

2024

# Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture to Assess Organizational Cybersecurity Risks

Ariel Luna

Follow this and additional works at: [https://nsuworks.nova.edu/gscis\\_etd](https://nsuworks.nova.edu/gscis_etd)



Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

Empirical Assessment of Remote Workers' Cyberslacking and Computer Security  
Posture to Assess Organizational Cybersecurity Risks

By

Ariel Luna

A dissertation submitted in partial fulfillment of the requirements  
for the degree of Doctor of Philosophy  
in  
Information Systems


College of Computing and Engineering  
Nova Southeastern University

2024


We hereby certify that this dissertation, submitted by Ariel Luna conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

  
\_\_\_\_\_  
Yair Levy, Ph.D.  
Chairperson of Dissertation Committee

4/26/24  
Date

  
\_\_\_\_\_  
Gregory E. Simco, Ph.D.  
Dissertation Committee Member

4/26/24  
Date

  
\_\_\_\_\_  
Wei Li, Ph.D.  
Dissertation Committee Member

4/26/24  
Date

Approved:

  
\_\_\_\_\_  
Meline Kevorkian, Ed.D.  
Dean, College of Computing and Engineering

4/26/24  
Date

College of Computing and Engineering  
Nova Southeastern University

2024

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment  
of the Requirements for the Degree of Doctor of Philosophy

## Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture to Assess Organizational Cybersecurity Risks

By  
Ariel Luna  
April 2024

Cyberslacking is conducted by employees who are using their organizations' 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. Since the COVID-19 pandemic, the increase in remote working has heightened the cybersecurity risk to organizational networks and infrastructure. Research has shown that cyberattacks on organizations continue to increase, specifically increases in cyberattacks directed at remote employees.

This work achieved the targeted goal of developing, validating and empirically testing a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. The taxonomy used productivity measures to determine their inclination to participate in cyberslacking and the computer security posture of the remote device being used to access organizational resource as inputs for conducting the assessment. Limited attention has been given cyberslacking by remote workers and the cybersecurity risks they pose to an organization. The study engaged cybersecurity and Information Technology (IT) Subject Matter Experts (SMEs) to participate in one round of the Delphi method in order to reach a consensus on the measures for Cyberslacking (CySI) and Computer Security Posture (CSP).

This study used a three-phased approach to develop a taxonomy to assess remote workers' risk level of cybersecurity threats. In phase one, 53 SMEs validated four indicators to measure CySI and 10 indicators to measure CSP derived from the literature. In addition, the SMEs were also asked to validate the Remote Worker Cyberslacking Security Risk Taxonomy developed. In phase two, a pilot was conducted with 15 participants to validate the instrument, measures, and data analytics process used for the main data collection. In Phase three, demographic data, CySI measures and CSP measures were collected and analyzed from 138 participants. Subsequently, in phase three, the Remote Worker Cyberslacking Security Risk Taxonomy was used to classify the level of risk remote workers could pose to the organization.

The findings demonstrated that while most participants were classified as "Low Risk," specific demographic groups could pose a risk to the organization due to their composite CySI and CSP scores. For example, males had higher CySI and lower higher CSP scores than females, indicating males could pose a cybersecurity risk to the organization. Conversely, technical staff had lower CySI and higher CSP scores than administrative and support staff, suggesting they are less likely to pose a risk to the organization.

This study has significant implications for both professional practice and research. From a practical standpoint, organizations can utilize the validated measures provided by SMEs to assess the potential risks posed by their remote workforce. The Remote Worker Cyberslacking Security Risk Taxonomy developed by this study can be used as a benchmarking tool based on SMEs' defined metrics from application usage and cybersecurity posture indicators to provide composite scores that would allow for a comparison. The results of this analysis can be leveraged by organizations to mitigate potential deficiencies in computer cybersecurity posture on remote worker devices, cybersecurity awareness training, and policy changes. In addition, the findings of this study contribute to the existing body of work in Information Systems (IS), cybersecurity, productivity, and remote work.

## Acknowledgements

First and foremost, I want to thank God for the strength, wisdom, and serenity that accompanied me throughout this research journey.

To my late uncle, Clarence, although you are no longer with us, your memory lives on as a guiding force. Your wisdom, encouragement, and unwavering belief in my abilities continue to inspire me. This dissertation is dedicated to you.

I want to thank Dr. Yair Levy, my Dissertation Chair, your expertise, constructive feedback, and mentorship were invaluable. You challenged me to think critically and pushed me to excel. Thank you for being a guiding light throughout this process.

Thank you to my Dissertation Committee Member Dr. Wei Li, and Dr. Gregory Simco - your insights and rigorous examination improved the quality of this work. Your commitment to academic excellence inspired me.

A special thank you to Marilyn, my wife, your unwavering support, encouragement, and patience sustained me during the late nights and countless revisions. Your belief in my abilities kept me going even when I doubted myself.

To my boys, AJ, Alex and Yadier, thank you for understanding when I had to bury myself in research and writing. Thank you for letting me bounce my ideas off you and going through my countless revisions.

I want to thank my parents, Carmen and Antonio, your sacrifices, guidance, and love have shaped me into the person I am today. Your unwavering faith in my dreams fueled my determination.

Thank you, Peter Chiasera and Troy Hahn, for your unwavering support through this process, the countless conversations about data collection methods and analysis helped me immensely through this process and I will be forever grateful.

To my dear friend Erik Malak, thank you for listening to my academic woes, celebrating small victories, and reminding me that life exists beyond research papers.

I extend heartfelt gratitude to my academic support team and dear friends, Dr. Michael Rooney and Dr. Patricia Baker. Together, we've embarked on this remarkable journey, offering unwavering encouragement, valuable insights, and countless moments of support

Lastly, I want to thank everyone who has played a role, whether directly or indirectly, in my academic journey. Your support, no matter how big or small, has been instrumental in completing this dissertation. This dissertation would not have been possible without the collective support of these remarkable individuals. Their belief in me fueled my determination, and for that, I am forever grateful.

## Table of Contents

**Abstract iii**

**List of Tables ix**

**List of Figures xi**

### Chapters

#### **1. Introduction 1**

Background 1

Problem Statement 2

Dissertation Goals 4

Research Questions 8

Relevance and Significance 9

Relevance 9

Significance 10

Barriers and Issues 10

Assumptions, Limitations, and Delimitations 11

Assumptions 11

Limitations 11

Delimitations 12

Definition of Terms 12

Summary 13

#### **2. Review of the Literature 15**

Introduction 15

Remote Workers 15

Remote Workers Productivity 16

Remote Workers and Cyberslacking 17

Productivity 20

Employee Productivity 21

Cyberslacking and Productivity Impact 21

Cyberslacking and Cybersecurity Posture 25

Computer Cybersecurity Posture 25

Cybersecurity Risk and Cyberslacking 26

Cybersecurity Risk Management 29

Cyber Risk Management of Remote Workers 30

Cyber Risk Management of Cyberslacking 31

Demographics 33

Theoretical Background: Routine Activity Theory 37

Summary of What Is Known and Unknown 43

#### **3. Methodology 45**

Overview of Research Design 45  
Measures 48  
    Productivity 48  
    Employee Productivity and Cyberslacking 48  
    Computer Cybersecurity Posture 50  
    Demographics 52  
Validity and Reliability 54  
    Validity 55  
    Reliability 55  
Proposed Sample 56  
Pre-analysis Data Screening 57  
Data Collection & Data Analysis 57  
    Phase One – Delphi Methodology (RQ1 & RQ2) 57  
    Phase Two – Pilot Study 59  
    Phase Three – Main Data Collection and Analysis (R3, RQ4, RQ5, & RQ6) 61  
Resources 63  
Summary 63

#### **4. Results 65**

Overview 65  
Phase One – Subject Matter Experts (SMEs) 65  
    Data Collection 66  
    Data Analysis 68  
Phase Two – Pilot Study 75  
    Data Collection 75  
    Data Analysis 75  
Phase Three – Main Data Collection 76  
    Data Collection 76  
    Data Analysis 76  
Summary 94

#### **5. Conclusions, Discussions, Implications, Recommendations, and Summary 96**

Conclusions 96  
Discussions 97  
Implications 99  
Recommendations 100  
Summary 101

#### **Appendices**

A. Institutional Review Board Approval Letter 104  
B. Queen’s College SRRC Board Approval 106  
C. Subject Matter Expert Recruitment Letter 107  
D. Information Users Recruitment Letter 108  
E. Participant Consent Email 109



**F. Subject Matter Expert Survey 110**

**G. Participant Survey 115**

**References 117**

## List of Tables

### Tables

1. Remote Worker Platform 5
2. Summary of Remote Workers 18
3. *Summary of Remote Workers (continued)* 19
4. Summary of Productivity and Cyberslacking 22
5. Summary of Productivity and Cyberslacking (continued) 23
6. Summary of Productivity and Cyberslacking (continued) 24
7. Summary of Cyberslacking and Cybersecurity Posture 28
8. Summary of Cyberslacking and Cybersecurity Posture 29
9. Summary of Cyber Risk Management 32
10. Summary of Cyber Risk Management (continued) 33
11. Summary of Demographics 35
12. Summary of Demographics (continued) 36
13. Summary of Demographics (continued) 37
14. Summary of Routine Activity Theory 42
15. Summary of Routine Activity Theory (continued) 43
16. Indicators to measure employee productivity (All Measured in Hours Per Day) 50
17. Indicators to Measure Computer Security Posture. 52
18. Demographic indicators 53
19. Descriptive Statistics of the SMEs (N=53) 67
20. Descriptive Statistics of the SMEs (N=53) (continued) 68
21. Productivity measures percentage of agreement (N=53) 69
22. Computer Security Posture (CSP) measures percentage of agreement (N=53) 70

23. SMEs validated indicators to measure employee productivity (All Measured in Hours Per Day) 74
24. SME validated indicators to measure computer security posture 75
25. Descriptive statistics of the participants (N=138) 77
26. Descriptive statistics of the participants (N=138) (continued) 78
27. Construct Statistics (N=138) 79
28. Remote Worker Cyberslacking Security Risk – Quadrant distribution (N=138) 80
29. ANOVA results for CySI (N=138) 81
30. ANOVA results for CSP (N=138) 81

## List of Figures

### Figures

1. Proposed Remote Worker Cyberslacking Security Risk Taxonomy 8
2. Routine Activity Theory – Adapted from Cohen & Felson (1979) 38
3. Adapted from Routine Activity Theory Cohen & Felson (1979) 41
4. Proposed Research Design Process 46
5. SME Frequency for Productivity (CySI) Measures (N=53) 71
6. SME Frequency for Cybersecurity Posture Score (CSP) Measures (N=53) 72
7. Percentage of Consensus for Cyberslacking and Cybersecurity Measures ranked by percentage level of agreement. 73
8. Remote Worker Cyberslacking Security Risk Scatter Plot of CySI and CSP Scores 80
9. Remote Worker Cyberslacking Security Risk Scatter by Gender (N=138) 83
10. Means and Standard Deviation of Aggregated Construct Scores Based on Age (N=138) 83
11. Remote Worker Cyberslacking Security Risk Scatter by Gender (N=138) 85
12. Means and Standard Deviation of Aggregated Construct Scores Based on Age (N=138) 85
13. Remote Worker Cyberslacking Security Risk Scatter by Education (N=138) 87
14. Means and Standard Deviation of Aggregated Construct Scores Based on Education (N=138) 87
15. Remote Worker Cyberslacking Security Risk Scatter by Job Role (N=138) 89
16. Means and Standard Deviation of Aggregated Construct Scores Based on Job Role (N=138) 89
17. Remote Worker Cyberslacking Security Risk Scatter by Job Level (N=138) 91

18. Means and Standard Deviation of the Aggregated Construct Scores Based on Job Level

(N=138) 91

19. Remote Worker Cyberslacking Security Risk Scatter by Experience (N=138) 93

20. Means and Standard Deviation of Aggregated Construct Scores Based on Experience

(N=138) 93

## Chapter 1

### Introduction

#### **Background**

Cyberslacking or cyberloafing can be defined as an employee's use of an organization's Information Technology (IT) resources for activities, such as surfing the web or checking personal email, which do not contribute to the completion of their job function (Lim, 2002).

Cyberslacking is usually associated with employee productivity losses or degradation of network services and not with the increased security risks related to cyberslacking or cyber deviant behaviors (Haddington & Parsons, 2017). However, Vernon-Bido et al. (2018) found that cyberslacking can be categorized as an expense due to the loss of productivity as well as a security risk.

Due to the COVID-19 world pandemic, organizations have increased and accelerated their adoption of remote work (Russo et al., 2020). Working remotely has been studied extensively in terms of employee satisfaction, commitment, and productivity (Abilash & Siju, 2021; Bloom et al., 2015; Ferreira et al., 2014). Additionally, O'Neill et al. (2014) 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 (2020) determined employees working remotely may be more susceptible to engage in activities that could be deemed cyberslacking or cyber deviance. These activities included using the internet for personal purposes such as checking email, gambling, and browsing the web. This study addressed the gap in the literature regarding cyberslacking by remote workers and the cybersecurity risks they pose to an organization.

The increased adoption of working remotely provided an opportunity to investigate the impact remote workers, specifically employees who engage in cyberslacking, can have on an organization's cybersecurity (Russo et al., 2020). According to Batabyal and Bhal (2020), cyberslacking can have serious consequences for organizations in terms of finance and security. When employees engage in cyberslacking, they may expose the organization's systems to malicious software or spyware that can compromise security (Vernon-Bido et al., 2018; Ozler & Polat, 2012). In addition, Strupczewski (2021) identified cyberslacking as a contributor to the cyber risk of an organization. Vishwanath et al. (2020) highlighted that the absence of proper cyber hygiene practices and proper cybersecurity posture of the device being used to engage in internet activities can contribute to the cyber breach of an organization. Similarly, Kalhor et al. (2021) found that organizations lacking proper cyber security posture controls can be deemed susceptible to cyber-attacks. Although both cyberslacking and cyber security posture can have an impact on cyber risk, these constructs appear to be independent of each other.

The goal that was achieved was to develop, validate, and empirically test a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This study measured workers' potential engagement in cyberslacking, and the computer security posture of the remote devices used to access the organization's resources. These measures were utilized to determine if an organization's remote workers posed an increased cybersecurity risk. This study expanded the research conducted by Jeong et al. (2020) and Bhomer et al. (2011) on the use of log analysis for application usage, as well as the research conducted by Ferreira et al. (2014) on work schedule, hours, usage reason, and log data.

### **Problem Statement**

The research problem this study addressed was remote workers engaged in cyberslacking and the potential cybersecurity risks to which they expose their organizations, such as malware,

spyware infection, or security breaches (Ozler & Polat, 2012; Vernon-Bido et al., 2018). Employees working remotely may be more inclined to take part in activities that could be categorized as cyberslacking or cyber deviance (O'Neill et al., 2014). Cyberslacking, also noted in the literature as cyberloafing is defined as “the act of employees using their companies’ Internet access for personal purposes during work hours” (Lim, 2012, p. 675). This term can be further refined into two categories: minor and major, whereby minor cyberslacking can be described as personal email use or surfing the web on reputable sites and major cyberslacking includes online gambling or visiting adult content websites (Hadington & Parsons, 2017; Ozler & Polat, 2012). Blanchard and Henle (2008) suggested that cyberslacking can be examined within the confines of disruptive and recreational cyberslacking. Disruptive cyberslacking encompasses activities such as visiting adult websites or online gaming, which increases the risk of malware and/or ransomware (Blanchard & Henle, 2008). Recreational cyberslacking includes activities such as checking email or online shopping during work hours on devices that connect to their organization’s networks.

Cyberslacking can have an adverse effect on the productivity of an organization as well as pose a cybersecurity risk by exposing the organizations’ systems to potential malware or spyware infection (Ozler & Polat, 2012; Vernon-Bido et al., 2018). Zakrzewski (2016) estimated that employees spend approximately two hours per day cyberslacking, costing organizations \$85 billion per year; however, what is less known is the risk that such activities pose to the organization from the cybersecurity perspective. In addition to the cost and potential malware exposure, organizations can be exposed to infrastructure constraints such as the degradation of network services and network security threats (Hadington & Parsons, 2017; Vitak et al., 2011).



Several studies utilized the Theory of Planned Behavior (TPB) to determine if an employee's attitude and/or internet addiction affected their propensity to engage in cyberslacking activities. For example, Galletta and Polak (2003), Jamaluddin et al. (2015), and Askew et al. (2014) used TPB to understand the intent of employees participating in cyberslacking and identify antecedents of these behaviors. Hadlington and Parsons (2017) posited that these studies were limited as they employed self-reported survey instruments, which could have had an adverse effect on the results.

O'Neill et al. (2014) highlighted that many of the studies on cyberslacking concentrated on behaviors in the physical workplace rather than those in a remote work setting. However, cyberslacking is likely more frequent when working remotely, as there are no colleagues or managers to detract from this behavior. With the COVID-19 world pandemic, the number of employees working remotely increased dramatically. This change provides an opportunity to investigate the impact remote workers can have on an organization's cybersecurity posture, specifically with employees who engage in cyberslacking (Russo et al., 2020). Thus, further empirical research into the cybersecurity risk posed to an organization by remote workers engaging in cyberslacking is vital, as cybersecurity breaches cost six trillion dollars in 2021 and surged fivefold after COVID-19 (Aljohani, 2021).

### **Dissertation Goals**

The goal that was achieved was to develop, validate, and empirically test a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This study measured a worker's potential participation in cyberslacking, and the computer security posture of the company-provided remote device used to access the organization's resources. The baseline characteristics of the company-provided devices are depicted in Table 1. Venktraman et al. (2019) described that despite an increase in cyberslacking and cyber deviance research, an

overall understanding of the issue by both practitioners and researchers is still limited. 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 (Vernon-Bido et al., 2018). In addition, Russo et al. (2020) highlighted that the increase in the adoption of working remotely facilitates the opportunity to research the impact remote workers can have on an organization's cybersecurity, specifically with employees who engage in cyberslacking.

**Table 1**

*Remote Worker Platform*

<b>Remote Worker System Attribute</b>	<b>Source/Adapted</b>
Company-Provided Device	Ratchford et al. (2022)
Virtual Private Network (VPN)	Such et al. (2019)
Internet Service Provider Cybersecurity Posture	CableLabs Security (2021)
Activity Log Monitoring	Vishwanath et al. (2019)

This study built on previous research by Alharthi et al. (2019), O'Neill et al. (2014), Weatherbee (2010), as well as Ramirez and Nembhard (2004) as the basis for developing a taxonomy to understand the cybersecurity risk implications of cyberslacking of remote workers. O'Neill et al. (2014) recommended measuring the tendency of cyberslacking from remote workers due to the increased feasibility and significant increase of remote work. This study used Ramirez and Nembhard's (2004) taxonomy for measuring the productivity of knowledge workers to create a new taxonomy for assessing cybersecurity risks by remote workers. This new taxonomy utilized employee productivity as an indicator of cyberslacking. Leveraging the methodology used by Eilts (2020) for developing assigned weights to measures, the specified elements of employee productivity will be weighed to derive a composite value for

cyberslacking. Another major component of the framework utilized the Mobile Cyberslacking Commitment Taxonomy (MCCT) developed by Alharthi et al. (2019) as the basis for a four-quadrant model to classify cyberslacking by its frequency and potential cyber risk.

Expanding on the studies conducted by Alharthi et al. (2019) on the MCCT and Ramirez and Nembhard (2004) on the knowledge worker productivity taxonomy, this research study had six specific goals. The first goal was to engage Subject Matter Experts (SMEs) to develop the specified elements of measure for cyberslacking, using employee productivity as defined by Ferreira and Du Plessis (2009), and to derive a composite value for determining potential security risk based on cyberslacking activity. The second goal was to identify and validate measures for the computer security posture score by collaborating with SMEs. The third goal was to consult with SMEs to develop and validate a taxonomy to determine if an organization's remote workers introduce additional cybersecurity threats. Figure 1 illustrates the taxonomy developed in the form of a 2x2 matrix to assess an organization's security risk based on an employee's cyberslacking activity and the security posture of the company-issued device being used to access the organization's resources.

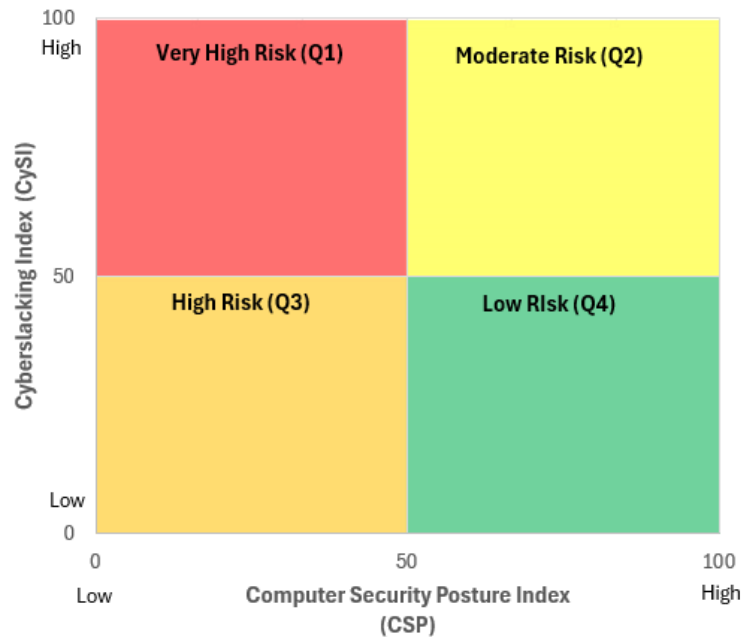
The taxonomy developed for Remote Worker Cyberslacking Security Risk consists of four quadrants: Q1, Q2, Q3, and Q4. The quadrants indicate the amount of cybersecurity risk the remote workers may pose for the organization based on their cyberslacking score and computer security posture. Quadrant one (Q1), labeled "Very High Risk," consists of a high Cyberslacking Score (CySI) and a low Cybersecurity Posture Score (CPS). Remote workers positioned in Q1 are more likely to engage in cyberslacking activity and have a low cybersecurity posture score. Quadrant two (Q2), labeled "Moderate Risk," consists of a high Cyberslacking Score (CySI) and a high Cybersecurity Posture Score (CPS). Remote workers positioned in Q2 are more likely to

engage in cyberslacking activity and have a high cybersecurity posture score. Quadrant three (Q3), labeled “High Risk,” consists of a low Cyberslacking Score (CySI) and a low Cybersecurity Posture Score (CPS). Remote workers positioned in Q3 are less likely to engage in cyberslacking activity and have a low cybersecurity posture score. Quadrant four (Q4), labeled “Low Risk,” consists of a low Cyberslacking Score (CySI) and a high Cybersecurity Posture Score (CPS). Remote workers who are positioned in Q4 are less likely to engage in cyberslacking activity and have a high cybersecurity posture score.

The fourth goal of the research study was to identify if there are statistically significant mean differences in the employees’ cyberslacking activity values based on the demographic characteristics of age, gender, education level, and years of work experience. The fifth goal of the research study was to identify if there are statistically significant mean differences in the employees’ computer security posture scores based on the demographic characteristics of age, gender, education level, and years of work experience. The sixth goal of this research study was to identify if there are differences in the employees’ positions on the Remote Worker Cyberslacking Security Risk Taxonomy based on the demographic characteristics of age, gender, education level, and years of work experience.

**Figure 1**

*Proposed Remote Worker Cyberslacking Security Risk Taxonomy*



### Research Questions

The main research questions this study addressed 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 organizational resources? The research study had six research questions:

- 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 the organizational 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?

## **Relevance and Significance**

### *Relevance*

This research study is relevant due to the increasing number of employees working remotely and the potential increase in cybersecurity risks. Before the start of the COVID-19 pandemic it was estimated that approximately 5% of Americans worked at home more than 50% of their workweek, as of April 2020 it is estimated that 37% of Americans worked from home (Barreo et al., 2020; Brynjolfsson et al., 2020). This upward trend in remote work provides an opportunity to gain insight by conducting empirical research to determine if cyberslacking by remote workers poses a higher cybersecurity risk to the organization. In addition to the increase in cyber risk, the cost of cyberslacking is also a factor that organizations are faced with. Cyberslacking has been estimated to be in the range of \$85 billion to \$183 billion per year, including lack of productivity, legal expenses, and infrastructure constraints (Saleh et al., 2018; Vitak et al., 2011; Zakrzewski, 2016).

Researchers have reported contradictory findings pertaining to demographics as antecedents to cyberslacking (Althari et al., 2019; Hartijasi & Fathonah, 2014; Sheikh et al., 2015). Hartijasi and Fathonah (2014), as well as Sheikh et al. (2015) stated age, gender, education, and work experience were factors that contributed to cyberslacking activities. Conversely, Hernandez et al. (2016) found that age, gender, level at organization, and education did not show a significant difference in cyberslacking activities. Thus, providing the opportunity

to develop and test a taxonomy to help determine the organization's cybersecurity risk from remote workers engaged in cyberslacking.

### *Significance*

The resultant findings and artifacts of this study could contribute to the body of knowledge in the areas of cybersecurity and cyberslacking. Several studies on cyberslacking and its potential cybersecurity impact on organizations have leveraged the use of self-reporting instruments and the use of theories such as TPB but have not accounted for the remote workers (Galletta & Polak, 2003; Jamaluddin et al., 2015; Hadlington & Parsons, 2017). Thus, this study provided a taxonomy as a benchmarking tool based on the SMEs' defined metrics from application usage and cybersecurity posture indicators to provide composite scores that would allow for a comparison. The results of this analysis can be leveraged by organizations to mitigate potential deficiencies in computer cybersecurity posture on remote worker devices, cybersecurity awareness training, and policy changes. Additionally, researchers will be able to leverage this study for future research.

