UNDERSTANDING CYBER SECURITY THREATS IN CLOUD-BASED SHADOW IT WORK-FROM-HOME APPLICATIONS USING THE GENERAL STRAIN THEORY LENS

by

PATRICIA AKELLO, M.Sc.

DISSERTATION
Presented to the Graduate Faculty of
The University of Texas at San Antonio
in Partial Fulfillment
of the Requirements
for the Degree of

DOCTOR OF PHILOSOPHY IN INFORMATION TECHNOLOGY

COMMITTEE MEMBERS:
Nicole L. Beebe, Ph.D., Co-Chair
Kim-Kwang Raymond Choo, Ph.D., Co-Chair
Gianluca Zanella, Ph.D.
Dina Krasikova, Ph.D.

THE UNIVERSITY OF TEXAS AT SAN ANTONIO
College of Business
Department of Information Systems and Cyber Security
August 2022

DEDICATION

"It does take a village!", so here we go

To my large and very dear family (friends near and far included): Thank you! First, this is a tribute to the love, friendship, and memory of my mama, Enrica…whose love for me knew no bounds, thank you so much. Your memory continues to lovingly be with me. We have come a long way and experienced war and peace together, and our lives continue to bear witness to the hope and endless possibilities that exists in the human personhood. Equally, I salute my dear baba, Kalisto...whose life is always inspiring to the spectator, acting upon his beliefs with hope, conscientiously. Grateful to have you as a pillar of strength and for ALL your sacrifices, too many to recount. To my lovely siblings Lucy, Franca, Olympia, Denis, Egidio, Innocent and Peter: Thank you for your good examples, for your prayers, for earnestly making your own ways in life, pursing your own paths, encouraging, and loving each other along the way! To my love, Chad: you love, support, encourage, mentor, and help with all things great and small…attentively with the best of heart. To extended family (no order of precedence): Silberbergs, McClains, Millers, Jenelle and the Rosecrances, Caitlin, Jane, and the Laws'... Thank you for your incredible support and encouragement.

And then..., to the war child... in Ukraine, the Congo, Afghanistan, Sudan, Yemen...and anywhere: your dreams will come true, keep on the pursuit

ACKNOWLEDGMENTS

This dissertation was completed thanks to the assistance and support of my mentors who are also my dissertation chairs: Dr. Nicole Beebe and Dr. Kim-Kwang Raymond Choo. It's been great to have your trust and support from the beginning, your patience with me during my learning and training, and your overall good will. Without you, I would not be where I am today. My gratitude also extends to the members of the committee, Dr. Gianluca Zanella and Dr. Dina Krasikova, for their time, guidance, and wisdom.

Dr. Nicole Beebe, Dr. Raymond Choo, Dr. Ravi Sandhu and the NSF-funded CREST Center for Security and Privacy Enhanced Cloud computing (C-SPECC): Thank you for funding my entire program through the NSF C-SPECC grant. It all came together because of this tie. Many thanks for this pivotal opportunity. I would like to express my gratitude to Dr. Rao, Dr. Valecha, and Dr. Vemprala for collaboration and advice in timely research projects all of which were a threshing floor. Our paper, "Retweets of officials' alarming vs reassuring messages during the COVID-19 pandemic: Implications for crisis management", gave me encouragement and assurance that I could still benefit from collaborative research, even during the pandemic. Additionally, I would like to acknowledge the substantial support, guidance, and inspiration that I have received from Drs. Utecht, Krasikova and Liu, all of whom have inspired me in my quest to be not only a successful researcher, but an exceptional teacher as well. It was a pleasure to be taught by you. Thank you to Dr. Lisa Montoya, Dr. Kevin Grant, and Ms. Rebecca Pollock for providing me with invaluable opportunities while here, including opportunities for international immersion leadership.

Friends and colleagues at the college of business who have been by my side throughout the PhD program: Dr. Kristen Faile, Federica Rossetti, Dr. Racheal Xiong, Dr. Zahra

Avivazpour, Dr. Naga Vemprala, Dr. Mohsen Jozani, Dr. Gianluca Zanella, Dr. Morteza Safour, Dr. Eric Bachura, Dr. Oluwafemi Akanfe, Dr. Thi Tran, Richard Alvarez, Oren Upton, and everyone who I shared the Ph.D. experience with during my time here: Thank you.

Special thanks to Caron Kiley for her help and kindness. Without her, it would be hard to be successful here.

UNDERSTANDING CYBER SECURITY THREATS IN CLOUD-BASED SHADOW IT WORK-FROM-HOME APPLICATIONS USING THE GENERAL STRAIN THEORY LENS

Patricia Akello, M.SC.
The University of Texas at San Antonio, 2022

Supervising Professors: Nicole L. Beebe, and Kim-Kwang Raymond Choo

The rapid rise of remote work in response to the COVID-19 pandemic resulted in a rise in the reliance on cloud computing for sharing data between secure office networks and un-secure remote networks. This greatly increases the impact and importance of answering critical questions regarding the blurring boundaries between work and non-work and any related the cyber security risks.

This individual-level survey design study aims to examine one of such risks, known as Shadow IT, a non-malicious insider-related data security threat whose acceleration is partly due to the power of the cloud. This research seeks to understand the acceleration of Shadow IT proliferation in the remote work setting by looking into the factors that influence adoption against the backdrop of COVID-Strains. Specifically, the research's aim is to understand the moderating effects of strain, along with other individual level variables on deviance (the volitional non malicious use of shadow IT in remote workplaces in violation of injunctive IT/ security norms).

This research's contributions are in the areas of information security, threat intelligence and management in the remote workplace, remote work security, insider threats, and shadow it and security compliance.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE: INTRODUCTION

1.1. BACKGROUND

In recent years, cloud computing (CC), which provides IT infrastructure/ hardware, software, data management, and network services on demand over a network, has become a mainstream phenomenon. Due to its benefits of flexibility, scalability, availability, and cost savings, the paradigm has emerged as a key trend in the IT infrastructure industry (Mell and Grance, 2011). Among remote workers for instance, SaaS or software as a service has emerged as the fastest-growing segment[1] [2], as users sign up to use new apps regularly for both personal and business use – often without organizational IT vetting them for data security and compliance risks. In the age of widespread cloud adoption and proliferation, as well as cloud computing in general, the long-standing debate surrounding the security of cloud-based applications has taken on a greater significance[3] [4].

Cloud computing and cloud-based applications have been the subject of numerous studies emphasizing the importance of security (Ab Rahman and Choo, 2015; Ali et al., 2015; Choo, 2010; Choo et al., 2017; Esposito et al., 2016; Hong et al., 2019; Iqbal et al., 2016; Singh and

[1] https://www.forbes.com/sites/forbestechcouncil/2021/01/15/how-the-pandemic-has-accelerated-cloud-adoption/?sh=438cd6c76621

[2] https://www.cpomagazine.com/cyber-security/shadow-saas-is-on-the-rise-in-the-hybrid-work-era-heres-how-to-regain-control/

[3] https://www.darkreading.com/cloud/as-remote-work-becomes-the-norm-security-fight-moves-to-cloud-endpoints

[4] https://newsroom.ibm.com/2020-06-10-IBM-Security-in-the-Cloud-Remains-Challenged-by-Complexity-and-Shadow-IT

Chatterjee, 2017). In these studies, researchers examine the security threats to the cloud, as well as those brought on by the use or misuse of cloud-based applications, and countermeasures to these threats. In part, due to the cloud's inherent characteristics (such as self-service on demand and broad network access), adopters face these significant security and privacy risks.

Anecdotally and in recent reports such as by the cloud security alliance, CSA[5] and others[6] [7], one top threat due to cloud computing and its inherent characteristics is shadow IT, a form of self-support computing where employees (either remotely or onsite) access, download or use apps and software that are readily available in the cloud, but not sanctioned, approved, known or authorized by their organizations to perform work related activities (Haag et al., 2019; Zimmermann et al., 2016). As remote workers work away from formal corporate governance, the Shadow IT problem has been exacerbated as workers made efforts to supplement official IT with unsanctioned cloud-based applications. Moreover, remote work appears to be a trend that will continue[8]. As described by the CSA, shadow IT is a cloud computing-related threat to information systems security due to limited visibility of cloud usage (LCV). The LCV concept refers to when an organization is unable to visualize and/or analyze whether cloud services and apps are used safely or maliciously within both the confines of the organization's network, but also with regard to remote access thereof and remote handling of organizational data. We

[5] https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-

[6] https://www.darkreading.com/cloud/as-remote-work-becomes-the-norm-security-fight-moves-to-cloud-endpoints

[7] https://cisomag.eccouncil.org/shadow-it-is-creating-an-ever-growing-problem-with-remote-teams/

[8] https://www.nytimes.com/2021/03/29/nyregion/remote-work-coronavirus-pandemic.html

examine the LCV concept through the lens of what past research has conceptualized or defined as the insider threat (Cappelli et al., 2012; Loch et al., 1992; Maasberg and Beebe, 2014; Warkentin and Willison, 2009). Accordingly, the insider threat is caused by users with authorized or legitimate access to an organization's assets such as information, networks, or systems, who abuse it in some way either deliberately or accidentally, thereby affecting the confidentiality, integrity, or availability of that organization's information and/or systems.

The LCV presents two scenarios: misuse of sanctioned apps and use of unsanctioned apps, in other words, asks two questions: who misuses sanctioned apps within the organization, and who uses unsanctioned apps (shadow IT) within the organization? Therefore, in the sanctioned app misuse scenario, a company does not have the ability to see how their approved apps are being utilized by their employees. This poses several risks, like when a disgruntled employee misuses cloud-based apps that the company has authorized, such as Google Drive, to steal the company's proprietary data such as IP data in an insider threat attack (Claycomb and Nicoll, 2012; Kandias et al., 2013; Moore et al., 2011). Since an employee in this case willfully takes advantage of an organization's IP, sanctioned app misuse presents a malicious Insider threat in this scenario (Cappelli et al., 2012). The insider threat is "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems". Examples of such threats include insider exploitation of cloud services and intellectual property theft (Moore et al., 2011).

In the other insider threat conceptualizations, the insider threat refers to end user actions that create insider risks that are volitional and non-malicious, but still detrimental to the information

security of the organization, since anyone with access privileges to a company's information, systems, and networks may be considered an insider threat if their actions expose the company's information systems to security risks (Bishop and Gates, 2008; Warkentin and Willison, 2009; S. L. Pfleeger et al., 2010). The act of accessing or using unvetted apps from the internet by an employee to accomplish the organization's work tasks (shadow IT), thus, may unintentionally open doors for unauthorized access, disclosure, and denial of service, presenting a volitional and non-malicious insider threat. There has been recent discussion and association of shadow IT with both the malicious, but mostly this kind of insider threat (Haag et al., 2019; Shaikh, 2018; Silic et al., 2017a). But in accordance with the insider threat taxonomies (Loch et al., 1992; Warkentin and Willison, 2009), shadow IT mainly presents security risks related to the volitional non-malicious insider threats since employees with access to the organization's information unwittingly expose the organizations information systems to potential security risks.

1.2. RESEARCH MOTIVATION AND QUESTIONS

There is growing concern about shadow IT in the workplace, both for onsite and remote work, although the latter is increasingly concerning given the increase in remote work since the COVID-19 global pandemic[9]. Several years ago, Gartner estimated that over three quarters of all intrusions into company information would be caused by shadow IT use[10]; a prediction that was later exacerbated by the compulsive and immediate move to remote work due to the COVID

[9] https://www.forbes.com/sites/gadlevanon/2020/11/23/remote-work-the-biggest-legacy-of-covid-19/?sh=129979397f59

[10] https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/?cm_mmc=social-_-rm-_-gart-_-swg

epidemic. In fact, IT leaders report that shadow IT installations have increased in the last few years, as well as the positive attitudes of remote employees towards utilizing it to supplement the IT needs of their organizations[11], perhaps due to its benefits of improved performance and efficiency among others (Haag et al., 2019; Mallmann et al., 2018a; Walterbusch et al., 2017). The prevalence of shadow IT is also exacerbated by the widespread adoption of the cloud, which makes it simpler to access tools beyond those an organization provides. None the less, shadow IT has the disadvantage of infiltrating enterprise environments with "limited visibility security risks", like the insider threat since an organization is at risk when it cannot visualize and analyze apps and software that are being used by end users to house and or process its data. Hence, end user actions can pose a threat to system security.

Research on end-user behavior, insider threats, and information security has demonstrated that inappropriate use of information systems tools and resources by end users can pose many known and unknown security risks to organizations' data and systems. Therefore, end-user behavior research is important to insider-related security research since even benign actions, such as storing and processing organizations data on shadow apps or tools, can harm their organization in the same ways as insiders (Crossler et al., 2013a; Guo et al., 2011; The CERT Insider Threat Center, 2014). It is also possible that Gartner's prediction took into consideration that there are a variety of malicious apps available on the internet these days.

[11] https://www.citrix.com/blogs/2020/05/28/the-new-work-order-of-covid-19-might-be-here-to-stay/

Recent anecdotes, such as in cite[12] [13], indicate that Apple Inc. removed millions of apps from its App Store because they were laced with malicious code. This is despite mechanisms being in place to stop malicious apps from entering the app ecosystem, such as scanning the apps for malware before they are sold through the app store or Google Play store. Furthermore, apps are scanned for malware both before they are downloaded and again after they have been installed on the user's device. None the less, in addition to evading detection through standard scanning, new variants of malware are spreading using unorthodox methods such as being hidden in other objects or releasing themselves in "multi-stages" (initially harmless, but gradually updated over time) These examples illustrate how non-maliciously intended actions by end users, such as shadow IT, can result in unexpected issues.

1.2.1. Research Context

The context in which we conduct this study is the remote work (RW)/work from home (WFH) environment against a backdrop of COVID strains. Until COVID-19, Remote work, which is the term used to refer to flexible, time- and location-independent work, was only needed temporarily or by specific departments. Even though the remote work shift has been eminent and rapidly expanding in many sectors (such as service, health care, and education (He et al., 2020), the pandemic forced it into implementation with limited planning, designing, or testing. This is because the outbreak of COVID-19 created the need for social distancing (the deliberate physical space between individuals) as a sound method of stopping the spread of the pandemic.

[12] https://www.cnbc.com/2021/05/11/apple-rejected-nearly-1-million-new-apps-in-2020-heres-why.html
[13] https://techcrunch.com/2015/09/21/apple-confirms-malware-infected-apps-found-and-removed-from-its-chinese-app-store/

Consequently, the move to remote work was compelled, though it has itself created some changes in how employees accomplish work-related tasks in the new work environment, specifically how they utilize technology for work-related tasks with new risks and benefits. As a result, this has awakened the debate about the blurring of boundaries between work and non-work, raising important cyber security questions that pertain to the study. This remote work norm is expected to continue after the epidemic is over. As Gallup News[14] points out, remote working is becoming more prominent. This requires the continual examination of new threats to enterprise information security in remote work settings, such as those arising from increased Shadow IT use. While scrambling to meet work-related performance challenges in unique working conditions away from organizational support, WFH employees are more likely to seek workaround IT solutions. However, even though data is more easily protected when the organization controls the IT systems that handle, store, and process organizational data; this kind of control is most effectively implemented by restricting work to systems that belong to and are maintained by the organization. Today, employees work remotely away from the organization's perimeter, so this is unlikely.

1.2.2. Research Questions

Employees who work at home with limited IT resources and support may be motivated to find workaround solutions. In this case, organizations would have no control over the systems that WFH employees use to process organizational data. Online presentation editing apps such as Prezi and Canva, or cloud-based file sharing apps like Dropbox, are examples of Shadow IT

[14] https://news.gallup.com/poll/355907/remote-work-persisting-trending-permanent.aspx

resources, whereby the data shared by Prezi or Canva gets into the hands of third-party agents who may use the data for other reasons that are hidden from the organization.

In this study, factors that contribute to Shadow IT being more preferred than sanctioned alternatives in the remote work setting are explored. Security behaviors of end users affect organization-wide information security, hence the focus is on the security behavior of end users and their role in the overall organizational information security climate. In recent years, this area has been recognized as a focal point of research related to insider threats. Accordingly, we make an effort to add knowledge to this field. Over the course of the pandemic, millions of people have continued to face the significant challenge of working from home under the significant stress of multitasking numerous responsibilities that range from managing their families to new remote work experiences, forcing them to scramble to find the tools they need to remain productive away from organizational functional and work-related support. Shadow IT increases the likelihood of data exfiltration, non-compliance with laws and regulations, and overall increased risk for an organization. Considering the large number of employees working remotely, COVID-19 and remote work trends make exacerbated this situation. We contribute to this discussion by examining the factors at play in the accelerated proliferation of shadow IT at the intersection of COVID-19 and remote work by exploring individual level cognitive and psychological factors and environmental factors that impact employees' use of Shadow IT away from traditional organizational structures, and well-designed, well-communicated and well-described governance policies.

In exploring factors contributing to shadow IT proliferation in the remote workplace despite sanctioned alternatives, shadow IT usage is positioned as an end-user behavior significantly contributing to the cyber security climate of the organization. The role of end user

security behavior in shaping the overall organizational information security climate has been widely recognized as a focal point of research related to insider related issues. We examine how strain, in particular situational strain caused by COVID and its times, plays a role in explaining this phenomenon. Through an individual level study based on established theoretical frameworks and survey data, psychological, cognitive, as well as environmental factors are examined in relation to how they impact shadow IT adoption and use in the remote workplace, with the aim of answering the following research questions:

1. How does the use of shadow IT in violation of injunctive IT/ security norms create new risks or amplify the existing risks associated with cloud-based applications as remote work becomes more common?
2. When working remotely, why do WFH employees choose shadow IT over organizationally provided IT solutions?
3. In a remote work setting where there is no formal organizational governance, which factors have a major impact on shadow IT adoption? Are individual factors or environmental factors dominant?
4. Generalized, what role does situational strain play in end-user security behavior in non-traditional work settings where compliance standards may not be easily enforced and security policies about IT phenomena such as shadow IT usage are not well defined or communicated?

Contributions are in the areas of information security, shadow IT risks and Threat Intelligence in the remote work settings. In the rest of the paper, the organization is as follows. Chapter 2 reviews the extant literature on related works, describes the theoretical foundation and grounds the study in past works. Chapter 3 describes the study variables, advances the research

hypotheses, and presents the research model. Chapter 4 describes the research methodology, including the study design procedure, instrumentation, and data collection protocols. Chapter 5 describes the data analysis procedures. Chapter 6 presents the results and discussion section, which includes the implications of the study. Chapter 7 presents the conclusion which includes the limitations of the study and any future works.

CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FOUNDATION

2.1 LITERATURE REVIEW

In behavioral research on information security related phenomena, such as the present study, emphasis is placed on factors that are psychological, cognitive, social, or environmental in nature that could influence end-user security postures and behavior, with the potential to expose the organization's information systems to cyber threats. Through this approach, antecedents, motivators, and inhibitors of end user behavior, as well as the decision processes leading to the behavior are examined through theoretical lenses drawn from areas such as psychology, philosophy, sociology, and criminology; for example: addiction theory and the Dark Triad trait of psychopathy (Maasberg and Beebe, 2014; Maasberg et al., 2015), rational choice (Bulgurcu et al., 2010), neutralization (Haag et al., 2019; Silic et al., 2017a; Siponen and Vance, 2010), fear appeals (Boss et al., 2015; Johnston and Warkentin, 2010; Johnston et al., 2015), social control (Cheng et al., 2013; Herath and Rao, 2009a, 2009b; Lee et al., 2004), moral reasoning (Myyry et al., 2009; Hu et al., 2011a), accountability (Vance et al., 2015; Vance et al., 2012a), disgruntlement (Willison and Warkentin, 2013; Willison et al., 2016), and deterrence (Cheng et al., 2013; Herath and Rao, 2009a; Pahnila et al., 2007; Silic et al., 2017a). Generally, these studies indicate that behaviors related to secure information systems are influenced by a range of factors (at both the employee and organizational levels) ranging from attitudes towards the behaviors, to organizational social norms related to the behavior, perceptions of risks related to the behavior, expectation of sanctions or benefits in association to the behavior, the employees' psychological states, and so forth. Additionally, the studies emphasize the importance of end-user-centric security as an essential element of the recommended socio-technical approach to

security and security research, which in turn can improve policies and improve control and countermeasure implementations. Before exploring the literature related to contextual behavioral research in more detail, it is important to analyze Shadow IT, along with the research streams in which it can be contextualized, such as insider threats, compliance with information security, and end-user's non-malicious security violations, which can all exist simultaneously within the same research domain.

2.1.1 Insider Threat and Information Security

The literature on insider non-compliance demonstrates that end-user actions and inactions can be major sources of security threats to organizations (Boss et al., 2015; Guo et al., 2011; Johnston and Warkentin, 2010; Willison and Warkentin, 2013), and this aspect is relevant to the research: "employees' voluntary adoption of shadow apps available for download or use on the Internet". From this statement, it follows that end users within an organization can negatively impact the organization's assets, such as its information by taking non-compliant actions that violate security policies or by engaging in risky security practices such as using shadow IT. It is therefore important to emphasize that even when non-maliciously intended, end user actions, such as using shadow IT, can produce such negative impacts on the organization's information and systems (Crossler et al., 2013a; Guo et al., 2011). Consequently, every employee has an important role in the security strategy of the company's information.

Existing studies in the insider threat and information security areas mainly emphasize this and help us to understand the threats posed by end users within an organization, though most offer generic perspectives and are generally associated with stereotypical associations or narrower conceptualizations, such as the insider threat (Cappelli et al., 2012; Pfleeger et al., 2010; Roy Sarkar, 2010; Willison and Warkentin, 2013) which has been largely associated with

malice and crime; or the explicit information security policy violators who go against well-constructed, well-communicated and well-delineated security policies (Cheng et al., 2013; Herath and Rao, 2009b; Johnston et al., 2016; Vance et al., 2015; Warkentin and Willison, 2009). Research attention is not given to issues like shadow IT usage, which can both be dangerous and helpful at the same time, is uncategorized, and not explicitly addressed by organizational security policies.

Thus, we intend to fill this gap by examining shadow IT, which overlaps phenomena such as insider threat and non-malicious end-user security deviations, in light of its special relevance to Information Security in the remote work setting, as people tend to find workarounds such as by embracing new technologies whenever they dislike existing solutions. The possibility that shadow apps could be insecure or that data loss could occur on the part of third parties makes for an insider threat.

2.1.2 The Insider Threat and Shadow IT

The Insider threat is a broader term for "the human factor" in security. All actions by insiders or employees posing threats to organizational assets are covered by this account (Pfleeger et al., 2010). The most widely adopted Insider threat definition is from the Carnegie Mellon Software Engineering Institute (SEI) Insider Threat Center (commonly referred to as CERT); where the insider threat is "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems" (Cappelli et al., 2012). According to the widely accepted definition, the Insider threat is usually associated

with malevolence and malice. The literature and anecdotal statistics do indeed suggest that there is a significant threat posed by these insiders (Crossler et al., 2013b; Homoliak et al., 2019)., a perspective widely researched in Insider threat research. An array of motives behind such malice are varied including revenge due to un-met expectations, the desire to appease unresolved grievances against the organization, like when a disgruntled ex-Amazon employee leaked property information of over millions of Capital One customers from an AWS bucket[15], or for profit. While this study does not focus on this kind of insider threat (the malicious), taking note of the differences is important.

