, N. M. (2021). Telecommuting: An empirical study on job performance, job satisfaction and employees commitment during pandemic circumstances. International Journal of Management, 8(3), 1-10.

[3] Aghaz, A., & Sheikh, A. (2016). Cyberloafing and job burnout: An investigation in the knowledge intensive sector. Computers in Human Behavior, 62, 51-60.

[4] Alharthi, S., Levy, Y., Wang, L., & Hur, I. (2019). Employees' mobile cyberslacking and their commitment to the organization. Journal of Computer Information Systems, 1–13. https://doi.org/10.1080/08874417.2019.1571455

[5] Aljohani, H. (2021). Cyber security threats during the pandemic. Journal of Contemporary Scientific Research, 5(1), 1-14.

[6] Atkins, R. B., Tolson, H., & Cole, B. R. (2005). Stability of response characteristics of a Delphi panel: application of bootstrap data expansion. BMC Medical Research Methodology 5(37), 1-12.

[7] Bloom, N., Lian, J., Roberts, J. & Ying, Z. J. (2015). Does working from home work? Evidence from a Chinese experiment. The Quarterly Journal of Economics, 130(1), 165-218. https://doi.org/10.1093/qje/qju032

[8] Burney, L. L., & Widener, S. K. (2013). Behavioral work outcomes of a strategic performance measurement system-based incentive plan. Behavioral Research in Accounting, 25(2), 115-143.

[9] Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36-45.

[10] Cao, H., Lee, C., Iqbal, S., Czerwinski, M., Wong, P. N. Y., Rintel, S., Hecht, B., Teevan, J., & Yang, L. (2021). Large scale analysis of multitasking behavior during remote meetings. Proceedings of the 2021

[11] Clayton, M. J. (1997). Delphi: a technique to harness expert opinion for critical decision-making tasks in education. Educational Psychology, 17(4), 373-386. https://doi.org/10.1080/0144341970170401

[12] Coventry L., Briggs P., Jeske D., van Moorsel A. (2014) SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In Marcus A. (Eds.) Design, User Experience, and Usability. Lecture Notes in Computer Science, Vol. 8517. Theories, Methods, and Tools for Designing the User Experience. Springer. https://doi.org/10.1007/978-3-319-07668-3_23

[13] Das, S. R., Seif, M.H., Ali, I. M., & Vafaei-Zadeh, A. (2020). Factors influencing the cyberslacking behavior and internet abusive intention in academic settings: A structural equation modeling approach. International Journal of Psychosocial Rehabilitation, 24(5), 7311-7318.

[14] Eldridge, L. P. & Pabilonia, S. W. (2010). Bringing work home: Implications for BLS productivity measures. *Monthly Labor Review, 133*(12), 19–36.

[15] Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. Issues in Informing Science and Information Technology, 6, 323-337.

[16] Ferreira, A., & Du Plessis, T. (2009). Effect of online social networking on employee productivity. South African Journal of Information Management, 11(1), 1-11.

[17] Ferreira, D., Goncalves, J., Kostakos, V., Barkhuus, L., & Dey, A. K. (2014). Contextual experience sampling of mobile application micro usage. Proceedings of the 16th international conference on human-computer interaction with mobile devices & services, Toronto, Canada, 91-100. https://doi.org/10.1145/2628363.2628367

[18] Fransilla, H., Okkonen, J., & Savolainen, R. (2014). Email intensity, productivity and control in the knowledge worker's performance on the desktop. Proceedings of the 18th International Academic MindTrek Conference: Media Business, Management, & Content Services. Tampere, Finland, 19-22. https://doi.org/10.1145/2676467.2676513

[19] Gibbs, M., Mengel, F., & Siemroth, C. (2021). *Work from home & productivity: Evidence from personnel & analytics data on IT professionals* (Working Paper 2021–56). University of Chicago, Becker Friedman Institute for Economics. https://bfi.uchicago.edu/working-paper/2021-56/

[20] Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organisational information security? Cyberpsychology, Behavior, and Social Networking, 20(9), 567–571.

[21] Hanaysha, J. (2016). Improving employee productivity through work engagement: Empirical evidence from higher education sector. Management Science Letters, 6(1), 61-70.

[22] Hartijasti, Y., & Fathonah, N. (2014). Cyberloafing Across generation X and Y in Indonesia. Journal of Information Technology Applications & Management, 21, 1-16.

[23] Hernandez, W., Levy, Y., & Ramim, M. M. (2016). An empirical assessment of employee cyberslacking in the public sector: The social engineering threat. Online Journal of Applied Knowledge Management, 4(2), 93-109.

[24] Kerlinger, F.N., & Lee, H.B. (2000). Foundations of behavioral research (Fourth edition.). Wadsworth Thomson Learning.