### **Barriers and Issues**

Several barriers and issues that surfaced during this study needed to be mitigated. The first potential barrier of this study was the recruitment and accreditation of the subject matter experts who participated in the first phase of this proposed study. To address this potential barrier the selection process of the SMEs considered the definition of an expert provided by Clayton (1997) which stipulates that knowledge and experience are requirements for participation in the Delphi method. Therefore, the members of the panel were limited to cybersecurity professionals with the required educational background, knowledge, experience, and professional certifications. Another barrier was the development of a method to connect data from two separate sources with disparate collection methodologies: demographic data and data

regarding the measurement of computer security posture and employee productivity. The last barrier that was addressed was obtaining Institutional Review Board (IRB) approval from both the college and the organization where the data collection took place. This was an essential barrier to overcome as a major component of the research study was collecting demographic data from human participants.

### **Assumptions, Limitations, and Delimitations**

#### *Assumptions*

This study assumed that the instrument used to gather feedback from the SMEs during the Delphi method would be clear and easily understood. Another assumption this study made was that the SMEs who participated in the Delphi method would provide honest feedback throughout the entire process. An additional assumption was the continuity of the SME participants during all iterations of the Delphi method. Lastly, this study assumed the instrument distributed to collect demographic data would be easily understood and answered honestly.

#### *Limitations*

This study developed a framework for assessing if remote workers pose an increased cybersecurity risk to an organization while engaging in cyberslacking, which Tandon et al. (2020) described as unethical behavior. Participation can be difficult if the participants feel there may be a negative consequence on their activities. Houston and Tran (2001) described the problem of encouraging participants to respond and be truthful in their responses to surveys. To overcome this limitation, the participants were assured that all data would be anonymized, kept confidential, and utilized exclusively for this study. Another limitation that was addressed was the difficulty in creating reports from the productivity suite and endpoint management systems to retrieve the key indicators required. To mitigate this limitation, an IT administrator will be engaged to create the required reports.



### *Delimitations*

A delimitation of this study was the recruitment of participants from one public higher education institution in the United States (U.S.); generalization to other business sectors or countries was not in the scope of this study. Another delimitation of this study was the utilization of measures limited to those validated by the SMEs during the Delphi method. In addition, this research precluded the use of mobile devices for the activities being measured.

### **Definition of Terms**

The following represents the terms and definitions used in this study.

**Cyber deviance** – “the intentional use of IT in the workplace that is contrary to the explicit and implicit norms of the organization, and that threatens the well-being of the organization and/or its members” (Venkatraman et al., 2018, p. 1061).

**Cyber hygiene** – “the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet enabled devices from being compromised in a cyber-attack” (Vishwanath et al., 2020, p. 2).

**Cyberloafing** – “employees’ voluntary non-work-related use of company provided email and Internet while working” (Hadlington & Parsons, 2017, p. 567).

**Cybersecurity risk** – “the risk of financial loss, disruption, or damage to the reputation of a firm as a result of a failure in its information technology systems due to external attacks” (Florackis et al., 2023, p. 351).

**Cybersecurity posture** – “The security status of your enterprise's software and hardware, networks, services, and information; your ability to manage your defenses; and your ability to react to and recover from security events are collectively referred to as your cybersecurity posture” (Abdel et al., 2021, p. 2).

**Cyberslacking** – “the act of employees using their companies’ Internet access for personal purposes during work hours” (Lim, 2002, p. 675).

**Delphi Method** – “a methodical and interactive research procedure for obtaining the opinion of a panel of independent experts concerning a specific subject” (Skinner et al. 2015, p. 32).

**Productivity** – “measure of the efficiency with which the economy turns inputs, such as labor and capital, into output” (Vogl & Abdel-Wahab, 2015, p. 2).

**Remote work** – employees performing “a portion of their work from areas outside the conventional office” (O’Neill et al., 2014, p. 153).

## **Summary**

Researchers have estimated that at least a third of U.S. employees work-from-home (Barreo et al., 2020; Brynjolfsson et al., 2020). Extensive studies focused on working remotely concentrated on employee satisfaction, commitment, and productivity (Abilash & Siju, 2021; Bloom et al., 2015; Ferreira et al., 2021). According to Russo et al. (2020), the increase in working remotely provided an opportunity to investigate the impact employees can have on an organization’s cybersecurity, specifically those who engage in cyberslacking. Though a similar increase in cyberslacking research has occurred, a limited understanding of the issue by researchers and practitioners remains (Venktraman et al., 2019). In addition, many of the studies conducted have focused on those working in a traditional office setting and not remote workers (O’Neill et al., 2014).

To address the gap in the literature regarding remote workers engaging in cyberslacking and the cybersecurity risk they introduce to an organization, this research study developed, validated, and empirically tested a taxonomy to assess an organization’s remote workers’ risk level of cybersecurity threats. The taxonomy has the potential to provide a benchmarking tool based on SMEs-defined metrics from application usage and cybersecurity posture indicators to

provide composite scores for assessing the level of cybersecurity risk posed by remote workers engaging in cyberslacking activities.

## Chapter 2

### Review of the Literature

#### **Introduction**

In this chapter, a literature review was conducted to establish a theoretical foundation for this proposed study. The review focused on relevant literature related to remote workers, productivity, cyberslacking, cybersecurity posture, cyber risk management, and demographic information of remote workers. The literature review provided support for a three-phased developmental study using productivity values to measure cyberslacking activity and device cybersecurity posture to assess the cybersecurity risk remote workers introduce to an organization.

#### **Remote Workers**

Nilles (1998) is credited with being a pioneer in developing the telecommuting concept in the 1970s. The concept was proposed as a method to decrease pollution by minimizing commuting to work and decreasing traffic congestion, as well as a method to provide employees with flexibility and work-life balance (Narayanan et al., 2017). Advancements in technology have afforded organizations of all sizes an opportunity for their employees to work from locations other than those within the confines of a traditional office (Blount, 2015).

Due to the COVID-19 world pandemic, organizations have increased and accelerated their adoption of remote work (Russo et al., 2020). In addition to the pandemic response, organizations have learned that there are competitive advantages, business continuity opportunities, and economic reasons for adopting work-from-home strategies (Ferreira et al., 2021). Prior to the COVID-19 pandemic, approximately 5% of Americans worked from home for more than 50% of their workweek (Barreo et al., 2020). By April 2020, approximately 37% of Americans worked from home (Brynjolfsson et al., 2020; Yang et al., 2020).

### *Remote Workers Productivity*

Telecommuting, also known as work-from-home, work-from-anywhere, and remote work, is not a recent phenomenon as it was introduced in the 1970s (Borkovich & Skovira, 2020; Nilles, 1998). Additionally, work-from-home has been studied quite extensively in terms of employee satisfaction, commitment, and productivity, however, very little is known from the cybersecurity perspective (Abilash & Siju, 2021; Bloom et al., 2015; Ferreira et al., 2021). For example, Ferreira et al. (2021) used a designed science research approach in which a systematic literature review was conducted, along with 129 structured interviews, to determine the driving factors of adopting the use of remote work. Ferreira et al. (2021) concluded that the adoption of remote work yielded positive results in the organization in terms of increased worker motivation and an increase in worker productivity. Similarly, bloom et al. (2015) found a 13% increase in performance from employees who worked from home, higher job satisfaction, and a 50% decrease in the attrition rate. Their study was conducted on a NASDAQ-listed firm using a sample size of 249 employees, half of whom worked from home while the remaining were observed in the confines of a traditional office. Abilash and Siju (2021) collected data utilizing a questionnaire distributed to a sample size of 220 participants from the education sector. Their results demonstrated a positive effect on job performance, job satisfaction, and working remotely. These findings are similar to prior studies conducted by Gajendran and Harrison (2007) as well as Harker Martin and MacDonnell (2012) in terms of the positive effects of remote work on job performance and satisfaction. Conversely, in the natural experiment conducted by Yang et al. (2020), anonymized individual data were collected and analyzed for 60,000 employees at a major technology firm. Their data included a summary of the amount of time spent using collaboration tools such as Microsoft Teams, Email, and video conferencing platforms both before and after a company-wide remote work mandate due to the COVID-19

pandemic. The analysis of their data utilized a modified difference-in-difference (DiD) model. The Standard DiD “is an econometric approach that enables researchers to infer the causal effect of a treatment by comparing longitudinal data from at least two groups” (Yang et al., 2020, p. 2). The results of their study indicated that a decrease in collaboration and communication patterns would negatively impact productivity, while it could also inhibit innovation in the long term.

### *Remote Workers and Cyberslacking*

The primary focus of many prior studies of cyberslacking has been within an office environment rather than a remote setting. Cyberslacking is defined as “the act of employees using their companies’ Internet access for personal purposes during work hours” (Lim, 2012, p. 675). 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 and not in the physical view of a supervisor (O’Neill, Hambley, & Bercovich, 2014; O’Neill, Hambley, & Chatellier, 2014). O’Neill, Hambley, and Chatellier (2014) distributed a survey to 148 U.S. working adults who worked remotely a minimum of one day per week. The survey intended 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 the direct implications of frequent cyberslacking by remote workers impacted their overall engagement in work activities (O’Neill, Hambley, & Chatellier, 2014). Although the findings of this study demonstrated the direct impact of cyberslacking on remote workers and their engagement in work activities, additional research should be conducted as it has been posited that the use of self-reported surveys tends to provide inaccurate information (Russo et al. 2020).

In the literature review and analysis conducted by Stich (2020) 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. (2020) 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 empirical research is warranted.

**Table 2**

*Summary of Remote Workers*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Abilash & Siju, 2021	Survey	220 employees	Job performance impact of working remotely.	Increase in performance, job satisfaction and commitment while working remotely.
Bloom et al., 2015	Empirical study via experiment	249 employees	Performance impact of working remotely.	Significant increase in performance working from home.

**Table 3***Summary of Remote Workers (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Ferreira et al., 2021	Literature review and analysis of field interviews	129 qualitative interviews of employees working remotely.	Remote work decisions factors.	Remote work promotes positive relationships with worker satisfaction.
Gajendran & Harrison, 2007	Literature review		Impact of remote work arrangements on job performance.	Remote work demonstrated beneficial effects on job satisfaction, performance, turnover intent, and role stress.
Harker Martin & MacDonnell, 2012	Literature review and analysis using meta-analytic method		Impact of remote work on retention, job performance and satisfaction.	Remote work positively affected job satisfaction and performance and contributed to overall retention.
O'Neill, Hambley, & Chatellier, 2014	Survey	148 employees	Effect of cyberslacking by remote workers.	The results of suggest that personality traits identified in their study could be used as a starting point to gauge the propensity of employees working from home to participate in cyberslacking



**Table 2**  
*Summary of Remote Workers (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Russo et al., 2020	Longitudinal study	192 participants	Effects on productivity from remote workers.	Remote workers are more frequently distracted and engaging in cyberslacking activities.
Yang et al., 2020	Empirical study via experiment	61,182 participants	Effects of remote work on collaboration	Remote work adoption directly affects remote worker's collaboration network.

### **Productivity**

Though research historically used productivity as the sole measure of financial success, recent studies are expanding the use of this term to reflect overall organizational success (Burney & Widener, 2013; Mohammad et al., 2019; Webber et al., 2015). Vogl and Abdel-Wahab (2015) defined productivity as the "measure of the efficiency with which the economy turns inputs, such as labor and capital, into output" (p. 2). The expanded use of productivity as a key indicator requires organizations to develop a method to ensure its accurate measurement. Further evidence of productivity as a key measure is demonstrated by Hanaysha (2016) on employee productivity. Hanaysha's (2016) provided empirical evidence that work engagement had a positive effect on an organization's overall success. Hanaysha (2016) recommended the implementation of a methodology that uses productivity as a key measure to evaluate the success of an organization.

### *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 (Hanaysha, 2016). In a research study conducted by Hanaysha (2016), a 5-point Likert scale instrument was distributed online to 870 administrative and academic staff at public universities in Malaysia. Hanaysha (2016) analyzed the data using structural equation modeling 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. His findings supported Markos and Sridevi (2010) findings that 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 (2009) suggested measuring employee productivity by using time spent executing required tasks to achieve the desired outcome according to job function. Similarly, Syed et al. (2020) utilized the amount of work completed within a respective period of time as the measurement for productivity. In addition, Gibbs et al. (2021) 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 proposed study.

### *Cyberslacking and Productivity Impact*

Das et al. (2020) found a decrease in overall work performance by employees who engaged in non-productive activities, such as cyberslacking, instead of tending to their assigned work activities. Their finding is in line with previous studies describing the effects of cyberslacking on employee productivity. In an early study, Henle et al. (2009) found that overall employee performance decreased by 30% to 40% due to cyberslacking activities. Similarly, Jia

et al. (2013) found that cyberslacking activities wasted valuable time and led to the loss of employee productivity. Jandaghi et al. (2015) also found a 40% decrease in productivity in their study due to engagement in cyberslacking activities. Conversely, studies conducted by Oravec (2002) and Anandarajan et al. (2006) determined that employees could benefit from a reasonable amount of online recreation during work hours as this could increase their job satisfaction directly impacting employee productivity. Similarly, Lim and Chen (2009) observed that small amounts of cyberslacking could be beneficial to an employee's overall performance and productivity. Coker (2011) found that employees who engaged in very low cyberslacking, less than 12% of their overall time at work, had higher productivity results than those who did not. Additionally, Syrek et al. (2018) and Wu et al. (2021) found that cyberslacking facilitated microbreaks that allowed employees to cope with work stressors and avoid decreased productivity. The disparate findings in the studies conducted to determine the impact cyberslacking has on employee productivity demonstrate the need for further research.

**Table 4**

*Summary of Productivity and Cyberslacking*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Coker, 2011	Survey	700 office workers	Workplace internet leisure browsing (WILB) and its effect on workplace productivity.	In moderation WILB can have a positive effect on overall workplace productivity.
Das et al., 2020	Survey	200 academic and non-academic staff	Abusive intention of cyberslacking.	The relationship between cyberslacking and abuse intention was significant.

**Table 5***Summary of Productivity and Cyberslacking (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Gibbs et al., 2021	Empirical study via experiment	10,000 skilled professionals	Comparison of productivity before and during work-from-home initiative due to COVID-19 pandemic.	Total hours worked increased by approximately 30 percent. Average output did not significantly change. Productivity decreased by 20 percent.
Hanaysha, 2016	Survey	242 administrative and academic staff	Employee engagement and performance outcomes and productivity.	Employee engagement has a significant positive effect on employee productivity.
Jia et al., 2013	Survey	147 participants	Measuring impact of personality five traits (conscientiousness, emotional stability, agreeableness, extroversion, and openness to experience) on cyberloafing.	Cyberslacking wastes valuable time and leads to loss of productivity.
Lim & Chen, 2009	Survey	191 respondents	Effects of cyberloafing on productivity.	Positive impact to productivity can be gained by small amounts of cyberloafing in the workplace.

**Table 6***Summary of Productivity and Cyberslacking (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Markos & Sridevi, 2010	Literature Review		Employee engagement affects productivity.	Employees that are not engaged in the workplace tend to focus on tasks that are of a lower priority or not essential to their job function.
Syrek et al., 2018	Survey	334 employees	Social media use relates to workplace engagement.	Cyberslacking allows for small breaks that provide employees with a method to deal with work stressors and avoid a decrease in productivity.
Vogl & Abdel-Wahab, 2015	Literature Review		Measuring productivity by overall output of labor, materials, and capital.	Measuring overall productivity required the analysis of key datapoints to develop benchmarking indicators for efficiency and overall output.
Wu et al., 2021	Survey	375 participants	Using ego-depletion theory and effort-recovery model to develop a framework explaining cyberloafing effects on employee's mental health.	An examination of the resource recovery and depletion effects of social cyberloafing on the employee's mental health.

## **Cyberslacking and Cybersecurity Posture**

Cybersecurity threats were estimated to have cost about six trillion dollars in 2021, and the increase in the number of cybersecurity attacks after COVID-19 was five times the rate before the pandemic (Aljohani, 2021). The pandemic has accelerated adoption of work-from-home options for many organizations and has strained their respective Information Technology (IT) departments by forcing the use of new methodologies to secure supporting infrastructure, such as home computers, home routers, and Wi-Fi access points (Aljohani, 2021). 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 (NIST, 2020). 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.

### *Computer Cybersecurity Posture*

Ifinedo (2012) posited that to ensure critical IT infrastructure has been safeguarded against attacks or misuse, organizations should utilize various security measures, such as firewalls, antivirus software, encryption, and proper access controls. Connolly and Wall (2019) found that an integral part of how organizations can mitigate cyberattacks is to utilize a holistic strategy including a combination of tools, such as security software, proper patch management, and recovery software. Similarly, Adel et al. (2021) referred to the overall security status and ability to manage an organization's technology stack, such as software, hardware, networks, and data, as its cybersecurity posture. In addition, Cain et al. (2018) suggested that the use of security software, such as antivirus, firewalls, and intrusion detection systems, should be used to ensure the proper cybersecurity posture of a device. The cybersecurity posture of a device is not solely

based on the use of the proper security controls, it is also important to regularly maintain these controls with the proper security and software updates to ensure their optimal effectiveness (Cain et al., 2018; Kabanda et al., 2018). Organizations that do not have the proper cybersecurity posture components in place risk being exposed to cyberattacks (Connolly et al., 2020).

Cain et al. (2018) posited users must adhere to good cyber hygiene practices for organizations and users to have devices with proper cybersecurity posture. Vishwanath et al. (2020) defined cyber hygiene as practices users should follow in order to protect their internet-accessible devices from being compromised in a cyberattack. Similarly, Banasinski and Rojszczak (2021) highlighted that cyber hygiene is a key component in establishing a comprehensive cybersecurity model. To safely access an organization's resources, proper cyber hygiene security controls should be used, including appropriate implementation of patch management for all software on the device, antivirus software, malware protection, firewall configuration, and VPNs (Coventry et al., 2014; Such et al., 2019; Vishwanath et al., 2020). For an organization to have an effective cybersecurity posture, cyber hygiene must extend beyond the organization's traditional workplace and into the remote workspace being utilized by the user to access their IT systems (Banasinski & Rojszczak, 2021). Rotas and Cahapay (2020) highlighted that remote users must adhere to the appropriate cyber hygiene procedures and proper cybersecurity posture of their devices to avoid being susceptible to cyberattacks.

#### *Cybersecurity Risk and Cyberslacking*

Florackis et al. (2023) described cybersecurity risk as the possibility of losing money, interrupting business operations, or harming the image of a company because of a failure in its IT systems caused by external threats. In addition to external threats such as hackers, malware, viruses, and ransomware, internal threats can increase the cybersecurity risk of an organization

(Algarni et al., 2021). For example, adverse user behaviors such as not complying with an organization's cyber hygiene practices can be considered internal threats to an organization's IT system, therefore contributing to an increase in its cybersecurity risk (Kalhor et al., 2021). Similarly, Cains et al. (2022) posited that users contributed to the increase in cybersecurity risks when not adhering to key security recommendations, such as password encryption or antivirus software. In addition, users' web browsing behaviors, including cyberslacking, can introduce additional security concerns and adversely affect the capacity of the overall IT system (Kalhor et al., 2021; Mishra & Tajeja, 2020).

Batabyal and Bhal (2020) found that cyberslacking can put organizations at considerable risk, both from a financial and a security perspective. Cyberslacking can pose a cybersecurity risk by subjecting an organization's systems to malware and/or spyware infection (Ozler & Polat, 2012; Vernon-Bido et al., 2018). In a study conducted by Koay and Soh (2018), as well as one by Papaginannidis and Markikyan (2020), the findings demonstrated that cyberslacking activities increased the risk of data loss due to spyware and virus infection. Exposure to malware and spyware can also cause degradation of network services and present network security threats to the organization (Hadington & Parsons, 2017; Vitak et al., 2011). Additionally, Wang et al. (2013) posited that cyberslacking can increase the susceptibility of an organization's network to cybersecurity risks in the form of breaches and degradation of network capacity. Similarly, Lim et al. (2021) stated that employees' cyberslacking activities could lead to security breaches and risk compromising the organization's key data.



**Table 7***Summary of Cyberslacking and Cybersecurity Posture*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Aljohani, 2021	Literature Review		Cybersecurity issues and breaches and mitigation factors.	Increase in cybersecurity threats during the COVID-19 pandemic due to decrease vigilance.
Hadington & Parsons, 2017	Survey	338 participants	Cyberloafing and internet addiction as indicators for Internet Security Awareness.	Internet abuse and cyberslacking activities can be utilized as indicators for poor cybersecurity practices and could increase the risk of a potential breach.
Ozler & Polat, 2012	Literature Review		Positive and negative impacts of cyberloafing on an organization.	Identified antecedents and consequences of this behavior as well as the controlling measures.
Vernon-Bido et al., 2018	Theoretical model development		Cyberloafing behavior and on the perceived risk that minor cyberloafing creates in an organization.	Sanctions play a role in mitigating cyberloafing, workload influences on cyberloafing tendencies are more impactful.
Vishwanath et al., 2020	Mixed method	404 internet users	Empirically identifying cyber hygiene and its sub-dimensions.	Developed Cyber Hygiene Inventory (CHI) measuring general internet users' cyber hygiene.

**Table 8***Summary of Cyberslacking and Cybersecurity Posture*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Vitak et al., 2011	Reanalysis of data	2,134 participants	Cyberslacking effect on workplace behaviors attributed to habits and internet addiction as indicators for cyberslacking propensity.	Identified areas that remain understudied with respect to their effect on cyberslacking, such as media habits and addictions, and average usage of internet services in the workplace. Additional areas of focus identified pertained to demographic information such as age, gender, and education and their relation to cyberslacking propensity.

**Cybersecurity Risk Management**

In the Framework for Improving Critical Infrastructure Cybersecurity created by the National Institute of Standards and Technology (NIST), risk is defined as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2018, p. 46). The recent increase in cyberattacks on organizations requires the development of methods and strategies to help measure and mitigate risk (Che Pa et al., 2017). Gouristetti et al. (2020) recommended that all organizations adopt cybersecurity frameworks to assess their overall cybersecurity posture. There are several cybersecurity frameworks in use across the world for example Cybersecurity Capability Maturity

Model, the NIST Cybersecurity Framework, the Lockheed Martin Kill Chain, and the Global Cybersecurity Index (Pattinson et al., 2018; Smith, 2019). However, the NIST Cybersecurity Framework has been widely adopted by chief information security officers across the globe and is considered the de facto standard (Badamasi & Utulu, 2021; Krumay et al., 2019).

The NIST Cybersecurity Framework (2018) provides a model for companies to address cyberthreats and is comprised of five domains: *Identify, Protect, Detect, Respond, and Recover*. The *Protect* domain includes components such as the development and implementation of required safeguards to ensure that critical services remain operational and potential risks are reduced; it also includes user training and awareness (NIST, 2018). In addition, Crossland and Ertan (2021) recommended that an organization's cyber risk management efforts should account for employee training to help identify cybersecurity risks and adhere to best practices. Proper training is vital, as the end user is considered to be the weakest link in computer security (Hakak et al., 2020; Heartfield & Loukas 2018).

#### *Cyber Risk Management of Remote Workers*

Although the increased number of remote workers provided organizations with the ability to continue key operations and minimize economic impact, it also increased cybersecurity attack surfaces that could be used in a breach (Vagal & Dillon, 2021). Many of the devices and networks being used to access organizational resources are unprotected and unsecured, providing an attack vector to hackers as well as cybercriminals (Hakak et al., 2020). Borkovich and Skovira (2020) found that remote workers presented a considerable threat to the cybersecurity posture of an organization and were more susceptible to cybersecurity attacks than those who worked in a traditional office environment. Similarly, Vagal and Dillon (2021) posited that working remotely introduces additional risk to organizations, as the traditional methods for a secure working

environment such as firewalls, intrusion prevention, and detection systems are not inherently in place. Weil and Murugesan (2020) suggested that organizations reevaluate their cyber risk strategies to include the threat of widespread adoption of working remotely. Similarly, Sebastian (2021) recommended organizations adopt a framework based on the NIST (2020) bulletin to incorporate remote work best practices into their existing cybersecurity policies.

#### *Cyber Risk Management of Cyberslacking*

In addition to the increase of cyber risk from remote workers' cybersecurity posture, employees who are outside the confines of the traditional workspace are more susceptible to engaging in deviant activities as they are less likely to be discovered by a supervisor or coworker (Reizer et al., 2021; Stich, 2020). Activities such as cyberslacking can affect an organization's business and increase the potential of cybersecurity attacks on its IT infrastructure (Alahmari & Duncan, 2020). Hadlington and Parsons (2017) found that cyberslacking activities and poor cybersecurity practices increased the risk of a potential breach. Similarly, Syed et al. (2020) and Reizer et al. (2021) described cyberslacking as a security risk to an organization, as it causes excessive internet usage and security threats. To mitigate the potential cybersecurity risks introduced by employee cyberslacking, organizations have adopted various security policies and countermeasures focusing on deterrence within the traditional workplace (Alharthi et al., 2019; Luo et al., 2022; Sheppard & Mejias, 2016). Yusif and Hafeez-Baig (2021) recommended an adjustment to these policies to account for the risks posed by remote workers engaging in non-work-related activities.