From the malicious insider threat point of view, CERT's early research identifies four categories (Hanley and Montelibano, 2011): IT sabotage, theft of intellectual property (IP), fraud, and espionage (Hanley and Montelibano, 2011). These early efforts led scholars such as (Maasberg and Beebe, 2014), who shed light on the malicious insider threat, to add to the concept a cross-disciplinary definition of malicious intent to define the insider threat as " a person having the malevolent desire and willingness to engage (or fail to engage) in a wrongful act and subsequently making the decision to do so (volitional)". The authors thus present the malicious insider threat as being one who possesses both malice and malevolence, while all others fall under the unintentional insider threat, UIT ("... without malicious intent, well intentioned, inadvertent, unintentional") (Maasberg and Beebe, 2014).

Most incidents of UIT are caused by end user actions or inactions, spanning the behavioral spectrum from carelessness, negligent deviance to pure accidents. Regardless,

[15] https://www.bloomberg.com/news/articles/2019-07-29/capital-one-data-systems-breached-by-seattle-woman-u-s-says

whether it is one of the above or any other, end-user actions and inactions have been covered in the literature and associated with the UIT (e.g, Crossler et al., 2013; Guo et al., 2011; Stanton et al., 2005; Willison and Warkentin, 2013); where there's acknowledgement that they create unintended, unmotivated risks which compromise the information security of the organization. As an accident, a UIT may be exemplified by an end-user accidentally sending sensitive business documents to the wrong email address, exposing the organization to security risks. On the other end of the UIT, we may also have negligent employees who violate security by doing things such as failing to properly dispose of sensitive documents, not heeding notifications about installing security updates and patches, losing or mishandling portable storage devices that contain sensitive information, and downloading malware-infected shadow apps to process company data, in which case, end-users may not realize the risk associated with their voluntary actions such as processing organizational information on shadow apps.

As such, the UIT insider definition is more aligned with the threat that shadow IT creates, specifically, because the risks are unintentionally generated by employees, who may not recognize the dangers of shadow apps, even if the decision to use shadow IT is volitional for whatever reason (improved productivity, efficiency and so forth). The researchers (Beebe & Chang, 2019) additionally noted an additional angle to the insider threat that shadow IT poses, noting that non-human threats can also result from technological insiders, such as rogue ML and AI processes that are assumed to be trustworthy (Beebe & Chang, 2019). As well, research on fog and edge computing security has supported this viewpoint regarding the threat that rogue edge devices and fog nodes may pose in the IoT environment where multiple devices have to authenticate each other (Khan et al., 2017; Stojmenovic and Wen, 2014). As such, from the perspective of shadow apps being potential sources of malware or points for data loss, shadow IT

can also be considered a type of technological insider threat. The UIT is a problematic issue, as evidenced by recent statistics that indicate this type of threat can cause enormous damage, as shown by the fact that 64% of all security breaches are caused by it[16].

2.1.3 Shadow IT: Defined, Risks, Benefits, Examples

Considering that the IT tools used by employees are not part of the organization's official IT infrastructure, and that there is no formal IT control or governance over them, shadow IT has been conceptualized as the voluntary use of any IT resources for work purposes in violation of injunctive IT norms in an effort *to cope with perceived constraints*(Haag and Eckhardt, 2014a). A number of scholars, including (György et al., 2012; Zimmermann and Rentrop, 2014), have endorsed this viewpoint, noting that user-driven innovations (shadow IT usage) are not necessarily driven by malicious or noncompliant intentions, restrictive policies that employees desire to violate, or limited user rights that employees wish to challenge, but instead stem from the inability of central IT to meet business requirements. As it turns out, most studies exploring shadow IT (Chua and Storey; Haag et al., 2019; Mallmann and Maçada, 2016; Mallmann et al., 2018a; Myers et al., 2017a; Silic and Back, 2014a; Silic et al., 2017a; Walterbusch et al., 2017, 2017; Zimmermann and Rentrop, 2014), approach this issue from this standpoint, emphasizing that end users use shadow IT as a workaround to overcome situational IT constraints in the work environment in order to, for example, maximize their job efficiency and productivity. Taking these into account, and without ignoring the fact that it is the "*voluntary usage of any IT resource*

[16] https://www.ibm.com/topics/insider-threats#:~:text=In%20the%20Ponemon%20Institute's%202020,the%20incidents%20attributed%20to%20negligence.

violating injunctive IT norms", we define shadow IT as employees' volitional but non-malicious autonomy in accessing and utilizing easily accessible cloud-based applications in the work-from-home environment for work-related tasks without the knowledge or familiarity (authorization, awareness, or vetting) of their organizations' security or IT (Haag and Eckhardt, 2014a; Zimmermann and Rentrop, 2014). From the insider threat perspective, the conceptualization described here relates to the "…volitional but non-maliciously motivated end user behavior and actions that put at risk an organization's data, processes, or resources" (Pfleeger et al., 2010).

Due to differing perspectives on shadow IT in the literature, shadow IT is fraught with ambiguity. According to some researchers, end user computing/end user development (EUC/EUD), which is whereby end users can develop shadow IT such as spreadsheets on their own or the company's devices (Chua and Storey; Mallmann et al., 2018a; Myers et al., 2017b; Panko and Port, 2012), and bring your own device (BYOD) where by employees are allowed to use "approved personal" devices for work purposes fall under shadow IT (French et al., 2014; Huber et al., 2017; Mallmann et al., 2018b). In both cases, this would be partially true, because in the case of employees developing their own spreadsheets for work tasks in the shadow, for example, this would be end user development and shadow IT as well, while in the case of employees using unknown apps on their approved BYOD hardware, this would be bring your own device-shadow IT. Hence, EUC/EUD and BYOD are each part of a broader shadow IT concept

In our review, we found that in general (despite a few scholars (e.g., Spierings et al., 2017)) the terms used for what is defined as shadow IT in literature are feral systems, IT workarounds, and shadow systems, based on the premise that it is IT that is not controlled by central IT. Table 1: presents a summary of these definitions.

Shadow IT	- Shadow IT describes the supplementation of "official" IT by several, autonomously developed IT systems and or processes that are part of the business departments; but not known, supported, and accepted by the official IT department." (Rentrop & Zimmermann, 2012). - Essentially, and according to Chua et al., (2014), this is the "development of systems outside of a central IT department." - It can also mean the "voluntary deployment of one or more systems by an individual in addition to or instead of the mandatory system when completing a task." (Haag et al., 2015)
Feral systems	- "Feral systems are argued to be mechanisms that circumvent normal systemic procedures in such a way that they create alternative means by which data can be accessed." Kerr et al., 2007. - Therefore, any technological artifact used by end-users rather than the desired Enterprise System (ES)." (Spierings et al., 2012) - According to Tambo & Baekgaard (2013), these behaviors are largely resultant as a reaction to discrepancies between official IT systems and actual business processes.
IT workaround	- "IT workarounds are a "form of anomalous system use within the organization. While these actions may be contrary to the intended uses and official rules, they nonetheless represent IT enactments in practice." (Azad & King 2012) - According to Ferneley & Sobreperez, (2006), when technology expectations lag behind actual working practices, employees will deviate from established methods in order to employ a 'workaround'.

Table 1: Shadow IT Definition

The use of shadow IT can take many different forms, including the use of unofficial project management tools, communication and collaboration tools, graphic design tools, video editing tools, peer-to-peer file sharing tools, and so on. This includes the tools that employees might be using on their approved (BYOD) mobile devices. In terms of negative and positive aspects of this phenomenon, the literature highlights, such as on the negative end, the risk of cyber security, information security, and also data loss at the third-party end as employees interact with organizational data on third-party apps creating limited visibility over data in the shadow apps. (Haag and Eckhardt, 2017; Haag et al., 2019; Shaikh, 2018; Silic and Back, 2014a;

Silic et al., 2017a). It leaves organizational data open to unauthorized access (and, sometimes, malicious actors who have deployed shadow apps in the cloud), since a security hole that is invisible to the organization and difficult to maintain is created when organizational data is fragmented across multiple shadow apps. The fragmentation of data also poses compliance and litigation risks. Even with the negative aspects of Shadow IT, Shadow IT is primarily used for its positive benefits, such as increased productivity, improved job performance, job satisfaction, collaboration, efficiency, flexibility, ease of use, convenience, and faster technological advancements(Györy et al., 2012; Haag and Eckhardt, 2014b; Harley et al., 2006; Mallmann et al., 2018a; Zimmermann and Rentrop, 2014)

Remote work environments, especially in the current pandemic climate, can exacerbate shadow IT by introducing certain constraints to the working environment and by distancing employees from work-related support. Research suggests that people use shadow IT to address perceived constraints or as a reaction to perceived situational constraints with the intent of enhancing performance, but not to harm the organization. However, beyond any situational constraints, the fact remains that employees are more likely than not to engage in behavior that poses a risk to their organization, such as violating proper security procedures (Guo et al., 2011). Taking a close look at shadow IT at both an individual and organizational level is essential. Having third-party applications readily available on the web as a result of the proliferation and adoption of the cloud also means shadow IT is more accessible and available (Mallmann et al.,2018), to employees who work from home without formal IT governance.

2.1.4 Shadow IT: Notable Studies

There is relatively little research on shadow IT in Information Systems and Information Security. In reference to shadow IT and information security, here are a few important studies. As seen in ((Silic and Back, 2014a) the topic of shadow IT is explored and presented as an understudied, misunderstood phenomenon. The primary objective of this paper is to understand what types of shadow IT software are used in organizations, what risks are associated with Shadow IT use, and what motivates shadow IT usage. As part of the Triangulation approach, the authors analyzed practitioner surveys found online to provide insights into real-life examples of Shadow IT used in organizations today, and secondly conducted expert interviews in order to confirm the shadow IT used within their organizations and to gain a deeper understanding of how they are used. As a third step, the authors extracted a database of installed software in employees' computers from a Fortune 500 firm with over 10,000 employees and compared it against the software found in employees' devices such as PCs, laptops, and other endpoint devices. The findings were as follows: 1) while some applications were legal and approved by the IT department, many others were not. Examples include greynet, content apps, and utility tools. 2) Shadow IT is largely facilitated by cloud computing services. 3) In terms of the motivation for shadow IT usage, the general consensus was that, in general, employees have no malicious intentions when they install unapproved software, instead, employees do not believe that they are violating any laws by installing software easily available on the internet. 4) Most employees simply lack a broader perspective on the potential risks to the organization's assets as they lack a broad understanding of these risks. The few people with advanced technical skills and knowledge of potential risks felt that merely using shadow IT would not be punished by the company. 5) In terms of perception of risk, the two biggest risks associated with Shadow IT are

data integrity and information leakage. One reason is that installing software that has not been approved increases the risk of malware, which directly affects data integrity and security. 6) Only mostly large organizations perceive themselves to be vulnerable to shadow IT risks, and even so, most do not have IT policies in place to regulate or control shadow IT.

In order to identify the factors that influence the adoption of shadow IT, (Silic et al., 2017a) conducted a multiorganizational survey study examining the role of deterrence and neutralization on shadow IT intention of usage and actual usage. Specifically, the effects of neutralization techniques (specifically “denial of responsibility, denial of injury, defense of necessity, defense of necessity, defense of necessity, condemn the condemner, appeal to higher loyalty, metaphor of the ledger”) are examined on both intentions to use Shadow IT (self-reported) and the actual behavior (shadow IT use), through the mediating role of shame. Study findings indicate that some neutralization strategies, like the "metaphor of the ledger", "defense of necessity" and "denial of injury", predict Shadow IT usage and others do not. There was a significant relationship between the metaphor of the ledger technique, and both intentions to use Shadow IT, and the actual behavior. Shame played a substantial role in mediating the relationship as well.

Following up on a previous study, the authors in (Haag et al., 2019) investigated the factors that influence shadow IT users' acceptance of usage justifications in light of IT constraints, as well as the types of factors that influence both non-users' and users' justifications. Furthermore, the authors investigated shadow IT users' and non-users' willingness to accept these shadow IT justifications based on IT constraints (factors that may drive acceptance) in order to explore the between group differences. They found that shadow IT users and non-users differed significantly in the factors that affect their justifications, and their acceptance of justifications in

the context of these constraints. Most importantly, the study found that non-users accepted justifications if they anticipated benefits related to shadow IT usage, whereas shadow IT users accepted justifications if they perceived others to be noncompliant.

And then finally, in attempt to link the malicious Insider Threat with Shadow IT, (Shaikh, 2018) proposes a conceptual model that links employee shadow IT usage with the potentials of employee fraud. The authors use the fraud triangle to analyze the phenomenon from the angle of the opportunity dimension, which depicts pressure, opportunity, and rationalization as factors that encourage people to commit fraud acts. Hence, the research seeks to understand the specific conditions that facilitate malicious threats in an organization that also facilitate shadow IT proliferation and use, with the aim of establishing the relationship between the various aspects of shadow IT culture and factors contributing to malicious insider threat. The main proposition is that there is a positive correlation between the use of shadow IT in an organization, and the susceptibility of that organizations to fraud from the employee. In other words, when shadow IT usage is prevalent within any organization, there is likely many opportunities for fraud to occur because opportunities for identity theft or fraud are always prevalent in a permissive environment with weak internal controls, poor management oversight, or a generally open environment where rules are not explicitly stated or consistently enforced. Hence, where there's a rampant use of shadow IT, fraud, such as identity theft, is more probable. As such, the proliferation of shadow IT within an organization is taken as an indication that the organizational climate and work environment organizational norms violations and fraud.

2.2 THEORETICAL FRAMEWORK

The Theory of Planned Behavior, TPB (Ajzen, 1991a, 199b), and General Strain Theory, GST (Agnew, 1992) are the proposed theories for examining the proliferation of shadow IT in the (remote) workplace away from formal organizational governance. TPB is a cognitive theory that links beliefs/perceptions and behavior, and GST is an environmental criminology theory that links crime and deviance behavior. Even though the TPB has been extensively used in the information systems (IS) AND information security research, the combination of TPB and GST (to model strenuous environmental factors) have not yet been empirically proposed or tested.

2.2.1 The Theory of Planned Behavior, TPB

The TPB descends from Ajzen and Fishbein's 1975 Theory of Reasoned Action, TRA (Fishbein and Ajzen, 1975), where behavior is presumed to be volitional (Ajzen, 1991a, 1991b; Arafat & Mohamed Ibrahim, 2018). These are the three components that make up the TPB: Attitude: person's positive or negative feelings regarding a particular behavior. In this study, it refers to attitudes towards using shadow IT in the WFH environment. Subjective norms: the opinions of those who are significant to a person about a particular behavior. In this study, it refers to the opinions of friends, coworkers, and supervisors on shadow IT. Perceived behavioral control: This refers to an individual's perception of how easy or difficult it is to perform. In this study, it refers to perceptions of how easy it is for WFH employees to access and utilize shadow IT. Both the definitions and contextualization of the constructs are listed in table 2

Construct	Definition
Attitude towards the behavior	**An individual's overall evaluation of the behavior.** It is assumed to have **two components that work together**: beliefs about the consequences of the behavior (**behavioral beliefs,** e.g., 'using E-APPS is a good idea' because it helps me be more productive as I work from home) and the corresponding positive or negative judgments of the **behavioral outcome evaluations**, e.g., 'being productive while I work from home is ... desirable/undesirable').
Subjective norms about the behavior	**An individual's own estimate of the social pressure to perform or not perform the target behavior in question.** Subjective norms are assumed to have **two components that work in interaction: beliefs about how other people, who may be in some way important to the person, would or would not approve of them being engaged in the behavior in question** (normative beliefs), e.g. 'I feel pressure from my colleagues who also work from home, to take advantage of using E-APPS') **and the positive or negative evaluations about the belief outcome**), e.g., 'in regard to my decision use E-PPS, doing what colleagues think I should do is important/ unimportant to me).
Perceived behavioral control of the behavior	**The extent to which a person feels able to enact the behavior.** It has **two aspects**: **how much a person has control over the behavior** (e.g., high control over being able to access or download E-APPS if the employee works from home vs at the office'), and **how confident a person feels about being able to perform or not perform the behavior** (e.g., not sufficiently skilled in finding, downloading and/or accessing E-APPS'). **It is determined by control beliefs about the power of both situational and internal factors to inhibit or facilitate the performing of the behavior** (e.g., 'Whether I use E-APPS is entirely up to me; 'I could access E-APPS if I wanted to').

Table 2: TPB Construct Definition (Ajzen, 1991b)

Across different phenomena in IS literature, the predictive and explanatory TPB has gained widespread acceptance and use. This is particularly true in studies that seek to predict or explain volitional behaviors such as IT security and technology adoption (Anderson and Agarwal, 2010); topics that both have to do with shadow IT proliferation in the remote workplace, where employees must decide whether or not to use shadow IT in lieu of sanctioned alternatives. There are various notable TPB related studies in the contextual research area (Information Security), and we highlight a few of them below, especially those that integrate TPB with other theories in order to remedy its economic and environmental limitations.

Using a proposed model that integrates Protection Motivation Theory (PMT) and TPB, Ifinedo, (2012) examined factors that influence insiders' compliance with established security

policies and used the findings to extract characteristics that influence compliance. According to the authors' findings, factors such as perceptions of one's ability to comply with a certain policy (self-efficacy), perceived effectiveness of the policy (response efficacy), attitudes and social norms around adherence to policies, and the perception of vulnerability if they fail to comply have a positive effect on employees' intentions to comply with security policies. It appears that compliance intentions in regard to security policies are shaped by social imperatives within the organization, attitudes towards compliance, and the threat of non-compliance and coping appraisals (Ifinedo, 2012). Balgurcu et al. (2010) also investigated insiders'/employees' compliance to security policies as part of a multi-organization field study based on TPB and RCT; where they concluded that compliance intentions are influenced by Attitude, Normative Beliefs, and Self-Efficacy. The study also found that attitudes toward compliance are affected by beliefs about the overall consequences of compliance and non-compliance, such as the benefits of compliance and the costs associated with non-compliance. A positive impact of Information Security Awareness was also found on Attitudes towards compliance and outcome beliefs. (Bulgurcu et al., 2010). Using General Deterrence Theory (GDT), PMT, TRA, Information Systems Success and Triandis' Behavioral Framework and Rewards, Pahnila et al. (2007) proposed a theoretical model which was tested. Employees' attitudes, normative beliefs, and habits were studied in order to understand security policy compliance by employees. Attitude, Normative Beliefs, and Habits were each found to significantly affect the likelihood of compliance with security policies. Attitude was also found to be affected by threat appraisal and facilitating conditions, but not by cope appraisal. Sanctions did not influence Intention to comply with security policies (Pahnila et al., 2007). Using the Decomposed TPB, PMT, and GDT, Herath and Rao (2009a, 2009b) examined factors that affect compliance, with the results

suggesting that organizational commitment and social influence compliance intentions, and policy attitudes are influenced by severity of breaches, response efficacy, self-efficacy, and response costs. The study also concluded that employees underestimate the probability of security breaches (Herath and Rao, 2009c, 2009b).

These studies and the likes of them are beneficial and important for a variety of reasons. Among the reasons is that they demonstrate how the TPB identifies important individual level cognitive variables that are predictive/explanatory of volitional behavior and the intentions thereof. These include beliefs and expectancy values, perceptions of control and power over a behavior, perceptions of self-confidence and competence when it comes to enacting the behavior in question, as well as social expectations, beliefs, and values. Moreover, the studies also show that combining TPB with other theories facilitates a deeper understanding of the phenomena. Of more importance, research like these emphasize the importance of information security research within the traditional work environments. In a traditional work environment, compliance can be enforced efficiently by monitoring, and security policies are well-defined, well-communicated, and well-implemented. As a matter of fact, compliance is expected, required and easily enforceable.

Despite the importance of studies, focus on security related end user behavior in traditional work environments where security policies are well-constructed, well-communicated, and well-defined with a clear understanding of the benefits and consequences of non-compliance, this study highlights the need for more information security research, especially research on end-users/insiders ***outside*** of the traditional work environment where compliance may be more difficult to enforce, and additionally where the need for well-designed, well-communicated, and well-defined security policies in regards to contextual end user actions

such as shadow IT use is even of more importance. As the work environment perimeter is dissolved, there may not also be mechanisms in place, such as end-to-end monitoring, that identify noncompliance.

The immediate risk of information security threats that shadow IT adoption poses in the rapidly growing remote workplace continues to be emphasized within the literature examining shadow IT self-adoption by employees (Haag et al., 2019; Silic and Back, 2014b; Silic et al., 2017b), raising important concerns about the safety of organizations information in the age of rapidly growing remote workplace. In non-traditional workplaces, research on individual-level decision-making processes and how they impact shadow IT proliferation, hence, plays an important role in advancing information security and end-user/insider-related security behavior today. And the decision-making process (which is regarded as a continuous cognitive process integrated in the interaction with the environment) as is corroborated by TPB is generally based on beliefs (or perceptions of a target behavior and the expected outcomes), assumptions of values (and norms regarding the course of action at hand), and the preferences of the decision maker in relation to the course of action at hand (which are often influenced by perceptions of controllability over the course of action, self-efficacy, etc.)

TPB is in agreement that decision-making (consisting of a continuous cognitive process embedded in interactions with the environment) is mainly driven by beliefs (or perceptions of a target behavior and its expected outcomes), assumptions of values (and norms regarding the course of action at hand), and the preferences of the decision maker in relation to the course of action at hand (which are often influenced by perceptions of controllability over the course of action, self-efficacy, etc.). A consideration of these factors combined with environmental factors precedes the selection of the optimal path, where the TPB constructs (attitude, perception of

control, and social norms) influence an individual's intention to take action depending on how they believe it will affect them. In other words, attitudes are shaped by beliefs about a behavior, including perceptions about its likely consequences (e.g., using shadow IT is justified since organizational IT support is limited at remote workplaces). Subjective norms are based on the individual's normative beliefs that are influenced by perceptions of specific salient others' preferences about whether or not to engage in a particular behavior (e.g., my workmates think using Shadow IT is a good idea, so I care about their opinions). Perceived Behavioral Control is based on beliefs about how to perform the behavior successfully (for example, I have easy access to Shadow IT since it is readily available and accessible through the cloud outside of normal organizational governance and direct oversight). These constructs represent an individual's will to engage in a behavior, such as adopting and utilizing Shadow IT.