[25] Levy, Y. (2006). Assessing the value of e-learning systems. Hershey, PA: Information Science Publishing.

[26] Levy, Y., & Ellis, T. J. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of Information, Knowledge & Management, 6*, 151–161.

[27] Lim, V. K. G. (2002). The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. Journal of Organizational Behavior, 23, 675–694. https://doi.org/10.1002/job.161

[28] Markos, S. & Sridevi, M.S. (2010) Employee engagement: The key to improving performance. International Journal of Business and Management, 5, 89-96.

[29] Mertler, C. A., & Reinhart, R. V. (2017). Advanced and multivariate statistical methods: Practical application and interpretation (Sixth edition.). Routledge.

[30] Mohammad, J., Quoquab, F., Halimah S. & Thurasamy, R. (2019). Workplace internet leisure and employees' productivity. The mediating role of employee satisfaction. Internet Research. 29(4), 725-748.

[31] National Institute of Standards and Technology. (2020). Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

[32] Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. Information & Management, 42(1), 15-29.

[33] O'Neill, T. A., Hambley, L. A., & Bercovich, A. (2014). Prediction of cyberslacking when employees are working away from the office. Computers in Human Behavior, 34, 291–298. https://doi.org/10.1016/j.chb.2014.02.015

[34] O'Neill, T. A., Hambley, L. A., & Chatellier, G. S. (2014). Cyberslacking, engagement and personality in distributed work environments.

Computers in Human Behavior, 40, 152–160. https://doi.org/10.1016/j.chb.2014.08.005

[35] Russo, D., Hanel, P. H. P., Altnickel, S., & van Berkel, N. (2020). Predictors of well-being and productivity among software professionals during the COVID-19 pandemic – A longitudinal study. http://arxiv.org/abs/2007.12580

[36] Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill-building approach (Seventh edition.). John Wiley & Sons Ltd.

[37] Sheikh, A., Atashgah, M. S., & Adibzadegan M. (2015). The antecedents of cyberloafing: A case study in an Iranian copper industry. Computer in Humber Behavior, 51, 172-179

[38] Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. Communications of the Association for Information Systems, 37(1), 31-63.

[39] Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. Journal of Information Technology Education, 6, 1-21.

[40] Smith, S. J. (1986). The growing diversity of work schedules. Monthly Labor Review, 109(11), 7-13.

[41] Stich, J. F. (2020) A review of workplace stress in the virtual office. Intelligent Buildings International ,12(3), 1-13.

[42] Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic cyber hygiene: Does it work? *Computer*, *52*(4), 21–31.

[43] Syed, S., Singh, H., Thangaraju, S. K., & Bakri, N. E. (2020) The impact of cyberloafing on employees' job performance: A review of literature. Journal of Advances in Management Sciences & Information Systems, 6, 16-28.

[44] Ugrin, J. C., Pearson, J. M., & Odom, M. D. (2007). Profiling cyber-slackers in the workplace: Demographic, cultural, and workplace factors. Journal of Internet Commerce, 6, 75–89.

[45] U.S. Bureau of Labor Statistics. (2021). *Workforce statistics for information:NAICS 51*. https://www.bls.gov/iag/tgs/iag51.htm#workforce

[46] van Teijlingen E., & Hundley V. (2002). The importance of pilot studies. Nursing Standard, 16(40), 33-36.

[47] Venkatraman, S., Cheung C. M. K., Lee, Z.W.Y., Davis, F. D., & Venkatesh, V. (2018). The "Darth" side of technology use: An inductively derived typology of cyberdeviance. Journal of Management Information System 35(4), 1060-1091.

[48] Vernon-Bido, D., Grigoryan, G., Kavak, H., & Padilla, J. (2018). Assessing the impact of cyberloafing on cyber risk. Simulation Series, 50(2), 116–124. https://doi.org/10.22360/springsim.2018.anss.020

[49] Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 1-11. https://doi.org/10.1016/j.dss.2019.113160

[50] Vogl, B., & Abdel-Wahab, M. (2015). Measuring the construction industry's productivity performance: Critique of international productivity comparisons at industry level. Journal of Construction Engineering and Management, 141(4), 1-10.

[51] Webber, J. K., Ser, E., & Goussak, G. W. (2015). Work habits as positive and negative influence on workplace productivity. *Global Journal of Business Research*, *9*(1), 39–48.

[52] Yang, L., Holtz, D., Jaffe, S., Suri, S., Sinha, S., Weston, J., Joyce, C., Shah, N., Sherman, K., Hecht, B., & Teevan, J. (2021). The effects of remote work on collaboration among information workers. Nature Human Behaviour. https://doi.org/10.1038/s41562-021-01196-