**Table 9***Summary of Cyber Risk Management*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Borkovich & Skovira, 2020	Literature Review and unstructured interviews.	12 participants	Determining if remote workers are a higher risk to the cybersecurity posture of an organization.	The human factor is identified as the weakest link to information security therefore the adopted cybersecurity framework of an organization must account for remote workers.
Goodwin, 2022	Phenomenological qualitative research.		Analysis of reported Financial Sector risks, failures and impacts due to weakness or lack of cybersecurity controls.	Adoption and implementation of cybersecurity framework such as NIST Cybersecurity Framework proved to reduce cyber-attacks and enhance the cybersecurity posture of organizations.
Krumay et al., 2018	Literature Review		Analysis of the NIST Cybersecurity framework domains in academic literature to determine varying implications.	Organizations need to adopt a security framework, such as NIST, to ensure a reasonable level of cybersecurity posture.

**Table 10***Summary of Cyber Risk Management (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Ncubekezi, 2022	Survey	30 respondents	Analysis of employee actions, behaviors, and attitudes that negatively influence the state of information and computer security.	Behaviors, attitudes, and actions of employees have the potential of contributing to the overall cyber risk of an organization.
Sebastian, 2021	Survey	109 participants	Using 8 controls to develop the WFH cyber-attack mitigation framework.	Development of an 8-step framework that allows organizations to incorporate remote work best practices into their security policy.
Shepard & Mejias, 2016	Longitudinal study	200 participants	Using technical and nontechnical deterrent policies to assess the impact on nonwork related internet use at work.	The results demonstrated that nontechnical deterrence methods in the form of use policies are effective approaches to mitigate employee Internet abuse.

### **Demographics**

Demographic characteristics such as age, gender, education level, and years of work experience have been studied as antecedents to cyberslacking, though results have been contradictory. For example, Ugrin and Pearson (2013) found younger employees were more inclined to participate in cyberslacking activities than their older colleagues. Similarly, Hartishi and Fathonah (2014) found age to be a contributing factor in an employee's participation in

cyberslacking activity. However, Hernandez et al. (2016) found no differences in cyberslacking activities based on the age of employees.

In terms of gender, Toker and Baturay (2021) found that males were more likely to engage in cyberslacking than females. Similarly, Hartijasi and Fathonah (2014), Sheikh et al. (2015), and Akbulut et al. (2017) found gender to be a contributing factor in cyberslacking activities. The analysis conducted by Akbulut et al. (2017) revealed that overall cyberloafing scores of male employees were much higher than those of female employees. Conversely, Hernandez et al. (2016) found that gender did not indicate a significant difference in cyberslacking engagement. Their findings were supported by Gokcearslan et al. (2018) and Gorenc et al. (2016), who determined that gender did not affect an employee's choice to engage in cyberslacking.

Education level has also been studied in terms of an employee's propensity to engage in cyberslacking activity. Sheikh et al. (2015) found education level was a factor that contributed to cyberslacking activities. Similarly, studies by Althari et al. (2019), as well as Hartishi and Fathonah (2014), showed that education level contributed to employees' cyberslacking activity. These findings directly conflict with the findings of Hernandez et al. (2016) in which an employee's education level did not show a significant difference in their cyberslacking activity.

Work experience is another characteristic investigated with respect to an employee's cyberslacking activities. Althari et al. (2019) found that the more work experiences an employee had, the less likely they were to engage in cyberslacking. These results were supported by Kemer and Ozcan (2021), who found that as the employee's work experience increased, the frequency of cyberslacking engagement decreased. Conversely, Arslan and Demir (2016) found that as work experience increased, the frequency of cyberslacking increased. Contrary to the results of

both studies, Marzuki et al. (2020) found that an employee's work experience did not affect their cyberslacking activity.

An employee's level in an organization is another factor that has been investigated in terms of cyberslacking. Ugrin et al. (2007) found that executives were more likely to engage in cyberslacking activities. Similarly, Marmat and Baqutayan (2019) found that employees of higher-level positions were more likely to be involved in cyberloafing. However, Aghaz and Sheikh (2016) found that senior staff were less likely to engage in cyberslacking activities than their junior counterparts.

**Table 11**

*Summary of Demographics*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Aghaz & Sheikh, 2016	Survey	298 participants	Relationship between cyberloafing activities and behaviors resulting in knowledge worker job burnout.	Senior staff were less likely to engage in cyberslacking activities than their junior counterparts.
Akbulut et al., 2017	Survey	1339 students and 996 jobholders	Relationship between cyberloafing and social desirability.	Cyberloafing more prevalent in male employees than female employees.
Althari et al., 2019	Empirical Investigation	1,063 employees	Employee Commitment to the organization and Frequency of Cyberslacking.	Created the mobile cyberslacking-commitment taxonomy (MCCT) for organizations to measure workplace productivity



**Table 12***Summary of Demographics (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Gokcearslan et al., 2018	Survey	885 undergraduate students	The relationships between smartphone addiction, cyberloafing, stress and social support.	There was a significant difference between genders in terms of perceived social support, stress, and smartphone addiction, but there was no significant difference between genders in terms of cyberloafing.
Gorenc et al., 2016	Survey	448 employees	Internet addiction and its impact on abuse of the internet at the workplace.	Demographic factors such as gender, age, education, and income do not have an effect on cyberslacking or internet abuse in the workplace.
Hartijasi & Fathonah, 2014	Survey	267 participants	Measured frequency of cyberloafing on 20 specified activities to determine effect on productivity.	Education contributed to the employees cyberslacking activity.

**Table 13***Summary of Demographics (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Hernandez et al., 2016	Survey	183 participants	Measure self-reported extent to which workers cyberslacking and its ethical severity.	Study found that there are no significant differences in employees' cyberslacking activities based on gender, age, level of education, job level, and years working for government.
Rahimnia et al., 2015	Survey	320 administrative employees	Control mechanisms to effect cyberloafing in the workplace.	Females were more likely to engage in cyberslacking than males.
Toker & Baturay, 2021	Survey	272 students	Cyberloafing affected by 11 key factors including internet experience, age, and gender.	Males were more likely to engage in cyberslacking than females.

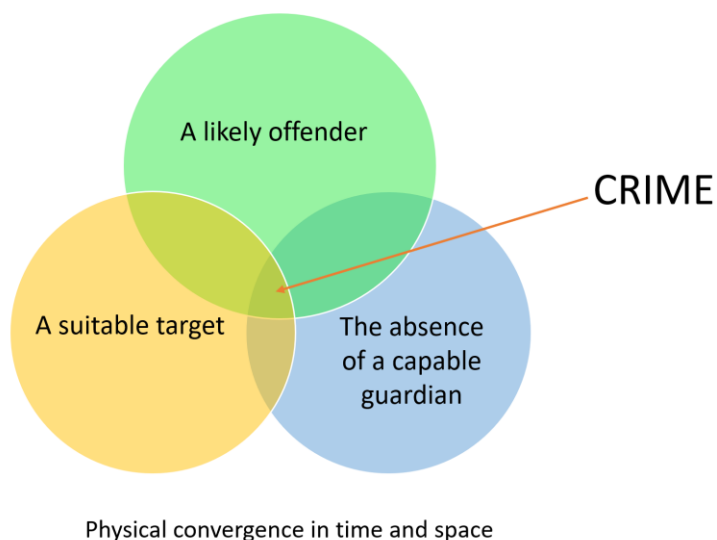
### **Theoretical Background: Routine Activity Theory**

Routine Activity Theory (RAT) was developed by Cohen and Felson (1979) as a method to analyze crime rate by focusing on the circumstances of the crime rather than the characteristics of the offender. Cohen and Felson (1979) posited that “most criminal acts require convergence in space and time of likely offenders, suitable targets, and the absence of capable guardians against crime” (p. 538). The likelihood of the criminal act occurring decreases or is potentially eliminated if one or more of these components is absent (Choi, 2008). Researchers have utilized RAT to provide a framework for identifying risk factors of victimization (Reyns et

al., 2016). RAT has been used extensively in criminology to provide an analysis of the various forms of deviance and crime (Navarro & Jasinski, 2012). A graphical depiction of the theory is shown in Figure 2.

**Figure 2**

*Routine Activity Theory – Adapted from Cohen & Felson (1979)*



Researchers have expanded the application of RAT from its initial use in criminology to include the analysis of cyber deviance and cybercrimes (Navarro & Jasinski, 2012; Reynolds et al., 2016). Additionally, Reynolds et al. (2016) noted an increasing number of studies have focused on online victimization, although RAT was originally deemed to be location-based and unsuitable for computer-based crimes. Leukfeldt and Yar (2016) posited that RAT was suitable for studies involving cybercrime and cyber deviant behavior but suggested that modifications were required to accommodate the non-spatial nature of the virtual environment.

Choi (2008) proposed combining components of lifestyle exposure theory and RAT to explain the causes of computer crime victimization via specific components. The combined

theory, Cyber Routine Activity Theory (Cyber-RAT), primarily focuses on computer hacking but can be used to explain computer crime victimization utilizing two factors, digital guardianship, and online activities (Choi & Lee, 2017). Lee and Choi (2021) utilized Cyber-RAT to explore potential links between Bitcoin, ransomware, and terrorist activities. In addition, Correia (2022) used Cyber-RAT to develop mitigation and detection strategies for the motivations of cyber terrorist offenders.

This research study used previous studies on RAT and Cyber-RAT to analyze cybersecurity risks posed by remote workers engaging in cyberslacking activities (Choi & Lee, 2017; Leukfeldt & Yar, 2016; Navaro & Jasinski, 2012). Leukfeldt and Yar (2016) noted that RAT could be used to provide an analysis of cyber deviant activities and suggested the key constructs be reviewed in terms of their applicability to the online environment. In RAT, the construct of lack of guardianship refers to persons or objects with the capability to prevent or deter crime (Cohen & Felson, 1979). Researchers have adapted this construct to expand their understanding of guardianship in various areas of cyberspace. For example, Holt and Bassler (2013) noted that antivirus, antispyware, and adware programs are the most common computer-based guardians. Ilievski (2016) posited that in terms of cybercrime and cyber deviance, guardianship can refer to the use of protective software such as firewalls, antivirus, and anti-spyware. Similarly, Jansen and Leukfeldt (2016) noted that technical security measures such as antivirus software could be used as a form of guardianship. Additionally, Choi (2008) described guardianship as digital guardianship, which included the use of security management software such as antivirus, anti-spyware, and firewalls.

The second construct in RAT is suitable targets, defined as persons or property that can be threatened by the offender (Cohen & Felson, 1979). Traditionally, the suitable target construct

of RAT required a physical location. Reyns et al. (2016) contended the intersection of parties within a network served as a replacement for the physical location requirement. Similarly, Brady et al. (2016) suggested that the construct of a suitable target should be changed to accommodate the digital world. Increased technology dependence also provides additional visibility to the targets due to the subsequent growth in online activity (Jansen & Leukfeldt, 2016). In addition, Ilievski (2016) found an increase in target suitability for those users who are engaging in risky online activities, such as frequently visiting unknown websites and downloading games or music.

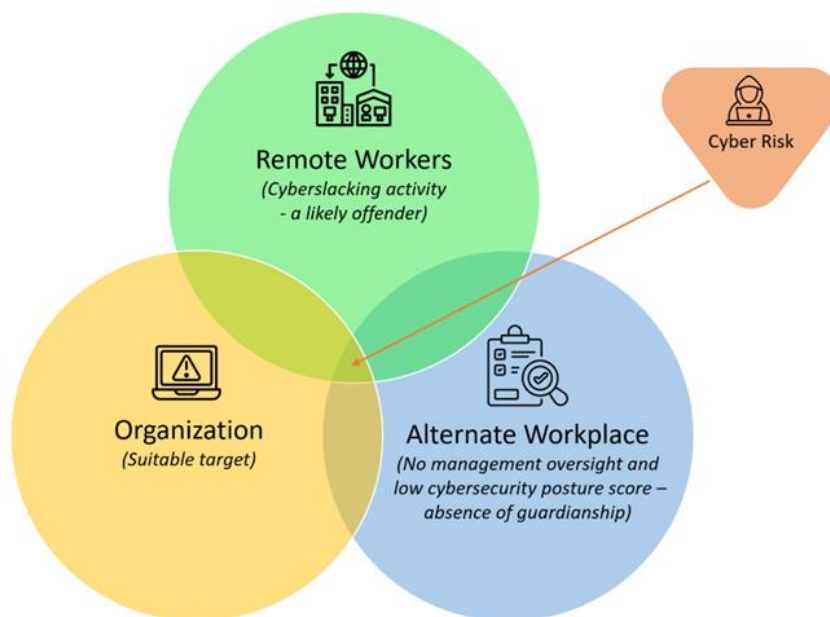
The last construct in RAT is that of a likely offender, described as a person with the capability and motive to commit a crime (Cohen & Felson, 1979). Although the original theory required frequent physical contact between the target and the likely offender, researchers have posited that this could be expanded to accommodate virtual environments (Ilievski, 2016; Jansen & Leukfeldt, 2016; Leukfeldt & Yar, 2016). Holt and Bossler (2008) postulated that routine computer use could increase the exposure to likely offenders. Similarly, Ilievski (2016) noted that the exposure to likely offenders, which they term motivated offenders, was increased by the users' daily online activities. The increase in dependency on the use of the Internet in users' daily activities creates the opportunity for likely offenders to have unlimited access to potential targets (Brady et al., 2016).

This research study used RAT as the foundation for research. The three fundamental RAT constructs, lack of guardianship, suitable targets, and likely offenders, along with the modifications proposed by researchers to accommodate a digital world were applied. In addition, this research expanded the constructs as follows: alternate workplace, organization, and remote workers. The alternate workplace construct aligns with lack of guardianship, as the remote site provides no physical management oversight. In addition, the alternate workplace presents the

potential that the device violates security policy for security software and updates. Secondly, the organization construct aligns with a suitable target, as the organization could be at risk if there is a lack of guardianship and a likely offender, which according to Brady et al. (2016) the internet increases the number of potential offenders. Lastly, the remote workers construct aligns with a likely offender, as the cyberslacking activities can be deemed as risky online activities which increase an organization's risk factor (Ilievski, 2016). A graphical depiction of the adapted theory is shown in Figure 3.

### Figure 3

*Adapted from Routine Activity Theory Cohen & Felson (1979)*



**Table 14***Summary of Routine Activity Theory*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Choi & Lee, 2018	Survey	272 participants	Cybersecurity issues and breaches and mitigation factors.	Participants that take part in risky online activities and do not effectively manage their cybersecurity are more likely to experience cyber-interpersonal violence victimization.
Jansen & Leukfeldt, 2016	Semi-structured interviews	30 participants	Cyberloafing and internet addiction as indicators for Internet Security Awareness.	Internet abuse and cyberslacking activities can be utilized as indicators for poor cybersecurity practices and could increase the risk of a potential breach.
Leukfeldt & Yar, 2016	Reanalysis of data	9,161 participants	The effects of value, visibility, accessibility, and guardianship on victimization of six cybercrimes.	Accessibility and personal capable guardianship show varying results. Value and technical capable guardianship show almost no effects on cybercrime victimization.

**Table 15***Summary of Routine Activity Theory (continued)*

<b>Study</b>	<b>Methodology</b>	<b>Sample</b>	<b>Instrument or Construct</b>	<b>Main Finding or Contribution</b>
Navarro & Jasinski, 2012	Survey	935 participants	Availability was measured by how often participants engaged in online activity. Suitability categorized the types of activity the participants engaged in. Guardianship was measured by engaging both physical and technical methods.	RAT demonstrated to be a viable theory to analyze cyberbullying among the participants by using the constructs defined. The results were mixed in terms of suitability and guardianship.
Choi & Lee, 2018	Survey	272 participants	Cybersecurity issues and breaches and mitigation factors.	Participants that take part in risky online activities and do not effectively manage their cybersecurity are more likely to experience cyber-interpersonal violence victimization.

### **Summary of What Is Known and Unknown**

Cyberslacking is estimated to cost organizations approximately \$85 billion per year, yet it remains an issue that researchers and practitioners are struggling to understand (Venktraman et al., 2019; Zakrzewski, 2016). Furthermore, the studies conducted have focused on cyberslacking within the confines of a traditional office and not on those employees working remotely (O'Neill et al., 2014). In response to the COVID-19 pandemic, many organizations have adopted remote work strategies to continue their business operations. In 2019, approximately 30% of the U.S. workforce was working remotely at least part of the week (Barreo et al., 2020; Brynjolfsson et



al., 2020). Few researchers have examined the effects of remote workers engaging in cyberslacking activities and the potential cybersecurity risks (Russo et al., 2020). In addition, the studies conducted have used self-reported survey instruments to collect data about participant's cyberslacking activity, this has been identified as a limitation of these studies as participants may be reluctant to report their activities accurately (Hadlington & Parsons, 2017; Russo et al., 2020; Syed et al., 2020). Akbulut et al. (2017) suggested that further research should be conducted using measures that are not obtained through self-reported instruments.

Research has shown that cyberattacks on organizations continue to increase, specifically increases in cyberattacks directed at remote employees. Therefore, organizations should develop and adopt methodologies to help understand and mitigate their cybersecurity risk (Che Pa et al., 2017; Moshin, 2020). Organizations have used various security policies and countermeasures focusing on deterrence within the traditional workplace but have not accounted for remote workers (Alharthi et al., 2019; Luo et al., 2022; Sheppard & Mejias, 2016).

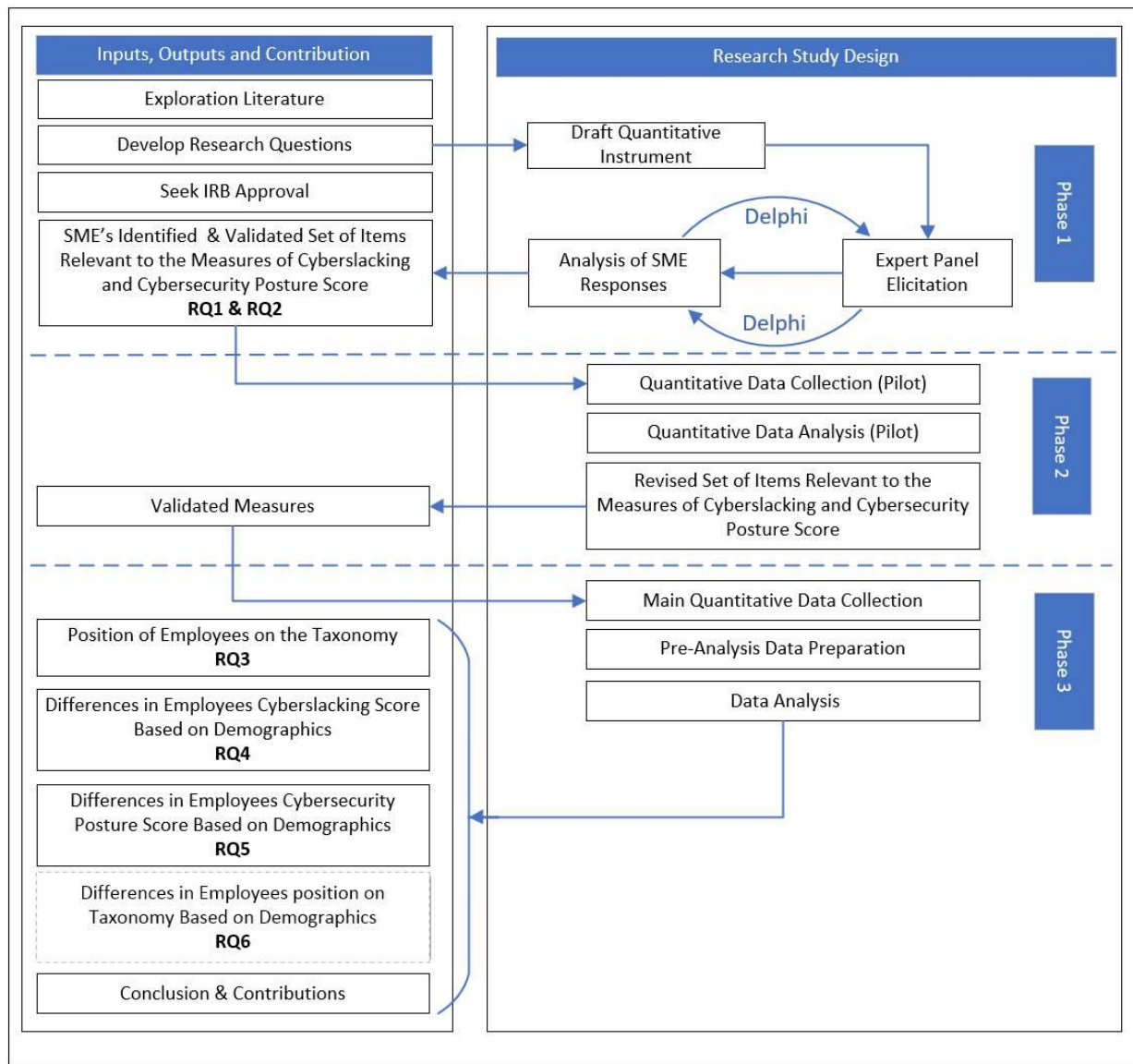
The literature review demonstrated disparate findings in terms of cyberslacking activity and various demographic characteristics such as age, gender, education level, and years of work experience. For example, Toker and Baturay (2021) found that males were more likely to engage in cyberslacking than females. Conversely, Hernandez et al. (2016) observed that gender did not indicate a significant difference in cyberslacking engagement. Additionally, the literature demonstrated contradictory results for age, education level, and work experience. As a result, additional research is required to explore the relationship between employee cyberslacking and demographic factors such as age, gender, education, and level in the organization.

## Chapter 3

### Methodology

#### **Overview of Research Design**

This research study, a three-phased developmental approach as depicted in Figure 2, created, and empirically validated the Remote Worker Cyberslacking Security Risk Taxonomy. This work was successful in achieving the goal of developing, validating, and empirically testing the taxonomy to assess an organization's remote workers' risk level of cybersecurity threats by using productivity measures to determine their inclination to participate in cyberslacking and the computer security posture of the remote device being used to access organizational resources. The data collection for this developmental study utilized an experimental field study approach as described by Levy and Ellis (2011). This experimental design is appropriate when randomization of the participants is not possible, leaving the use of pre-defined groups. The Remote Worker Cyberslacking Security Risk Taxonomy was leveraged as the artifact or "thing" that was built to address the identified research problem (Ellis & Levy, 2009). This research developed, validated, and empirically tested a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This research study was conducted in three phases to address the main question: 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 organizational resources?

**Figure 4***Proposed Research Design Process*

Phase one recruited SMEs from the cybersecurity/IT field to identify and validate measures for the computer security posture score. This process of identification and validation of the measures leveraged the Delphi method to obtain anonymous feedback from experts (Okoli & Pawlowski, 2004). This method sought to build a consensus among the SMEs identified via a well-defined process that included identifying measures, rating those measures, providing

reasons behind their responses, and finally driving towards an agreement of all parties involved (Parekh et al., 2018).

Phase two involved collaboration with the identified SMEs to define, develop, and test the Remote Worker Cyberslacking Security Risk Taxonomy by collecting data from a pilot group of participants to verify the validity of the defined measures for device cybersecurity posture and their derived composite value. Building on the research conducted by Jeong et al. (2020) and Bhomer et al. (2011) in which log analysis was used to determine application usage patterns as well as the research conducted by Ferreira et al. (2014) that included additional details "such as work schedule, hours, the purpose of use, and log data" (p. 17), this study utilized the reporting capabilities of the productivity suite that contains application usage and endpoint management software data points to collect the key indicators as defined by the SMEs. This differs from prior studies conducted by Jamaluddin et al. (2015), and Askew et al. (2014) where self-reported instruments were used to collect cyberslacking activity. As prior studies have suggested that age, gender, education level, and years of work experience could impact cyberslacking behaviors, this study gathered these demographic indicators via a survey instrument (Alharthi et al., 2019; Luqman et al., 2020; Rahimnia & Mazidi., 2015; Sheikh et al., 2015). An integral outcome of this pilot phase was to help validate a particular instrument before moving to the primary data collection stage of this study (van Teijlingen & Hundley, 2002).

Phase three of this study, the main data collection and analysis phase, used the defined measures for cyberslacking and device cybersecurity posture, with their derived composite values and demographic information. This study focused on remote workers from a public higher education institution in the U.S.

## **Measures**

### *Productivity*

Vogl and Abdel-Wahab (2015) defined productivity as the "measure of the efficiency with which the economy turns inputs, such as labor and capital, into output" (p. 2). 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 (Burney & Widener, 2013; Mohammad et al., 2019; Webber et al., 2015). Hanaysha (2016) provided empirical evidence that work engagement has a positive effect on employee productivity and recommended organizations provide a methodology for measurement and evaluation.

### *Employee Productivity and Cyberslacking*

Employee productivity is focused on the efficiency of the employee or employees and can be evaluated by measuring their respective output within a given time period (Hanaysha, 2016). Ferreira and Du Plessis (2009) suggested that assessing employee productivity can be accomplished by measuring time spent executing required tasks to provide the desired outcome according to respective job functions. Syed et al. (2020) leveraged the amount of work completed within a respective period of time as the measurement for productivity. Specifically, an employee's engagement in work activities demonstrates a positive effect on overall employee productivity (Hanaysha, 2016). Similarly, Das et al. (2020) attributed a decrease in an employee's overall work performance to their engagement in non-work activities such as cyberslacking.