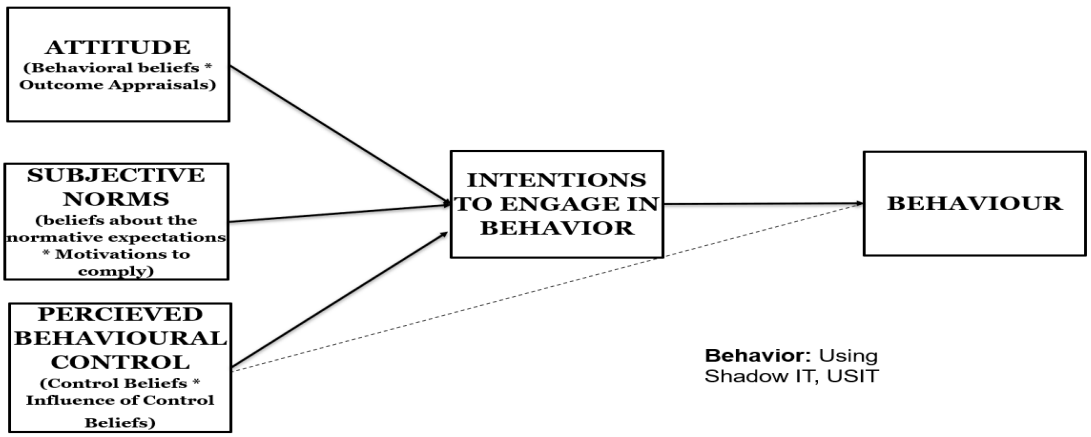

Figure 1: TPB Model (Ajzen, 1991)

2.2.2 General Strain Theory, GST

GST attempts to connect crime and delinquency at the individual level from the perspective of Sociology and Criminology. And the key proposition of GST is that strain leads to an increase in the likelihood of deviance or delinquency (Agnew, 1985, 1992). GST originates from the Strain theory by Merton, (1938) which proposed that the gap between aspirations and expectations led to a sense of frustration that ultimately led to deviant behavior as a result of not achieving positively valued goals (Merton, 1938). Merton's notion of strain was criticized for its narrow focus (Agnew, 1985), which was failure to achieve conventional or positive goals. This represents just one source of strain. Consequently, Agnew expanded upon this earlier conception by focusing on situations that result in delinquent or deviant behavior, such as situations in which individuals are confronted with noxious circumstances, or when they lose something to which they attribute positive meaning (Agnew, 1985, 1992). Hence, Agnew identifies three kinds of strain: 1) strain attributable to the actual or anticipated failure to achieve a positively valued goal; 2) strain attributable to the actual or anticipated loss of positively valued stimuli (e.g. stressful life events such as parental loss during the pandemic; or when an individual loses any other thing that they value such as a close friend, or a nice day care to send their kids to during COVID, etc.), and 3) strain attributable to the actual or anticipated introduction of noxious or negatively valued stimuli. With regard to this (situations where individuals are faced with noxious circumstances), the COVID-19 outbreak has introduced a variety of unpleasant circumstances into the (remote) workplace (e.g., struggles with on-the-job tasks away from work-related social support, digital management of on-the-job conflicts, a sense of uncertainty, job insecurity). The strain categories presented here are ideal strain categories, rather than constructs of strains. One cannot expect, for example, that a factor analysis of strainful events will reproduce these categories (Agnew, 1985). Several empirical studies support GST claim, such as those by Agnew, (2013), Agnew et al., (2002), Agnew & White, (1992), Aseltine

et al., (2000), Bao & Wierzbicki, (2004), Baron, (2007), Botchkovar et al., (2009), Broidy & Agnew, (1997), Broidy, (2001), Jang & Johnson, (2003), Mazerolle & Maahs, (2000), Mazerolle & Piquero, (1997), Moon et al., (2009), Paternoster & Mazerolle, (1994) and Piquero & Sealock, (2000). They show support for the key proposition of GST, suggesting that individuals exposed to strain are more likely to engage in deviant behavior to adjust to the strain (Agnew, 2013; Agnew et al., 2002; Agnew & White, 1992; Aseltine et al., 2000; Bao & Wierzbicki, 2004; Baron, 2007; Botchkovar et al., 2009; Broidy & Agnew, 1997; Broidy, 2001; Jang & Johnson, 2003; Mazerolle & Maahs, 2000; Mazerolle & Piquero, 1997; Moon et al., 2009; Paternoster & Mazerolle, 1994; Piquero & Sealock, 2000).

The GST also asserts that strain creates a negative emotional state, that is to say, feeling strain may lead to negative emotions like anger, depression, and frustration. This leads to delinquent adaptations (i.e., anger, anxiety, and depression) (Agnew, 1992). That is, people who experience negative emotions, such as situational anger (not trait anger), depression, and frustration, as a result of exposure to noxious stimuli (e.g., failure to achieve desired goals or ending a valued relationship), may commit delinquent behaviors as a way to manage or relieve the negative emotions. Several empirical studies also support this claim, such as those by Aseltine et al., (2000), Jang & Johnson, (2003), Mazerolle & Piquero, (1997), Moon et al., (2009) and Piquero & Sealock, (2000) give support to the notion that negative emotions mediate the connection between strains and deviant copying (Aseltine et al., 2000; Jang and Johnson, 2003, 2003; Mazerolle and Piquero, 1997, 1997; Moon et al., 2009, 2009; Piquero and Sealock, 2000). When it comes to characteristics of strains that lead to deviance, Agnew, (2001, 2016) proposes that strains likely to generate pressure or opportunities for criminogenic copying will lead to more deviance than other strains (Agnew, 2001, 2016).

CHAPTER 3: HYPOTHESES DEVELOPMENT AND RESEARCH MODEL

Based on the above discussion, the two relevant theories are integrated together to understand the phenomenon of Shadow IT adoption and use in the (remote) workplace. Specifically, the dependent variable is shadow IT adoption and use (henceforth USIT) in the workplace, i.e., end-user self-adoption of IT that exposes organizational information to untraceable security risks. In previous studies that have used TPB, results have shown that it is useful for predicting and explaining user behavior in relation to security both in the traditional and remote workplaces. The proposed research model, which is integrated with GST, an environmental criminology theory that has never been tested in the Information Security/Adoption domain, looks at the role of Strain through a mediating role played by negative affect, such as situational anger, depression, or frustration, in the adoption and use of Shadow IT in the (remote) workplace, testing strain's effects on the TPB model. The GST framework, along with TPB, facilitates a deeper understanding of threats at (remote) workplaces. Next, the research hypotheses are discussed.

3.1.1 USIT Intentions and USIT Behavior

TPB places importance on the behavior-intention relationship, whereby individuals' intentions to engage in a given behavior are used as an indicator of their readiness to carry out that behavior. IS literature on predicting technology usage suggests that behavioral intentions are largely predictive of actual IT usage (Shropshire et al., 2015; Tan et al., 2014; Venkatesh et al., 2008; Wu and Chen, 2005). Thus, an employee's intention to adopt and use Shadow IT is positively correlated with their actual shadow IT behavior, that is the downloading and or use of the software. Additionally, an employee's likelihood to use Shadow IT is positively correlated with the strength of their intention since intention represents commitment to take action. This means that the

stronger the intention to USIT, the more likely it is for an employee at a (remote) workplace to download and/or use USIT compared to when the intention is weak. The Theory of Reasoned Action and Theory of Planned Behavior both stress the strong relationship between intentions and behavior, wherein TPB holds that intention precedes behavior and intention strength influences the likelihood that the behavior will be performed. According to many subsequent studies that empirically tested this relationship in the literature of information systems and information security (eg., Bulgurcu et al., 2010; Herath & Rao, 2009a, 2009b; Ifinedo, 2012; Pahnila et al., 2007), therefore, we hypothesize that an employee's intention to adopt and/or use USIT affects USIT behavior.

- **H1a:** WFH Employee Intentions to use Shadow IT will have a positive effect on actual Shadow IT Usage Behavior

Although both TPB and TRA position behavior as a function of an individual's intentions to engage in certain behaviors, The TPB additionally positions the intention-behavior relationship to be stronger under the moderating effect of Perceived Behavioral Control (Ajzen, 1991b). Considering the context of this study, it appears plausible that if an individual intends to use Shadow IT at the (remote) workplace for work related purposes, they will actually use it if they perceive that they can. Accordingly, we hypothesized the following:

- **H1b:** Perceived Behavioral Control will moderate the positive relationship between an employee's Intention to USIT and the actual USIT behavior

As per TPB, an individual's intention to engage in a behavior, such as the USIT, depends upon attributes, including Attitude, Subjective Norms, and Perceived Behavioral Control. These attributes are discussed further below.

3.1.2 Attitude towards USIT in the (Remote) Workplace

The concept of attitude is psychological in nature (Jung, 1971). It is postulated that attitudes towards a stimulus object influence behavioral intentions (Ajzen, 1991, 2001). In IS research that uses TPB models, the relationship between Attitude and Intention has been extensively studied and found to be significant (Barki and Hartwick, 1994; Bulgurcu et al., 2010; Dienlin and Trepte, 2015; Herath and Rao, 2009b; Pahnila et al., 2007; Shropshire et al., 2015). In general, an individual's attitude toward a particular course of action is determined by their overall beliefs about it and their assessment of its results, i.e., using Shadow IT to do work is justified because it allows me to do work tasks at home versus using Shadow IT to do work is risky because the apps could have malware, etc. These represent the individual's positive or negative views toward participating in a specific behavior (Herath and Rao, 2009c, 2009b; Ifinedo, 2012)). Hence, WFH employees' attitudes about shadow IT in the work from home environment are reflected through their positive or negative beliefs about that behavior.

In related works in Information Security, for example, various studies demonstrate this by determining that employees who consider themselves vulnerable to security threats are more likely to adhere to security measures at work than employees who perceive themselves as invulnerable (Bulgurcu et al., 2010; Herath and Rao, 2009c, 2009b; Ifinedo, 2012; Pahnila et al., 2007). In a similar way, we can predict that individuals who perceive their organizations' information as vulnerable to security risks when shadow IT is used to process their sensitive information will be more likely to refrain from using Shadow IT than those who perceive that using Shadow IT does not expose the organization's information to security risks. The hypothesis in this study is also consistent with many subsequent studies including (Bulgurcu et al., 2010; Herath and Rao, 2009c, 2009b; Ifinedo, 2012; Pahnila et al., 2007). Those with

positive attitudes toward USIT are more likely to engage in USIT, and those with negative attitudes will refrain from engaging in USIT. Accordingly, we hypothesize that WFH employees positive attitude towards Shadow IT and its usage in (remote) workplaces and positive outcome appraisals will have a significant and positive effect on their intentions to USIT, and WFH employee negative attitude towards USIT in (remote) workplaces along with negative outcome appraisals will have a significant and negative effect on their intentions to USIT:

- **H2:** Attitude towards Shadow IT with respect to work will be significantly and positively related to WFH Employees' intentions to access, adopt and or use them

3.1.3 WFH Employee Subjective Norms and Social Influence in the Work from Home Environment

Psychology has found that humans have a psychological need to feel connected to others in order to be fulfilled (Ryan and Deci, 2000). If this need is met in any given context, intrinsic motivations to engage in activities related to that context are enhanced (Ryan and Deci, 2000; (Zhang et al., 2008). This is the basis for the concept of Subjective Norms. TPB explains subjective norms as the interpretation of social influences and norms that affect people's behavior and are formed through observing or consulting with the behavior of others (Ajzen, 2002; Ifinedo, 2012; Kim et al., 2019). Further, this is in line with McClelland, (1988) theory of needs which assumes that individuals are predisposed to behave in ways that are admired by their referent groups because they desire things like admiration, relationships, and group affiliations (McClelland, 1988). This provides insight into the perceptions people have about what they see as being normal in their environment (Chan and Goldthorpe, 2005; Johnston and Warkentin, 2010; Knapp et al.,

2006). Based on this definition, Subjective Norm represents individuals' beliefs about how they would be viewed by their referent groups if they, for example, adopted or used Shadow IT (Ajzen, 2002; Ifinedo, 2012).

Taking this argument into account, it is likely that if other employees (peers) self-opt for Shadow IT, a general feeling of acceptance can develop among employees. With the pandemic requiring remote employees to work away from organizational culture and IT support, it is also reasonable to assume that employees will use their social networks to gain support, advice, and insights to accomplish various ad hoc work tasks at home. We hypothesize therefore that the social aspect of Shadow IT in the remote workplace contributes to employee adoption and use of Shadow IT in the (remote) workplace. In a nutshell, do your colleagues endorse or disapprove of Shadow IT or have they used it in the past?

For instance, there is evidence that employees are more likely to adhere to regulations regarding information security if they notice how those around them, i.e., superiors, peers, and subordinates, adhere to such regulations (Bulgurcu et al., 2010; Ifinedo, 2012; Kim et al., 2019; White et al., 2009). These studies indicate that Subjective Norms play a crucial role in ensuring that Information Security policies are followed. Researchers in the area of information technology adoption such as (Zhang et al., 2008) have also observed that when consumers experience relatedness through the use of systems, they are more inclined to engage with them and continue to use them. Therefore, it is expected that USIT intentions of employees will be positively influenced by Subjective Norms. Thus, we hypothesize that:

- **H3:** WFH Employee Subjective norms regarding USIT will have a significant and positive effect on USIT intentions

3.1.4 WFH Employee Perceived Behavioral Control

The TPB holds that PBC pertains to individuals' judgments of their capacities to engage in certain behaviors, such as the USIT phenomenon (Ajzen, 1991b, 2002). This refers to an individual's perception that they have control over the target behavior, which is the expectation that they will successfully execute the behavior. As a result, people will engage in a target behavior when they are confident that they can succeed at it. Also included in PBC is the idea of how easy or difficult the behavior is for that person to perform. Based on social cognitive theory, PBC is influenced by Self-Efficacy (Bandura, 1991). The PBC, as defined in this study, therefore refers to how much control employees perceive that they have over using Shadow IT and accessing it. It also is a measure of how easy it is to perform the behavior.

Perceived Controllability (PC) and Self Efficacy (SE) determine PBC, according to the TPB. The concept of perceived controllability is closely related to the concept of perceived power. This refers to how an individual’s views their ability to make use of Shadow IT, and how much freedom or opportunity is available in the (remote) workplace, as opposed to on-site locations where there are more controls and oversight. Conversely, perceived controllability can also be defined as the perception of barriers to Shadow IT usage and can refer to anything that prevents Shadow IT usage in onsite workplaces, rather than in (remote) workplaces. The other end of the spectrum is perceived access to Shadow IT, which could affect how remote workers use Shadow IT. Taking all of these factors into account, it appears that controllability and perceived power can be interpreted differently in various types of locations and situations. Based on the proposed model, we believe it is higher in (remote) workplaces than in typical onsite environments because onsite workers tend to feel less powerless when working from home without direct organization oversight, which creates an enhanced sense of 'control' over the USIT phenomenon. The second component of the PBC Construct is Self-Efficacy, which represents the individual's ability to

successfully accomplish a task. In many studies, self-efficacy has been shown to positively influence a person's ability to complete a task. The Information Systems Continuance of Use research indicates that individuals who have high levels of self-efficacy when it comes to using information systems are more likely to use those systems (Bhattacherjee, 2001; Kim, 2010; Lee, 2010). According to Information Security research, individuals with a high level of IS security capabilities and competence are more likely to be conscious of the importance of following an organization's Information Security policies as well as to be more aware of the risks of noncompliance. Researchers such as Bulgurcu et al., (2010), Herath & Rao, (2009a, 2009b) and Ifinedo, 2012, Pahnila et al., (2007) have found this to be the case (Bulgurcu et al., 2010; Herath and Rao, 2009c, 2009b; Ifinedo, 2012; Pahnila et al., 2007). As a result, the following is hypothesized:

- **H4a:** PBC will have a significant and positive effect on the USIT intentions.

An individual's intention to become involved in a behavior (e.g., using Shadow IT) is influenced by these antecedents, where intentions are a person's motivation (Conner and Norman, 2017); intention being the most determinative factor of a volitional behavior (e.g., using Shadow IT).

3.1.5 Perceived Situational Strain, Negative Affect & USIT

TPB was initially criticized for not adequately accounting for the effect of environmental and economic factors that might influence a person's intentions and motivation to perform a target behavior. In this research, the environment has been cited as one of the major influences. Environmental stressors in this study are a result of COVID-19, a sudden move to a remote work model, and widespread lockdown during the pandemic. GST proposes that negative emotions motivate deviance due to Strain, which increases the likelihood that individuals will experience

negative emotions, which may then lead to deviance. GST proves to be an appropriate theoretical framework for understanding the USIT phenomenon at the (remote) workplace, particularly in light of COVID-19.

GST examines strain as a possible source of motivation for deviant behavior, including crime, as a coping strategy. Strain can trigger negative emotions in many ways, e.g., failure to achieve positively valued goals, loss of positively valued stimuli, presentation of negative stimuli. It has been hypothesized that these factors contribute to negative emotions. Among the negative emotions are situational depression, anxiety, anger, frustration, fear, and uncertainty. It is common to feel frustrated when goals and motivations are hindered, and frightened when there is a real threat of loss, such as the threat of losing income, family dynamics, job security, etc.

Agnew asserts, and supporting literature supports, that strain generates negative emotions that spur motivation to deviate as a coping strategy as such forces create pressure for corrective action. Due to the unmitigated effect of Strain on deviance being explained by alternative theoretical accounts (Agnew, 1995c), GST's empirical validity depends on the degree to which negative emotions influence deviance and crime. This study hypothesizes that COVID-associated strains and situational strains due to pandemics will be positively related to USIT, and the relationship will be mediated by negative affect, and which also moderate the relationships between the core TPB constructs and intention to USIT. COVID-related strains and pandemic-related situational challenges at work (remotely) may therefore be important determinants of intentions to adopt and USIT as mediated by a negative effect.

Because of COVID-19 and the lack of IT resources and support in a (remote) work setting away from formal office privileges, the (remote) workplace presents numerous obstacles. When individuals are stressed by losing positive stimuli, being confronted by negative stimuli, or unable

to reach desired goals, they can become disorganized, which results in individuals being less careful about whether or not they use approved apps for work tasks. According to this theory, deviations that occur in the (remote) workplace, such as the use of Shadow IT, may be a reflection of a general strain that affects employees today, as COVID-19 and remote work proliferate. This conceptualization led us to derive the following hypothesis by assuming that employees' motivations and subsequent intentions to USIT are due to strains and related negative emotions. Based on these assumptions,

- **H5a:** Perceived Situational Strain through the mediating role of Negative Affect will have a significant and positive effect on Intentions to USIT
- **H5b:** Negative Emotions/Affect will have positive effect on Intentions to USIT

As described in General Strain Theory, the coping mechanisms that individuals use in response to negative emotions are cognitive, behavioral, and emotional. The TPB and GST are integrated into an integrated model to incorporate these coping mechanisms. We therefore hypothesize that strain moderates the main TPB variables in the following way:

- **H6a:** Perceived Situational Strain will significantly moderate the relationship between Attitude and USIT intention such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain
- **H6b:** Perceived Situational Strain will significantly moderate the positive relationship between PBC and USIT intention such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain
- **H6c:** Perceived Situational Strain will significantly moderate the positive relationship between Subjective Norms and USIT intention such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain

- **H6d:** Perceived Situational Strain will significantly moderate the relationship between USIT intention and USIT (Behavior) such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain

Following the preceding discussion, the research model is presented in Figure 2. The dependent construct is USIT Behavior (the use of Shadow IT). In summary, the above constructs all represent the will and control an employee has over USIT, therefore the theory concludes that when an employee uses USIT, they have both volition and non-malicious intent. Further, USIT is a secretive process initiated by internal employees with 'trusted' and authorized access credentials to organizational data. However, USIT occurs in the shadows without IT/Security approval, which is harmful to confidentiality, integrity, and availability of information. This support this study's overarching proposing that USITs are volitional-non malicious acts of insider threats (The CERT Insider Threat Center, 2014), which makes them an element of Insider Threats according to Cappelli et al.'s definition of Insider Threats (Cappelli et al., 2012)

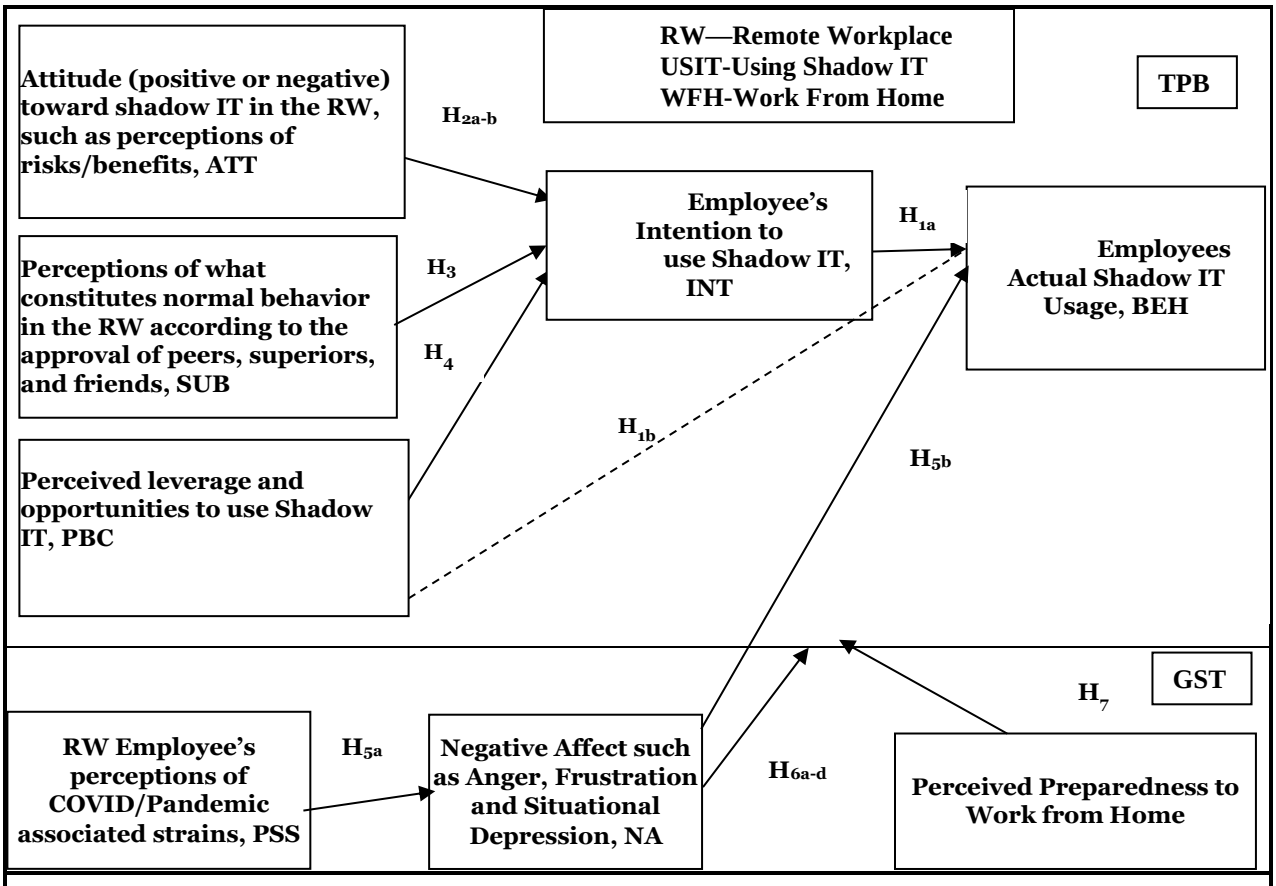

Figure 2: Integrated Model-based on The Theory of Planned Behavior and The General Theory of Strain

CHAPTER 4: RESEARCH METHODOLOGY

This section entails a discussion of the study design, the instrumentation process and the data collection process. As part of the study design process, IRB approval was sought and attained (Appendix 1), after which a web-based survey study was developed and deployed to test the research model and evaluate the proposed research hypotheses. Prior to the final data collection and analysis, two pilot studies were conducted for the assessment of the measurement model and the refinement of the measurement items. All measurement items were adopted from previous literature, and necessary adaptations were made to the items to reflect the study context. Almost all questions in the survey were measured on a 7-point Likert scale, ranging from "1= strongly disagree" to "7= strongly agree"; except for a few questions including the demographic questions. Detailed descriptions of the instrument development and data collection processes are given below

4.1. INSTRUMENTATION AND CONSTRUCT OPERATIONALIZATION

All psychometric constructs were operationalized and measured using previously validated instruments. As TPB is widely used in IS and security studies, a variety of measures were used from previous studies including Ajzen, (2006), Francis et al., (2004), Ifinedo, (2012), Balgurcu et al. (2010), Silic et al., (2017), and Herath and Rao, (2009a, 2009b). The behavioral intentions scale and behavior scales were modified from Ajzen, (2006), Francis et al., (2004) and Silic et al., (2017); the attitude scale was adapted from Ifinedo, (2012), Ajzen, (2006), Francis et al., (2004), and Bulgurcu et al., (2010), and Herath & (Rao, 2009a). For subjective norms, we used measures adapted from Ajzen, (2006), Francis et al., (2004), Ifinedo, (2012), Lee & Larsen, (2009), Chan et al., (2005), and Johnston & Warkentin, (2010). Perceived behavioral Control

was measured with items adapted from Ajzen, (2006), Francis et al., (2004), Compeau & Higgins, (1995), Workman et al., (2008), and Ifinedo, (2012). We note that behavioral intention corresponds to self-reported intentions towards the consideration of, search for and intended access or use of Shadow IT. Behavior is also self-reported use of Shadow IT by downloading and using it from the internet or accessing and using it from the web. The TPB construct definitions and measures as they pertain to this study are summarized in Appendix 3. We also included the GST construct definitions and its measures, however, as part of the focus of this study (measuring the role of situational strain on deviance), a detailed discussion of the GST instrumentation and construct operationalization is detailed below.

4.1.1 Measuring COVID-Related Strain

Related research including Piquero and Sealock, (2000, 2004) suggest that different strains can have unique effects on different types of deviance (Piquero and Sealock, 2000, 2004). In the current study, we have considered a variety of strains and only one kind of deviance, that is, choosing to use Shadow IT instead sanctioned alternatives in the (remote) workplace to process organizational data; a behavior that can pose risks to organizational information security. We identified certain types of strain in accordance with the variety of experiences seemingly common among WFH employees during COVID (e.g., financial strain such as whether one had unexpected expenses, loss of income, loss of investments or stock market downturn; health-related strain such as whether someone or their loved one was faced with a Cancer or COVID diagnosis at the time they were working from home; strain due to unanticipated increase in childcare or elder care responsibilities; and the general strain of home officing). Items were then adapted from the literature, modified to fit the context, and used to them.

The GST proposed by Agnew, (2006) is innovative because it suggests that Strain can be measured using a broad variety scale that reflects the specific kinds of strains encapsulated in the failure to achieve positively valued goals, the presentation of negative stimuli, and the removal of positive stimuli (Agnew, 2006). Strain measurements in accordance with Chilton et al., (2005), Ruiz et al., (2006), Fuller et al., (2003) were therefore adapted to the study context (Chilton et al., 2005; Fuller et al., 2003; Ruiz et al., 2006), in accordance with Agnew's work (Agnew, 1985, 1992, 2001, 2006b), and recent COVID 19 stress related studies (Arpaci et al., 2020; Cortez et al., 2020; Hamouche, 2020; Pedrozo-Pupo et al., 2020; Taylor et al., 2011). In the pilot, the measure was a 12-item variety scale (ranging from 0 to 7) with higher values representing higher levels of strain.

4.1.2. Measuring Negative Affect

GST argues that anger and frustration mediate the relationship between strain and deviance, and for this relationship to exist, strain must first be significantly related to anger/frustration. We measured the situational-based negative affect (frustration, anger, and depression). The situational-based negative emotions scale was adapted from items that tapped information on frustration, anger, situational depression. These items used are the COVID 19 stress scales (Arpaci et al., 2020; Cortez et al., 2020; Hamouche, 2020), adapted in accordance with Agnew, (1992), Brezina, (1996), and Piquero and Sealock, (2000, 2004). (Agnew, 1992; Brezina, 1996; Piquero and Sealock, 2000, 2004). Respondents were asked whether they reacted with anger, frustration, or depression (sadness) to a range of situations.

4.2 STUDY DESIGN

A web-based survey that was administered to 302 participants recruited at a southwestern university, was created with in Qualtrics. As part of proper research protocols, a consent form and instructions on the survey were presented to survey participants at the start of the survey. The consent form explains the purpose of the study, which is to understand cognitive and environmental factors at play in the acceleration of Shadow IT adoption and use in (the) remote workplace, instead of sanctioned alternatives. In addition, respondent was informed of their rights to participate, which is based on a voluntary basis. After the participants acknowledged the consent form with a "Yes, I agree to participate", they were presented a small scenario to make the Shadow IT phenomenon well understood; then a quality pledge which asked them to commit to providing high-quality responses. Respondents who chose the options "No, I do not agree to participate" in the consent section, or "I will not provide my best answers" to quality pledge were routed to the end of the survey. A filter question regarding age was also included in the survey to make sure that all respondents were also routed to the end of the survey; so were respondents who indicated that they have never worked from home working from home. This was to make sure that all respondents fit our sample population. In order to bring more clarity and to avoid any possible misunderstandings of the study phenomenon (Shadow IT), we also provided an explanation of what Shadow IT is (known as E-APPS or External Applications in the study to avoid biasing responses) by defining it as "any apps that employees might find on the internet and use for work related tasks on their own accord". We also defined what using E-APPS could look like in real work settings with the help of a scenario and clarified that it can mean anything from "downloading it on company PC and using it or accessing it on the cloud and processing company data on it". This is suggested in the literature (cite Silic and Back). By doing so, we complied with the guidelines suggested for improving contextual relevance in IS

security research (cite). After taking all these precautions, respondents were then presented with items for the measurement of the research model constructs.

In order to examine the presence of common method bias a marker variable (i.e., fashion consciousness (Lumpkin and Darden, 1982) was added. This was a methodological attempt to control for common method variance since we are collecting our data through self-reported survey. This technique is also recommended in circumstances where both the dependent variable and independent variable are being measured in the same survey. The questions are for an examination of the correlations between the marker variable and all other constructs to indicate if the measured variance in the research model is contributed by the research method rather than the variance that is expected to be contributed from the construct used for measurement (Podsakoff et al., 2003).

To account for careless responses by participants, we also included instructed response items (e.g., please choose “strongly disagree” for this item) in the survey (Meade and Craig, 2012). It is recommended in the literature that approximately one instructed response item should be added for every 50 to 100 items up to a maximum of three (Meade and Craig, 2012).

4.3. PILOT STUDY

The pilot process started with a pretest that involved 6 participants that include two former ISCS Ph.D. Students (professors at other universities), one consumer research professional and two ISCS professors They examined the survey for timing, content, and face validity. The pretest was done in early 2022. Based on suggestions from pretest stage, minor changes were made to the pilot survey, including a change in some of the wordings of the items.

Next, in order to check scale validity and reliability, we conducted 2 pilot studies. In pilot 1, data was collected from undergraduate and graduate master's students from mid-March 2022 End of April 2022. In the second Pilot, data was collected from Amazon Mechanical Turk, to corroborate the measurement model results from pilot 1. As we proceed into the next section, a discussion of data collection for both pilot 1 and pilot 2 are presented in more detail.

4.3.1. Pilot 1

For this phase, our respondents were students at a business school at a southwestern United States university. The students were at the time enrolled in the "Principles of Management Information Systems", "Introduction to Digital Forensics" and Java Programming II classes. The course instructors sent a message to students describing the study and asking them to complete the online survey. Instructors agreed to offer extra credit points in exchange for participation. The survey requests were sent out through blackboard to a total of 302 students and 230 responses returned. The response rate was about 60%, however, not all of the responses were usable. Out of the 230, 70 of the respondents were excluded due to a failure to adhere to all survey instructions, a failure on any of the survey quality checks, or a failure on any other screen questions.

For participants whose responses were used in the preliminary analysis, they adhered to all the instructions and passed screening questions as below detailed. As explained in the study design section, screening criteria included age, whether respondents have worked from home anytime during the pandemic (or if they work from home now), and whether they committed to giving their best responses. The required age of respondents is 18 and above. Respondents were expected to have worked from home at any time during the pandemic or at the moment. Respondents were expected to click "I have understood" to demonstrate that they understand the

scenario in the survey. Respondents were also expected to commit to providing thoughtful and honest answers by clicking “I will provide my best responses”. The three attention check questions that were embedded in the questionnaire survey instructed respondents to choose “strongly disagree” for all the items. They questions were as follows: Barack Obama was the first American president. "Please select strongly disagree"; The United States of America consists of 10 states. "Please select strongly disagree"; And I am happy with receiving a very large bill from the IRS. "Please select strongly disagree". Of the total of 302 students that were contacted through blackboard to participate in the survey via Qualtrics, 230 responses were returned, 160 of which are usable observations after data cleansing. Table 3 shows the number and reason for removing some response

Categories of Responses		**Quantity**	**Definition**
Total Observations (before cleaning)		230	Total number of observations before data cleaning
Unusable Observations	Consent Form	7	Did not agree to participate
	Quality and Screening Checks	40	Failed one or more quality criteria, or did not meet screening requirements such as age, etc.
	Attention Checks	23	Failed one or two attention criteria checks
Usable Observations		160	Respondents adhered to all instructions (consent form, screening criteria, quality checks and attention checks

Table 3: Pilot 1 Data Collection Details

4.3.2. Pilot 2

A second pilot was conducted in the same way as pilot 1 but with a more diverse sample population comprised of people from different organizations provided by Amazon Mechanical Turk. This is instead of the student sample. With the second pilot, we further checked for the

quality criteria using a more diverse sample, and after we refined the items from the first pilot. A total of 314 respondents were surveyed via Amazon Mechanical Turk during this study, which took place in mid-late June 2022. The response rate was 100%, but not all responses were useful. In total, 267 of the 314 were usable, while the rest were not usable due to a failure to follow all survey instructions, including providing consent. Others were not usable due to failing to pass quality checks and screening questions, as explained earlier in the study design section. Table 4 shows the number and reason for removing some responses.

Categories of Responses		**Quantity**	**Definition**
Total Observations (before cleaning)		314	Total number of observations before data cleaning
Unusable Observations	Consent Form	2	Did not agree to participate
	Screening Questions	10	Failed one or more screening questions such as age/WFH requirements
	Attention Checks	29	Failed any of the attention checks
	Quality Checks	6	Failed one or more quality criteria
Usable Observations		267	Respondents adhered to all instructions (consent form, screening criteria, quality checks and attention checks

Table 4: Pilot 2 Data Collection Details

4.4. MAIN STUDY

Main data collection happened in mid-late June 2022, where we collected 807 responses from respondents on Amazon Mechanical Turk. Out of these responses, however, not all of them were usable for the reasons documented in Table 5 below. As elaborated in the study design section and pilot 1 phase, respondents were required to provide consent prior to participating in the study, as well as adhere to all the instructions, including the passing of the screening questions

incorporated within the questionnaire instrument, attention check questions and quality check questions. We excluded responses from participants who did not adhere to all instructions

Categories of Responses		Quantity	Definition
Total Observations (before cleaning)		807	Total number of observations before data cleaning
Unusable Observations	Consent Form	14	Did not agree to participate
	Screening Questions	46	Failed one or more screening questions such as WFH requirements, Age
	Attention Checks	58	Failed any of the attention checks
	Quality Checks	15	Failed one or more quality criteria
Usable Observations		674	Respondents adhered to all instructions (consent form, screening criteria, quality checks and attention checks

Table 5**:** Main Data Collection Details

CHAPTER 5: DATA ANALYSIS

All data were checked in accordance with methodologies recommended in the literature (Moore and Benbasat 1991; Straub et al. 2004) Details provided below.

5.1 PILOT ANALYSIS

The component-based PLS-SEM approach (Hair et al., 2011) was used to test both the measurement and structural models in the pilot and main study. Component-based PLS (PLS-SEM) offers a number of advantages over covariance-based structural equation models (CB-SEM). The first one is that it is non-parametric, and therefore does not make assumptions about distributions of data, as does CB-SEM. Secondly, PLS-SEM is considered to be a more suitable method for prediction-oriented studies (Hair et al., 2011) while co-variance-based SEM is better suited for testing which models best fit the data (Anderson and Gerbing, 1988; Chin et al., 2003). Details on pilot data analysis is provided below.

5.1.1 Pilot 1

Because of the modifications and adaptations that were made to the instruments, an exploratory factor analysis (EFA) was conducted in Smart PLS in order to check the construct reliability and validity at the item level before performing a confirmatory factor analysis (CFA) in the main study. The overall sample was assessed, and items having factor loadings that were smaller than 0.45 were highlighted for further refinement as part of a reliability and validity establishment process. Standardized factor loadings greater than 0.45 were considered as a fair rating (Tabachnick and Fidell, 2007). Since we used already tested and well-established items, except for Strain which uses a variety scale, no items were dropped but highlighted for further refinement for a second pilot.

All of the items that reflect Negative affect loaded highly on the parent construct than all others, as well as all items that reflect Intention (INT) and Behavior (BEH). Four out of fourteen items loaded highly (over 0.45) or relatively highly (0.38) on the parent construct of Attitude (ATT), four out of seven loaded highly (over 0.45) or relatively highly (0.382) on the parent construct of Perceived Behavioral Control (PBC), eight out of twelve loaded highly (over 0.45) or relatively highly (0.402, 0.381) on the parent construct of Situational Strain (STR), and one out of six loaded highly (over 0.45) on the parent construct of Subjective Norms (SUBNs). This means ten out of fourteen items that reflect ATT, three out of seven items that reflect PBC, four out of twelve items that reflect STR, and one out of six items that reflect SUBNs were temporarily removed and highlighted for improvement. All factor loadings for initial model are reported in Table 6, and in Table 7; factor loadings after temporarily excluding low loading items are also reported.

	ATT	BEH	INT	NA	PBC	SUBNs	SSTR
ATT+1	**0.772**	-0.069	-0.158	0.048	-0.023	0.098	-0.019
ATT+2	**0.777**	-0.084	-0.203	0.013	-0.104	0.032	0.002
ATT+3	**0.83**	-0.162	-0.267	-0.029	-0.015	-0.037	0.045
ATT+a	**0.017**	0.129	0.103	0.091	-0.188	-0.015	0.03
ATT+b	**0.251**	-0.012	-0.095	-0.004	-0.019	-0.134	-0.031
ATT+c	**0.123**	0.059	-0.049	0.044	0.016	-0.197	-0.091
ATT+d	**0.163**	0.033	0	0.077	-0.093	-0.074	0.002
ATT-1	**0.064**	0.058	0.03	-0.158	-0.064	-0.05	0.117
ATT-2	**0.277**	0.012	-0.082	-0.177	-0.033	-0.107	0.008
ATT-3	**0.251**	-0.016	-0.106	-0.198	-0.138	-0.097	0.069
ATT-a	**0.289**	-0.093	-0.112	-0.044	0.177	-0.023	0.152
ATT-b	**0.048**	-0.085	-0.044	-0.045	-0.001	0.178	-0.028
ATT-c	**0.387**	-0.093	-0.149	0.08	0.025	-0.009	0.012
ATT_d	**0.204**	-0.145	-0.073	0.13	0.093	0.056	0.281
BEH 1	-0.093	**0.895**	0.362	-0.063	-0.203	-0.052	-0.062
BEH 2	-0.188	**0.983**	0.504	-0.072	-0.152	0.082	-0.071
BEH3	-0.217	**0.981**	0.5	-0.049	-0.154	0.075	-0.043
INT1	-0.233	0.326	**0.882**	0.082	-0.222	0.093	-0.117

INT2	-0.344	0.515	**0.97**	-0.014	-0.203	0.159	-0.098
INT3	-0.31	0.486	**0.949**	-0.031	-0.213	0.141	-0.113
NA 1	-0.099	0.008	0.083	**0.734**	0.079	0.223	0.346
NA 10	-0.025	-0.026	0.029	**0.882**	0.123	0.128	0.34
NA 2	-0.067	-0.043	0	**0.866**	0.09	0.097	0.265
NA 3	-0.092	-0.011	0.068	**0.728**	0.014	0.209	0.286
NA 4	0	-0.099	-0.037	**0.91**	0.011	0.05	0.301
NA 5	-0.041	-0.027	-0.025	**0.875**	0.004	0.11	0.306
NA 6	0.038	-0.059	0.051	**0.811**	0.084	0.097	0.347
NA 7	-0.087	0.034	-0.06	**0.732**	0.147	0.059	0.096
NA 8	0.088	-0.161	-0.078	**0.719**	0.002	-0.003	0.232
NA 9	-0.006	-0.105	-0.069	**0.82**	0.012	0.01	0.242
PBC2_E	-0.068	-0.101	-0.147	0.069	**0.946**	0.036	0.046
PBC_C1	0.189	-0.152	-0.109	0.044	**0.167**	0.063	0.04
PBC_C2	-0.036	0.056	0.105	-0.068	**-0.094**	-0.107	-0.374
PBC_C3	0.032	-0.129	-0.055	0.026	**0.268**	-0.109	-0.066
PBC_C4	0.167	-0.031	-0.098	-0.122	**0.382**	0.005	0.003
PBC_E2	-0.074	-0.133	-0.18	0.051	**0.95**	0.035	0.063
PBC_E3	-0.077	-0.146	-0.205	0.083	**0.948**	0.027	0.088
STR_1	-0.218	0.197	0.054	0.213	0.113	0.093	**0.463**
STR_10	0.186	-0.143	-0.13	0.05	0.206	0.063	**0.335**
STR_11	0.105	0.006	-0.28	0.143	-0.043	0.031	**0.402**
STR_12	-0.025	-0.112	-0.266	0.193	0.018	-0.003	**0.517**
STR_2	0.129	-0.122	0.063	0.249	0.1	0.079	**0.681**
STR_3	0.111	-0.058	0.074	0.261	0.127	0.095	**0.64**
STR_4	0.14	-0.143	-0.04	0.17	0.065	0.167	**0.595**
STR_5	0.222	-0.068	0.016	0.001	-0.038	0.048	**0.067**
STR_6	0.031	-0.18	-0.159	0.092	0.066	0.029	**0.381**
STR_7	0.012	-0.069	-0.051	0.023	-0.054	0.112	**0.281**
STR_8	-0.011	-0.014	-0.125	0.165	0.048	0.103	**0.538**
STR_9	-0.054	0.192	-0.047	0.121	0.003	0.05	**0.269**
SUB_1	-0.116	-0.065	0.055	0.187	0.127	**0.7**	0.198
SUB_2	-0.133	0.041	0.029	0.054	0.094	**0.74**	0.103
SUB_3	-0.069	0.007	0.046	0.066	0.2	**0.481**	0.043
SUB_a	0.085	-0.121	-0.008	0.142	-0.023	**0.226**	0.124
SUB_b	0.028	0.096	0.182	0.072	-0.036	**0.94**	0.105
SUB_c	0.021	-0.054	0.055	0.202	0.042	**0.766**	0.166

Table 6: Factor Loadings for Pilot Data (Before excluding low loading items)

After excluding all items with low factor loadings and those that cross loaded incorrectly, the model measurement model was greatly improved with most items loading at greater than 0.45 in accordance with Tabachnick and Fidell 2007, as shown in Table 7.

	ATT	BEH	INT	NA	PBC	SUBNs	SSTR
ATT+1	**0.842**	-0.069	-0.158	0.048	-0.036	0.102	-0.036
ATT+2	**0.91**	-0.084	-0.203	0.009	-0.136	0.036	-0.039
ATT+3	**0.932**	-0.162	-0.268	-0.034	-0.044	-0.034	0.017
ATT-c	**0.337**	-0.093	-0.15	0.077	0.002	-0.008	0.061
BEH 1	-0.07	**0.895**	0.362	-0.06	-0.152	-0.056	-0.096
BEH 2	-0.139	**0.983**	0.505	-0.067	-0.113	0.078	-0.066
BEH3	-0.171	**0.981**	0.501	-0.044	-0.116	0.072	-0.035
INT1	-0.174	0.326	**0.879**	0.085	-0.177	0.093	-0.034
INT2	-0.284	0.515	**0.971**	-0.009	-0.175	0.157	-0.034
INT3	-0.25	0.486	**0.95**	-0.025	-0.186	0.139	-0.04
NA 1	-0.057	0.008	0.082	**0.751**	0.063	0.224	0.364
NA 10	0.005	-0.026	0.028	**0.877**	0.102	0.13	0.315
NA 2	-0.008	-0.043	0	**0.865**	0.076	0.099	0.258
NA 3	-0.056	-0.011	0.068	**0.741**	0.014	0.211	0.297
NA 4	0.044	-0.099	-0.038	**0.912**	-0.006	0.053	0.295
NA 5	0.027	-0.027	-0.025	**0.879**	-0.021	0.114	0.3
NA 6	0.087	-0.059	0.05	**0.806**	0.059	0.102	0.34
NA 7	-0.013	0.034	-0.061	**0.729**	0.13	0.06	0.08
NA 8	0.098	-0.161	-0.079	**0.699**	-0.026	-0.002	0.163
NA 9	0.045	-0.105	-0.071	**0.805**	0.011	0.013	0.205
PBC2_E	-0.078	-0.101	-0.147	0.069	**0.978**	0.036	0.058
PBC_C4	0.081	-0.031	-0.099	-0.12	**0.345**	0.004	0.042
PBC_E2	-0.093	-0.133	-0.18	0.052	**0.981**	0.035	0.078
PBC_E3	-0.097	-0.146	-0.205	0.084	**0.974**	0.027	0.098
STR_1	-0.21	0.197	0.055	0.219	0.104	0.095	**0.538**
STR_12	-0.039	-0.112	-0.265	0.19	-0.011	-0.002	**0.343**
STR_2	0.119	-0.122	0.061	0.255	0.067	0.083	**0.803**
STR_3	0.067	-0.058	0.073	0.269	0.091	0.096	**0.811**
STR_4	0.105	-0.143	-0.04	0.174	0.048	0.17	**0.722**
STR_8	-0.08	-0.014	-0.125	0.164	-0.024	0.102	**0.371**
SUB_1	-0.128	-0.065	0.056	0.187	0.106	**0.701**	0.143
SUB_2	-0.075	0.041	0.03	0.056	0.079	**0.736**	0.075

SUB_3	-0.036	0.007	0.046	0.068	0.189	**0.484**	0.038
SUB_b	0.095	0.096	0.183	0.08	-0.046	**0.94**	0.12
SUB_c	0.002	-0.053	0.056	0.208	0.015	**0.769**	0.161

Table 7: Factor Loadings for Pilot Data

5.1.1 Construct Reliability and Validity Check

After the temporary exclusion of low factor-loaded items we assessed reliability of the constructs using Cronbach alpha and Composite Reliability known as reliability omega, (CR). Convergent validity was assessed with three metrics: average variance extracted (AVE), composite reliability (CR), and Cronbach's alpha (Alpha). Most of the convergent validity metrics were greater than the thresholds cited in relevant literature (AVE should be greater than 0.5, CR greater than 0.7 (McDonald (1999); Fornell and Larcker, 1981), and Cronbach's alpha above 0.7 (Nunnally, 1978). All the CR loadings were higher than the recommended value of 0.700. Cronbach's alpha of each construct exceeded the 0.700 threshold, except for ATT (0.64). Therefore, convergent validity was acceptable for some variables at the first pilot stage (BEH, INT, N_AFF) and below the recommended values for some (ATT, PBC AND STR). The results for reliability and validity along with the factor loadings for the items are presented in Table 8.