This study expanded on work conducted by Eldridge and Pabilonia (2010) in which total hours worked by supervisory and nonsupervisory employees in a week, Current Population Survey ratio, and total number of work weeks in a year were used as inputs in an equation for

determining total hours for production. Similarly, this study measured cyberslacking activity by using the following inputs: employee productivity, total hours in the workday, and a constant measure for breaks, as depicted in Equation 1.

$$CySI = k * (WkD (hrs) - (Brk (hrs) + EP (hrs))) \quad (1)$$

As shown in Equation 1, the value for CySI is normalized using the k coefficient, to a value between 0 and 100 for consistency representing a percentage of the workday devoted to cyberslacking. WkD represents the typical workday, in the U.S. a typical workday is eight hours (Smith, 1986). The U.S. Bureau of Labor Statistics (2021) reported the average workweek for employees in the information sector in October of 2021 was 36.7 hours. The information sector includes traditional publishing, and telecommunications, which plays a large role in cybersecurity (U.S. Bureau of Labor Statistics, 2021). 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.

This study used the literature and SMEs feedback to identify key indicators by which employee productivity can be measured. For example, Yang et al. (2020) utilized data on emails, calendars, instant messages, and video/audio calls to measure the effects of remote work on employees' productivity. Similarly, Fransilla et al. (2014) measured extensive email usage by knowledge workers and its potential to decrease productivity. Additionally, Cao et al. (2021) collected data about the usage of major productivity tools such as Microsoft Teams, Outlook, OneDrive, and SharePoint to measure productivity and multitasking behaviors. This study used an aggregate of time spent on productivity software such as Microsoft's Office 365 suite of productivity tools, Email usage, Microsoft Teams, a web browser, OneDrive, and SharePoint as

the indicators for measurement. Table 2 lists the indicators of employee productivity as derived from the literature that will be utilized to measure cyberslacking.

**Table 16**

*Indicators to measure employee productivity (All Measured in Hours Per Day)*

<b>PMID</b>	<b>Indicator</b>	<b>Source/Adapted</b>
PM01	Browser usage	Czerwinski et al. (2004) Coker (2011)
PM02	Email apps usage	Mark et al. (2016)
PM03	OneDrive for Business usage	Cao et al. (2021)
PM04	Microsoft 365 Apps usage (Word, Excel, PowerPoint)	Yang et al. (2020)
PM05	SharePoint site usage	Cao et al. (2021)
PM06	Microsoft Teams user activity	Yang et al. (2020)

#### *Computer Cybersecurity Posture*

To measure the computer security posture of the device being used by remote workers to access corporate systems, this study used an aggregate value of key indicators that have been identified from the literature and subsequently validated and assigned proper weights using feedback from SMEs. These indicators were obtained from an endpoint management system to overcome issues with self-reporting anomalies. Abdel et al. (2021) referred to cybersecurity posture as overall security status and 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 in order to protect an organization from potential

cyber threats. This study focused on cybersecurity posture from the endpoint device used to access an organization's resources with company-provided devices and their overall cyber hygiene, which plays a significant role in cybersecurity breaches (Cain et al., 2018). Vishwanath et al. (2020) defined cyber hygiene as a practice users should follow in order to protect their internet-accessible devices from being compromised in a cyber-attack. 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 VPNs for accessing an organization's resources (Coventry et al., 2014; Such et al., 2019; Vishwanath et al., 2020). Thus, this study used the indicators of proper cyber hygiene, as derived from the literature, and listed in Table 9, to determine an aggregate score for computer security posture, as depicted in Equation 2.

$$CSP = j * \sum_{i=1}^n (w_i * CSP_i) \quad (2)$$

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  $CSP_i$ ,  $n$  is the total number of proper cyber hygiene indicators, and  $i$  represents the value of the specific proper cyber hygiene indicator. The arithmetic means of the SME scores for each computer security posture indicator was used as their respective weight and is represented by  $w_i$ . To normalize the value for CSP this study used a coefficient represented by  $j$ . This coefficient is derived by dividing one by the sum of the maximum value of each computer security posture indicator ( $MaxCSP_i$ ), depicted in Table 9, and multiplied by its respective weight. This is represented by Equation 3. 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.

$$j = \frac{1}{\sum_{i=1}^n (w_i * MaxCSP_i)} \quad (3)$$

**Table 17**

*Indicators to Measure Computer Security Posture.*

<b>CSPID</b>	<b>Indicator</b>	<b>Rating Scale</b>	<b>Source</b>
CSP01	Operating System Version	1 – 4	Such et al. (2019)
CSP02	Operating System Patching (systems are up to date)	1 – 4	Such et al. (2019)
CSP03	Antivirus/Malware Detection programs	1 – 4	Cain et al. (2018)
CSP04	Antivirus/Malware signature updates	1 – 4	Cain et al. (2018)
CSP05	Software updates	1 – 4	Such et al. (2019)
CSP06	Disk encryption enabled	1 – 2	Such et al. (2019)
CSP07	Firewall enabled	1 – 2	Cain et al. (2018)
CSP08	VPN usage	1 – 2	Such et al. (2019)
CSP09	Collection of security logs enabled	1 – 2	Vishwanath et al. (2020)
CSP10	End Point Protection	1 – 2	Vishwanath et al. (2020)

### *Demographics*

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” (Sheikh et al., 2015, p. 174).

Although the literature does support demographics as antecedents, inconsistent findings exist pertaining to age, gender, education, and work experience with respect to employees' cyberslacking (Althari et al., 2019; Hartijasi & Fathonah, 2014; Sheikh et al., 2015). Hartijasi and Fathonah (2014), as well as Sheikh et al. (2015), stated age, gender, education, and work experience were factors that contributed to cyberslacking activities. Conversely, Hernandez et al. (2016) 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 (2007) where executives were more likely to engage in cyberslacking activities. Similarly, Aghaz and Sheikh (2016) 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 as depicted in Table 10.

**Table 18**

Demographic indicators

<b>DMID</b>	<b>Demographic</b>	<b>Source</b>
DM_AGE	Age	Hernandez et al. (2016) Althari et al. (2019)
DM_GEN	Gender	Hernandez et al. (2016)
DM_EDU	Education	Hernandez et al. (2016)
DM_ROL	Job role	Ugrin et al. (2007)
DM_JOB	Level on the organization	Aghaz and Sheikh (2016)
DM_EXP	Experience	Hartijasi and Fathonah (2014)

## **Validity and Reliability**

This study followed a three-phased developmental approach that combines quantitative methodologies, qualitative methodologies, and the development of a Remote Worker Cyberslacking Security Risk Taxonomy. In phase one, SMEs were asked to: (1) validate measures for the computer cybersecurity posture score, (2) develop and derive a composite value used for determining the computer cybersecurity posture score, (3) use the measures and composite values to validate a taxonomy measuring if an organization's remote workers present a higher risk of cybersecurity threats. These components will allow for measuring the remote workers' propensity to engage in cyberslacking activities and gauging the computer cybersecurity posture of the remote device being utilized to access organizational resources. In addition, phase one used the Delphi method in an effort to build a consensus among the SMEs via a well-defined process that includes identifying the measures, rating the measures, providing reasons behind their responses, and finally driving towards an agreement of all SMEs (Parekh et al., 2018).

Phase two validated the proposed Remote Worker Cyberslacking Security Risk Taxonomy by collecting data from a pilot group of 15 participants to verify the validity of the defined measures for cyberslacking, the device cybersecurity posture score, and their derived composite value. In addition, an instrument was used to collect demographic information such as age, gender, education level, and years of work experience, as studies have indicated that these factors may impact cyberslacking behaviors (Alharthi et al., 2019; Luqman et al., 2020; Rahimnia & Mazidi, 2015; Sheikh et al., 2015). This phase helped validate the taxonomy prior to the main data collection phase. Lastly, phase three consisted of the main data collection of the larger group where pre-analysis data screening will occur before statistical analysis is conducted.

### *Validity*

Kimberlin and Winterstein (2008) defined validity “as the extent to which an instrument measures what it purports to measure” (p. 2278). As discussed by Salkind (2017), content validity can be addressed by conducting a proper literature review. This study provided a synthesis of the body of knowledge in the literature regarding cybersecurity posture measures as well as cyberslacking activities affecting productivity. This review served as the basis for the list of SMEs approved measures to help validate the Remote Worker Cyberslacking Security Risk Taxonomy. Criterion validity was addressed by leveraging SMEs feedback on (1) validated measures for the computer security posture score, and (2) the development and validation of a composite value used for determining the computer security posture score. To address construct validity, the literature review and synthesis provided the basis for cybersecurity implications for remote workers who are engaging in cyberslacking. In addition, collaborating with the SMEs on the Delphi method, as well as having multiple iterations, increased the validity of the constructs (Hasson et al., 2000).

### *Reliability*

Ihantola and Kihn (2011) described reliability as the consistency of a variable or set of variables in what they intend to measure. In phase one, the initial data collection was obtained with the assistance of SMEs via an instrument distributed via email. To increase the participation and commitment of the SMEs to the research study, a \$5 Starbucks gift card was given to each. The data collection process in Phase Two and Phase Three was conducted in the same manner, collecting the same data points across all participants, and leveraging the same methodology to ensure consistency. The values for these coefficients range between zero and one; the higher the value, the more reliable the measures (Terrell, 2016).

## **Proposed Sample**

Currently, there is no consensus in terms of panel size and number of rounds for the Delphi method that is proposed to be leveraged in phase one of this study (Atkins et al., 2005; Skulmoski et al., 2007), although Okoli and Pawlowski (2004) suggested that an expert panel size should have 10 to 18 experts participating in each round. Similarly, Skinner et al. (2015) posited that expert panels can range from 10 to 30 experts. For phase one of this research study, the proposal was to contact 75 experts, with a desired response rate of 15. The expert panel was recruited via LinkedIn and professional cybersecurity organizations. Clayton (1997) defined an expert as “someone who possesses the knowledge and experience necessary to participate in a Delphi” (p. 377). According to Clayton’s (1997) definition, members of the panel were limited to cybersecurity professionals with the requisite knowledge, education, experience, and professional certification credentials such as CompTIA Security+, and Certified Information Systems Security Professional (CISSP).

For the second phase of this study, the research collected demographic data, cyberslacking activity, and computer cybersecurity posture indicators in the form of a pilot study to ensure the taxonomy met the requirements set forth. The ten participants for the pilot were recruited via email and were a subset of employees of the intended larger sample. In order to participate in this study, the employees had to be information workers with technology backgrounds who work-from-home. Pilot users were excluded from the main data collection to avoid adversely affecting the participants’ behavior, as this can be a common drawback of using a pilot (van Teijlingen & Hundley, 2002).

Phase three of this study utilized a sample of the population as described by Sekran and Bougie (2016) as representative of the overall population by which conclusions can be drawn, specifically a target of 125 participants. This study leveraged a sample of convenience from a

public higher education institution, specifically targeting information workers with technology backgrounds who primarily work-from-home. A total of 625 potential participants were contacted via email to participate in this study to achieve the intended target of 125 participants.

### **Pre-analysis Data Screening**

To ensure the data being collected in this study did not contain irregularities or presented issues during the collection process, pre-analysis data screening was utilized prior to conducting the final analysis, as recommended by Levy (2006). Mertler and Vannatta (2017) 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 (2006) discussed the four main reasons for ensuring pre-analysis screening is conducted on the data collected before the 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 (Kerlinger & Lee, 2000; Levy, 2006). The third reason is to validate that 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 (Levy, 2006; Mertler & Vannatta, 2017). Lastly, pre-analysis screening should address outliers, which can have an adverse effect on the results and conclusions made from the analysis.

### **Data Collection & Data Analysis**

#### *Phase One – Delphi Methodology (RQ1 & RQ2)*

Phase one of this research study sought to validate measures for employee cyberslacking and the computer security posture score of the device being used to access organizational

resources using the Delphi method. This method was established by the RAND Corporation as “a methodical and interactive research procedure for obtaining the opinion of a panel of independent experts concerning a specific subject” (Skinner et al. 2015, p. 32). This iterative process seeks to build consensus among a group of SMEs that intends to yield agreement on final ratings (Parekh et al., 2018). This method consisted of multiple rounds until a consensus among the SMEs was attained. Sumsion (1998) recommended a 70% SME response rate as acceptable of consensus.

### *Data Collection*

This research study distributed an anonymous survey via email and LinkedIn to 75 information systems and cybersecurity SMEs in order to attain a total of 15 responses, representing a 20% response rate. The survey consisted of four distinct sections that were utilized to validate measures for employee cyberslacking and the computer security posture score of the device being used to access organizational resources. In addition, the survey was also used to validate the proposed taxonomy for classifying if an organization’s remote workers present a higher risk of cybersecurity threats based on CySI and CSP measures. Questions one through question seven of the survey collected demographic information from the SMEs in order to validate their qualifications, such as years of education level, years of experience, description of their professional role, and industry-based certifications. Questions eight through 11 of the survey asked the SMEs to evaluate the importance of the cyberslacking and computer security posture measures identified in the literature using a seven-point Likert ranging from (1) “Not at all important” to (7) “Extremely important”. Question twelve in the survey asked the SME to evaluate the proposed taxonomy using the CySI and CSP measures to classify if an organization’s remote workers present a higher risk of cybersecurity threats using a seven-point

Likert ranging from (1) “Strongly Disagree” to (7) “Strongly Agree”. The last question, question thirteen, allowed the SMEs to provide recommendations on how to adjust the Remote Worker Cyberslacking Security Risk Taxonomy. The results of the data collected were used to answer RQ1 and RQ2.

#### *Data Analysis*

To validate the key indicators for employee cyberslacking and cybersecurity posture for the endpoint devices the data collected via the instrument went through the Delphi method, in order to obtain a consensus among the SMEs identified via a well-defined process that includes identifying and rating the indicators. These indicators were used as the basis for measuring employee cyberslacking activity and the cybersecurity posture of the devices accessing organizational resources. The subsequent output was used to answer RQ1 and RQ2, respectively.

#### *Phase Two – Pilot Study*

##### *Data Collection*

Phase two was comprised of a pilot group of 15 participants in order to validate the collection method of this study. The data collection method was a two-step process. The first step was to collect the participants’ demographic data using a Microsoft Forms Survey. Potential participants were recruited via an email sent by the IT administrator of the organization where the data is to be collected. The email contained information regarding the purpose of this study and asked the potential participants if they were willing to participate. The participants could agree to their inclusion in this study by voting “yes” in the email. This response communicated to the IT administrator that the potential participant was willing to participate, at which time the IT administrator responded with a unique participant code and a link to the survey that collected the demographic data.



Once the participants completed the demographic survey collection process, the second step utilized the organization's reporting capabilities to collect usage metrics of productivity software, such as the Microsoft 365 suite of productivity tools, Microsoft Teams, web browser usage, OneDrive, and SharePoint, for the last 90 days. In addition to the productivity software activity metrics, the IT administrator provided data on the computer security posture of the devices used to work remotely. During the same period, the IT administrator used the reporting capabilities of their endpoint management system to provide the values of the computer security posture indicators identified by the SMEs in phase one of this study. Once both sets of data were collected, the IT administrator provided a link to an anonymized Microsoft Excel spreadsheet that contained the data collected. The rows in the anonymized spreadsheet contained the unique user participant IDs and the columns contained the data points collected from the productivity user activity reports and the endpoint management reports.

### *Data Analysis*

The pilot study was used to obtain feedback regarding the validity of (a) the instrument utilized to collect the required demographic information, (b) the defined computer security posture measures, (c) the defined productivity usage measure, and (d) the organization's capability to accurately report the computer security posture and productivity usage measures. This anonymized data was provided to a spreadsheet that contained the unique user participant IDs in the rows. The columns of the spreadsheet will contain the data points collected from both the productivity usage metrics and the computer security posture reports. Microsoft Excel was used to consolidate the resultant data with the demographic data collected via the Microsoft Forms survey. In terms of analysis of data, this study used ANOVA to check for differences based on demographic information collected and the cyberslacking activity score. In

addition, a subsequent ANOVA was used to determine if there were differences based on the demographic information collected and the computer security posture score.

*Phase Three – Main Data Collection and Analysis (R3, RQ4, RQ5, & RQ6)*

*Data Collection*

In phase three, an instrument was distributed via email to 625 potential participants of a higher education based in the United States, in order to attain the intended target of 125 participants, representing a 20% response rate. Similar to phase two of this study, the data collection method for phase three was a two-step process. The first step was to collect the participants' demographic data using a Microsoft Forms survey. Potential participants were recruited via an email sent by the IT administrator of the organization where the data was to be collected. The email contained information regarding the purpose of this study and asked the potential participants if they were willing to participate. The participants can agree to their inclusion in this study by voting "yes" in the email. This response will communicate to the IT administrator that the participant was willing participate, at which time the IT administrator responded with a unique participant code and a link to the survey that will collect the demographic data.

Once all the participants had completed the demographic survey collection process, the second step was to utilize the organization's reporting capabilities to collect usage metrics of productivity software such as Microsoft's 365 suite of productivity tools, Microsoft Teams, web browser usage, OneDrive, and SharePoint, for the last 90 days. In addition to the productivity software activity metrics, the IT administrator provided data on the cyber security posture of the devices used to work remotely. During the same period, the IT administrator used the reporting capabilities of their endpoint management system to provide the values of the computer security

posture indicators identified by the SMEs in phase one of this study. Once both sets of data had been collected, the IT administrator provided a link to an anonymized Microsoft Excel spreadsheet that contained the data collected. The rows in the anonymized spreadsheet contained the unique user participant IDs and the columns contained the data points collected from the productivity user activity reports and the endpoint management reports.

### *Data Analysis*

Like phase two of this study, the anonymized data was provided in a spreadsheet that contained the unique user participant IDs in the rows. The columns of the spreadsheet contained the data points collected from both the productivity usage metrics and the computer security posture reports. Microsoft Excel was used to consolidate the resultant data with the demographic data collected via the Microsoft Forms survey. RQ3 was answered using the cyberslacking score, the computer cybersecurity posture score derived from the data collected and plotted on the developed Remote Worker Cyberslacking Security Risk Taxonomy to demonstrate the employee's positioning. Mertler and Vannatta (2017) described one-way ANOVA as a statistical test that evaluates the mean significant differences between two or more treatments or groups on a dependent variable. To answer RQ4, ANOVA was leveraged to check if there are differences based on (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience of the Dependent Variable (DV), remote workers' cyberslacking activity score. Similarly, to address RQ5 a one-way ANOVA was used to check if there were differences based on (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience of the DV, employees' computer cybersecurity posture index. Lastly, RQ6 utilized the developed taxonomy to determine if demographics such as age, gender, education level, and

years of work experience identify differences in the position of the employees on the developed Remote Worker Cyberslacking Security Risk Taxonomy.

## **Resources**

This research study had human participants and, therefore, requires Institutional Review Board (IRB) approval from both the college and the organization where the data collection will occur. In addition, this study engaged cybersecurity SMEs to validate cyberslacking activity and cybersecurity posture measures via the Delphi method. To increase the participation and commitment of the SMEs to the research study, a \$5 Starbucks gift card was given to each. In phase one, a Microsoft Forms survey was used to collect the data from the SMEs to complete all feedback loops of the Delphi method until a consensus was achieved. Additionally, phase two and phase three used Microsoft Forms surveys to obtain the demographic information required. Productivity usage data and cybersecurity posture data were collected from use the organization's reporting capabilities built into their productivity suite and endpoint management systems, respectively. Once all the data had been collected, this study utilized the SPSS® Statistics™ for statistical analysis.

## **Summary**

This chapter provides an overview of the design and methodology for the experimental field study conducted. This study developed 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 were recruited to identify and validate measures for the computer security posture score. The Delphi method was utilized to validate the key indicators for employee cyberslacking and cybersecurity posture.

Phase two involved collaboration with the identified SMEs to define, develop, and test the proposed Remote Worker Cyberslacking Security Risk Taxonomy. Data was 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 utilized ANOVA to check for differences based on demographic information collected and the cyberslacking activity score. Additionally, a subsequent ANOVA was used to determine if there were differences based on the demographic information collected and the computer security posture score.

Phase three of this study consisted 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 group in phase two, ANOVA was used to check for differences based on demographic information collected and the dependent variables of cyberslacking activity score. In addition, ANOVA was used to check for differences based on demographic information collected and the computer security posture index.

## Chapter 4

### Results

#### **Overview**

This chapter presents the data collection findings from all three phases of this developmental research study as depicted in Figure 2. Phase one of this study collaborated with SMEs to identify and validate the key indicators to derive composite scores for cyberslacking and the computer security posture of the devices. In addition, the phase facilitated the opportunity for SME feedback on the Remote Worker Cyberslacking Security Risk Taxonomy depicted in Figure 1. The second phase, phase two, was the pilot phase where the data collection methodology was tested and validated with 15 participants. Subsequently, the chapter concludes with the results of the main data collection where an analysis was conducted on the cyberslacking and computer security posture indicators and applied to the Remote Worker Cyberslacking Security Risk Taxonomy to assess potential risk by demographic.

#### **Phase One – Subject Matter Experts (SMEs)**

This developmental study asked SMEs to validate productivity values used to measure cyberslacking activity and the values to measure device cybersecurity posture to assess the cybersecurity risk remote workers introduce to an organization. The process of identification and validation of the measures leveraged the Delphi method to obtain anonymous feedback from experts (Okoli & Pawlowski, 2004). The Delphi method was established by the RAND Corporation as “a methodical and interactive research procedure for obtaining the opinion of a panel of independent experts concerning a specific subject” (Skinner et al. 2015, p. 32). The Delphi method is an iterative process that seeks to build consensus among a group of SMEs that

intends to yield agreement on final ratings (Parekh et al., 2018). Sumsion (1998) recommended a 70% SME response rate as acceptable of consensus.

### *Data Collection*

The survey consisted of four distinct sections that were utilized to validate measures for employee cyberslacking (CySI) and the Computer Security Posture (CSP) score of the device being used to access organizational resources. In addition, the survey also served to validate the proposed taxonomy for classifying if an organization's remote workers present a higher risk of cybersecurity threats based on CySI and CSP measures. Questions one through seven of the survey collected demographic information from the SMEs to validate their qualifications, such as years of education level, years of experience, description of their professional role and industry-based certifications. Question eight through eleven of the survey asked the SMEs to evaluate the importance of the cyberslacking and computer security posture measures identified in the literature using a seven-point Likert ranging from (1) "Not at all important" to (7) "Extremely important". Question twelve in the survey, asked the SME to evaluate the proposed taxonomy using the CySI and CSP measures to classify if an organization's remote workers present a higher risk of cybersecurity threats using a seven-point Likert ranging from (1) "Strongly Disagree" to (7) "Strongly Agree". The last question, question thirteen, allowed the SMEs to provide recommendations on how to adjust the Remote Worker Cyberslacking Security Risk Taxonomy depicted in Figure 1. The results of the data collected were used to answer RQ1 and RQ2.

An anonymous Microsoft Forms survey was distributed via email and LinkedIn to approximately 113 information systems and cybersecurity SMEs to attain a total of 20 responses, representing a 20% response rate. The survey yielded a 51% response rate of which 53

cybersecurity and information technology experts participated in the Delphi method from May 2023 to June 2023, which a consensus on the CySI and CSP measures was met, as well as the validation of the Remote Worker Cyberslacking Security Risk Taxonomy. The SMEs that participated in the Delphi method included cybersecurity analysts, cybersecurity engineers, and senior IT. The criteria used to validate the SMEs in this study were education, years of experience in cyber security and industry cybersecurity certifications. Five of the respondents were omitted from participation as they did not meet the criteria set for SMEs, specifically the experience requirement was not met. The remaining N=53 respondents to the survey met the criteria set forth as over 74% of the respondents had one or more industry cybersecurity certifications, 89% of the respondents had more than five years of experience in the cybersecurity and information technology field and 85% of the respondents had a college degree. Table 11 represents the detailed demographic statistics of the SMEs.

**Table 19**

*Descriptive Statistics of the SMEs (N=53)*

<b>Demographic Indicator</b>	<b>Frequency</b>	<b>Percentage</b>
<b>Age</b>		
18-24	1	2%
25 -34	5	9%
35-44	22	42%
45-54	16	30%
55-64	9	17%
<b>Gender</b>		
Male	47	89%
Female	6	11%
<b>Education</b>		
High School	8	15%
Associate Degree	2	4%
Bachelor's Degree	18	34%
Master's Degree	18	34%
Ph.D.	7	13%



**Table 20***Descriptive Statistics of the SMEs (N=53) (continued)*

<b>Demographic Indicator</b>	<b>Frequency</b>	<b>Percentage</b>
<b>Professional Role</b>		
Cybersecurity Analyst	3	6%
Cybersecurity Engineer	10	19%
Cybersecurity Architect	13	25%
Information Security Analyst	1	2%
Network Security Engineer	4	8%
Other	22	42%
<b>Cybersecurity Certifications</b>		
No cybersecurity industry certifications	14	26%
One cybersecurity industry certifications	19	36%
Two cybersecurity industry certifications	7	13%
Three cybersecurity industry certifications	1	2%
More than three cybersecurity industry certifications	12	23%
<b>Experience</b>		
1 to 3 years	4	8%
3 to 5 years	2	4%
6 to 10 years	5	9%
11 to 15 years	9	17%
16 to 20 years	9	17%
Above 20 years	24	45%

*Data Analysis*

The SMEs were asked to evaluate and validate six measures for employee cyberslacking (CySI) based on the research conducted by Ferreira and Du Plessis (2009), Hanaysha (2016), and Gibbs et al. (2021) which focused on time and on-task can be an effective measure of employee productivity as employees who were not engaged in the workplace tended to focus on tasks of lower priority or those not essential to their job function. This study sought to validate the six measures identified in determining the aggregate of time spent on productivity software such as Microsoft's Office 365 suite of productivity tools, Email usage, Microsoft Teams, a web browser, OneDrive, and SharePoint as the indicators for measurement. In addition, the SMEs were asked to evaluate and validate ten measures for computer security posture (CSP) based on the work

conducted by Cain et al., (2018), Such et al., (2019) and Vishwanath et al. (2020) in which proper security controls were identified in order to increase the security of the devices used for accessing an organization's resources. These items include proper patch management for all software on the device, antivirus and malware protection, firewall configuration, and VPNs.