Before excluding low loading items below

Construct	No. of Items	Mean	Standard Deviation	Reliability (Cronbach's Alpha) (>0.70)	CR (>0.70)	(AVE) (>0.50)
ATT	14/14			0.64	0.631	0.172
BEH	3/3			0.95	0.968	0.909
INT	3/3			0.928	0.954	0.873
NA	10/10			0.941	0.95	0.657
PBC	7/7			0.736	0.759	0.422
SUBNs	6/6			0.775	0.822	0.465
SSTR	11/11			0.717	0.739	0.214

After excluding low loading items below

Construct	No. of Items	Mean	Standard Deviation	Cronbach's Alpha Alpha) (>0.70)	Composite Reliability (>0.70)	Average Variance Extracted (AVE) (>0.50)

ATT	4/14			0.756	0.861	0.63
BEH	3/3			0.95	0.968	0.909
INT	3/3			0.928	0.954	0.873
NA	10/12			0.941	0.95	0.655
PBC	4/7			0.845	0.914	0.747
SUBNs	5/6			0.812	0.854	0.548
SSTR	6/11			0.647	0.78	0.395

Table 8: Construct Reliability in Pilot 1

Discriminant validity was assessed, firstly, through comparison of the square root of the AVE of each construct to all of the correlation between it and other constructs (Fornell and Larcker, 1981), where all of the square root of the AVEs should be greater than any of the correlations between the corresponding construct and another construct (Chin, 1998, Jöreskog and Sörbom, 1996). This was corroborated using the Fornell-Larcker criterion, which establishes discriminate validity for each construct using the square root of the Average Variance Extracted (AVE) of each latent construct (Gefen and Straub, 2005). For each construct, the square root of AVE for the constructs was greater than the correlation values with other constructs (or the inter-construct correlation). These results support discriminant validity according to Fornell and Larcker (1981) as shown in Table 9

Before excluding low loading items below

	ATT	**BEH**	**INT**	**NA**	**PBC**	**SUBNs**	**SSTR**
ATT	**0.794**						
BEH	-0.138	**0.954**					
INT	-0.26	0.486	**0.934**				
NA	0.019	-0.059	0.01	**0.81**			
PBC	-0.072	-0.13	-0.191	0.045	**0.864**		
SUBNs	0.022	0.042	0.143	0.139	0.032	**0.74**	
SSTR	0	-0.065	-0.038	0.351	0.084	0.144	**0.628**

After excluding low loading items below

	ATT	**BEH**	**INT**	**NA**	**PBC**	**SUBNs**	**SSTR**
ATT	**0.415**						
BEH	-0.181	**0.954**					
INT	-0.322	0.485	**0.934**				

NA	-0.032	-0.064	0.006	**0.811**			
PBC	0.006	-0.173	-0.225	0.065	**0.649**		
SUBNs	-0.027	0.046	0.144	0.129	0.051	**0.682**	
SSTR	0.061	-0.061	-0.115	0.361	0.131	0.146	**0.463**

Table 9: Divergent Validity - Fornell Larcker Criterion

Discriminant Validity was also assessed in accordance with Pavlou, Liang, and Xue (2007), whereby, no inter-correlation between constructs should be higher than 0.9. in order to indicate Divergent Validity (Pavlou et al., 2007). This was assessed by the Heterotriat-montrait ratio (Henseler et al., 2015) with values below the threshold of 0.90 as shown in Table 10

Before excluding low loading items below

	ATT	**BEH**	**INT**	**NA**	**PBC**	**SUBNs**	**SSTR**
ATT							
BEH	0.152						
INT	0.297	0.497					
NA	0.092	0.076	0.082				
PBC	0.137	0.145	0.216	0.12			
SUBNs	0.17	0.112	0.113	0.185	0.144		
SSTR	0.259	0.229	0.231	0.423	0.173	0.249	

After excluding low loading items below

	ATT	**BEH**	**INT**	**NA**	**PBC**	**SUBNs**	**SSTR**
ATT							
BEH	0.203						
INT	0.285	0.497					
NA	0.245	0.076	0.082				
PBC	0.345	0.197	0.234	0.144			
SUBNs	0.353	0.14	0.115	0.211	0.188		
SSTR	0.442	0.236	0.24	0.31	0.32	0.252	

Table 10: Divergent Validity-Hetero-trait Monotrait Ratio (HTMT)

Discriminant Validity was also assessed by confirming that every item had the highest loading with its corresponding construct, as shown in Table 11

	ATT	**BEH**	**INT**	**NA**	**PBC**	**SUBNs**	**SSTR**
ATT+1	**0.842**	-0.069	-0.158	0.048	-0.036	0.102	-0.036

ATT+2	**0.91**	-0.084	-0.203	0.009	-0.136	0.036	-0.039
ATT+3	**0.932**	-0.162	-0.268	-0.034	-0.044	-0.034	0.017
ATT-c	**0.337**	-0.093	-0.15	0.077	0.002	-0.008	0.061
BEH 1	-0.07	**0.895**	0.362	-0.06	-0.152	-0.056	-0.096
BEH 2	-0.139	**0.983**	0.505	-0.067	-0.113	0.078	-0.066
BEH3	-0.171	**0.981**	0.501	-0.044	-0.116	0.072	-0.035
INT1	-0.174	0.326	**0.879**	0.085	-0.177	0.093	-0.034
INT2	-0.284	0.515	**0.971**	-0.009	-0.175	0.157	-0.034
INT3	-0.25	0.486	**0.95**	-0.025	-0.186	0.139	-0.04
NA 1	-0.057	0.008	0.082	**0.751**	0.063	0.224	0.364
NA 10	0.005	-0.026	0.028	**0.877**	0.102	0.13	0.315
NA 2	-0.008	-0.043	0	**0.865**	0.076	0.099	0.258
NA 3	-0.056	-0.011	0.068	**0.741**	0.014	0.211	0.297
NA 4	0.044	-0.099	-0.038	**0.912**	-0.006	0.053	0.295
NA 5	0.027	-0.027	-0.025	**0.879**	-0.021	0.114	0.3
NA 6	0.087	-0.059	0.05	**0.806**	0.059	0.102	0.34
NA 7	-0.013	0.034	-0.061	**0.729**	0.13	0.06	0.08
NA 8	0.098	-0.161	-0.079	**0.699**	-0.026	-0.002	0.163
NA 9	0.045	-0.105	-0.071	**0.805**	0.011	0.013	0.205
PBC2_E	-0.078	-0.101	-0.147	0.069	**0.978**	0.036	0.058
PBC_C4	0.081	-0.031	-0.099	-0.12	**0.345**	0.004	0.042
PBC_E2	-0.093	-0.133	-0.18	0.052	**0.981**	0.035	0.078
PBC_E3	-0.097	-0.146	-0.205	0.084	**0.974**	0.027	0.098
STR_1	-0.21	0.197	0.055	0.219	0.104	0.095	**0.538**
STR_12	-0.039	-0.112	-0.265	0.19	-0.011	-0.002	**0.343**
STR_2	0.119	-0.122	0.061	0.255	0.067	0.083	**0.803**
STR_3	0.067	-0.058	0.073	0.269	0.091	0.096	**0.811**
STR_4	0.105	-0.143	-0.04	0.174	0.048	0.17	**0.722**
STR_8	-0.08	-0.014	-0.125	0.164	-0.024	0.102	**0.371**
SUB_1	-0.128	-0.065	0.056	0.187	0.106	**0.701**	0.143
SUB_2	-0.075	0.041	0.03	0.056	0.079	**0.736**	0.075
SUB_3	-0.036	0.007	0.046	0.068	0.189	**0.484**	0.038

SUB_b	0.095	0.096	0.183	0.08	-0.046	**0.94**	0.12
SUB_c	0.002	-0.053	0.056	0.208	0.015	**0.769**	0.161

Table 11: Divergent Validity Cross Loadings

5.1.2 Pilot 2: Quality Criteria

Following the revision of the previously excluded items for clarity, a second pilot was conducted through Amazon Mechanical Turk (pilot 2) with a more diverse sample population. In Tables 12, 13, 14, and 15, the resultant measurement model and quality criteria (including convergent and discriminant validity) are presented, which is the basis for the main data measurement model.

	ATT	**BEH**	**INT**	**NA**	**PBC**	**STR**	**SUBNs**
ATT_1	**0.716**	0.105	0.098	0.239	0.518	0.41	0.364
ATT_2	**0.585**	0.089	0.088	0.373	0.434	0.554	0.389
ATT_3	**0.633**	-0.003	0.003	0.253	0.575	0.441	0.377
ATT_4	**0.679**	0.012	0.076	0.306	0.584	0.489	0.376
ATT_O1	**0.74**	0.097	0.117	0.337	0.658	0.52	0.539
ATT_O2	**0.834**	0.155	0.233	0.319	0.522	0.412	0.429
ATT_O3	**0.793**	0.121	0.15	0.319	0.6	0.502	0.547
BEH 1	0.093	**0.89**	0.388	0.009	0.106	0.057	0.096
BEH 2	0.15	**0.983**	0.527	0.019	0.108	0.056	0.128
BEH3	0.167	**0.979**	0.523	0.022	0.114	0.069	0.111
INT1	0.154	0.353	**0.892**	0.223	0.147	0.117	0.209
INT2	0.164	0.54	**0.964**	0.127	0.121	0.06	0.185
INT3	0.231	0.519	**0.951**	0.123	0.172	0.102	0.2
NA_1	0.314	0.059	0.14	**0.776**	0.315	0.549	0.446
NA_10	0.413	0.045	0.174	**0.873**	0.417	0.621	0.552

NA_2	0.368	0.116	0.25	**0.845**	0.423	0.63	0.507
NA_3	0.362	0.054	0.216	**0.83**	0.322	0.523	0.487
NA_4	0.29	-0.076	0.072	**0.854**	0.356	0.61	0.501
NA_5	0.339	-0.084	0.067	**0.818**	0.299	0.537	0.447
NA_6	0.402	0.028	0.124	**0.892**	0.439	0.63	0.534
NA_7	0.414	0.016	0.134	**0.79**	0.377	0.541	0.463
NA_8	0.29	-0.066	-0.003	**0.822**	0.361	0.561	0.43
NA_9	0.319	0.034	0.164	**0.862**	0.306	0.549	0.514
PBC1	0.56	0.098	0.086	0.286	**0.708**	0.46	0.514
PBC2	0.557	-0.007	0.042	0.355	**0.742**	0.564	0.576
PBC3	0.567	0.117	0.127	0.317	**0.83**	0.507	0.577
PBC4	0.594	0.056	0.12	0.338	**0.855**	0.611	0.62
PBC5	0.608	0.094	0.189	0.365	**0.871**	0.574	0.613
PBC6	0.677	0.171	0.134	0.403	**0.861**	0.616	0.65
PBC7	0.593	0.015	0.067	0.428	**0.671**	0.599	0.618
STR1	0.487	0.066	0.147	0.616	0.52	**0.821**	0.584
STR2	0.452	0.089	0.117	0.528	0.5	**0.776**	0.544
STR3	0.499	0.066	0.093	0.53	0.453	**0.757**	0.544
STR4	0.463	0.011	-0.013	0.517	0.563	**0.789**	0.516
STR5	0.477	-0.02	0.04	0.482	0.485	**0.722**	0.476
STR6	0.494	-0.04	-0.007	0.478	0.563	**0.732**	0.508
STR7	0.548	0.023	0.093	0.53	0.554	**0.742**	0.503
STR8	0.5	0.086	0.054	0.486	0.576	**0.779**	0.488
STR9	0.335	-0.113	-0.114	0.357	0.373	**0.545**	0.418
STR10	0.285	0.159	0.098	0.362	0.314	**0.504**	0.42
STR11	0.278	0.006	-0.029	0.345	0.4	**0.488**	0.46
STR12	0.501	0.063	0.136	0.515	0.51	**0.707**	0.563
STR13	0.497	0.091	0.131	0.562	0.642	**0.817**	0.604

STR14	0.429	0.049	0.069	0.577	0.476	**0.752**	0.54
STR15	0.455	0.121	0.142	0.49	0.507	**0.795**	0.536
SUBN1	0.336	0.117	0.182	0.47	0.443	0.484	**0.811**
SUBN2	0.264	0.08	0.153	0.418	0.486	0.472	**0.816**
SUBN3	0.409	0.08	0.18	0.448	0.528	0.49	**0.822**
SUB4	0.484	0.037	0.131	0.481	0.538	0.65	**0.722**
SUB5	0.5	0.084	0.142	0.416	0.569	0.416	**0.67**
SUB6	0.596	0.132	0.167	0.462	0.663	0.411	**0.739**

Table 12: Factor Loadings-Pilot 2

	No. of Items	**Cronbach Alpha (>0.70)**	**Composite Reliability (>0.70)**	**Average Variance Extracted (>0.50)**
ATT	6	0.861	0.879	0.513
BEH	3	0.948	0.967	0.906
INT	3	0.93	0.955	0.877
NA	10	0.952	0.959	0.7
PBC	6	0.904	0.922	0.632
STR	15	0.932	0.941	0.523
SUB	6	0.858	0.894	0.586

Table 13: Construct Reliability-Pilot 2

	ATT	**BEH**	**INT**	**NA**	**PBC**	**STR**	**SUB**
ATT	**0.716**						
BEH	0.147	**0.952**					
INT	0.198	0.51	**0.936**				
NA	0.421	0.018	0.163	**0.837**			
PBC	0.637	0.114	0.157	0.435	**0.795**		
STR	0.625	0.064	0.097	0.69	0.591	**0.723**	
SUB	0.599	0.118	0.21	0.585	0.537	0.513	**0.765**

Table 14: Fornell Larcker Criterion (Divergent Validity) -Pilot 2

	ATT	BEH	INT	NA	PBC	STR	SUB
ATT							
BEH	0.123						
INT	0.166	0.529					
NA	0.458	0.072	0.181				
PBC	0.859	0.108	0.15	0.478			
STR	0.716	0.1	0.131	0.726	0.769		
SUB	0.693	0.127	0.235	0.648	0.861	0.815	

Table 15: Hetero-trait Monotrait Ratio (HTMT) (Divergent Validity)-Pilot 2

5.2 MAIN DATA ANALYSIS

5.2.2. Demographic characteristics & Descriptive Statistics

As part of the main study, respondents were asked to give demographic information such as their gender, age, and ethnicity. In Table 16, we provide these demographic statistics. Accordingly, the gender breakdown of the sample appeared to be fairly equal with male respondents making up 51.6% and female respondents making up 48.4%. Regarding gender, while the 19-29 age group is more represented in the data than other age groups, the age distribution is wide (19-69). As far as ethnicity is concerned, over half of the respondents identified as Caucasian. The second largest groups of respondents represented in the data were Black and Asian, followed by other groups (American Indians or Alaska Natives, Native Hawaiians or Other Pacific Islanders, and Mixed Race). Aside from demographics, respondents were also asked other important information of interest to the researchers, such as whether they used their own devices for work purposes; or company-owned, or both devices while they worked from home. These options were not mutually exclusive, which meant respondents could

choose both personal devices, company devices, or both. The data shows that employees who used personal devices for work purposes accounted for a higher percentage of data points than those who used company devices, or both personal and company devices. Additionally, and of importance to the study also, respondents were asked as to whether they had worked from home before COVID started, or if they did so after COVID began (and due to COVID). The data also showed that those employees who worked from home after COVID began (and as a result of COVID) were more prevalent in the data than those who had already worked from home before COVID began. In this situation, the researchers could not evaluate the between-group differences between the working from home group before COVID, and the working from home group only after COVID. In addition, it hampered the examination of the impact of the exploratory variable "perceived readiness to work from home" on Shadow IT use in the remote workplace. Further, respondents were asked to provide the duration of their employment with their current company. Most had worked for their respective organizations for five or more years.

		Freq	%			Freq	%
GENDER	**Female**	326	48.4	**ETHNICITY**	**Caucasian**	561	83.2
	Male	348	51.6		**Black**	46	6.8
AGE	**M**in	19			**Asian**	50	7.4
	Max	69			**Other**	17	2.5
	Mean	37.96		**WFH STATUS**	**@COVID**	541	80.3
	Std. Dev	10.884			**Before COVID**	133	19.7
DEVICE USED	**Comp. Owned**	239	35.5	**ORG. TENURE**	**< 1Yr**	34	5.0
	Personal	79	11.7		**1Yr≤ x ≤ 2Yrs**	110	16.3
	Both	356	52.8		**2Yrs≤ x ≤ 3Yrs**	149	22.1
					3Yrs≤ x ≤ 4Yrs	128	19.0
					≥5Yrs	253	37.5

Table 16: Demographic and Relevant Descriptives (N=674)

5.2.3 Measurement Model

Figure 3 depicts our outer model with high factor loadings, and in Table 17, the factor loadings of each construct against itself is presented in comparison to other constructs. Accordingly, all items have a stronger correlation with their respective constructs than with others, indicating evidence of discriminant validity.

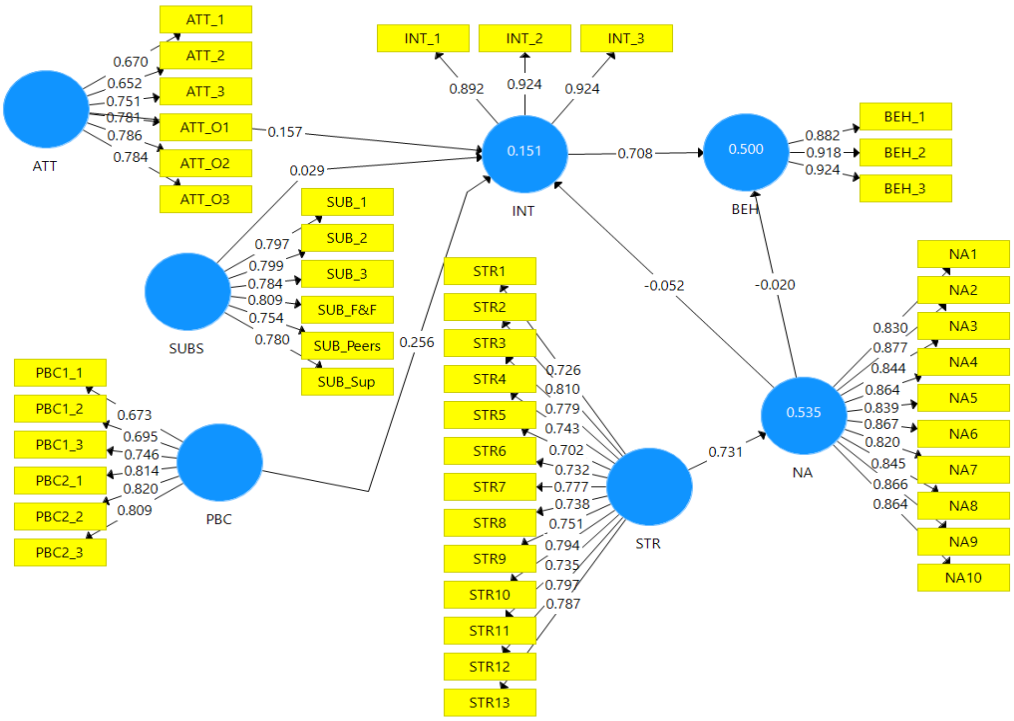

Figure 3: Outer Model with indicator loadings

In order to further corroborate discriminant validity, the square root of the AVE of each construct was compared to all of the correlations between it and other constructs (Fornell and Larcker, 1981), where all of the square root of the AVEs should be greater than any of the correlations between the corresponding construct and another construct (Chin, 1998, Jöreskog and Sörbom, 1996). This was corroborated using the Fornell-Larcker criterion as presented in Table 17. Lastly, discriminant validity was also corroborated in accordance with Pavlou, Liang, and Xue (2007), where no inter-correlation between constructs should be greater than 0.9. in

order to indicate Divergent Validity (Pavlou et al., 2007). As shown in the Heteotriat-montrait ratio in Table 18, this is corroborated with all values below 0.90 (Henseler et al., 2015).

	ATT	BEH	INT	NA	PBC	STR	SUBS
ATT_1	**0.67**	0.233	0.244	0.126	0.509	0.247	0.483
ATT_2	**0.652**	0.234	0.249	0.084	0.455	0.203	0.399
ATT_3	**0.751**	0.195	0.232	0.187	0.469	0.321	0.437
ATT_O1	**0.781**	0.235	0.254	0.125	0.515	0.291	0.455
ATT_O2	**0.786**	0.26	0.252	0.15	0.455	0.288	0.413
ATT_O3	**0.784**	0.23	0.248	0.126	0.524	0.292	0.468
BEH_1	0.284	**0.882**	0.59	0.014	0.286	0.142	0.204
BEH_2	0.267	**0.918**	0.676	0.027	0.271	0.147	0.234
BEH_3	0.306	**0.924**	0.655	0.029	0.301	0.139	0.234
INT_1	0.323	0.59	**0.892**	0.096	0.362	0.163	0.289
INT_2	0.293	0.674	**0.924**	0.046	0.308	0.128	0.252
INT_3	0.301	0.672	**0.924**	0.039	0.334	0.151	0.276
NA1	0.118	0.018	0.072	**0.83**	0.233	0.593	0.296
NA10	0.149	0.047	0.079	**0.864**	0.235	0.627	0.328
NA2	0.172	0.019	0.059	**0.877**	0.268	0.636	0.373
NA3	0.157	0.05	0.069	**0.844**	0.264	0.648	0.327
NA4	0.11	0.018	0.071	**0.864**	0.238	0.624	0.353
NA5	0.203	0.02	0.034	**0.839**	0.264	0.619	0.342
NA6	0.169	0.001	0.044	**0.867**	0.281	0.646	0.399
NA7	0.191	0.021	0.061	**0.82**	0.283	0.593	0.351
NA8	0.109	-0.001	0.012	**0.845**	0.261	0.617	0.318
NA9	0.15	0.028	0.056	**0.866**	0.266	0.623	0.359
PBC1_1	0.389	0.188	0.266	0.328	**0.673**	0.369	0.505
PBC1_2	0.402	0.154	0.214	0.228	**0.695**	0.36	0.519
PBC1_3	0.476	0.224	0.264	0.181	**0.746**	0.318	0.561
PBC2_1	0.551	0.273	0.301	0.227	**0.814**	0.403	0.592
PBC2_2	0.572	0.277	0.315	0.199	**0.82**	0.371	0.628
PBC2_3	0.598	0.294	0.298	0.24	**0.809**	0.413	0.681
STR1	0.313	0.147	0.151	0.573	0.357	**0.726**	0.403
STR10	0.3	0.138	0.105	0.511	0.4	**0.794**	0.43
STR11	0.262	0.121	0.153	0.576	0.347	**0.735**	0.367
STR12	0.219	0.056	0.064	0.629	0.345	**0.797**	0.373
STR13	0.251	0.087	0.133	0.606	0.434	**0.787**	0.475
STR2	0.281	0.137	0.124	0.567	0.368	**0.81**	0.419
STR3	0.263	0.107	0.146	0.632	0.385	**0.779**	0.431
STR4	0.223	0.094	0.07	0.538	0.314	**0.743**	0.391
STR5	0.314	0.146	0.191	0.474	0.337	**0.702**	0.38

STR6	0.321	0.171	0.164	0.52	0.409	**0.732**	0.425
STR7	0.3	0.133	0.09	0.531	0.377	**0.777**	0.414
STR8	0.3	0.138	0.096	0.511	0.389	**0.738**	0.435
STR9	0.343	0.097	0.112	0.51	0.367	**0.751**	0.395
SUB_1	0.451	0.193	0.236	0.348	0.602	0.424	**0.797**
SUB_2	0.522	0.205	0.238	0.283	0.65	0.435	**0.799**
SUB_3	0.472	0.183	0.22	0.355	0.585	0.454	**0.784**
SUB_F&F	0.542	0.252	0.313	0.255	0.629	0.398	**0.809**
SUB_Peers	0.352	0.151	0.168	0.381	0.575	0.448	**0.754**
SUB_Sup	0.437	0.144	0.178	0.345	0.561	0.417	**0.78**

Table 17: Factor Loadings/Discriminant Validity Main

	ATT	**BEH**	**INT**	**NA**	**PBC**	**STR**	**SUBS**
ATT	**0.739**						
BEH	0.314	**0.908**					
INT	0.334	0.707	**0.914**				
NA	0.179	0.026	0.065	**0.852**			
PBC	0.661	0.315	0.366	0.304	**0.762**		
STR	0.37	0.157	0.161	0.731	0.489	**0.76**	
SUBS	0.6	0.247	0.298	0.405	0.766	0.54	**0.787**

Table 18: Discriminant Validity-Fornell Larcker Criterion Main

	ATT	**BEH**	**INT**	**NA**	**PBC**	**STR**
ATT						
BEH	0.364					
INT	0.386	0.785				
NA	0.202	0.035	0.071			
PBC	0.776	0.354	0.414	0.34		
STR	0.424	0.174	0.176	0.766	0.546	
SUBS	0.685	0.268	0.321	0.452	0.875	0.599

Table 19: Discriminant Validity-Hetero-trait Monotrait Ratio (HTMT) Main

To ascertain convergent validity, three metrics were used: average variance extracted (AVE), composite reliability (CR), and Cronbach's alpha (Alpha). All convergent validity metrics were greater than the thresholds cited in relevant literature (AVE should be greater than 0.5, CR greater than 0.7 (Fornell and Larcker, 1981), and Cronbach’s alpha above 0.7 (Nunnally, 1978).