The results of the expert panel indicated that four of the six measures for employee cyberslacking, assessed by the SMEs, met the acceptable rate of consensus of higher than 70% as depicted in Table 12. Specifically, Microsoft's Office 365 suite of productivity tools, Email usage, Microsoft Teams, and web browser usage received a rating of five or higher on the seven-point Likert scale. However, OneDrive usage and SharePoint site usage did not meet the acceptable rate of consensus from the SMEs as their scores were 67% and 60% respectively and therefore will not be used as measures.

**Table 21**

*Productivity measures percentage of agreement (N=53)*

<b>PMID</b>	<b>Indicator</b>	<b>% of Agreement</b>
PM01	Browser usage	83.0%
PM02	Email apps usage	75.5%
PM03	OneDrive for Business usage	64.2%
PM04	Microsoft 365 Apps usage (Word, Excel, PowerPoint)	71.7%
PM05	SharePoint site usage	58.5%
PM06	Microsoft Teams user activity	86.8%

In addition, the results indicated that all the measures of computer security posture assessed by the SMEs achieved a rating of five or higher on the seven-point Likert scale and met an acceptable rate of consensus higher than 70%. The SMEs unanimously agreed that operating system patches and software updates are key measures of the computer security posture as the rate of consensus was 100%. In addition, 96.2% of the SMEs found that Antivirus/Malware detection programs and their respective updates were also important measures to assess the

computer security posture of devices. The complete list of the CSP measures and the SME percentage of agreement are depicted in Table 13.

**Table 22**

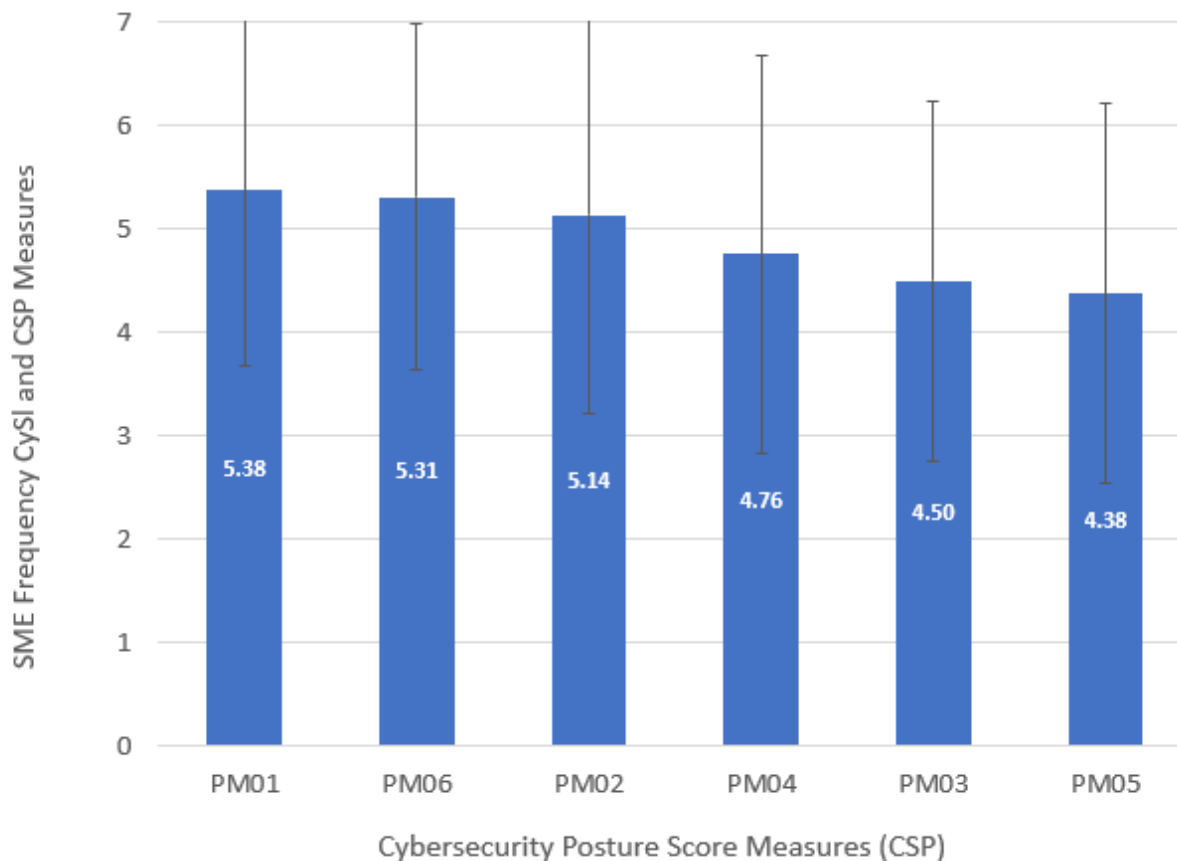
*Computer Security Posture (CSP) measures percentage of agreement (N=53)*

<b>CSPID</b>	<b>Indicator</b>	<b>% of Agreement</b>
CSP01	Operating System Version	92.5%
CSP02	Operating System Patching (systems are up to date)	100%
CSP03	Antivirus/Malware Detection programs	96.2%
CSP04	Antivirus/Malware signature updates	96.2%
CSP05	Software updates	100%
CSP06	Disk encryption enabled	90.6%
CSP07	Firewall enabled	94.3%
CSP08	VPN usage	90.6%
CSP09	Collection of security logs enabled	92.5%
CSP10	End Point Protection	98.1%

In their evaluation of the six measures for employee CySI and the 10 measures for CSP the expert panel was asked to determine the importance of each of these measures. The responses from the SMEs were analyzed using the arithmetic mean and the standard deviation values. The scores reflected the frequency for each CySI and CSP measures, higher scores indicated the more frequent the SMEs indicated the measures to be important. The SMEs (N=53) validated indicators to measure employee productivity ranked according to their arithmetic mean and standard deviation. The validated productivity measures in order of importance are as follows: PM01 (M = 5.38, SD = 1.69), PM06 (M = 5.31, SD = 1.68), PM02 (M = 5.14, SD = 1.92), and PM04 (M = 4.76, SD = 1.93). The SME feedback demonstrated that PM03 (M = 4.50, SD = 1.74) and PM05 (M = 4.38, SD = 1.83) were not validated as important measures of cyberslacking. The results of the validated indicators to measure employee productivity are graphically depicted in Figure 5.

**Figure 5**

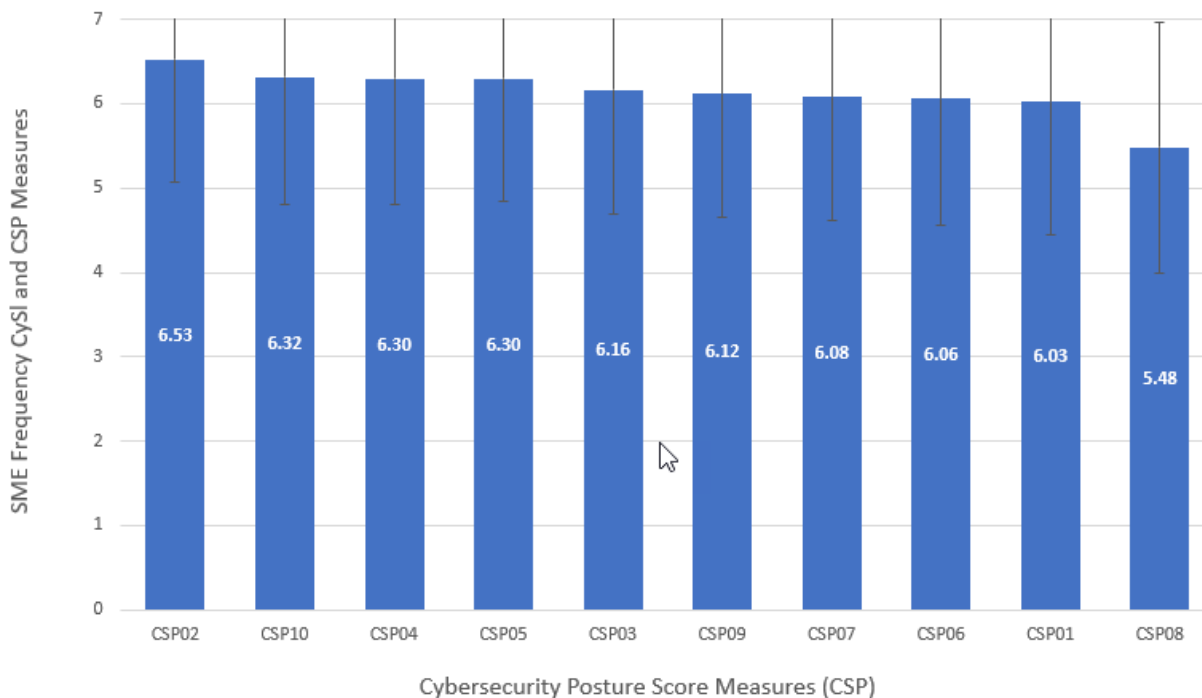
*SME Frequency for Productivity (CySI) Measures (N=53)*



In addition, the SMEs (N=53) validated all the indicators to measure cybersecurity posture score ranked by their arithmetic mean and standard deviation. The cybersecurity posture score measures in order of importance are as follows: CPS02 (M = 6.53, SD = 1.46), CPS10 (M = 6.32, SD = 1.52), CPS04 (M = 6.30, SD = 1.49), CPS05 (M = 6.30, SD = 1.45), CPS03 (M = 6.16, SD = 1.46), CPS09 (M = 6.12, SD = 1.47), CPS07 (M = 6.08, SD = 1.46), CPS06 (M = 6.06, SD = 1.50), CPS01 (M = 6.03, SD = 1.58) and CPS08 (M = 5.48, SD = 1.48). The results of the validated indicators to measure cybersecurity posture score measures are graphically depicted in Figure 6.

**Figure 6**

*SME Frequency for Cybersecurity Posture Score (CSP) Measures (N=53)*



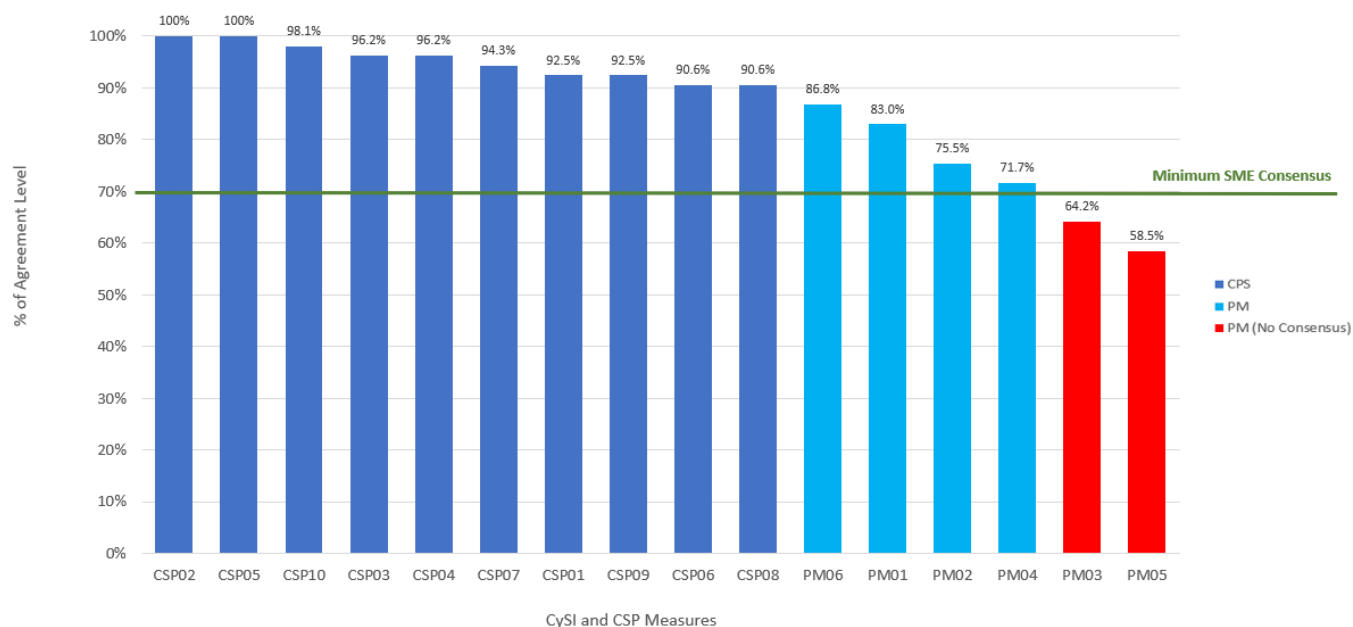
Lastly, the SMEs were asked to evaluate and validate the proposed Remote Worker Cyberslacking Security Risk Taxonomy to assess an organization’s remote workers present a higher risk of cybersecurity threats. The taxonomy will be used to assess the composite scores derived from the SME validated measures for CySI and CSP. The instrument asked the SMEs to validate the taxonomy based on a seven-point Likert scale on the criteria for each of the four quadrants of the taxonomy as described in Figure 1. The results of the expert panel indicated that the taxonomy met the acceptance criteria of consensus having achieved a rating of five or higher by 84% of the SMEs. Taxonomy. To determine the acceptable rate of consensus as a percentage the all the SMEs scores of (5) “Moderately Important”, (6) Very Important, and (7) “Extremely Important” were counted and divided by the total of number of SMEs, which is 53 as depicted in equation 4.

$$\text{Percentage of Agreement} = \frac{\text{Total Number of SMEs score of 5, 6, and 7}}{53} \quad (4)$$

Figure 7 graphically depicts the percentage of agreement for the cybersecurity posture score and cyberslacking measures.

### Figure 7

*Percentage of Consensus for Cyberslacking and Cybersecurity Measures ranked by percentage level of agreement. (N=53)*



This study provides the results of the validation process completed by cybersecurity and IT SMEs on the productivity values used to measure cyberslacking activity and the values to measure device cybersecurity posture to assess the cybersecurity risk remote workers introduce to an organization. According to the SMEs, the specific elements identified to measure cyberslacking that will enable an aggregated score to determine cybersecurity risk are the Microsoft Office 365 suite of productivity tools, Email usage, Microsoft Teams, and web browser usage, answering RQ1. The final SMEs validated elements for measuring cyberslacking

are depicted in Table 1. In addition, the SMEs identified the key factors to assess the device's security level for connecting to the company's data. These are: keeping all software updated, using antivirus and anti-malware tools, setting up the firewall properly, and using VPNs.

**Table 23**

*SMEs validated indicators to measure employee productivity (All Measured in Hours Per Day)*

<b>PMID</b>	<b>Indicator</b>
PM01	Browser usage
PM02	Email apps usage
PM04	Microsoft 365 Apps usage (Word, Excel, PowerPoint)
PM06	Microsoft Teams user activity

The SMEs identified the specific elements to measure the computer cybersecurity posture of the device being used to access corporate resources such as proper patch management for all software on the device, antivirus and malware protection, firewall configuration, and VPNs, answering RQ2. The final SMEs validated elements for measuring the computer security posture score are depicted in Table 14. In addition, this study presented the results from the expert panel on the recommendations with respect to the validity of the Remote Worker Cyberslacking Security Risk Taxonomy to classify the cybersecurity risk that may be posed by employees based on cyberslacking (CySI) and the computer security posture of the remote device (CSP). The SMEs agreed that taxonomy can be used to classify the cybersecurity risk that may be posed by employees based on the measures identified.

**Table 24***SME validated indicators to measure computer security posture*

<b>CSPID</b>	<b>Indicator</b>
CSP01	Operating System Version
CSP02	Operating System Patching (systems are up to date)
CSP03	Antivirus/Malware Detection programs
CSP04	Antivirus/Malware signature updates
CSP05	Software updates
CSP06	Disk encryption enabled
CSP07	Firewall enabled
CSP08	VPN usage
CSP09	Collection of security logs enabled
CSP10	End Point Protection

**Phase Two – Pilot Study***Data Collection*

In phase two of this study, the pilot phase, an email was sent to 50 potential participants containing the link to a Microsoft Forms survey of which 15 participants responded, representing a 30% response rate. The instrument was utilized to collect the demographic information required for this phase of this study. In addition to the demographic data collected, the IT administrator provided a link to an anonymized Microsoft Excel spreadsheet that contained the data collected. The rows in the anonymized spreadsheet contained the unique user participant IDs and the columns contained the data points collected from the productivity user activity reports and the endpoint management reports.

*Data Analysis*

The pilot phase of this study provided feedback on the instrument utilized to collect demographic data that was clear and concise. All surveys were submitted complete with no omissions to any of the data points. The anonymized Microsoft Excel spreadsheet containing the



productivity user activity reports and endpoint management was also complete with no data validation issues. This phase did provide a change to how the value of the normalization coefficient,  $j$ , for the value of CSP, is calculated. Using the indicators of computer security posture in Equation 2, the determination was made that the  $j$  coefficient was not being derived correctly and the calculations were to be derived by dividing one by the sum of the maximum value of each computer security posture indicator ( $\text{MaxCSP}_i$ ), depicted in Table 9, and multiplied by its respective weight. This is represented by Equation 3.

### **Phase Three – Main Data Collection**

#### *Data Collection*

In phase three, an instrument was distributed via email to 625 potential participants of a higher education based in the United States, of which 138 participants responded, representing a 22% response rate. All 138 participants were used as there were no validation errors with the user activity reports provided by the IT administrator as part of the pre-analysis data screening.

#### *Data Analysis*

Upon completion of the pre-analysis data screening, the data of the remaining 138 participants were analyzed beginning with the demographic data. The participants of this study were faculty members, administrative staff, technical staff, support staff, and research staff that work remotely at least part of the week. All the respondents to the survey met the criteria set forth as the targeted group of 625 participants identified by the IT administrator work from home at least 20% of the time. The demographic data demonstrated that 52.17% of the participants were male, 46.38 were female and 1.45% preferred not to say. In addition, 82.61% of the participants were 35 years of age or older, and 97.83% had a college degree. With respect to job roles, 33.33% of the participants were faculty members, while the remaining 66.77% were a

combination of administrative, support, or technical staff. In terms of the respondents who had one or more industry cybersecurity certifications, 90% of the respondents had more than one year of experience in the cybersecurity and information technology field and 85% of the respondents had a college degree. Most of the participants, 92.03%, had 11 years or more of experience, while the remaining 7.97% had five years or less. The distribution of job level was split between individual contributors, 52.90%, and the remaining 47.10% were in an executive or supervisory role. Table 16 represents the detailed demographic statistics of the participants. Considering the demographic data of the target organization, these findings suggest that the overall sample of the employees is well represented.

**Table 25**

*Descriptive statistics of the participants (N=138)*

<b>Demographic Indicator</b>	<b>Frequency</b>	<b>Percentage</b>
<b>Age</b>		
18-24	3	2%
25 -34	19	14%
35-44	32	23%
45-54	49	36%
55-64	25	18%
65-74	10	7%
<b>Gender</b>		
Male	74	54%
Female	64	46%
<b>Education</b>		
High School	8	6%
Associate Degree	6	4%
Bachelor's Degree	31	31%
Master's Degree	48	49%
Ph.D.	56	44%

**Table 26***Descriptive statistics of the participants (N=138) (continued)*

<b>Demographic Indicator</b>	<b>Frequency</b>	<b>Percentage</b>
<b>Job Role</b>		
Faculty Member	30	22%
Administrative Staff	56	41%
Technical Staff	33	24%
Other	19	14%
<b>Job Level</b>		
Individual Contributor	70	51%
Supervisor	19	14%
Middle Manager	19	14%
Senior Manager	14	10%
Executive Level / C-Suite	16	12%
<b>Experience</b>		
1 year or less	1	1%
1 to 3 years	4	3%
3 to 5 years	7	5%
6 to 10 years	18	13%
11 to 15 years	24	17%
16 to 20 years	25	18%
Above 20 years	59	43%

To answer RQ3, Remote Worker Cyberslacking Security Risk Taxonomy was developed to determine if an organization's remote workers introduce additional cybersecurity threats using the measure of CySI and CSP. The measures for CySI and CSP were normalized to a scale between 0 and 100 for consistency as depicted in Figure 2. The taxonomy for Remote Worker Cyberslacking Security Risk consists of four quadrants: Q1 (Very High Risk), Q2 (Moderate Risk), Q3 (High Risk), and Q4 (Low Risk). The scores for CySI indicated that overall cyberslacking activity is low as indicated by a positive skew, .38 ( $M = 33.16$ ,  $SD = 20.18$ ,  $N = 138$ ). Similarly, the scores for CSP indicated devices being utilized were secure as demonstrated by a positive skew, .10 ( $M = 70.35.16$ ,  $SD = 12.78$ ,  $N = 138$ ). Table 17 contains the full construct statistics for CySI and CSP.

**Table 27***Construct Statistics (N=138)*

<b>Item</b>	<b>CySI</b>	<b>CSP</b>
N	138	138
Mean	33.16	70.35
Std. Deviation	20.18	12.78
Skewness	.38	.10
Minimum	0	46.17
Maximum	86.67	86.37

Figure 8 shows the scatter plot of the two constructs, CySI and CSP derived from the data provided by the IT administrator and using the equations defined to develop the respective scores. Most of the participant scores, 85%, are found in Q4 – Low Risk, classifying most remote workers in the organization as demonstrating a high computer security posture and a low cyberslacking score, thus indicating the participants of this study did not introduce additional cybersecurity threats to the organization.

The distribution of the participants in the various quadrants is depicted in Figure 8, Q1 – Very High Risk has the least number of participants with a total of three, and the highest number of participants in Q4 – Low Risk with a total of 117 participants. Q1 of the Remote Worker Cyberslacking Security Risk taxonomy indicates that 2% of the participants pose the highest risk to the organization as their devices have a lower cybersecurity posture and their opportunity for cyberslacking is higher. Conversely, Q4 of the Remote Worker Cyberslacking Security Risk taxonomy indicates that 85 of the participants pose the lowest risk to the organization as their devices have a higher cybersecurity posture and their opportunity for cyberslacking is lower. A full description of the distribution of participants is detailed in Table 18.

**Figure 8**

*Remote Worker Cyberslacking Security Risk Scatter Plot of CySI and CSP Scores (N=138)*

**Table 28**

*Remote Worker Cyberslacking Security Risk – Quadrant distribution (N=138)*

<b>Quadrant</b>	<b>Frequency</b>	<b>Percent</b>
Q1 – Very High Risk	3	2%
Q2 – Moderate Risk	13	9%
Q3 – High Risk	5	4%
Q4 – Low Risk	117	85%

#### One-way Analysis of Variance ANOVA

To answer RQ4, an ANOVA was performed to determine if there are differences based on (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience of the Dependent Variable (DV), remote worker's cyberslacking activity score (CySI). The ANOVA for job level was significant  $F = 2.464$ ,  $p = .048$  and suggests that CySI scores differed by job level due to a p-value that is less than .05. The results of the one-way

ANOVA did not demonstrate significance for (a) age, (b) gender, (c) education level, (d) job level, or (e) years of work experience, suggesting that there is no difference in CySI scores.

**Table 29**

*ANOVA results for CySI (N=138)*

<b>Demographic Indicator</b>	<b>Sum of Squares</b>	<b>df</b>	<b>Mean Square</b>	<b>F-Value</b>	<b>Significance</b>
Age	1151.463	5	230.293	.552	.736
Gender	537.721	2	537.721	1.314	.254
Education	2616.959	4	654.240	1.624	.172
Job Role	1916.480	3	638.827	1.577	.198
Job Level	3875.981	4	968.995	2.464	<b>.048*</b>
Experience	2786.991	6	464.498	1.140	.343

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

Similarly, to address RQ5 a one-way ANOVA was performed to determine check if there were differences based on (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience of the DV, employees' computer cybersecurity posture index. The results of the one-way ANOVA did not demonstrate significance for (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience, suggesting that there is no difference in CSP scores.