	No of items	CA (>0.70)	CR (>0.70)	AVE (>0.50)
ATT	6	0.832	0.878	0.547
BEH	3	0.894	0.934	0.825
INT	3	0.901	0.938	0.835
NA	10	0.958	0.964	0.726
PBC	6	0.854	0.892	0.581
STR	15	0.939	0.947	0.578
SUBS	6	0.879	0.907	0.619

Table 20: Construct Reliability Main

5.2.4 Multicollinearity Check

To further assess the reliability of the instruments, we assess the assumption of no multicollinearity. In this regard, variance inflation factor (VIF) is evaluated, as shown in Table 21. Our evaluations showed that VIF values were well below the generally accepted threshold of 10, which indicates that multicollinearity is not a cause of concern for any of the constructs (Petter et al. 2007).

Attributes	VIF	Attribute	VIF
ATT_1	1.584	**NA1**	2.795
ATT_2	1.544	**NA10**	3.284
ATT_3	1.765	**NA2**	3.688
ATT_O1	1.946	**NA3**	2.992
ATT_O2	2.034	**NA4**	3.356
ATT_O3	2.014	**NA5**	2.978
BEH_1	2.345	**NA6**	3.438
BEH_2	2.865	**NA7**	2.74
BEH_3	3.074	**NA8**	2.991
INT_1	2.41	**NA9**	3.615
INT_2	3.245	**STR1**	1.908
INT_3	3.201	**STR10**	2.488
NA1	2.795	**STR11**	1.926
NA10	3.284	**STR12**	2.335
NA2	3.688	**STR13**	2.333
NA3	2.992	**STR2**	2.627
NA4	3.356	**STR3**	2.25

NA5	2.978	**STR4**	2.008
NA6	3.438	**STR5**	1.978
NA7	2.74	**STR6**	1.972
NA8	2.991	**STR7**	2.215
NA9	3.615	**STR8**	2.038
PBC1_1	1.645	**STR9**	2.142
PBC1_2	1.683	**SUB_1**	2.119
PBC1_3	1.705	**SUB_2**	2.098
PBC2_1	2.256	**SUB_3**	2.111
PBC2_2	2.334	**SUB_F**	1.949
PBC2_3	2.298	**SUB_P**	2.116
		SUB_S	2.333

Table 21: variance inflation factor (VIF)

5.2.5 Other Diagnostic

Additionally, because the data was collected via self-reported surveys with both the independent and dependent variables measured in the same survey, we examined Common Method Variance (CMV). According to Podsakoff et al. (2003), CMV is the measured variance that is contributed by the research method rather than the variance that is expected to be contributed by the construct itself (Podsakoff et al. 2003). By using 1) Harman's single factor test (Podsakoff et al. 2003), 2) partial correlation technique with marker variables (Lindell and Whitney 2000), and 3) full collinearity assessment (Kock & Lynn, 2012), we assessed common method bias. For Harman's single factor test, all of the items were loaded on a single factor in an EFA through SPSS. When running the EFA model with a single unrotated factor, the largest eigenvalue 15.839 explained 32.99% of variance, indicating that the majority of variance cannot be accounted for by one factor and therefore CMV is l=not a concern based on Harman's single factor test. Using marker variable technique, we added an unrelated variable (Fashion Consciousness). In theory, a marker variable has no relationship to the variables and framework under study. Based on the assumption that all constructs have no relationship with each other, we

examined the correlation between this marker variable and the remaining constructs (Son and Kim, 2008). Accordingly, if the average of correlation coefficients of the constructs is less than 0.1, CMV effects are not substantial (Malhotra et al. 2006; Son and Kim 2008). It is reasonable to conclude that common methods bias does not pose a serious threat to our research since the results of the test were 0.017. In addition, and in accordance full collinearity test, all inner VIF values were smaller than 3.3 with the highest being 2.867, showing that there are no concerns regarding common method bias (Kock & Lynn, 2012).

5.2.5 Model Fit

To determine the model fit for the measurement model, four model fit indices are considered: Chi-Square (χ^2), Tucker-Lewis Index (TLI) (Bentler & Bonett, 1980; Tucker & Lewis, 1973), Comparative Fit Index (CFI) (Bentler, 1990), and Root Mean Square Error of Approximation (RMSEA) (Steiger, 1990; Steiger & Lind, 1980). Due to its sensitivity to sample size, model complexity, and violations of multivariate normality, less emphasis is placed on the χ^2 statistic. Accordingly, a CFI and TLI cutoff of above .95 indicates excellent model fit and between .90 and .95 indicates acceptable model fit. For the RMSEA, values of less than or equal .08 indicate a good model fit, those between .06 and .08 indicate an adequate model fit, those between .08 and .10 indicate a mediocre model fit, and those greater than .10 indicate a poor model fit (Schumacker and Lomax 2004). In our case, the following results for model fit in the measurement model showed: $\chi 2$ is 2951.815, CFI=0.93, TLI=.0.908, RMSEA= 0.053. We may thus conclude that we reached a satisfactory or good overall model fit (see Table 16).

$\chi 2$	**df**	**P-value**	**CFI**	**TLI**	**RMSEA**
2951.815	1022	0.000	0.93	0.908	0.053

Table 22:Path Model Fit Indices

CHAPTER 6: RESULTS AND DISCUSSION

6.1 RESULTS

6.1.1 Assessment of the structural model

The structural model reflects the paths hypothesized in the research framework. The structural model uses the path coefficients (*) and squared R (R) to show the path significance of hypothesized relationships. The strength of the relationship is indicated by the β. The R^2 measures the model's predictive power by indicating its variance percentage.

6.1.2 Goodness of Fit

The coefficient of determination (R^2), effect size (F^2), and predictive relevance measure (Q^2) were assessed to determine the goodness of fit. R-Square statistics explains the variance in the endogenous variable explained by the exogenous variable(s). To determine whether a particular endogenous construct adequately explains variance, Falk and Miller (1992) recommended that R^2 values be equal to or greater than 0.10. According to Cohen (1988), R^2 values are measured as: 0.26 (substantial), 0.13 (moderate), and 0.02 (weak). As shown in table 17, the R^2 analyses for the endogenous variables in the model are 0.508 for BEH, 0.151 for INT, and 0.534 for NA. Accordingly, 50.8% of variance in Behavior (USIT) can be attributed to INT and STR; 15.1% of variance in INT can be attributed to ATT, SUB, PBC STR, and NA; and 53.4% of variance in NA can be attributed to STR. For all endogenous variables, we obtained acceptable R2 statistics based on Falk and Miller's 1992 cutoff value of 0.10.

Further, a variable in a structural model may be affected/influenced by a number of different variables, such that the removal of an exogenous variable can have an impact on the dependent variable. In the present study, the influence on BEH and INT (and NA MAYBE) are

assessed through several predictor variables. The F-square (F^2) effect size statistic indicates whether the removal of any exogenous variable impacts the dependent variable or the endogenous variable significantly (Hair et al.2013); therefore, the F^2 is the effect size (or change in R^2) when an exogenous variable is removed. As per Cohen (1988), F^2 of >=0.02 is considered small; >= 0.15 is considered medium; >= 0.35 is considered large. Hair et al. (2013) recommends presenting F^2 effect size statistics as well. Based on the present study's analysis, the removal of STR and INT variables will have a large and significant influence on R^2 values of BEH and NA respectively. Additionally, the removal of PBC will also have a small effect on the R^2 of INT.

Q-square (Q^2) is predictive relevance and it measures whether a model has predictive relevance or not. In order for a model to demonstrate predictive validity, it needs to have a Q2 > 0. In addition, Q2 establishes the predictive relevance of the endogenous constructs. According to the results (Table 17), BEH, INT, and NA are significantly predicted with Q2 values of 0.413, 0.123, and 0.384, respectively.

Having discussed the foregoing, the predictive capability of the model can now be established.

Endogenous Variable	**R^2** **(≥ 0.26 =substantial), (≥ 0.13= moderate), (≥ 0.02 =weak)**	**Q^2** **(>0)**
BEH	0.508	0.413
INT	0.151	0.123
NA	0.534	0.384

Table 23: Model's Predictive Capabilities

	F^2 **(>=0.02=small); (>= 0.15 =medium); (>= 0.35 large)**	**Effect Size**	**P Values**
ATT -> INT	0.016	Small	0.173
INT -> BEH	0.788	Large	0.00
NA -> BEH	0.009	Small	0.148
PBC -> INT	0.027	Small	0.019

STR -> NA	1.149	Large	0.00
SUB -> INT	0.00	Small	0.432

Table 24: Effect Size for Independent Variables

6.1.3 Structural Model

The SmartPLS 3.0 results are shown in Figures 4, and Tables 25, 26, and 27. The bootstrapping method was used to estimate the levels of path coefficients and significance. The results of the hypothesized relationships are as follows. For **H1a:** "Employee's Intentions to use Shadow IT in the remote workplace will have a significant and positive effect on Shadow IT Usage Behavior" which evaluates whether WFH employees' intentions (INT) to access, adopt and use Shadow IT in the remote workplace will be significantly and positively related to the adoption of shadow apps and or its usage in the remote workplace (BEH); the results are confirmed (ß= 0.673, t=12.939, p=.0.000). Hence, H1a was supported. **H1b:** "Perceived Behavioral Control (PBC) will moderate the positive relationship between an employee's Intention to USIT and the actual USIT behavior" evaluates whether the relationship between intention to use shadow apps (INT), and the actual usage is strengthened or weakened by WFH Employees' perception of control over using shadow apps. The results revealed a negative and an insignificant moderating role of PBC on the relationship between INT and BEH (ß= -0.014, t=0.322, p=0.374). Hence, H1b was not supported. **H2:** "Attitude towards Shadow IT usage for work purposes will be significantly and positively related to intentions to access, adopt and or use Shadow IT" explores the impact of a WFH employee's attitude toward Shadow IT usage (ATT), whether positive or negative, on their intentions to adopt, access, and use it (INT). The results revealed that ATT has a significant and positive impact on INT (ß= 0.119, t=1.998, p=0.023), hence H2 was supported to affirm the prediction. **H3:** "WFH employee subjective

norms (SUB) will have a significant positive effect on USIT intentions (the intentions to adopt, access, or use INT)" explores whether WFH employees' individual perceived norms regarding Shadow IT, which are shaped by social influences from friends/family, work colleagues and superiors (SUB), will positively influence WFH employees' intentions (INT) to access, adopt, or use it (INT). Contrary to the stated prediction, the data did not support this hypothesis (ß= 0.019, t=0.281, p=0.390). Hence, in remote workplaces, social influences do not significantly influence the individual employee's intention to access, adopt, or use Shadow IT. **H4:** "Perceived Behavioral Control will have a significant and positive effect on USIT intentions (INT)" examines the effects of WFH employees' perceptions of control and leverage over Shadow IT access and usage (PBC) on their intentions to access, adopt and use them (INT). In remote work settings, perception of leverage over Shadow IT significantly influences employees' intentions to access, adopt, and or use Shadow IT (ß= 0.290, t=3.883, p=.0.000). Hence H4 was supported. **H5a:** "Negative Affect will have a positive effect on the use of Shadow IT" assesses whether WFH employees' feelings of frustration, anger and situational depression (Negative Affect) (NA) influence employees' likelihood to access, adopt and use unapproved Shadow apps (BEH) for work purposes against injunctive IT/security norms. The results reveal that the hypothesized impact of NA on Shadow IT usage was also supported by the data; however, the direction of the path strength is inconsistent with the prediction made that NA would have a positive effect on the usage of Shadow IT in remote work settings (ß= -0.096, t=2.228, p=0.013). There are a number of factors that could explain this result, including scale composition, research sample, and contextual factors as well as extraneous ones. **H5b:** "Perceived Situational Strain (PSS) through the mediating role of Negative Affect will have a significant and positive effect on the use of use of Shadow IT" investigates whether perceived situational strain (PSS) will positively

influence people's use of unapproved Shadow apps in the WFH environment, against injunctive IT and security norms. Here, a mediation analysis was performed to assess the mediating role of NA on PSS. The data analysis related to hypothesis H5b (Table 20) indicated that the total effect of PSS on BEH was insignificant (ß= -0.000, t=0.009, p=0.497) indicating that without accounting for the involvement of any moderation or mediation in the model, effect there is no influence of PSS on Shadow IT access, adoption or use. The direct effect which is the effect of PSS on BEH when we have mediators or moderators in the model, was positive and significant (ß= 0.093, t=2.274, p=0.011). The Indirect Effect of PSS on BEH was also significant (ß= -0.070, t=2.202, p=0.014). Hence, H5b is supported, even though the direction of the path strength is inconsistent with the prediction made that STR through the mediating role of NA would have a positive effect on the usage of Shadow IT in remote work settings. As aforementioned, there are a number of factors that could explain this result, including scale composition, research sample, and contextual factors as well as extraneous factors. This could also be the case for reverse causality.

H6a: "PSS will significantly moderate the positive relationship between Attitude and USIT (BEH) such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain"; **H6b**: "PSS will significantly moderate the positive relationship between PBC and USIT (BEH) such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain"; **H6c**: "PSS will significantly moderate the positive relationship between Subjective Norms and USIT (BEH) such that the relationship is stronger with increased levels of Strain and lower with lower levels of Strain"; **H6d**: "PSS will significantly moderate the positive relationship between Intention to use Shadow IT (INT) and USIT (BEH) such that the relationship is stronger with increased levels of Strain and lower with

lower levels of Strain"; Moderation analysis was performed to evaluate the moderating role of STR through the mediating role of NA on the TPB variables. Contrary to our prediction, the results revealed an insignificant modorating role of PSS through the mediating role of NA on all of the relationships as follows: INT and INT (ß =0.004, t=0.061, p=0.476) and ATT and INT (ß=0.03, t=0.378, p=0.353), PBC and INT ((ß=0.053, t=0.678, p=0.249), SUB and INT (ß=-0.174, t=0.934, p=0.175). It may be that the dataset was not large enough to test for four moderating relationships, thus the non-significant moderating effect. Another possible reason for the inconsistency in prediction and outcome is the composition of the scale, the research sample, as well as contextual and extrinsic factors. Furthermore, STR may not moderate the TPB relationships through NA, explaining the non-significant moderating effect, though this conclusion may be premature given that only one dataset was used to test the moderation hypotheses.

Base Model

	B Coefficients	**Standard Deviation**	**T Statistics**	**P Values**
INT -> BEH	0.673***	0.051	13.25	0.000
ATT -> INT	0.157**	0.056	2.777	0.003
SUB -> INT	0.028^{ns}	0.067	0.416	0.339
PBC -> INT	0.255***	0.068	3.748	0.000
INT -> BEH	0.673***	0.051	13.25	0.000
NA -> BEH	-0.097^{sod}**	0.037	2.606	0.005
STR -> NA	0.731***	0.025	29.539	0.000
STR -> BEH	0.096*	0.043	2.251	0.012

Table 25: Summary of Base Model Results

Legend: Path significance: ∗ p<0.05, ∗∗ p<0.01, ∗∗∗ p<0.001, ns= non-Significant, sod= Significant opposite direction

Complete Model

Hypotheses	**Relationship**	**B Coefficient**	**Status**	**Standard Deviation**	**T-Statistics**	**P Value**
H1a	INT -> BEH	0.673***	S	0.052	12.939	0.000

H1b	PBC->INT > BEH	-0.014^{ns}	NS	0.044	0.322	0.374
H2 (a-b)	ATT -> INT	0.119*	S	0.059	1.998	0.023
H3	SUB -> INT	0.019^{ns}	NS	0.187	0.281	0.390
H4	PBC -> INT	0.29***	S	0.079	3.883	0.000
H5a	STR -> NA	0.731***	S	0.025	29.179	0.000
H5b	NA -> BEH	-0.096**	SOD	0.043	2.228	0.013
H6a	PSS(NA)-> ATT>INT	0.03^{ns}	NS	0.079	0.378	0.353
H6b	PSS(NA) -> PBC>INT	0.053^{ns}	NS	0.079	0.678	0.249
H6c	PSS(NA) -> SUB>INT	-0.174^{ns}	NS	0.187	0.934	0.175
H6d	PSS(NA) -> INT>BEH	0.004^{ns}	NS	0.061	0.061	0.476
-	STR -> BEH	0.093**	S	0.041	2.274	0.011

Table 26: Summary of Path Model Analysis

Legend: S= Supported; NS= Not Supported; SOD= Significant opposite direction

Mediation Analysis

Hypotheses	**Relationships**	**β (TE)**	**T-Stat**	**P Value**	**β (DE)**	**T-Stat**	**P Value**
	STR>BEH	-0.000 ^{ns}	0.009	0.497	0.093**	2.274	0.011
		β (IE)	**T-Stat**	**P Value**			
H5b	**STR>NA>BEH**	-0.070**^{sod}	2.202	0.014			

Table 27: Summary of Mediation Analysis

Legend: TE= Total Effects; DE=Direct Effects; IE=Indirect Effects, S= Supported, NS= Not Supported, SOD= Significant opposite direction

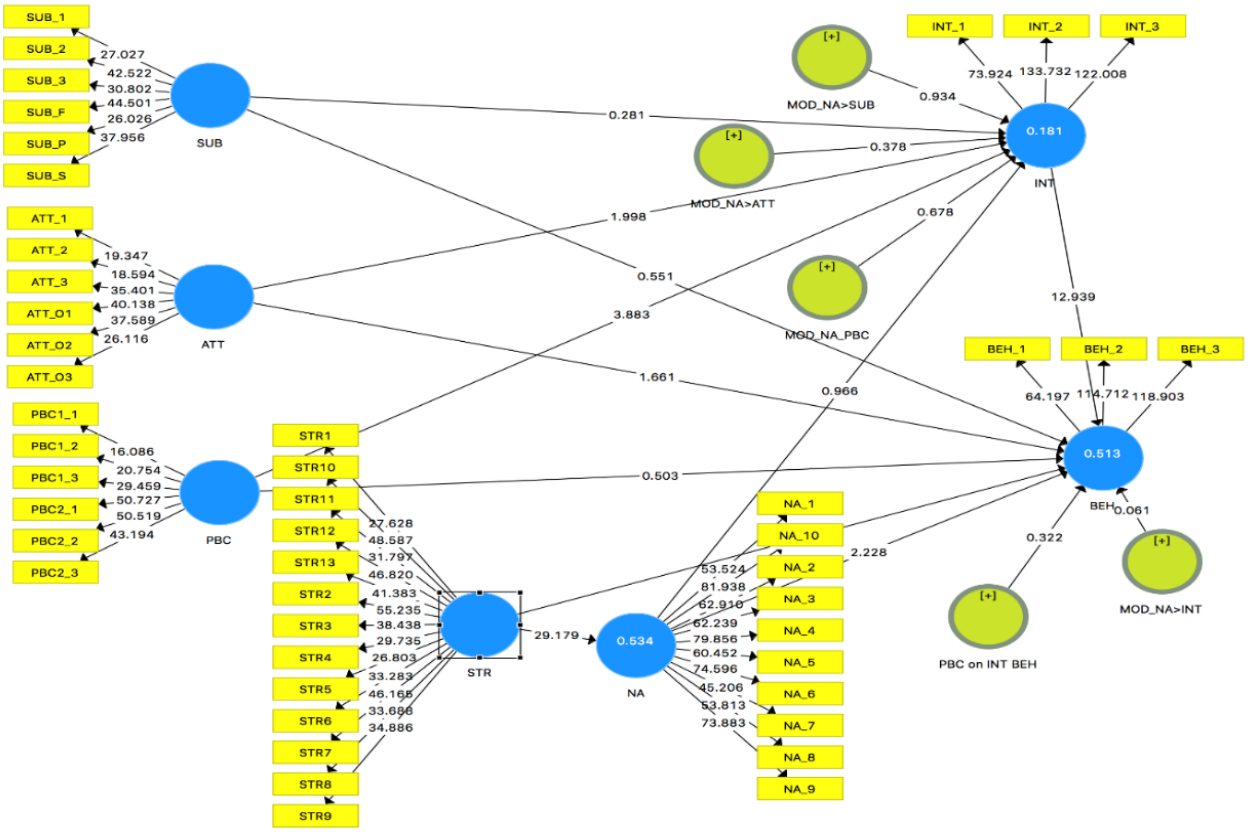

Figure 4: The SmartPLS 3.0 Complete Model with Moderation and Mediation Analysis

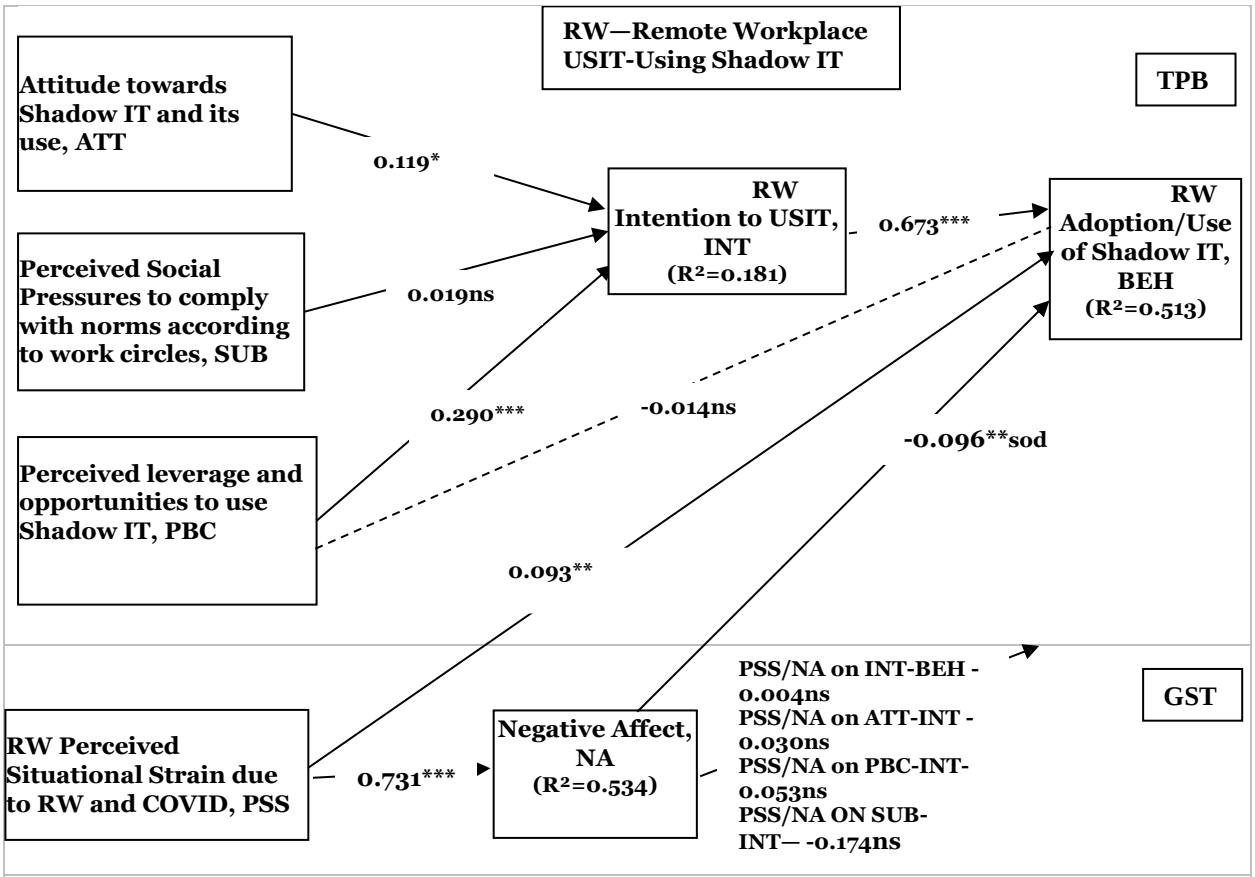

Figure 5: Summary of results for the tested hypotheses. Path significance: * p<0.05, ** p<0.01, *** p<0.001, ns = not significant, sod= Significant opposite direction

6.2 DISCUSSION

This study investigated the variables that might be contributing to shadow IT proliferation in remote workplaces against a backdrop of COVID strains. Shadow IT is positioned as a volitional non-malicious insider related data security threat that is accelerated in the work from home environment due to unique conditions in the COVID-19 and post-COVID-19 work from home era. A research model designed to enhance our understanding of the phenomenon was developed and validated based on two theoretical perspectives, TPB and GST. At the heart of the study is the examination of the role of strain as is seen through the General Strain Theory lens, on the deviant adoption and or use of Shadow IT in remote workplaces

against injunctive IT/security norms. STR does have theoretical implications for deviant behavior. Firstly, our model reveals that at the individual level, Strain positively and significantly influences the adoption and usage of unapproved shadow apps (BEH) in the context of the remote workplace. This confirms Agnew's key proposition (which states that strain increases the likelihood of deviance) in this specific context, as well as potentially, in the context of other (grey area) behavioral related Information Security phenomena. Based on the data analysis of this variable, the paths from STR to BEH was positive significant. This is notwithstanding the hypothesized, positive impacts of STR through the mediating role of NA on Shadow IT usage, which was hypothesized be positive, but partially showed negative results. It is somewhat unexpected to see the path from NA to BEH being negative since logic would predict that emotions like anger, frustration, and depression would most likely people's brains go into "fight or flight" mode, disrupting attention and memory, as well as making them incapable of adhering to security norms or IT/security standards, which could result in Shadow IT. Hence, we believe this result might have been impacted by contextual or extraneous influences. It might also be possible that this particular factor is negatively related with the use of Shadow IT against injunctive IT/security norms in the rotework setting.

Regarding the hypothesized paths according to TPB; all paths to INT and BEH (i.e., ATT to INT and PBC to INT; NA to BEH, INT to BEH) are significant, except for SUB to INT. These (in addition to PSS (STR) through NA, were the proposed antecedents to shadow IT adoption and use against injunctive IT or security norms in the remote workplace. Although the data failed to confirm the prediction that perception of control and leverage over shadow IT (PBC) use will strengthen the relationship between intentions to access, adopt and or use Shadow IT (INT) and the use of shadow IT (BEH), perceived behavioral control (PBC), and attitude (ATT) towards

Shadow IT and its adoption or use were found to have a significant and positive effect on remote employees' intentions to access, adopt and or use Shadow IT, where Intention, which indicates the readiness to carry out a behavior was a positive and significant factor in WFH employees ’enaction of the behavior (accessing, adopting and or using Shadow IT against injunctive IT/security norms). These results suggest that an employee’s individual attitude toward using Shadow IT in the remote workplace against injunctive IT norms, and the perception of power, control, and leverage that they have over the use of shadow IT do play vitally important roles in the proliferation of Shadow IT in non-traditional work environments. In light of these results, organizations can work towards reshaping attitudes around Shadow IT, as well as developing appropriate protocols, frameworks, and policies that limits and balances the perception of power and control that employees may perceive they have over using shadow IT. In the mainstream workforce, shadow IT may be new and not be well known or understood as a cyber and information security risk phenomenon, hence, information security and cyber risks associated with it may not be well understood by mainstream workers. And as the workplace environment continually changes, targeted Shadow IT security protocols, frameworks, awareness, and training programs are increasingly important. Hence, our research emphasizes the importance of a continuous and dynamic security protocols and frameworks, awareness and training programs that are continuously adaptable in order to facilitate employees' engagement in maintaining a positive cybersecurity climate in remote workplaces. It is also important to make such policies dynamic allowing employees to become more aware of new, upcoming Security threats as opposed to a one-time effort, as postulated in previous studies. Our research also underscores the importance of pursuing a more modular approach to security policies which mirrors the multilevel or perimeter security model used in the design of security solutions. This will ensure

that “grey area” but equally detrimental security threats and vulnerabilities such as the shadow IT phenomenon are adequately regulated and managed rather than being left as mere IT/security injunctive norms. Accordingly, our research confirms the need for formal Shadow IT policies and frameworks that guide employees' decisions in remote workplaces regarding shadow resources and applications.

Results related to the third component of TPB i.e., subjective norms show that this factor did not positively influence the proliferation of Shadow IT use in the remote workplace as the research data did not confirm the prediction that Subjective Norms will have a positive effect on intentions to use shadow IT. The direction of the relationship is consistent with prediction and findings elsewhere (TPB studies on subjective norms); however, the strength of the relationship is inadequate to affirm the stated hypothesis. Subjective norms encapsulate employees’ views of friends, colleagues, and superiors in remote workplaces regarding the use of Shadow IT, hence these results might mean that WFH employees are unaffected by social pressure from family, friends, and significant others to adopt and or use Shadow IT for work purposes, which is a plausible consideration since there’s not a lot of social interactions with work circles as people work from home. There may also be another explanation for this result, namely that this hypothesis was not able to be confirmed due to the sampling composition and research design. Accordingly, our study indicates that employees' perceptions about the views of their friends, colleagues, and superiors were insignificant in influencing the adoption and use of Shadow IT in remote settings, which means that social imperatives are not, in themselves, driving adoption and use.

In terms of the moderation relationships, the impact that ATT, PBC SUB, and INT have on the respective dependent variables (INT, and BEH) are hypothesized to vary depending on the

perception of STR that WFH employees are experiencing in remote work setting such that the relationships are positively significant with increased levels of STR. The directions of the relationships are consistent with our prediction (except for SUB), but the strengths are insignificant. Hence, while strain in itself played a role in shadow IT proliferation in the remote workplace, there's no support for the moderating effects of STR on the four TPB variables used in this study. There is a possibility that the dataset was too small to test for four moderating relationships, thus the moderating effect was not significant. It is also possible that STR may not have a significant moderating effect on the TPB variables in the Shadow IT context. The third reason may be related to the characteristics of the participant; hence it would be premature to reject the moderating effect based on the results of this study.

6.2.1. Theoretical Contribution

Through this dissertation, we attempted to extend the theoretical foundations on individuals' security behaviors in the work-from-home environment during crisis situations. This is accomplished through the examination of the effects of strenuous environmental influences (modeled by GST) on WFH employees' use of Shadow IT in violation of injunctive IT norms, in which strenuous conditions common to those working from home are introduced as potential moderators of cognitive, social, and psychological factors (modeled by TPB) that influence security behaviors at the individual level. This integration of the TPB with the GST has been previously implemented, to the best of our knowledge. As a result, our study is unique in several ways, and therefore contributes to the field in the following ways. Research on information security has largely focused on analyzing employee security behaviors within the context of traditional work environments that have extensive security standards and procedures to guide employees, including well-constructed security policies and standards that are well-defined and

well communicated, and that can be enforced by managers. In addition, most security related end-user behavioral research provides implications for threat intelligence in traditional work environments where security policies are well-constructed, well-communicated with an understanding of the benefits and consequences of non-compliance; however, the COVID pandemic has shown us all that it may not always be the case for employees to work in traditional work environments with well-organized boundaries and security enforcements. Due to the pandemic, companies had to relocate their entire workforce to a home location with little planning. Therefore, our study contributes by studying the security behaviors of employees outside of the traditional work environment where compliance may be more difficult to enforce. Furthermore, in addition to highlighting the need for more information security research, especially research into end-users' and insiders' behavior in remote work environments where compliance may be hard to enforce, we also highlight the importance of well-designed, well-communicated, and well-defined security policies regarding contextual end user actions such as shadow IT usage. Due to these implications, we provide significant insights into threat awareness and intelligence in remote work environments

6.2.2. Practical Contribution

To mitigate Shadow IT's information and cybersecurity risks at both the employee and organizational level, it must be better understood. The Associated Press reported[17] that employees of an Atlanta-based organization called Insight Global contracted to do COVID-

[17] https://apnews.com/article/coronavirus-data-privacy-technology-business-health-4b9a172a90bc1a82f83e6a44ff06a445

related contact tracing in 2021 mishandled and compromised the private information (potentially HIPAA protected) of at least 72,000 people due to Shadow IT use, costing Insight Global $28.7 million. In this Shadow IT related data breach, it was determined that employees had set up several unauthorized collaboration channels, specifically unauthorized Google accounts for sharing information, including the names of people exposed to COVID-19, whether they had any symptoms, how many people lived with them, and, in some cases, their email addresses and phone numbers. Considering such examples, our study offers the following implications for practitioners. To guide strategies for mitigation at both the organizational and employee levels, a better understanding of shadow IT as an information and cyber risk phenomenon, as well as the factors that lead to its rapid growth in the organization (remote or onsite) is important. While shadow IT is not maliciously intended, research and other anecdotal information indicate that most security incidents are as such: caused by non-malicious actions of employees or end users. By further acknowledging and understanding the predictors of such behaviors that are most times volitional, organizations can have more insight into the organizational threat landscape, and employees can have a better understanding of the potential outcomes of such behavior. As we found in our study within the context of the WFH environment that attitudes and perceptions of power and leverage over Shadow IT have a strong impact on shadow IT adoption among WFH employees, our research suggests that there is a need for modular security protocols, trainings, frameworks, and policies that both shape attitudes around shadow IT and shift the power balance over shadow IT leverage from the employee to the organization. As mentioned in the discussion section, shadow IT may be new and not well known or understood as a cyber and information security risk phenomenon, hence, information security and cyber risks associated with it may not be well understood by mainstream workers. Hence, as the workplace environment continually

changes, targeted Shadow IT security protocols, frameworks, awareness, and training programs become increasingly important, as well as dynamic and adaptable security policies and frameworks in general. When the creation of security policies and frameworks are revised in the above suggested manner, it is our argument that employees are able to, in a timely manner, become more aware of new, upcoming security threats. Ultimately, this study highlights the need for contextual and formal Shadow IT policies and frameworks to guide employee decisions within remote workplaces, as well as urging the redesign of security policies and frameworks in general, to be more dynamic and adaptable.

CHAPTER 7: LIMITATIONS AND CONCLUSION

7.1 LIMTATIONS AND FUTURE RESEARCH

This study has a number of limitations. As a first step, we rely heavily on self-reported survey responses which raises a couple of potential issues, and our final dataset consists entirely of Mechanical Turk respondents. Self-reporting is used instead of actual observation to measure the behavior under study. As is the case with “single source" survey studies where both the dependent and independent variables are collected from the same source using the same instrument, the issue of common method variance arises. Although formal tests proved that common method variance was not prevalent, a longitudinal design with a lag between collecting dependent and independent variables would strengthen the research. Secondly, the results for some of our central hypotheses were inconsistent, either in direction or strength. As an example, the path between NA and BEH was significant in the opposite direction, contrary to the prediction that NA would have a positive effect on Shadow IT adoption. This could be a case of reverse causality, and the authors are interested in further investigating this angle. For the case of the moderating role of strain on the TPB variables as modeled through the GST lens which showed that strain did not significantly moderate the relationships, future works will examine the role of STR on the individual TPB variables, instead of examining them as moderations to the relationships. In addition, and in light of the possibility of reverse causality, we hope to examine the role of other appropriate theories in explaining the phenomenon. Thirdly, we also propose adding additional control variables not investigated or not included in this study but included in prior research strain related research to future estimation models. Also, we recommend studies that include data from a variety of organizations as this would further strengthen the study in light of the significant relationships that were confirmed as predicted.

7.2 CONCLUSION

It is true that the continued use of new and cutting-edge technology by companies and employees to accelerate information transfer and enhance various work processes in the remote workplace is game-changing. However, from an information security risk perspective, it is also increasingly risky as, in tandem with technological advancements, security threats evolve. At the center of this dilemma is the end-user or employee, whose security posture, behavior, or actions, though non malicious might open up the organization to a range of security threats. Shadow IT is such an end user security behavior and has garnered limited research thus far and our research helps increase the spotlight on the phenomenon, providing important implications for threat awareness and mitigation in today's dynamic organization. Being a security behavior that is accelerated especially in remote work settings, our study additionally adds to the understanding of new threats in the non-traditional work environment, as here has also been very little research into individuals' security behavior in non-traditional work environments where compliance may be difficult to enforce and monitor as well.

With the aid of central theoretical constructs which derived from prominent theories of decision making, volitional behavior and environmental criminology, this dissertation proposed and validated a model that examines why people working from home during and after COVID might engage in the deviant security behavior of adopting and or using shadow IT for work purposes in violation of injunctive IT and security standards. Importantly, we examined how strain might impact the security behavior of people who work from home, and revealed that strain contributes to the proliferation and accelerated adoption of Shadow IT in remote workplaces, as well as individual level variables that were stipulated in past research, such as

attitude towards shadow IT and perceptions of control and leverage over shadow IT. Contributions are in the areas of information security, threat intelligence in remote work settings, remote security, insider threats, and shadow IT.

APPENDIX

APPENDIX 1: IRB Approval Notice

October 4, 2021

Dear Patricia Akello:

On October 1, 2021, the IRB approved the following:

Type of Review: Initial
Title: The Volitional Insider Threat At The Intersection of The COVID-19 Pandemic, The New Work From Home (nWFH) and Cloud Based Applications.
Principal Investigator: Patricia Akello
IRB Number: FY20-21-302
Faculty Sponsor: Kim-Kwang Choo
HHS grant title and ID, if any:
Documents reviewed: Protocol

In conducting this study, you are required to follow the requirements in "INVESTIGATOR GUIDANCE: Investigator Obligations (HRP-800)."

If you plan on conducting this research for more than 3 years, or if you wish to make any changes to your study, contact the IRB Office.

Sincerely,

Tammy Lopez, JD, CIP
Senior Research Compliance Coordinator
Designee of the Chair
UTSA Office of Research Integrity - IRB Office

APPENDIX 2: RESEARCH QUESTIONNAIRE

CONSENT

We are inviting you to participate in a study about the adoption and use of "external" third party applications and software in the remote workplace. In this study, they are called E-APPS, short for external applications and software (applications not provided by the company).

We want to understand individual-level factors, and environmental factors that influence (motivate or inhibit) the adoption of E-APPS by remote workers.

Our findings will help research and practice in the areas of remote work success and security. Your participation is important because you satisfy the following conditions: a) You are an employee of any organization who has a remote workforce at this time. b) You work from home

now or have worked from home at any time during COVID. c) You use a computer, applications, and software in your everyday work life.

As we proceed, please note the following: I ask that you respond to the items in the questionnaire, knowing that there is no right or wrong answer. Your participation is voluntary. Your responses are anonymous as there are no any identifying information in the survey. The survey is self-administered, taking a maximum of 10 minutes. Please complete the survey in one sitting so your responses are recorded. Please do not answer randomly, random questions cannot be valid for analysis. Also, there are questions that can identify random responses.

If you have any questions or concerns at any time, please email the research principal investigator at patricia.akello@utsa.edu. This research has been approved by UTSA's Institutional Review Board (IRB@utsa.edu).

Please indicate that you have read this information sheet by clicking Yes, I agree to participate...then proceed to the scenario

Thank you for your participation!

1. Yes, I agree to participate
2. No, I do not agree to participate

DEMOGRAPHICS

What is your age (in years)? --------

What is your gender?

1. Male
2. Female

Where do you physically live?

1. United States
2. Outside of the United States

What is your ethnicity

1. White/Caucasian
2. Black or African American
3. Asian
4. Mixed Ethnicity
5. Other

ORGANIZATIONAL TENURE

How long have you been employed by your organization?

1. Less than 1 year
2. Between 1 year and 2 years
3. Between 2 year and 3 years
4. Between 3 years and 4 years
5. 5 years or more

INSTRUCTIONS/SCENARIO

Please read the scenario fully. You will be asked to answer follow up questions based on it for 10 minutes. Please pay attention to the names of the characters.

John currently works for a medium sized Texas company. He works remotely due to COVID-19. His company abruptly relocated him 2 years ago. To maintain his job performance while he works from home, John on several occasion searches the internet for apps and software to help with work related tasks. These include apps and software for perfecting presentations &

drawings, visualizing data, transferring files, collaborating, and even for signing documents. These apps are referred to as E-APPS in this study. In fact, John downloaded a PDF converter to his work computer just this morning because he needed to convert PDF files to word quickly.

1. I have read and understood the scenario
2. I have NOT read and understood the scenario

QUALITY CHECK

We care about the quality of our survey data and hope to receive the most accurate measures of your opinions, so it is important to us that you thoughtfully provide your best answer to each question in the survey. Do you commit to providing your thoughtful and honest answers to the questions in this survey?

1. I will provide my best answers

2. I can't promise either way, but will try my best

3. I will NOT provide my best answers

OTHER FILTER QUESTIONS/QUESTIONS OF INTEREST

Please read carefully and choose the answer that applies to you:

Like John, I work from home now, have worked from home at some point during the pandemic, or have worked from home before.

1. Yes
2. No

Tell me about your work from home situation...

1. I worked from home when COVID started
2. I already worked from home before COVID, I just continued
3. NO, I have never worked from home

What device(s) did you use while you worked from home?

1. both my own and company-owned device(s) for work purposes
2. company owned device(s) for work purposes
3. my own device(s) only. My company did not provide

INSTRUCTIONAL/QUALITY

Remember ALL of the following questions are about the period of time when you worked from home **E-APPS** are any applications/software that are not provided by your organization, but are accessed and used by you the employee, at your judgement and choice, to get work tasks done. When we say, "**downloading E-APPS**", we also mean "**accessing E-APPs**" or "**using E-APPS**"

1. Got it, let's proceed
2. No, I don't understand

Referring back to the scenario, putting yourself in John's shoes, and remembering your own experience when you worked from home: please provide your responses to the statements

I'm OK with John's choice: Yes **(Go to I'd do as John and Rate your levels of agreement),** No **(SKIP and go to Rate level of Disagreement and proceed)**

I would do as John. Yes (1), No (2)

ATTITUDE, ATT

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

ATT_Positive

ATT I am ok with John's choice to access E-APPS for work purposes

ATT What is your level of agreement with John's choice?

ATT_+b1 I believe that using E-APPS for work purposes in the remote setting is necessary

ATT_+b2I I believe that using E-APPS for work purposes in the remote setting is justifiable

ATT_O/E1 State your level of agreement with the following statements:

My favorable views regarding the use of E-APPS by employees while working from home in this COVID era is because ...

1. it is impossible to be as productive without them
2. they have better performance than sanctioned alternatives
3. they have better functionalities than sanctioned alternatives
4. as long as they work efficiently there should be no issue

ATT_Negative

ATT_-B: I would NOT do as John

ATT_-B: What is your level of disagreement with John's choice?

ATT_-b1: I believe that using E-APPS is a bad idea

ATT_-b2: I believe that using E-APPS is a risky behavior

ATT_O/E1 State your level of agreement with the following statements:

My unfavorable views regarding the use of E-APPS by employees while working from home in this COVID era is because of the potential…

1. security risks
2. of a third-party owner accessing my data
3. violation of company policies and protocol
4. loss of access if the site goes down

SUBJECTIVE NORMS, SUB

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

I believe the choice of John and most people to use or not use E-APPS would most likely be influenced by their...

1. Friends & Family
2. Coworkers
3. Supervisor

Regarding my personal choice to use or not use E-APPS, the following peoples' opinions matter to me...

1. Friends & Family
2. Coworkers
3. Supervisor

The following people would likely use or approve the use of E-APPS. My...

1. Friends & Family
2. Coworkers

3. Supervisor

The following people would likely NOT use or approve the use of E-APPS. My...

1. Friends & Family

2. Coworkers

3. Supervisor

PERCEIVED BEHAVIORAL CONTROL, PBC

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

PBC1_cp I believe that John's decision to use E-APPS is likely a result of his working from home and the perceived...

1. high control over using E-APPS, he works away from the office.

2. increased liberty to decide for himself to choose tools for work

3. increased level of access when it comes to attaining the tools that he wants from the internet

PC_1 Like John, these factors would influence my decision to use or not to use E-APPS

SE_1 My decision to use E-APPS would also be affected by how easy the are to …

1. Find

2. Access

3. Download

INTENTION TO adopt/USIT, INT

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

Please complete the following statements: While working from home, I

1. thought about downloading E-APPS

2. considered to use E-APPS

3. searched for E-APPS with the aim of using them for work purposes

4. Tried to use E-APPS

BEHAVIOR (SHADOW IT ADOPTION/UIST), BEH

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

Please complete the following statements: While working from home, I

1. downloaded EAPPS
2. used EAPPS
3. accessed EAPPS

ATTENTION CHECK

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

1. Barack Obama was the first American president. "Please select strongly disagree"
2. The United States of America consists of 10 states. "Please select strongly disagree"
3. I am happy with receiving a very large bill from the IRS. "Please select strongly disagree"

MARKER VARIABLE

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

1. When I must choose between the two, I usually dress for fashion, not for comfort.
2. An important part of my life and activities is dressing smartly.
3. A person should try to dress in style.