**Table 30**

*ANOVA results for CSP (N=138)*

<b>Demographic Indicator</b>	<b>Sum of Squares</b>	<b>df</b>	<b>Mean Square</b>	<b>F-Value</b>	<b>Significance</b>
Age	115.709	5	231.142	1.428	.218
Gender	80.627	2	80.627	.489	.996
Education	420.633	4	105.158	.633	.640
Job Role	697.719	3	232.573	1.428	.237
Job Level	261.507	4	65.377	.391	.815
Experience	867.412	6	144.869	.875	.516

\* -  $p < .05$ , \*\* -  $p < .01$ , \*\*\* -  $p < .001$

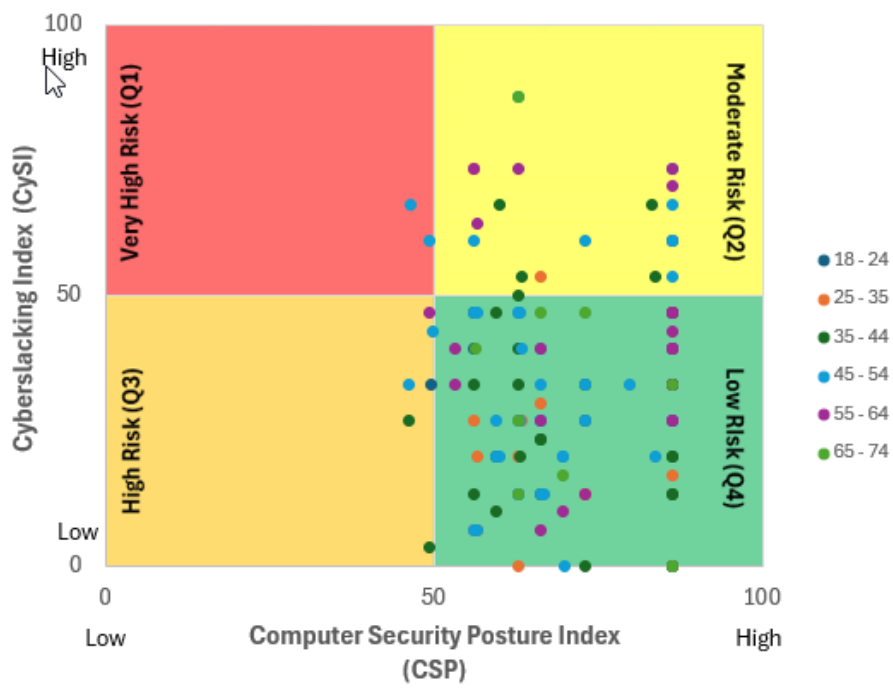
To address RQ6, the taxonomy developed was utilized to determine if there were any differences in a participant's position in the Remote Worker Cyberslacking Security Risk Taxonomy based on the demographic indicators of (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience.

#### *Age Analysis via Taxonomy*

This study explored distinct patterns by analyzing cross-tabulated data between the quadrants of the Remote Worker Cyberslacking Security Risk Taxonomy and the demographics indicator of age. As shown in Figure 9, the age groups were predominately concentrated in Q4, Low Risk, indicating that all participants regardless of age had low CySI and CSP scores. This is consistent with the overall scores for CySI and CSP as depicted in Figure 8, the primary taxonomy, suggesting that the participants did not pose additional cybersecurity risk to the organization. Applying the taxonomy to the means of the aggregated construct scores based on age, depicted in Figure 10, demonstrated that both the 18 to 24 and 25 to 35-year-olds had lower CySI scores than the other age groups. In addition, although 55 to 65-year-olds had higher CSP scores, they also had higher CySI scores than the other groups. Lastly, the 18 to 24-year-old group had lower scores in both CySI and CSP than the other age groups. Thus, suggesting that this age group could pose a moderate risk to the organization due to their lower CSP scores.

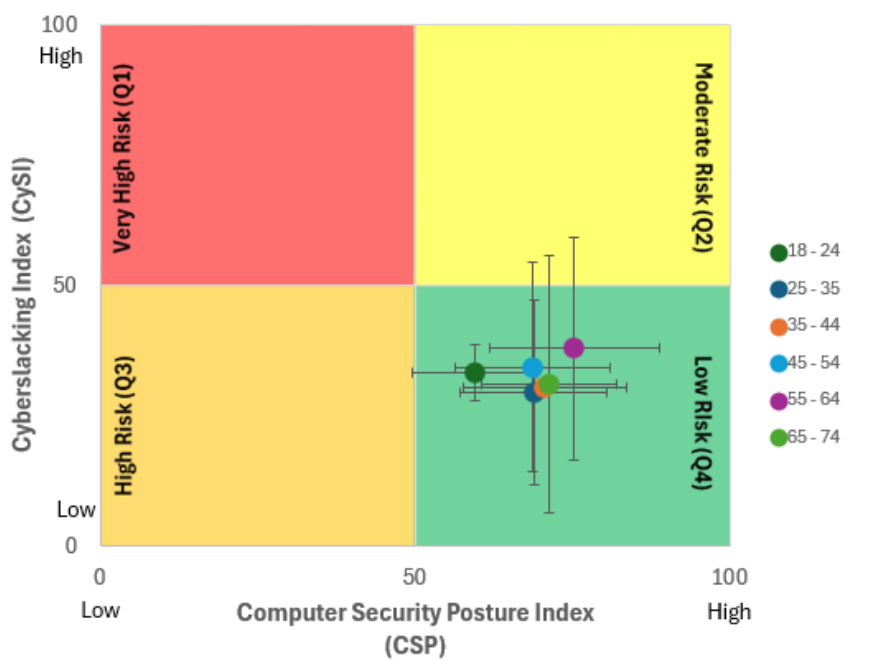
**Figure 9**

*Remote Worker Cyberslacking Security Risk Scatter by Age (N=138)*



**Figure 10**

*Means and Standard Deviation of Aggregated Construct Scores Based on Age (N=138)*



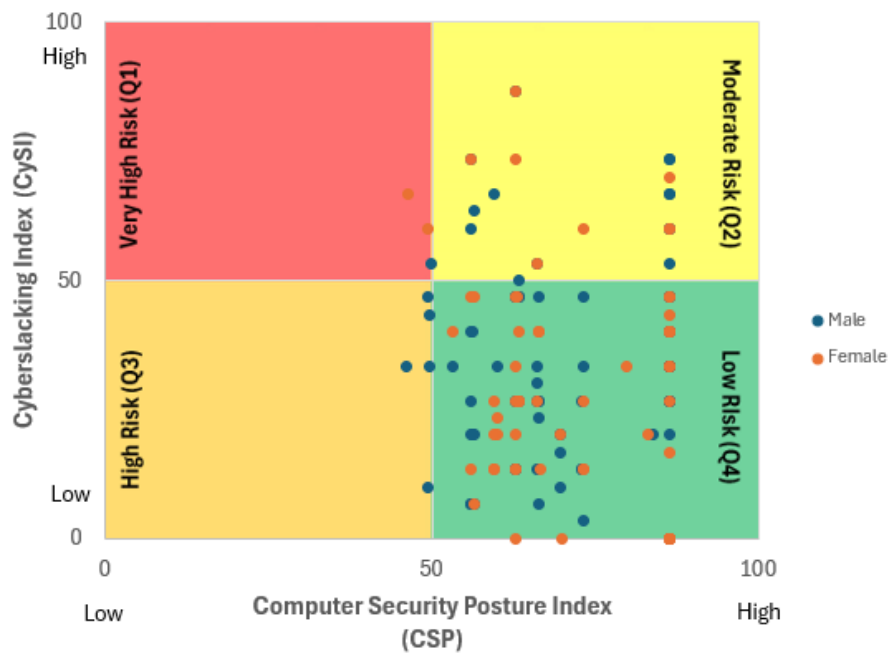


### *Gender Analysis via Taxonomy*

This study also explored distinct patterns by analyzing cross-tabulated data between the quadrants of the Remote Worker Cyberslacking Security Risk Taxonomy and the demographics indicator of gender. As shown in Figure 11, the gender group, consisting of males and females, was predominately concentrated in Q4, Low Risk, indicating that all participants regardless of age had low CySI and CSP scores. This is consistent with the overall scores for CySI and CSP as depicted in Figure 8, the primary taxonomy, suggesting that the participants did not pose additional cybersecurity risk to the organization. Applying the taxonomy to the means of the aggregated construct scores based on gender, depicted in Figure 12, demonstrated that females had lower CySI and CSP scores than males. Thus, suggesting females are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy.

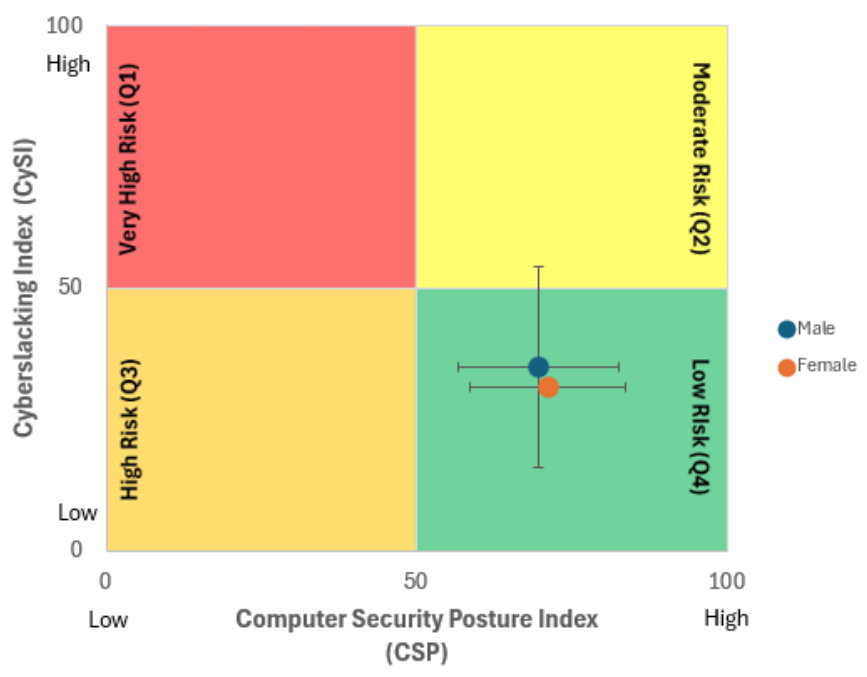
**Figure 11**

*Remote Worker Cyberslacking Security Risk Scatter by Gender (N=138)*



**Figure 12**

*Means and Standard Deviation of Aggregated Construct Scores Based on Age (N=138)*



### *Education Analysis via Taxonomy*

In addition, this study explored distinct patterns by analyzing cross-tabulated data between the quadrants of the Remote Worker Cyberslacking Security Risk Taxonomy and the demographics indicator of education. As shown in Figure 13, the education demographic was predominately concentrated in Q4, Low Risk, indicating that all participants regardless of gender had low CySI and CSP scores. This is consistent with the overall scores for CySI and CSP as depicted in Figure 8, the primary taxonomy, suggesting that the participants did not pose additional cybersecurity risk to the organization. Applying the taxonomy to the means of the aggregated construct scores based on gender, depicted in Figure 14, demonstrated that the participant with only a high school diploma had the lowest CySI scores, conversely, those participants with an Associate's degree had the highest CySI scores than the other education groups. This suggests participants with a high school diploma are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy.

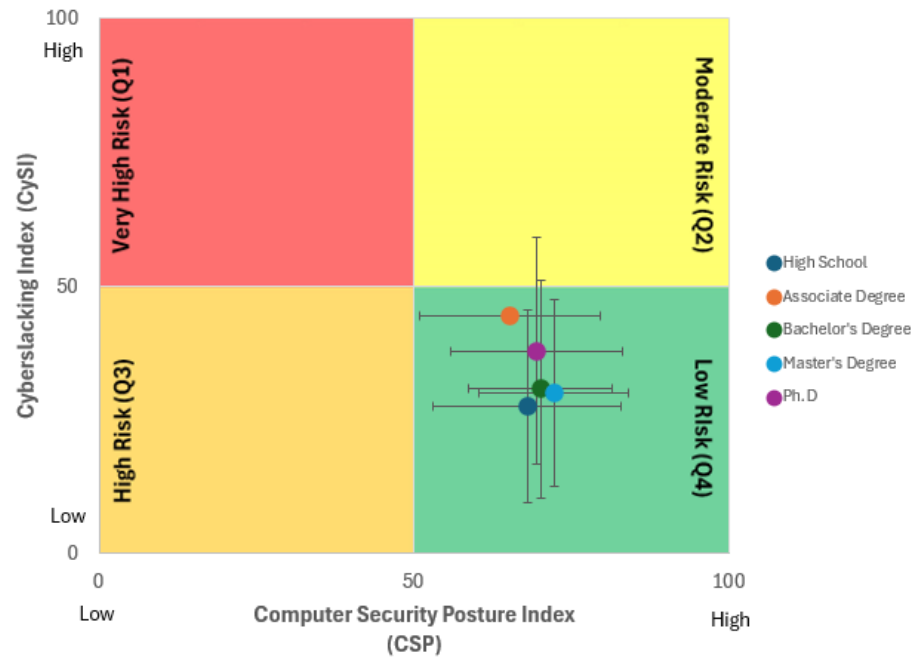
**Figure 13**

*Remote Worker Cyberslacking Security Risk Scatter by Education (N=138)*



**Figure 14**

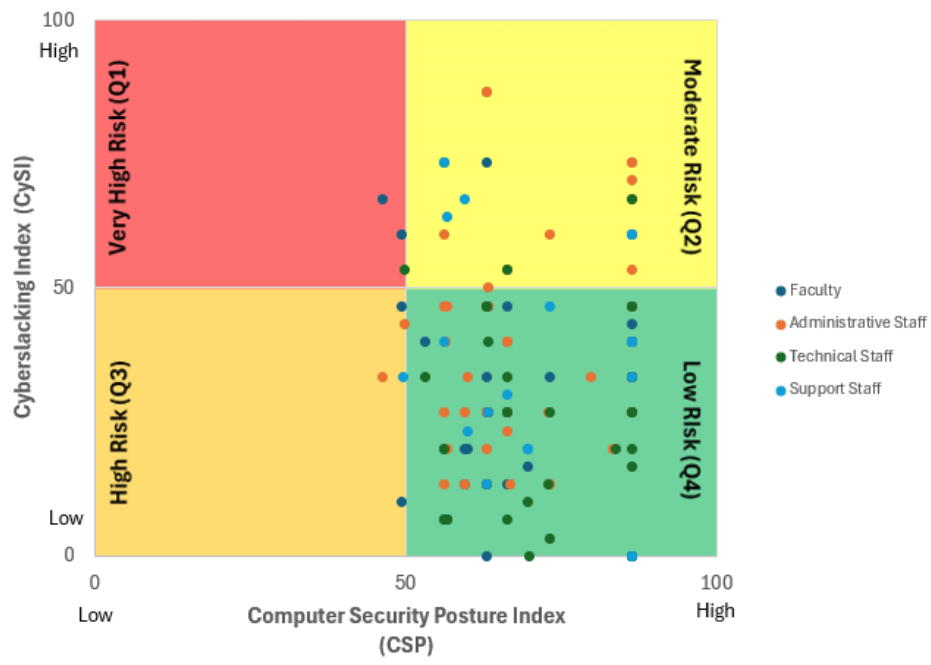
*Means and Standard Deviation of Aggregated Construct Scores Based on Education (N=138)*



This study explored distinct patterns by analyzing cross-tabulated data between the quadrants of the Remote Worker Cyberslacking Security Risk Taxonomy and the demographics indicator of job role was also conducted. As shown in Figure 15, the job role demographic was concentrated in Q4, Low Risk, indicating that all participants regardless of job role had low CySI and CSP scores. This is consistent with the overall scores for CySI and CSP as depicted in Figure 8, the primary taxonomy, suggesting that the participants did not pose additional cybersecurity risk to the organization. Applying the taxonomy to the means of the aggregated construct scores based on job role, depicted in Figure 16, demonstrated that support staff and administrative staff had higher CySI scores than faculty and technical staff. In addition, the taxonomy depicted that technical staff had the highest CSP scores and lowest CySI scores. This suggests participants in technical roles are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy.

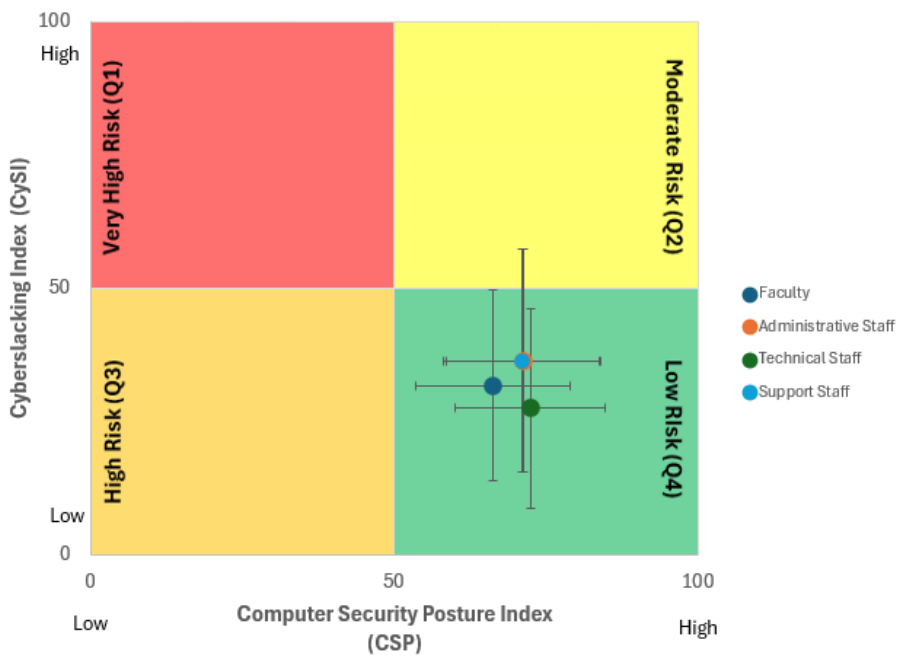
**Figure 15**

*Remote Worker Cyberslacking Security Risk Scatter by Job Role (N=138)*



**Figure 16**

*Means and Standard Deviation of Aggregated Construct Scores Based on Job Role (N=138)*



### *Job Level Analysis via Taxonomy*

Subsequently, this study explored distinct patterns by analyzing cross-tabulated data between the quadrants of the Remote Worker Cyberslacking Security Risk Taxonomy and the demographics indicator of job level. As shown in Figure 17, the job level demographic was concentrated in Q4, Low Risk, indicating that all participants regardless of job level had low CySI and CSP scores. This is consistent with the overall scores for CySI and CSP as depicted in Figure 8, the primary taxonomy, suggesting that the participants did not pose additional cybersecurity risk to the organization. Applying the taxonomy to the means of the aggregated construct scores based on job level, depicted in Figure 18, demonstrated that supervisors had the lowest CySI and CSP scores than the other job levels. In addition, the taxonomy depicted middle managers had the highest CSP scores and lowest CySI scores. Thus, suggesting participants in the middle managers category are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy.

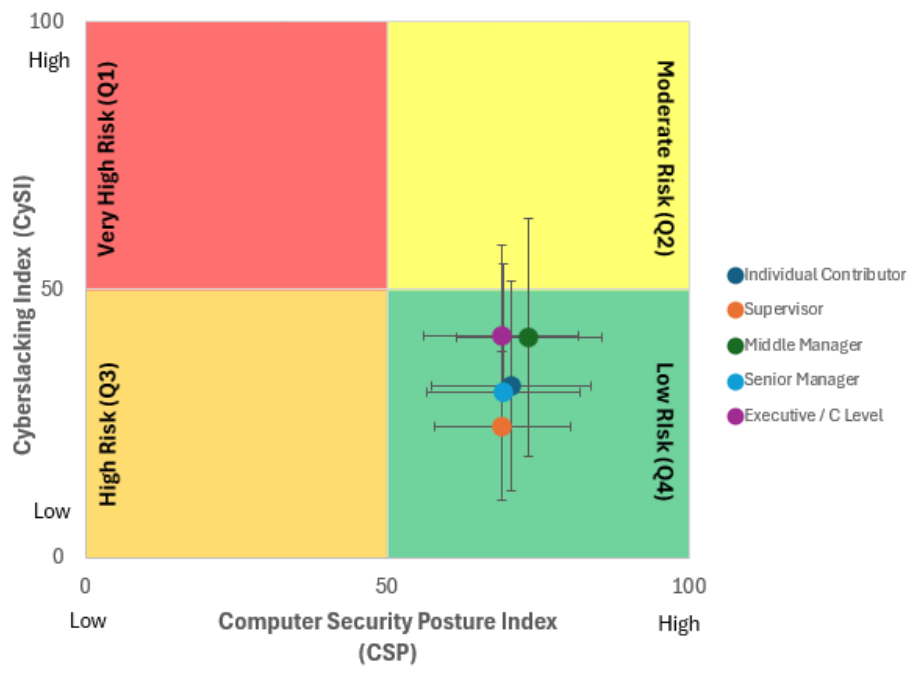
**Figure 17**

*Remote Worker Cyberslacking Security Risk Scatter by Job Level (N=138)*



**Figure 18**

*Means and Standard Deviation of the Aggregated Construct Scores Based on Job Level (N=138)*



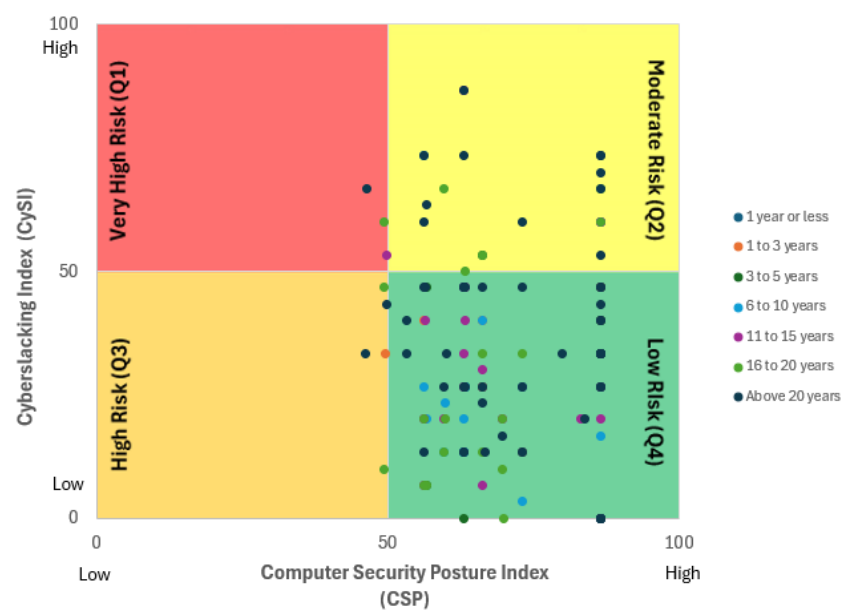


### *Experience Analysis via Taxonomy*

Lastly, this study explored distinct patterns by analyzing cross-tabulated data between the quadrants of the Remote Worker Cyberslacking Security Risk Taxonomy and the demographics indicator of experience. As shown in Figure 19, it was predominately concentrated in Q4, Low Risk, indicating that all participants regardless of job level had low CySI and CSP scores. This is consistent with the overall scores for CySI and CSP as depicted in Figure 8, the primary taxonomy, suggesting that the participants did not pose additional cybersecurity risk to the organization. Applying the taxonomy to the means of the aggregated construct scores based on experience, depicted in Figure 20, demonstrated that participants with less than 1-3 years of experience had the highest CySI scores yet had the lowest CSP score. This suggests participants in this experience range are more likely to pose a risk to the organization due to their higher CySI scores and lower CSP scores. Participants with 3-5 years of experience had the lowest CySI scores. In addition, the taxonomy depicted those participants with 1 year or less and above 20 years of experience had the highest CSP scores. Thus, suggesting participants with over 20 years of experience are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy.

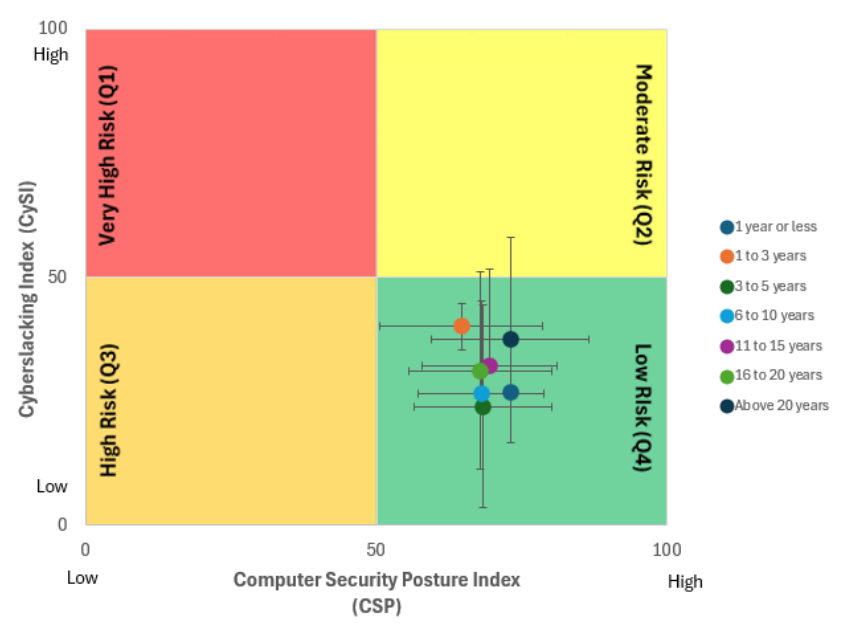
**Figure 19**

*Remote Worker Cyberslacking Security Risk Scatter by Experience (N=138)*



**Figure 20**

*Means and Standard Deviation of Aggregated Construct Scores Based on Experience (N=138)*



## Summary

The results of the data collection and the data analysis conducted were presented in phases. In phase one of this study, in collaboration with SMEs, the Delphi method was used to answer RQ1 and RQ2. Phase two, the pilot phase, was conducted to verify and validate the collection and data processing method of this study. Phase three, the main data collection phase, was used to address RQ3, RQ4, RQ5, and RQ6.

Phase one of this research study validated the measures for employee cyberslacking and the computer security posture score of the device being used to access organizational resources using the Delphi method. The result of the expert panel indicated that four of the six measures for employee cyberslacking, assessed by the SMEs, met the acceptable rate of consensus. The SMEs validated measures for CySI are Microsoft's Office 365 suite of productivity tools, Email usage, Microsoft Teams, and web browser usage. In addition, the results in phase one indicated that all the measures of computer security posture assessed by the SMEs met an acceptable rate of consensus. The SMEs validated measures for CPS are operating system versions, operating system patching, antivirus/malware detection programs, antivirus/malware signature updates, Software updates, Disk encryption enabled, firewall enabled, VPN usage, collection of security logs enabled, and endpoint protection. Phase two of this study was used to ensure that the collection methodology and the formulas set forth to determine CySI and CSP scores were valid.

The results of phase three, the main collection phase, utilized the taxonomy developed to determine if there are differences in remote workers' cyberslacking activity score based on their (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience. In addition, the taxonomy developed was used to determine if there are differences in employees' workers computer security posture scores based on their (a) age, (b) gender, (c) education level, (d) job role, (e) job level, and (f) years of work experience. The majority of the

participant scores were classified as low risk as they were primarily in the fourth quadrant of the taxonomy. This indicated that most remote workers who participated in this study demonstrated a high computer security posture and a low cyberslacking score, thus would not introduce additional cybersecurity threats to the organization.

## Chapter 5

### Conclusions, Discussions, Implications, Recommendations, and Summary

#### Conclusions

Eze et al. (2024) described the effects of cyberslacking to be detrimental to organizations not only in terms of productivity loss but also susceptible to security breaches. In addition, Karthikeyan and Thomas (2017) posit that cyberslacking could cost organizations billions of dollars due to the associated costs such as loss in productivity, security issues, and legal proceedings. Cyberslacking has been researched extensively within the confines of the traditional workplace setting, an area where additional research is needed is hybrid and remote work structures and the propensity of employees to engage in cyberslacking activities during work hours (Lim & Teo, 2024). Therefore, the main goal of this research study was to develop, validate, and empirically test a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats. This study measured workers' potential engagement in cyberslacking, and the computer security posture of the remote devices used to access the organization's resources. To achieve the main goal of this study, a three-phased developmental approach in developing the Remote Worker Cyberslacking Security Risk Taxonomy to assess remote workers' potential risk to the organization. In the first phase, phase one, the Delphi method was used to validate measures for employee cyberslacking and the computer security posture score of the device being used to access organizational resources. This phase sought the consensus of the SMEs on the indicators that would be used to derive a composite score for both CySI and CSP. This phase also sought consensus from the SMEs on the Remote Worker Cyberslacking Security Risk Taxonomy. The second phase of this study, phase two, conducted a small pilot to validate the collection methodology as well as the process used to derive the composite score for both

CySI and CSP. The last phase of this study, phase three, was the main data collection and analysis phase concluded with using the developed Remote Worker Cyberslacking Security Risk Taxonomy to assess the participants of this study to determine if they would introduce additional cybersecurity threats to the organization.

## **Discussions**

In phase one, this study collaborated with SMEs to validate indicators for measuring CySI and the CSP that were derived from the literature. In addition, the SMEs were also asked to validate the Remote Worker Cyberslacking Security Risk Taxonomy. After one round of the Delphi method the SMEs reached a consensus on four of the six indicators to measure CySI as well as all 10 of the indicators to measure CSP. Phase two of this study was conducted to ensure the validity of (a) the instrument utilized to collect the required demographic information, (b) the defined computer security posture measures, (c) the defined productivity usage measure, and (d) the organization's capability to accurately report the computer security posture and productivity usage measures. In addition, this phase provided the ability to validate the data analytics process that would be used for the main data collection.

In phase three of this study, statistical analysis was used, specifically a one-way ANOVA to check for differences based on demographic information collected and the cyberslacking activity score. The results of the one-way ANOVA demonstrated a significance for the job role, suggesting that there is a difference in CySI scores for this demographic. Conversely, the ANOVA did not demonstrate significance for (a) age, (b) gender, (c) education level, (d) job level, or (e) years of work experience, suggesting that there is no difference in CySI scores for these demographics. A subsequent one-way ANOVA was used to check for differences based on demographic information collected and the computer security posture score. The results of the one-way ANOVA did not demonstrate significance for (a) age, (b) gender, (c) education level,

(d) job role, (e) job level, and (f) years of work experience, suggesting that there is no difference in CSP scores for the demographics tested.

In addition to the one-way ANOVA analysis conducted, the SMEs validated Remote Worker Cyberslacking Security Risk Taxonomy was used to plot the two constructs, CySI and CSP, derived from the data provided by the IT administrator and using the equations defined to develop the respective scores. The results demonstrated that while the participants were predominately classified as “Low Risk” using the taxonomy there were specific demographic groups that could pose a risk to the organization as a result of their composite CySI and CSP scores. For example, the taxonomy depicted middle managers had the highest CSP scores and lowest CySI scores. Thus, suggesting participants categorized as middle managers are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy. Additionally, the taxonomy depicted that technical staff had the highest CSP scores and lowest CySI scores. These results suggest participants in technical roles are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy. In terms of experience the results showed that participants with 1 year or less and above 20 years of experience had the highest CSP scores. Thus, participants with over 20 years of experience are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy. The results depicted for education demonstrated that the participant with only a high school diploma had the lowest CySI scores, conversely, those participants with an associate degree had the highest CySI scores than the other education groups. This suggests participants with a high school diploma are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in

Q4 - Low Risk of the taxonomy. In reviewing the results for gender, the taxonomy depicted females had lower CySI and CSP scores than males. Thus, suggesting females are less likely to pose a risk to the organization due to their lower CySI and higher CSP scores and are predominantly in Q4 - Low Risk of the taxonomy. Lastly, in reviewing the results for age, the results demonstrated that both the 18 to 24 and 25 to 35-year-olds had lower CySI scores than the other age groups. In addition, although 55 to 65-year-olds had higher CSP scores, they also had higher CySI scores than the other groups. Lastly, the 18 to 24-year-old group had lower scores in both CySI and CSP than the other age groups. Thus, suggesting that this age group could pose a moderate risk to the organization due to their lower CSP scores.

### **Implications**

There are several implications for professional practice and research provided by this study. From a professional practice perspective, an organization can use the SMEs' validated measures to understand the potential risks introduced by their remote workers. From a research perspective, this study contributes to the overall body of work for IS studies, cybersecurity, productivity, and remote work. In addition, this study can be used to further the development of theoretical foundations and frameworks to contribute to the body of knowledge.

As the adoption of remote work continues organizations will need to develop methodologies to mitigate the risks introduced by workers in non-traditional workspaces. This study provides organizations with a taxonomy to help assess and mitigate the cybersecurity risk posed by remote workers who engage in cyberslacking. Using the taxonomy cybersecurity professionals of organizations can evaluate the risk level of remote workers in an organization using the indicators of CySI and CSP as validated by SMEs. This can be used as a benchmarking tool based on SMEs' defined metrics from application usage and cybersecurity posture indicators to provide composite scores that would allow for a comparison. The results of this analysis can



be leveraged by organizations to mitigate potential deficiencies in computer cybersecurity posture on remote worker devices, cybersecurity awareness training, and policy changes.

From a theoretical perspective, several research studies have employed the Theory of Planned Behavior (TPB) to explore whether an employee's attitude and/or internet addiction influence their likelihood of engaging in cyberslacking. Galletta and Polak (2003), Jamaluddin et al. (2015), and Askew et al. (2014) have utilized TPB to delve into employees' intentions behind cyberslacking and to identify the underlying factors driving these behaviors. This study expands the body of knowledge by adapting a theory used in the field of criminology, Routine Activity Theory, to provide insight into the potential risk introduced by remote workers who may have the opportunity to engage in cyberslacking activities. This provides an opportunity to expand the body of knowledge using a different foundational theory.

### **Recommendations**

The participants of this study included SMEs (N=53) and remote workers (N=138) from a large four-year educational institution in the northeastern part of the U.S. Although the goals set forth by this study were met, it did not account for users who may have been multitasking or using multiple productivity products collectively during the data collection. Another area of focus that should be explored is the use of portals and web-based versions of productivity tools. With the increased availability of features in web-based versions of Microsoft's productivity suite, organizations are less inclined to install the full version of the software on the device being leveraged by the users. While telemetry is being collected for these web-based products, there is still feature parity that needs to be accounted for when measuring the usage of these products in this manner. In addition to using web-based portals and applications, this study did not monitor overall web usage, therefore delineation of using the web browser for personal use was not always captured, future studies should incorporate data from web proxies and other web traffic

monitoring tools to determine the time spent in a web browser that is not business related. This study looked at information workers who primarily used the Microsoft Office Suite and Microsoft Teams, it should be noted that expanding this study to collect usage data that encompasses other business applications used by the organization to conduct daily functions would enhance this study. The organization that participated in this study primarily used the Microsoft Windows operating system; future studies should look to expand this to other operating systems. This study should be conducted in other organizations outside of an academic setting such as corporate enterprise environments, nonprofit environments as well organizations that are based outside of the U.S. to enhance generality.

### **Summary**

The research problem this study addressed was the identification and classification of remote workers engaged in cyberslacking and the potential cybersecurity risks to which they expose their organizations, such as malware, spyware infection, or security breaches (Ozler & Polat, 2012; Vernon-Bido et al., 2018). The main goal of developing, validating, and empirically testing a taxonomy to assess an organization's remote workers' risk level of cybersecurity threats has been addressed in this study. This was completed by using a three-phased developmental approach, where in phase one the literature and SMEs feedback were used to identify key indicators by which cyberslacking and computer security posture can be measured. The SMEs participated in one round of the Delphi method in order to reach a consensus on the measures for CySI and CSP. This phase was used to answer the first two research questions of this study:

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 organizational resources?

The second phase of this study consisted of conducting a pilot with a small set of participants, N=15, to validate the data collection and analysis methods before moving to the primary data collection stage of this study as recommended by van Teijlingen and Hundley (2002). This pilot did provide a change to how the value of the normalization coefficient,  $j$ , for the value of CSP, is calculated. As it was determined there was an error in the formula for calculating the weights for CSP, this was addressed by adding Equation 3.

The last phase of this study encompassed a larger sample size of participants, N=138, where Microsoft Excel and SPSS were utilized to analyze the collected data points from the three distinct data sources, specifically the demographic survey, the endpoint management system data, and the cyberslacking measures identified by the SMEs in phase one. To answer RQ3, the data points for cyberslacking measures were used as inputs to Equation 1 to calculate the CySI score for each participant. Similarly, the data points from the endpoint management system were used as inputs to Equation 2 and Equation 3 to calculate the CSP scores. Using the scores for CySI and CSP, SPSS was used to complete a one-way ANOVA to answer RQ4 and RQ5. Lastly, the results of the aggregated data of CySI and CSP and the corresponding analytics were visualized using the Remote Worker Cyberslacking Security Risk Taxonomy that was developed to answer RQ6. The main data collection and analysis in phase three was used to answer the remaining research questions:

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 research study provides visibility into the potential security risks posed by remote workers who could be engaging in cyberslacking activities, contributing to the larger cybersecurity field, and providing a methodology to classify the level of risk remote workers could pose to the organization. The identification of key indicators to measure CySI and CSP using the Delphi method provides an opportunity for future research in this area. In addition to the SMEs' identified metrics, the research provides a taxonomy, the Remote Worker Cyberslacking Security Risk Taxonomy, that can function as a classification tool for the risk level that may be posed by remote workers in the organization. The data analysis and classifications the taxonomy provide allows organizations to address potential deficiencies in computer cybersecurity posture for remote worker devices, enhance cybersecurity awareness training, and implement necessary policy changes.

## Appendix A

### Institutional Review Board Approval Letter



**INSTITUTIONAL REVIEW BOARD**  
3301 College Avenue  
Fort Lauderdale, Florida 33314-7796  
PHONE: (954) 262-5369

#### MEMORANDUM

**To:** Ariel Luna  
College of Engineering and Computing

**From:** Ling Wang, Ph.D.  
College Representative, College of Engineering and Computing

**Date:** March 14, 2023

**Subject:** IRB Exempt Initial Approval Memo

**TITLE:** Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture  
to Assess Organizational Cybersecurity Risks– NSU IRB Protocol Number 2023-77

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **March 14, 2023**. You may proceed with your study.

*NOTE: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.*

**Level of Review:** Exempt

**Type of Approval:** Initial Approval

**Exempt Review Category:** Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies

**Annual Status of Research Update:** You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm*.

**Changes:** Any changes in the study (e.g., procedures, consent forms, investigators, etc.) must be approved by the IRB prior to implementation using the *Amendment xForm*.



**INSTITUTIONAL REVIEW BOARD**  
3301 College Avenue  
Fort Lauderdale, Florida 33314-7796  
PHONE: (954) 262-5369

**Post-Approval Monitoring:** The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

**Final Report:** You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

**Translated Documents:** No

***Retain this document in your IRB correspondence file.***

CC: Ling Wang, Ph.D.

Yair Levy, Ph.D.

## Appendix B

### Queen's College SRRC Board Approval

---

**From:** [QNS qcinreoie](#)  
**Sent:** Friday, April 21, 2023 7:39 PM  
**To:** [Ariel Luna](#)  
**Cc:** [Troy Hahn](#); [Peter Chiasera](#); [Yongwu Rong](#); [Paul Kran](#)  
**Subject:** Re: Ariel Luna SRRC Request

Dear Ariel,

Thank you for the clarifications. Regarding CUNY IRB approval, you may learn more about the process for that here: <https://www.qc.cuny.edu/academics/orc/>.

For SRRC approval, we need only to see that your study has IRB approval at your institution and that the study poses no risks to potential participants. Hence, the SRRC grants its approval for recruitment --but again, please be reminded that QC SRRC approval means that the SRRC places a posting about your study to the [QC website](#). Because Queens College regularly fields its own surveys, we direct our community to a website that list studies with permission to recruit, rather than allow researchers to survey our community directly. We do send out mailers promoting this website and encouraging study participation regularly.

The posting for your study is up and may be viewed here: <https://www.qc.cuny.edu/ie/srrc-studies/>. Please note that the posting directs those interested in participating to contact you, the PI, via email in order to obtain your user consent form.

Finally, the SRRC does have one suggestion regarding your survey, which is that it make clear who exactly have access to the data, as the current language included in the survey (third paragraph) makes this unclear.

We wish you the best of luck with your study and look forward to hearing about what you learn!

Best,  
Lizandra, Yongwu and Paul  
Study Recruitment Review Committee

---

Lizandra A. Friedland  
Associate Director, Survey Research & Assessment  
Queens College | City University of New York

## Appendix C

### Subject Matter Expert Recruitment Letter

Dear Information Systems Security Subject Matter Expert (SMEs),

I am a Ph.D. Candidate in Information Systems at the College of Computing and Engineering at Nova Southeastern University (NSU). My dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<https://infosec.nova.edu/cylab/>).

You are receiving this survey because you have been identified as a cybersecurity or information security person. The 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. The survey will be used to validate measures for employee cyberslacking (CySI) and the computer security posture (CSP) score of the device being used to access organizational resources.

You will be taking an anonymous survey for a multi-phased Delphi method. The survey process will continue until a consensus is achieved. The survey will take approximately 10-15 minutes to complete. Your participation will contribute to the current literature about Cybersecurity and Remote Workers. This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. You can decide not to participate in this research, and it will not be held against you. There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law, and in an aggregated manner. Only the Principal investigator will have access to the raw data. The participant's identifiable information will be excluded from this study. This data will be available to the researcher, the Institutional Review Board (IRB) and other representatives of this institution. All confidential data will be kept secure. Data will be securely stored on a device protected by password and disk encryption.

I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

Very respectfully,

Ariel Luna  
Ph.D. Candidate in Information Systems  
College of Computing and Engineering  
Nova Southeastern University  
Email: [al1572@mynsu.nova.edu](mailto:al1572@mynsu.nova.edu)



## Appendix D

### Information Users Recruitment Letter

Dear Information Systems User Participant,

I am a Ph.D. Candidate in Information Systems at the College of Computing and Engineering at Nova Southeastern University (NSU). My dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<https://infosec.nova.edu/cylab/>). I am seeking participants for my dissertation study. My research study seeks to validate productivity and security measures for remote workers.

If you choose to participate in this research study, you understand and agree that your participation and responses are entirely voluntary. All your responses will be completely anonymous, and no personal identifiable information will be collected or traced to the originator. You also understand that you may choose to stop your participation in this research at any time.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law, and in an aggregated manner. Only the Principal investigator will have access to the raw data. The participant's identifiable information will be excluded from this study. This data will be available to the researcher, the Institutional Review Board (IRB) and other representatives of this institution. All confidential data will be kept secure. Data will be securely stored on a device protected by password and disk encryption.

I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

The survey should take 5 minutes. If you would like to participate, please go to:

Thank you very much for your time.

Very respectfully,

Ariel Luna  
Ph.D. Candidate in Information Systems  
College of Computing and Engineering  
Nova Southeastern University  
Email: [al1572@mynsu.nova.edu](mailto:al1572@mynsu.nova.edu)

## Appendix E

### Participant Consent Email

Dear associate, [insert organization] has a unique opportunity to participate in a cybersecurity study focused on validating productivity and security measures for remote workers. The learnings from this research will help organizations, like [insert organization name], enable productivity and cybersecurity best practices for remote workers, and how best to train the organizations end users and associates.

This study is being performed by a Ph.D. Candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. This dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy Cylab projects (<https://infosec.nova.edu/cylab/>) Participation consent is needed from you to ensure the dissertation study data is academically compliant.

In order for your consent to be registered, please click on the voting buttons at the top of this email. “Yes” means you consent to participate in the study, and “No” means you prefer not to participate. Participation in this study is voluntary, and if you choose “Yes” all responses and any data gathered will remain anonymous and no Personally Identifiable Information (PII) will be collected as part of the study. In addition, if you choose “Yes” you may rescind your participation in the study at any time by replying to this email.

Please select “Yes” or “No” from the voting buttons above. *Thank you in advance for your participation in this important cybersecurity academic study!*

## Appendix F

### Subject Matter Expert Survey

College of Computing and Engineering  
NOVA SOUTHEASTERN UNIVERSITY

NSU  
Florida

SME Survey

The survey will take approximately 10 minutes to complete. Empirical Assessment of Remote Workers' Cyberslacking and Computer Security Posture to Assess Organizational Cybersecurity Risks

Dear Information Systems Security **Subject Matter Expert (SMEs)**,

I am a Ph.D. Candidate in Information Systems at the College of Computing and Engineering at Nova Southeastern University (NSU). My dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<http://CyLab.nova.edu>).

You are receiving this survey because you have been identified as a cybersecurity or information security person. The 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. The survey will be used to validate measures for employee cyberslacking (CySI) and the computer security posture (CSP) score of the device being used to access organizational resources.

You will be taking an anonymous survey for a multi-phased Delphi method. The survey process will continue until a consensus is achieved. The survey will take approximately 10 minutes to complete. Your participation will contribute to the current literature about Cybersecurity and Remote Workers. This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. You can decide not to participate in this research, and it will not be held against you. There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law, and in aggregated manner. Only the Principal Investigator will have access to the raw data. The participant identifiable information will be excluded from this study. This data will be available to the researcher, the Institutional Review Board (IRB) and other representatives of this institution. All confidential data will be kept securely. Data will be securely stored on a device protected by password and disk encryption.

I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

Very respectfully,

Ariel Luna

Ph.D. Candidate in Information Systems  
College of Computing and Engineering  
Nova Southeastern University  
Email: [al1572@mynsu.nova.edu](mailto:al1572@mynsu.nova.edu)

\* Required

1

What is your age group? \*

18 - 24

25 - 34

35 - 44


45 - 54

55 - 64

65 - 74

75 and over

2

What is your gender? \* 


- Male
- Female
- Non-binary
- Prefer not to say
- Other

3

What is your highest level of education? \* 

- High School
- Associate Degree
- Bachelor's Degree
- Master's Degree
- Ph.D.

4

Which of the following describes your professional role? \* 

- Cybersecurity Analyst
- Cybersecurity Engineer
- Cybersecurity Architect
- Information Security Analyst
- Network Security Engineer
- Other

5

How many cybersecurity industry certifications do you hold?

\* 

- No cybersecurity industry certifications
- One cybersecurity industry certifications
- Two cybersecurity industry certifications
- Three cybersecurity industry certifications
- More than three cybersecurity industry certifications

6

How many years of experience do you have in the field of cybersecurity/IT?

\*

- 1 year or less
- 1 to 3 years
- 3 to 5 years
- 6 to 10 years
- 11 to 15 years
- 16 to 20 years
- Above 20 years

7

Please evaluate the **importance level** of the following measures in understanding an employee's overall productivity using the following scale 1 – Not at all important to 7 – Extremely important \*


	1 – Not at all important	2 – Low importance	3 – Slightly im
Web Browser usage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email Application Usage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
OneDrive for Business usage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Microsoft 365 Apps usage (Word, Excel, PowerPoint)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SharePoint site usage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Microsoft Teams user activity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8

Please provide additional **measures** to be considered in understanding an employee's overall productivity.


Enter your answer

9

Please evaluate the **importance level** of the following measures in understanding the computer security posture of a device using the following scale 1 – Not at all important to 7 – Extremely important \* 


	1 – Not at all important	2 – Low importance	3 – Slightly im
Operating System Version	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Operating System Patching (systems are up to date)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Antivirus / Malware Detection programs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Antivirus / Malware signature updates	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software updates	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Disk Encryption enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall Enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VPN usage	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Collection of security logs enabled	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
End Point Protection	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

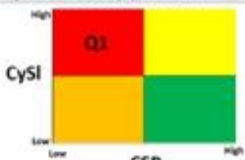
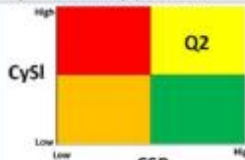

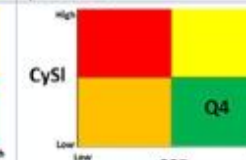
10

Please provide additional **measures** that can be used to understand the **computer security posture** of a device. 

Enter your answer

11

Please rate your level of agreement from 1 (Strongly Disagree) to 7 (Strongly Agree) that the **Remote Worker Cyberslacking Security Risk Taxonomy** is valid to classify the cybersecurity risk that may be posed by employees based on cyberslacking (**CySI**) and the computer security posture of the remote device (**CSP**) \* 

Quadrant 1 (Q1) Very High Risk posed to the Organization	Quadrant 2 (Q2) Moderate Risk posed to the Organization	Quadrant 3 (Q3) High Risk posed to the Organization	Quadrant 4 (Q4) Low Risk posed to the Organization
Consists of a <b>High</b> Cyberslacking Score (CySI) and a <b>Low</b> Cybersecurity Posture Score (CPS).	Consists of a <b>High</b> Cyberslacking Score (CySI) and a <b>High</b> Cybersecurity Posture Score (CPS).	Consists of a <b>Low</b> Cyberslacking Score (CySI) and a <b>Low</b> Cybersecurity Posture Score (CPS).	Consists of a <b>Low</b> Cyberslacking Score (CySI) and a <b>High</b> Cybersecurity Posture Score (CPS).
Remote Workers that are positioned in this quadrant are more likely to engage in cyberslacking activity and have a low cybersecurity posture.	Remote Workers that are positioned in this quadrant are more likely to engage in cyberslacking activity and have a high cybersecurity posture.	Remote Workers that are positioned in this quadrant are less likely to engage in cyberslacking activity and have a low cybersecurity posture.	Remote Workers that are positioned in this quadrant are less likely to engage in cyberslacking activity and have a high cybersecurity posture.
			

1

2

3

4

5

6

7

<--Strongly  
Disagree

Strongly Agree-->

12

If your answer to Question #11 above is **below 5**, please provide information on how to adjust the **Remote Worker Cyberslacking Security Risk Taxonomy** 

Enter your answer

Submit

Never give out your password. [Report abuse](#)

## Appendix G

### Participant Survey



## Participant Survey

Dear Information Systems User Participant,

I am a Ph.D. Candidate in Information Systems at the College of Computing and Engineering at Nova Southeastern University (NSU). My dissertation is chaired by Dr. Yair Levy, and this work is part of the Levy CyLab Projects (<http://CyLab.nova.edu/>). I am seeking participants for my dissertation study. My research study seeks to validate productivity and security measures for remote workers.

If you choose to participate in this research study, you understand and agree that your participation and responses are entirely voluntary. All your responses will be completely anonymous, and no personally identifiable information will be collected or traced to the originator. You also understand that you may choose to stop your participation in this research at any time.

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law, and in aggregated manner. Only the Principal investigator will have access to the raw data. The participant identifiable information will be excluded from this study. This data will be available to the researcher, the Institutional Review Board (IRB) and other representatives of this institution. All confidential data will be kept securely. Data will be securely stored on a device protected by password and disk encryption.

I appreciate the support and assistance in contributing to this research study. If you wish to receive the study's findings, please contact me via email, and I will provide a copy of the academic research publication resulting from this study.

The survey should take 5 minutes.

Thank you very much for your time.

Very respectfully,

Ariel Luna  
Ph.D. Candidate in Information Systems  
College of Computing and Engineering  
Nova Southeastern University  
Email: [al1572@mynsu.nova.edu](mailto:al1572@mynsu.nova.edu)

1. Please enter the participation code provided to you in email:

2. What is your age group?

- 18 - 24
- 25 - 34
- 35 - 44
- 45 - 54
- 55 - 64
- 65 - 74
- 75 and over





3. What is your gender?

Male

Female

Non-binary

Prefer not to say

Other

4. What is your highest level of education?

High School

Associate Degree

Master's Degree

Doctoral Degree

5. What is your job role at the college?

Faculty member

Administrative staff

Technical staff

Support staff

Research staff

Other

6. Which of the following describes your current job level?

Individual Contributor

Supervisor

Middle Manager

Senior Manager

Executive / C Level

7. How many years of experience do you have working in your field?

1 year or less

1 to 3 years

3 to 5 years

6 to 10 years

11 to 15 years

16 to 20 years

Above 20 years

Submit

## References

- Adel, A., Sarwar, D., & Hosseinian-Far, A. (2021). Transformation of cybersecurity posture in IT telecommunication: A case study of a telecom operator. In H. Jahankhani, A. Jamal, & S. Lawson (Eds.), *Cybersecurity, privacy, and freedom protection in the connected world*. 441–457. Springer. [https://doi.org/10.1007/978-3-030-68534-8\\_28](https://doi.org/10.1007/978-3-030-68534-8_28)
- Abilash, K. M., & Siju, N. M. (2021). Telecommuting: An empirical study on job performance, job satisfaction and employee's commitment during pandemic circumstances. *International Journal of Management*, 8(3), 1–10. <https://doi.org/10.34293/management.v8i3.3547>
- Aghaz, A., & Sheikh, A. (2016). Cyberloafing and job burnout: An investigation in the knowledge intensive sector. *Computers in Human Behavior*, 62, 51–60. <https://doi.org/10.1016/j.chb.2016.03.069>
- Akbulut, Y., Donmez, O., & Dursun, O. O. (2017). Cyberloafing and social desirability bias among students and employees. *Computers in Human Behavior*, 72, 87–95. <https://doi.org/10.1016/j.chb.2017.02.04>
- Alharthi, S., Levy, Y., Wang, L., & Hur, I. (2019). Employees' mobile cyberslacking and their commitment to the organization. *Journal of Computer Information Systems*, 61(2), 1–13. <https://doi.org/10.1080/08874417.2019.1571455>
- Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. Dublin, Ireland, 1–5. IEEE. <https://doi.org/10.1109/CyberSA49311.2020.9139638>
- Algarni, A. M., Thayanathan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences*, 11(8), 1–23. <https://doi.org/10.3390/app11083678>
- Aljohani, H. (2021). Cyber security threats during the pandemic. *Journal of Contemporary Scientific Research*, 5(1), 1–14.
- Anandarajan, M., Paravastu, N., & Simmers, C. (2006). Perceptions of personal web usage in the workplace: A Q-Methodology approach. *Cyberpsychology and Behavior*, 9(3), 325–335. <https://doi.org/10.1089/cpb.2006.9.325>
- Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coovert, M. D. (2014). Explaining cyberloafing: The role of the theory of planned behavior. *Computers in Human Behavior*, 36, 510–519. <https://doi.org/10.1016/j.chb.2014.04.006>
- 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. <https://doi.org/10.1186/1471-2288-5-37>

- Banasinski, C., & Rojszczak, M. (2021). Cybersecurity of consumer products against the background of the EU model of cyberspace protection. *Journal of Cybersecurity*, 7(1), 1–15. <https://doi.org/10.1093/cybsec/tyab011>
- Barrero, J. M., Bloom, N., & Davis, S. (2020). 60 million fewer commuting hours per day: How Americans use time saved by working from home. University of Chicago Becker Friedman Institute for Economics Working Paper No. 2020–132. [https://bfi.uchicago.edu/wp-content/uploads/2020/09/BFI\\_WP\\_2020132.pdf](https://bfi.uchicago.edu/wp-content/uploads/2020/09/BFI_WP_2020132.pdf)
- Batabyal, S.K., & Bhal, K.T. (2020), Traditional cyberloafing, mobile cyberloafing and personal mobile-internet loafing in business organizations: Exploring cognitive ethical logics. *Journal of Information, Communication and Ethics in Society*, 18 (4), 631–647. <https://doi.org/10.1108/JICES-07-2019-0081>
- Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, 21(4). [http://doi.org/10.48009/4\\_iis\\_2020\\_234-246](http://doi.org/10.48009/4_iis_2020_234-246)
- Brady, P. Q., Randa, R., & Reynolds, B. W. (2016). From WWII to the World Wide Web: A research note on social changes, online “places,” and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice*, 32(2), 129–147.
- Blanchard, A. L., & Henle, C. A. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior*, 24(3), 1067–1084. <https://doi.org/10.101/j.chb.2007.03.008>
- 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>
- Blount, Y. (2015). Pondering the fault lines of anywhere working (telework, telecommuting): A literature review. *Foundations and Trends in Information Systems*. 1(3), 163–276. <http://doi.org/10.1561/29000000001>
- Bohmer, M., Hecht, B., Schoning, J., Kruger, A., & Bauer, G. (2011). Falling asleep with Angry Birds, Facebook, and Kindle: A large scale study on mobile application usage. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*. Stockholm, Sweden, 47–56. <https://doi.org/10.1145/2037373.2037383>
- Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma G., & TuYe, H. (2020). COVID-19 and remote work: An early look at US data. NBER Working Paper No. 27344.
- 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. <https://doi.org/10.2308/bria-5050>

- CableLabs Security. (2021). Gateway device security best common practices. (Cable Television Laboratories Report Number CL-GL-GDS-BCP-V01-211007).  
<https://www.cablelabs.com/specifications/CL-GL-GDS-BCP>
- 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.  
<https://doi.org/10.1016/j.jisa.2018.08.002>
- Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643–1669.
- 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 CHI Conference on Human Factors in Computing Systems*. New York, NY, 1–13. <https://doi.org/10.1145/3411764.3445243>
- Che Pa, N., Anthony Jnr, B., Jusoh, Y., Nor, H., Nor, R., Aris, M., & Noranis, T. (2017). A risk mitigation decision framework for information technology organizations. *Journal of Theoretical & Applied Information Technology*, 95(10), 2102–2113.
- Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1), 588–608.  
<https://doi.org/10.2307/2094589>
- Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, 73, 394–402. <http://doi.org/10.1016/j.chb.2017.03.061>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44, 588–608.
- Coker, B. (2011). Freedom to surf: The positive effects of workplace internet leisure browsing. *New Technology, Work and Employment*, 26(3), 238–247. <https://doi.org/10.1111/j.1468-005X.2011.00272.x>
- Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware I n a changing cybercrime landscape: Taxonomising countermeasures. *Computers and Security*, 87, 1–18.  
<https://doi.org/10.1016/j.cose.2019.101568>
- Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, 6(1), 1–18. <https://doi.org/10.1093/cybsec/tyaa023>
- Correia, V. J. (2022). An explorative study into the Importance of defining and classifying cyber terrorism in the United Kingdom. *SN Computer Science* 3(84), 1-31.  
<https://doi.org/10.1007/s42979-021-00962-5>

- 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 A. Marcus (Ed.), *Design, user experience, and usability. Theories, methods, and tools for designing the user experience*. Springer. [https://doi.org/10.1007/978-3-319-07668-3\\_23](https://doi.org/10.1007/978-3-319-07668-3_23)
- Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approach*. SAGE Publications.
- Crossland, G., & Ertan, A. (2021). *Remote working and (in) security [White paper]*. Research Institute for Sociotechnical Cyber Security. <https://www.riscs.org.uk/wp-content/uploads/2021/07/RemoteWorking.pdf>
- 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>
- Czerwinski, M., Horvitz, E., & Wilhite, S. (2004). A diary study of task switching and interruptions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, 175–182. <https://doi.org/10.1145/985692.985715>
- 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. <https://doi.org/10.37200/ijpr/v24i5/pr2020764>
- Eilts, D. (2020). *An empirical assessment of cybersecurity readiness and resilience in small businesses*. (Publication No. 2392421605) [Doctoral dissertation, Nova Southeastern University].
- Eldridge, L. P., & Pabilonia, S. W. (2010). Bringing work home: Implications for BLS productivity measures. *Monthly Labor Review*, 133(12), 19–36.
- 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. <http://doi.org/10.28945/1062>
- Eze, I., Lose, T., & Ijeoma, O. (2024). The effects of cyberloafing on employees' ob performance among administrative staff at a university. *International Journal of Social Science Research and Review*, 7(1), 400–413. <https://doi.org/10.47814/ijssrr.v7i1.1736>
- Fransilla, H., Okkonen, J., & Savolainen, R. (2014). Email intensity, productivity, and control in the knowledge worker's performance on the desktop. *Proceedings of the 18<sup>th</sup> International Academic MindTrek Conference: Media Business, Management, & Content Services*. Tampere, Finland, 19–22. <https://doi.org/10.1145/2676467.2676513>

- Ferreira, A., & Du Plessis, T. (2009). Effect of online social networking on employee productivity. *South African Journal of Information Management*, 11(1), 1–11. <http://doi.org/10.1108/03055721311329945>
- 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>
- Ferreira, R., Pereira R., Bianchi I. S., & Mira da Silva, M. (2021). Decision factors for remote work adoption: Advantages, disadvantages, driving forces and challenges. *Journal of Open Innovation Technology Market and Complexity*, 7(1), 1–24. <https://doi.org/10.3390/joitmc7010070>
- Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). *Cybersecurity Risk. Review of Financial Studies*, 36(1), 351–407. <https://doi.org/10.1093/rfs/hhac024>
- Gajendran, R. S., & Harrison, D. A. (2007). The good, the bad, and the unknown about telecommuting: Meta-analysis of psychological mediators and individual consequences. *Journal of Applied Psychology*, 92, 1524–1541. <https://doi.org/10.1037/0021-9010.92.6.1524>
- Galletta, D. F., & Polak, P. (2003). An empirical investigation of antecedents of Internet abuse in the workplace. *Proceedings of the Second Annual Workshop on HCI Research in MIS*, Seattle, WA, 47–51.
- 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/>
- Gokcearslan, S., Uluyol, C., & Sahin, S. (2018). Smartphone addiction, cyberloafing, stress and social support among university students: A path analysis. *Children and Youth Services Review*, 91, 47–54. <https://doi.org/10.1016/j.childyouth.2018.05.036>
- Gorenc, M., Blažič, B. J., & Urnaut, A. G. (2016). Abuse of Internet services in the workplace and the emergence of addiction. *IIASS: Innovative Issues and Approaches in Social Sciences*, 9(2), 116–136. <https://doi.org/10.12959/issn.1855-0541.IIASS-2016-no2-art7>
- Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, 105, 410–431. <http://doi.org/10.1016/j.future.2019.12.018>
- Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, 32(4), 1008–1005. <http://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x>



- Hadlington, L., & Parsons, K. (2017). Can cyberloafing and Internet addiction affect organisational information security? *Cyberpsychology, Behavior, and Social Networking*, 20(9), 567–571. <https://doi.org/10.1089/cyber.2017.0239>
- Hakak, S., Khan, W. Z., Imran, M., Choo, K. K. R., & Shoaib, M. (2020). Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access*, 8, 124134–124144. <https://doi.org/10.1109/ACCESS.2020.3006172>
- Hanaysha, J. (2016). Improving employee productivity through work engagement: Empirical evidence from higher education sector. *Management Science Letters*, 6(1), 61–70. <http://doi.org/10.5267/j.msl.2015.11.006>
- Harker Martin, B., & MacDonnell, R. (2012). Is telework effective for organizations? A meta-analysis of empirical research on perceptions of telework and organizations outcomes. *Management Research Review*, 35(7), 602–616. <https://doi.org/10.1108/01409171211238820>
- Hartijasti, Y., & Fathonah, N. (2014). Cyberloafing across generation X and Y in Indonesia. *Journal of Information Technology Applications & Management*, 21, 1–16.
- Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security*, 76, 101–127. <https://doi.org/10.1016/j.cose.2018.02.020>
- 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.
- Henle, C., Kohut, G., & Booth, R. (2009). Designing electronic policies to enhance perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory. *Computers in Human Behaviour*, 25(3), 902–910. <http://doi.org/10.4324/9781315259468-4>
- Holt, T. J., & Bossler, A. M. (2008) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization, *Deviant Behavior*, 30(1), 1–25. <https://doi.org/10.1080/01639620701876577>
- Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, 29(4), 420–436.
- Houston, J., & Tran, A. (2001). A survey of tax evasion using the randomized response technique. *Advances in Taxation*, 13, 69–94. <http://doi.org/10.4324/9781315259468-4>
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, 31(1), 83–85. <https://doi.org/10.1016/j.cose.2011.10.007>

- Ihantola, E., & Kihn, L. (2011). Threats to validity and reliability in mixed methods accounting research. *Qualitative Research in Accounting & Management*, 8(1), 39–58.  
<https://doi.org/10.1108/11766091111124694>
- Ilievski, A. (2016). An explanation of the cybercrime victimisation: self-control and lifestyle/routine activity theory. *Innovative Issues and Approaches in Social Sciences*, 9(1), 30–47. <https://doi.org/10.12959/issn.1855-0541.IIASS-2016-no1-art02>
- Jandaghi, G., Alvani, S. M., Matin, H. Z., & Fakheri, S. (2015). Cyberloafing management in organizations. *Iranian Journal of Management Studies*, 8(3), 335–349.  
<https://doi.org/10.22059/ijms.2015.52634>
- Jamaluddin, H., Ahmad, Z., Alias, M., & Simun, M. (2015). Personal Internet use: The use of personal mobile devices at the workplace. *Procedia - Social and Behavioral Sciences*, 172, 495–502. <https://doi.org/10.1016/j.sbspro.2015.01.391>
- Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79–91.
- Jia, H., Jia, R., & Karau, S. (2013). Cyberloafing and personality: The impact of the big five traits and workplace situational factors. *Journal of Leadership and Organizational Studies*, 20(3), 358–365. <https://psycnet.apa.org/doi/10.1177/1548051813488208>
- Jeong, Y., Jung, H., & Lee, J. (2020). Cyberslacking or smart work: Smartphone usage log-analysis focused on app-switching behavior in work and leisure conditions. *International Journal of Human-Computer Interaction* 36(1), 1–15.  
<https://doi.org/10.1080/10447318.2019.1597574>
- Lee, H., & Choi, K. (2021). Interrelationship between Bitcoin, ransomware, and terrorist activities: Criminal opportunity assessment via cyber-routine activities theoretical framework. *Victims & Offenders*, 16(3), 363–384.  
<https://doi.org/10.1080/15564886.2020.1835764>
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280.  
<https://doi.org/10.1080/01639625.2015.1012409>
- Kabanda, S., Tanner, M., & Kent, C. (2018) Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269–282. <https://doi.org/10.1080/10919392.2018.1484598>
- Kalhor, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access*, 9, 99339–99363.



- Karthikeyan, C., & Thomas, P. (2017). A review on impact of counter productive work behaviour (CWBS) in organisations a leaders psychology perspective. *International Journal of Management, IT and Engineering*, 7(7), 18–45.
- Kerlinger, F.N., & Lee, H.B. (2000). *Foundations of behavioral research* (4th ed.). Wadsworth Thomson Learning. <http://doi.org/10.4018/978-1-59140-726-3>
- Kimberlin, C. L., & Winterstein, A. G. (2008). Validity and reliability of measurement instruments used in research. *American Journal of Health-System Pharmacy*, 65(23), 2276–2284.
- Koay, K. Y., & Soh, P. (2018). Should cyberloafing be allowed in the workplace? *Human Resource Management International Digest*, 26 (7) 4–6. <https://doi.org/10.1108/HRMID-05-2018-0107>
- Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST Cybersecurity Framework. *Secure IT Systems*, 369–384. [https://doi.org/10.1007/978-3-030-03638-6\\_23](https://doi.org/10.1007/978-3-030-03638-6_23)
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Information Science Publishing.
- 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. <http://doi.org/10.28945/1373>
- Lim, P. K., Koay, K. Y., & Chong, W. Y. (2021). The effects of abusive supervision, emotional exhaustion, and organizational commitment on cyberloafing: a moderated mediation examination. *Internet Research*, 31(2), 497–518. <https://doi.org/10.1108/INTR-03-2020-0165>
- Lim, V. (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>
- Lim, V. K. G., & Chen, D.J.Q. (2009). Cyberloafing at the workplace: Gain or drain on work? *Behavior and Information Technology*, 1(11), 1–12. <https://doi.org/10.1080/01449290903353054>
- Lim, V. K., & Teo, T. S. (2024). Cyberloafing: A review and research agenda. *Applied Psychology*, 73(1), 441–484.
- Luo, X., Xu, F., Zhang, J., Xiao, S., & Xue, B. (2022). Effects of organizational controls on employees' cyber-loafing: The moderating effects of trait mindfulness. *ACM SIGMIS Database: The Database for Advances in Information Systems*, 53(1), 61–79. <https://doi.org/10.1145/3514097.3514102>

- Luqman, A., Masood, A., Shahzad, F., Rasheed, M. I., & Weng, Q. (2020). Enterprise social media and cyber-slacking: An integrated perspective. *International Journal of Human-Computer Interaction*, 36(15), 1426–1436. <https://doi.org/10.1080/10447318.2020.1752475>
- Markos, S. & Sridevi, M.S. (2010). Employee engagement: The key to improving performance. *International Journal of Business and Management*, 5, 89–96. <https://doi.org/10.5539/ijbm.v5n12p89>
- Mertler, C. A., & Vannatta, R. A. (2017). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). Routledge.
- Mishra, D., & Tageja, N. (2020) Cyberslacking for coping stress? Exploring the role of mindfulness as personal resource. *International Journal of Global Business and Competitiveness*, 17, 56–67. <https://doi.org/10.1007/s42943-022-00064-w>
- 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. <https://doi.org/10.1108/IntR-05-2017-0191>
- Mohsin, K. (2020). Cybersecurity in corona virus (COVID-19) Age. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3669810>
- Narayanan, L., Menon, S., Plaisent, M., & Bernard, P. (2017). Telecommuting: The work anywhere, anyplace, anytime organization in the 21st century. *Journal of Marketing & Management*, 8(2), 47–54.
- Navarro, J. N., & Jasinski, J. L. (2012) Going cyber: Using routine activities theory to predict cyberbullying experiences, *Sociological Spectrum*, 32(1), 81–94. <https://doi.org/10.1080/02732173.2012.628560>
- National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*. <https://doi.org/10.6028/NIST.CSWP.04162018>
- 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>
- National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations*. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. *Proceedings of the 17th International Conference on Information Warfare and Security*. Albany, NY. 395–403.

- Nilles, J. M. (1998). *Managing telework: Strategies for managing the virtual workforce*. John Wiley & Sons.
- 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.  
<https://doi.org/10.1016/j.im.2003.11.002>
- 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>
- 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>
- Oravec, J. (2002). Constructive approaches to internet recreation in the workplace. *Communications of the ACM*, 60–63. <https://doi.org/10.1145/502269.502298>
- Ozler, D. E., & Polat, G. (2012). Cyberloafing phenomenon in organizations: Determinants and impacts. *International Journal of eBusiness and eGovernment Studies*, 4(2), 1–15.
- Papagiannidis, S., & Marikyan, D. (2020). Smart offices: A productivity and well-being perspective. *International Journal of Information Management*, 51, 1–11.  
<https://doi.org/10.1016/j.ijinfomgt.2019.10.012>
- Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sherman, A. T. (2018). Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Transactions on Education*, 61(1), 11–20. <https://doi.org/10.1109/TE.2017.2715174>
- Pattinson, M. R., Butavicius, M. A., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018). Adapting cyber-security training to your employees. *Human Aspects of Information Security & Assurance*. 67–79.
- Rahimnia, F., Reza, A. & Mazidi, K. (2015). Functions of control mechanisms in mitigating workplace loafing; evidence from an Islamic society. *Computer in Human Behavior*, 48, 671–681. <https://doi.org/10.1016/j.chb.2015.02.035>
- Ramirez, Y. W., & Nembhard, D. A. (2004). Measuring a knowledge worker productivity: A taxonomy. *Journal of Intellectual Capital*, 5(4), 602–628.  
<https://doi.org/10.1108/14691930410567040>
- Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, 32(2), 148–168.

- Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, 31(3), 253–273.
- Reizer, A., Galperin, B. L., Chavan, M., Behl, A., & Pereira, V. (2022). Examining the relationship between fear of COVID-19, intolerance for uncertainty, and cyberloafing: A mediational model. *Journal of Business Research*, 145, 660–670. <https://doi.org/10.1016/j.jbusres.2022.03.037>
- Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal*, 38(2), 555–572. <http://doi.org/10.2307/256693>
- 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>
- Rotas, E., & Cahapay, M. (2021). Does threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid COVID-19 crisis? *Journal of Pedagogical Sociology and Psychology*, 3(1), 45–53. <https://doi.org/10.33902/JPSP.2021167595>
- Sebastian, G. (2021). A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan. *Communications of the IBIMA*, 2, 2–7. <http://doi.org/10.5171/2021.589235>
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). John Wiley & Sons.
- Sheikh, A., Atashgah, M. S., & Adibzadegan M. (2015). The antecedents of cyberloafing: A case study in an Iranian copper industry. *Computer in Human Behavior*, 51, 172–179. <https://doi.org/10.1016/j.chb.2015.04.042>
- Shepherd, M. M., & Mejias, R. J. (2016). Nontechnical deterrence effects of mild and severe internet use policy reminders in reducing employee internet abuse. *International Journal of Human-Computer Interaction*, 32(7), 557–567. <https://doi.org/10.1080/10447318.2016.1183862>
- 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. <https://doi.org/10.17705/1CAIS.03702>
- Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education*, 6, 1–21. <https://doi.org/10.28945/199>

- Smith, S. J. (1986). The growing diversity of work schedules. *Monthly Labor Review*, 109(11), 7–13.
- Smith, W. (2019). *A comprehensive cybersecurity defense framework for large organizations*. [Doctoral dissertation, Nova Southeastern University]. Available from Dissertations & Theses @ Nova Southeastern University.
- Stitch, J. F. (2020) A review of workplace stress in the virtual office. *Intelligent Buildings International*, 12(3), 1–13. <https://doi.org/10.1080/17508975.2020.1759023>
- Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, 135. 1–10. <https://doi.org/10.1016/j.ssci.2020.105143>
- Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic cyber hygiene: Does it work? *Computer*, 52(4), 21–31. <https://doi.org/10.1109/MC.2018.2888766>
- Sumsion T. (1998). The Delphi technique: An adaptive research tool. *British Journal of Occupational Therapy*, 61(4), 153–156. <https://doi.org/10.1177/030802269806100403>
- 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. <https://doi.org/10.6000/2371-1647.2020.06.02>
- Syrek, C.J., Kuhnel, J., Vahle-Hinz, T., & De Bloom, J. (2018). Share, like, Twitter, and connect: Ecological momentary assessment to examine the relationship between non-work social media use at work and work engagement. *Work and Stress*, 32(3), 209–227. <https://doi.org/10.1080/02678373.2017.1367736>
- Terrell, S. R. (2016). *Writing a proposal for your dissertation. Guidelines and examples*. Guilford Press.
- Toker, T., & Baturay, M. H. (2021). Factors affecting cyberloafing in computer laboratory teaching settings. *International Journal of Educational Technology in Higher Education*, 18(1), 1–24. <https://doi.org/10.1186/s41239-021-00250-5>
- Ugrin, J. C., & Pearson, J. M. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior*, 29, 812–820. <https://doi.org/10.1016/j.chb.2012.11.005>
- 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. [https://doi.org/10.1300/J179v06n03\\_04](https://doi.org/10.1300/J179v06n03_04)
- U.S. Bureau of Labor Statistics. (2021). *Workforce statistics for information: NAICS 51*. <https://www.bls.gov/iag/tgs/iag51.htm#workforce>

- Vagal, V., & Dillon, R. (2021). Reducing cyber risk in remote working. In V. Vagal & R. Dillon (Eds.), *Digital Transformation in a Post-COVID World*, (1<sup>st</sup> ed., pp.155–170). CRC Press.
- van Teijlingen, E., & Hundley, V. (2002). The importance of pilot studies. *Nursing Standard*, 16(40), 33–36. <https://doi.org/10.7748/ns2002.06.16.40.33.c3214>
- 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 Systems*, 35(4), 1060–1091. <https://doi.org/10.1080/07421222.2018.1523531>
- 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>
- 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>
- Vitak, J., Crouse, J., & Larose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, 27(5), 1751–1759. <https://doi.org/10.1016/j.chb.2011.03.002>
- 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. [https://doi.org/10.1061/\(ASCE\)CO.1943-7862.0000944](https://doi.org/10.1061/(ASCE)CO.1943-7862.0000944)
- Wang, J., Tian, J., & Shen, Z. (2013). The effects and moderators of cyber-loafing controls: An empirical study of Chinese public servants. *Information Technology and Management*, 14, 269–282. <https://doi.org/10.1007/s10799-013-0164-y>
- Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, 20(1), 35–44. <https://doi.org/10.1016/j.hrmr.2009.03.012>
- 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.
- Weil, T., & Murugesan, S. (2020). IT risk and resilience—Cybersecurity response to COVID-19. *IT Professional*, 22(3), 4–10. <https://doi.org/10.1109/MITP.2020.2988330>
- Wu, J., Mei, W., Liu, L., & Urgin, J. C. (2021). The bright and dark sides of social cyberloafing: Effects on employee mental health in China. *Journal of Business Research*, 112, 56–64. <https://doi.org/10.1016/j.jbusres.2020.02.043>

- 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*, 6, 43–54. <https://doi.org/10.1038/s41562-021-01196-4>
- Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, 16(4), 490–513. <http://doi.org/10.1080/19361610.2021.1918995>
- Zakrzewski, C. (2016, March 13). The key to getting workers to stop wasting time online. *Wall Street Journal*. <http://www.wsj.com/articles/the-key-to-getting-workers-to-stop-wasting-time-online-1457921545>.