PERCEPTION OF COVID/WFH Times

SCALE: *1=Hated it very much, 2=Hated it, 3=Hated it somewhat, 4=Didn't mind it, 5=Liked it somewhat, 6=Liked it, 7=Liked it very much.*

In general, how did you feel about these COVID-related lifestyle changes...?

1. Working Remotely
2. Reduced social events

3. Less time with Friends & Family

4. More time alone

5. Restricted travel

SITUATION STRAIN OR PERCCIEVED SITUATIONAL STRAIN, STR, PSS

SCALE: *1=Strongly disagree, 2=Disagree, 3=Somewhat disagree, 4=Neither agree nor disagree, 5=Somewhat agree, 6=Agree, 7= Strongly agree*

STR_1 Regarding your life now, during, and after the pandemic, please indicate how much you agree or disagree with the following statements

1. It felt like my life was surrounded by a feeling of precariousness

2. It felt like the goals I had prior to the pandemic seemed almost irrelevant and unimportant

3. My job was something I loved, and I committed myself to it

4. There were a lot of roadblocks that prevented me from doing my job

5. I had a vague idea what I wanted to do with my life

6. My plans for the future seemed fragile to me

7. When it came to my job, I felt like procrastinating most of the time

8. In my mind, the future of my career seemed rather uncertain when viewed through the prism of the pandemic

STR_2 Please reflect on the time you were working from home during COVID: Indicate how much strain each of these caused you if any:

SCALE*: 5=Very much, 4=Rather much, 3=Some extent, 2=Little, 1=Not at all*

1. FINANCIAL PRESSURES

2. CHILDCARE/ELDERCARE responsibility increase

3. HOME OFFICE burdens, inconveniences, and distractions

4. HEALTH ISSUES

5. SOCIAL ISOLATION

NEGATIVE AFFECT, NA

SCALE: *7= Strongly agree, 6=Agree, 5=Somewhat agree, 4=Neither agree nor disagree, 3=Somewhat disagree, 2=Disagree, 1=Strongly disagree*

N_AFF While reflecting on the time you were working from home during COVID, please complete the following statement:

1. I lost my temper many times
2. Little things irritated me
3. I often stayed mad when someone, such as my boss or colleagues hurt or irritated me
4. I often felt the urge to yell when hurt
5. I had a general feeling that life often gives me raw deals and it's kind of unfair
6. I often felt the urge to get even when I felt hurt
7. I had a feeling that other employees were luckier in regard to work
8. I felt jealousy towards other people who got good breaks at work when I didn't
9. I feel like a powder keg ready to explode
10. I feel like physically lashing out against others at home or at my work

APPENDIX 3: Measurement Instruments

Construct	Definitions	Adapted From
Attitude, ATT 6/6	Individuals' overall assessment of the target behavior such as Shadow IT and/or its use	(Ifinedo, 2012; Ajzen, 2006; Francis et al., 2004; Bulgurcu et al., 2010; and Herath & Rao, 2009a)

Subjective Norms, SUB 6/6	An individual's perception of "significant" others' opinions, and how much social pressure they are under to act accordingly	(Ajzen, 2006; Francis et al., 2004; Ifinedo, 2012; Lee & Larsen, 2009; Bulgurcu et al., 2010; Chan et al., 2005; Johnston & Warkentin, 2010)
Perceived Behavioral Control, PCB 6/6	Whether or not a person feels capable of enacting a certain behavior in terms of opportunity and leverage	(Ajzen, 2006, Francis et al., 2004; Compeau & Higgins, 1995; Workman et al., 2008; Bulgurcu et al. 2010; Ifinedo, 2012)
Intention to USIT, INT 3/3	Represents an individual's plan to exert effort in performing the target behavior. It is indicative of readiness to engage in the target behavior.	(Ajzen, 2006; Francis et al., 2004; Silic et al., 2017; Ifinedo, 2012)
Behavior (USIT), BEH 3/3	The target course of action or action that's taken	(Ajzen, 2006; Francis et al., 2004; Ifinedo, 2012; Silic et al., 2017)
Strain, STR or PSS 13/13	As is defined by the GST is encapsulated in the *failure to achieve positively valued goals*, the *presentation of negative stimuli*, and the *removal of positive stimuli*	(Piquero and Sealock, 2000, 2004; Chilton et al., 2005; Ruiz et al., 2006; Fuller et al., 2003; Agnew, 2006; Arpaci et al., 2020; Cortez et al., 2020; Hamouche, 2020)
Negative Affect, NA 10/10	The internal state or feeling that results from not reaching positive goals, receiving negative stimuli, or losing a positive stimulus. In context of this study, situational frustration, situational anger, and situational depression due to COVID-19.	Arpaci et al., 2020; Cortez et al., 2020; Hamouche, 2020; Brezina, 1996; Derogatis 1977; Piquero and Sealock 2000)

REFERENCES

Ab Rahman, N.H., and Choo, K.-K.R. (2015). A survey of information security incident handling in the cloud. Comput. Secur. 49, 45–69. https://doi.org/10.1016/j.cose.2014.11.006.

Agnew, R. (1985). A Revised Strain Theory of Delinquency*. Soc. Forces 64, 151–167. https://doi.org/10.1093/sf/64.1.151.

Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency*. Criminology 30, 47–88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x.

Agnew, R. (2001). Building on the foundation of general strain theory: Specifying the types of strain most likely to lead to crime and delinquency. J. Res. Crime Delinquency 38, 319–361. https://doi.org/10.1177/0022427801038004001.

Agnew, R. (2006a). Pressured Into Crime: An Overview of General Strain Theory (Oxford University Press USA).

Agnew, R. (2006b). Pressured Into Crime: An Overview of General Strain Theory (Oxford University Press USA).

Agnew, R. (2013). When Criminal Coping is Likely: An Extension of General Strain Theory. Deviant Behav. 34, 653–670. https://doi.org/10.1080/01639625.2013.766529.

Agnew, R. (2016). Building on the Foundation of General Strain Theory: Specifying the Types of Strain Most Likely to Lead to Crime and Delinquency. In Recent Developments in Criminological Theory, (Routledge), p.

Agnew, R., and White, H.R. (1992). An Empirical Test of General Strain Theory*. Criminology 30, 475–500. https://doi.org/10.1111/j.1745-9125.1992.tb01113.x.

Agnew, R., Brezina, T., Wright, J.P., and Cullen, F.T. (2002). Strain, Personality Traits, and Delinquency: Extending General Strain Theory. Criminology 40, 43–72. https://doi.org/10.1111/j.1745-9125.2002.tb00949.x.

Ajzen, I. (1991a). The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Ajzen, I. (1991b). The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.

Ajzen, I. (2001). Nature and Operation of Attitudes. Annu. Rev. Psychol. 52, 27–58. https://doi.org/10.1146/annurev.psych.52.1.27.

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior1. J. Appl. Soc. Psychol. 32, 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x.

Ali, M., Khan, S.U., and Vasilakos, A.V. (2015). Security in cloud computing: Opportunities and challenges. Inf. Sci. 305, 357–383. https://doi.org/10.1016/j.ins.2015.01.025.

Anderson, C.L., and Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Q. 34, 613–643. https://doi.org/10.2307/25750694.

Anderson, J.C., and Gerbing, D.W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. Psychol. Bull. 103, 411–423. https://doi.org/10.1037/0033-2909.103.3.411.

Arafat, Y., and Mohamed Ibrahim, M.I. (2018). Chapter 4 - The Use of Measurements and Health Behavioral Models to Improve Medication Adherence. In Social and

Administrative Aspects of Pharmacy in Low- and Middle-Income Countries, M.I.M. Ibrahim, A.I. Wertheimer, and Z.-U.-D. Babar, eds. (Academic Press), pp. 53–69.

Arpaci, I., Karataş, K., and Baloğlu, M. (2020). The development and initial tests for the psychometric properties of the COVID-19 Phobia Scale (C19P-S). Personal. Individ. Differ. 164, 110108. https://doi.org/10.1016/j.paid.2020.110108.

Aseltine, R.H., Gore, S., and Gordon, J. (2000). Life Stress, Anger and Anxiety, and Delinquency: An Empirical Test of General Strain Theory. J. Health Soc. Behav. 41, 256–275. https://doi.org/10.2307/2676320.

Bandura, A. (1991). Social cognitive theory of self-regulation. Organ. Behav. Hum. Decis. Process. 50, 248–287. https://doi.org/10.1016/0749-5978(91)90022-L.

Bao, Y., and Wierzbicki, T. (2004). On fracture locus in the equivalent strain and stress triaxiality space. Int. J. Mech. Sci. 46, 81–98. https://doi.org/10.1016/j.ijmecsci.2004.02.006.

Barki, H., and Hartwick, J. (1994). Measuring User Participation, User Involvement, and User Attitude. MIS Q. 18, 59–82. https://doi.org/10.2307/249610.

Baron, S.W. (2007). Street Youth, Gender, Financial Strain, and Crime: Exploring Broidy and Agnew's Extension to General Strain Theory. Deviant Behav. 28, 273–302. https://doi.org/10.1080/01639620701233217.

Bhattacherjee, A. (2001). Understanding Information Systems Continuance: An Expectation-Confirmation Model. MIS Q. 25, 351–370. https://doi.org/10.2307/3250921.

Bishop, M., and Gates, C. (2008). Defining the insider threat (ACM).

Boss, S.R., Galletta, D.F., Benjamin Lowry, P., Moody, G.D., and Polak, P. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. MIS Q. 39, 837–864. .

Botchkovar, E.V., Tittle, C.R., and Antonaccio, O. (2009). General Strain Theory: Additional Evidence Using Cross-Cultural Data*. Criminology 47, 131–176. https://doi.org/10.1111/j.1745-9125.2009.00141.x.

Brezina, T. (1996). Adapting to strain: An examination of delinquent coping responses. Criminology 34, 39. http://dx.doi.org/10.1111/j.1745-9125.1996.tb01194.x.

Broidy, L.M. (2001). A Test of General Strain Theory. Criminology 39, 9–36. .

BROIDY, L., and AGNEW, R. (1997). Gender and Crime: A General Strain Theory Perspective. J. Res. Crime Delinquency 34, 275–306. https://doi.org/10.1177/0022427897034003001.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Q. 34, 523–548. https://doi.org/10.2307/25750690.

Byongook, M., and Morash, M. (2004). Adaptation of Theory for Alternative Cultural Contexts: Agnew's General Strain Theory in South Korea. Int. J. Comp. Appl. Crim. Justice 28, 77–104. https://doi.org/10.1080/01924036.2004.10855341.

Cappelli, D.M., Moore, A.P., and Trzeciak, R.F. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). (Upper Saddle River, NJ: Addison-Wesley Professional).

Chan, T.W., and Goldthorpe, J.H. (2005). The social stratification of theatre, dance and cinema attendance. Cult. Trends 14, 193–212. https://doi.org/10.1080/09548960500436774.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Comput. Secur. 39, 447–459. https://doi.org/10.1016/j.cose.2013.09.009.

CHILTON, M.A., HARDGRAVE, B.C., and ARMSTRONG, D.J. (2005). Person-Job Cognitive Style Fit for Software Developers: The Effect on Strain and Performance. J. Manag. Inf. Syst. 22, 193–226. https://doi.org/10.1080/07421222.2005.11045849.

Chin, W.W., Marcolin, B.L., and Newsted, P.R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. Inf. Syst. Res. 14, 189–217. https://doi.org/10.1287/isre.14.2.189.16018.

Choo, K.-K.R. (2010). Cloud computing: Challenges and future directions. Trends Issues Crime Crim. Justice.

Choo, K.-K.R., Rana, O.F., and Rajarajan, M. (2017). Cloud Security Engineering: Theory, Practice and Future Research. IEEE Trans. Cloud Comput. 5, 372–374. https://doi.org/10.1109/TCC.2016.2582278.

Chua, C.E.H., and Storey, V.C. Central IT or Shadow IT? Factors Shaping Users' Decision To Go Rogue With IT. 14. .

Claycomb, W.R., and Nicoll, A. (2012). Insider threats to cloud computing: Directions for new research challenges. In Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual, (IEEE), pp. 387–394.

Conner, M., and Norman, P. (2017). Health behaviour: Current issues and challenges. Psychol. Health 32, 895–906. https://doi.org/10.1080/08870446.2017.1336240.

Cortez, P.A., Joseph, S.J., Das, N., Bhandari, S.S., and Shoib, S. (2020). Tools to measure the psychological impact of the COVID-19 pandemic: What do we have in the platter? Asian J. Psychiatry 53, 102371. https://doi.org/10.1016/j.ajp.2020.102371.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. (2013a). Future directions for behavioral information security research. Comput. Secur. 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. (2013b). Future directions for behavioral information security research. Comput. Secur. 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010.

Dienlin, T., and Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. 45, 285–297. https://doi.org/10.1002/ejsp.2049.

Esposito, C., Castiglione, A., Martini, B., and Choo, K.-K.R. (2016). Cloud Manufacturing: Security, Privacy, and Forensic Concerns. IEEE Cloud Comput. 3, 16–22. https://doi.org/10.1109/MCC.2016.79.

Fishbein, M., and Ajzen, I. (1975). Belief, attitude, intention and behavior: an introduction to theory and research.

Fornell, C., and Larcker, D.F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. J. Mark. Res. 18, 39. https://doi.org/10.2307/3151312.

French, A., Guo, C., and Shim, J.P. (2014). Current Status, Issues, and Future of Bring Your Own Device (BYOD). Commun. Assoc. Inf. Syst. 35. https://doi.org/10.17705/1CAIS.03510.

Fuller, J.A., Stanton, J.M., Fisher, G.G., Spitzmüller, C., Russell, S.S., and Smith, P.C. (2003). A Lengthy Look at the Daily Grind: Time Series Analysis of Events, Mood, Stress, and Satisfaction. J. Appl. Psychol. 88, 1019–1033. http://dx.doi.org/10.1037/0021-9010.88.6.1019.

Gefen, D., and Straub, D. (2005). A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example. Commun. Assoc. Inf. Syst. 16. https://doi.org/10.17705/1CAIS.01605.

Guo, K.H., Yuan, Y., Archer, N.P., and Connelly, C.E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. J. Manag. Inf. Syst. 28, 203–236. https://doi.org/10.2753/MIS0742-1222280208.

György, A., Cleven, A., Uebernickel, F., and Brenner, W. (2012). EXPLORING THE SHADOWS: IT GOVERNANCE APPROACHES TO USER-DRIVEN INNOVATION. ECIS 2012 Proc.

Haag, S., and Eckhardt, A. (2014a). Normalizing the Shadows – The Role of Symbolic Models for Individuals' Shadow IT Usage. ICIS 2014 Proc.

Haag, S., and Eckhardt, A. (2014b). Normalizing the Shadows – The Role of Symbolic Models for Individuals' Shadow IT Usage. ICIS 2014 Proc.

Haag, S., and Eckhardt, A. (2017). Shadow IT. Bus. Inf. Syst. Eng. 59, 469–473. http://dx.doi.org/10.1007/s12599-017-0497-x.

Haag, S., Eckhardt, A., and Schwarz, A. (2019). The Acceptance of Justifications among Shadow IT Users and Nonusers – An Empirical Analysis. Inf. Manage. 56, 731–741. https://doi.org/10.1016/j.im.2018.11.006.

Hair, J.F., Ringle, C.M., and Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. J. Mark. Theory Pract. 19, 139–151. https://doi.org/10.2753/MTP1069-6679190202.

Hamouche, S. (2020). COVID-19 and employees' mental health: stressors, moderators and agenda for organizational actions. Emerald Open Res. 2, 15. https://doi.org/10.35241/emeraldopenres.13550.1.

Hanley, M., and Montelibano, J. (2011). Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination.

Harley, B., Wright, C., Hall, R., and Dery, K. (2006). Management Reactions to Technological Change: The Example of Enterprise Resource Planning. J. Appl. Behav. Sci. 42, 58–75. https://doi.org/10.1177/0021886305284857.

Henseler, J., Ringle, C.M., and Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. 43, 115–135. https://doi.org/10.1007/s11747-014-0403-8.

Herath, T., and Rao, H.R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47, 154–165. https://doi.org/10.1016/j.dss.2009.02.005.

Herath, T., and Rao, H.R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inf. Syst. 18, 106–125. https://doi.org/10.1057/ejis.2009.6.

Herath, T., and Rao, H.R. (2009c). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support Syst. 47, 154–165. https://doi.org/10.1016/j.dss.2009.02.005.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., and Ochoa, M. (2019). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. ACM Comput. Surv. 52, 30:1-30:40. https://doi.org/10.1145/3303771.

Hong, J.B., Nhlabatsi, A., Kim, D.S., Hussein, A., Fetais, N., and Khan, K.M. (2019). Systematic identification of threats in the cloud: A survey. Comput. Netw. 150, 46–69. https://doi.org/10.1016/j.comnet.2018.12.009.

Huber, M., Zimmermann, S., Rentrop, C., and Felden, C. (2017). Integration of shadow IT systems with enterprise systems : a literature review. pp. 1–12.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. 31, 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

Iqbal, S., Mat Kiah, M.L., Dhaghighi, B., Hussain, M., Khan, S., Khan, M.K., and Raymond Choo, K.-K. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. J. Netw. Comput. Appl. 74, 98–120. https://doi.org/10.1016/j.jnca.2016.08.016.

Jang, S.J., and Johnson, B.R. (2003). Strain, Negative Emotions, and Deviant Coping Among African Americans: A Test of General Strain Theory. J. Quant. Criminol. 19, 79–105. https://doi.org/10.1023/A:1022570729068.

Johnston, A.C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Q. 34, 549–566. https://doi.org/10.2307/25750691.

Johnston, A.C., Warkentin, M., and Siponen, M. (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. Manag. Inf. Syst. Q. 39, 113–134. .

Johnston, A.C., Warkentin, M., McBride, M., and Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. Eur. J. Inf. Syst. 25, 231–251. https://doi.org/10.1057/ejis.2015.15.

Kandias, M., Virvilis, N., and Gritzalis, D. (2013). The Insider Threat in Cloud Computing. In Critical Information Infrastructure Security, S. Bologna, B. Hämmerli, D. Gritzalis, and S. Wolthusen, eds. (Springer Berlin Heidelberg), pp. 93–103.

Khan, S., Parkinson, S., and Qin, Y. (2017). Fog computing security: a review of current applications and security solutions. J. Cloud Comput. 6, 19. https://doi.org/10.1186/s13677-017-0090-3.

Kim, B. (2010). An empirical investigation of mobile data service continuance: Incorporating the theory of planned behavior into the expectation–confirmation model. Expert Syst. Appl. 37, 7033–7039. https://doi.org/10.1016/j.eswa.2010.03.015.

Kim, J., Kim, G., Choi, H., Seok, B., and Lee, N. (2019). Effects of social network services (SNS) subjective norms on SNS addiction. J. Psychol. Afr. 29, 582–588. https://doi.org/10.1080/14330237.2019.1694735.

Knapp, K.J., Marshall, T.E., Rainer, R.K., and Ford, F.N. (2006). Information security: management's effect on culture and policy. Inf. Manag. Comput. Secur. 14, 24–36. https://doi.org/10.1108/09685220610648355.

Lee, M.-C. (2010). Explaining and predicting users' continuance intention toward e-learning: An extension of the expectation–confirmation model. Comput. Educ. 54, 506–516. https://doi.org/10.1016/j.compedu.2009.09.002.

Lee, S.M., Lee, S.-G., and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Inf. Manage. 41, 707–718. https://doi.org/10.1016/j.im.2003.08.008.

Loch, K.D., Carr, H.H., and Warkentin, M.E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Q. 16, 173–186. https://doi.org/10.2307/249574.

Lumpkin, J.R., and Darden, W.R. (1982). Relating Television Preference Viewing to Shopping Orientations, Life Styles, and Demographics: The Examination of Perceptual and Preference Dimensions of Television Programming. J. Advert. 11, 56–67. https://doi.org/10.1080/00913367.1982.10672822.

Maasberg, M., and Beebe, N.L. (2014). The Enemy Within the Insider: Detecting the Insider Threat Through Addiction Theory. J. Inf. Priv. Secur. 10, 59–70. https://doi.org/10.1080/15536548.2014.924807.

Maasberg, M., Warren, J., and Beebe, N.L. (2015). The Dark Side of the Insider: Detecting the Insider Threat through Examination of Dark Triad Personality Traits. In 2015 48th Hawaii International Conference on System Sciences, pp. 3518–3526.

Mallmann, G., and Maçada, A. (2016). Behavioral Drivers Behind Shadow IT and Its Outcomes in Terms of Individual Performance. AMCIS 2016 Proc.

Mallmann, G.L., Maçada, A.C.G., and Oliveira, M. (2018a). The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users. Bus. Inf. Rev. 35, 17–28. https://doi.org/10.1177/0266382118760143.

Mallmann, G.L., Maçada, A.C.G., and Oliveira, M. (2018b). The influence of shadow IT usage on knowledge sharing: An exploratory study with IT users. Bus. Inf. Rev. 35, 17–28. https://doi.org/10.1177/0266382118760143.

Mazerolle, P., and Maahs, J. (2000). General strain and delinquency: An alternative examination of conditioning influences. Justice Q. 17, 753–778. https://doi.org/10.1080/07418820000094751.

Mazerolle, P., and Piquero, A. (1997). Violent responses to strain: an examination of conditioning influences. Violence Vict. 12, 323–343. https://doi.org/10.1891/0886-6708.12.4.323.

McClelland, D.C. (1988). Human Motivation (Cambridge University Press).

Meade, A.W., and Craig, S.B. (2012). Identifying careless responses in survey data. Psychol. Methods 17, 437–455. https://doi.org/10.1037/a0028085.

Mell, P., and Grance, T. (2011). The NIST definition of cloud computing.

Merton, R.K. (1938). Social Structure and Anomie. Am. Sociol. Rev. 3, 672–682. https://doi.org/10.2307/2084686.

Moon, B., Morash, M., McCluskey, C.P., and Hwang, H.-W. (2009). A Comprehensive Test of General Strain Theory: Key Strains, Situational- and Trait-Based Negative Emotions, Conditioning Factors, and Delinquency. J. Res. Crime Delinquency 46, 182–212. https://doi.org/10.1177/0022427808330873.

Moore, G.C., and Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation. Inf. Syst. Res. 2, 192–222. https://doi.org/10.1287/isre.2.3.192.

Moore, A.P., Cappelli, D.M., Caron, T.C., Shaw, E., Spooner, D., and Trzeciak, R.F. (2011). A Preliminary Model of Insider Theft of Intellectual Property (CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST).

Myers, N., Starliper, M.W., Summers, S.L., and Wood, D.A. (2017a). The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. Account. Horiz. 31, 105–123. https://doi.org/10.2308/acch-51737.

Myers, N., Starliper, M.W., Summers, S.L., and Wood, D.A. (2017b). The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. Account. Horiz. 31, 105–123. https://doi.org/10.2308/acch-51737.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. Eur. J. Inf. Syst. 18, 126–139. https://doi.org/10.1057/ejis.2009.10.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), pp. 156b–156b.

Panko, R.R., and Port, D.N. (2012). End User Computing: The Dark Matter (and Dark Energy) of Corporate IT. In 2012 45th Hawaii International Conference on System Sciences, pp. 4603–4612.

PATERNOSTER, R., and MAZEROLLE, P. (1994). General Strain Theory and Delinquency: A Replication and Extension. J. Res. Crime Delinquency 31, 235–263. https://doi.org/10.1177/0022427894031003001.

Pavlou, P.A., Liang, H., and Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. MIS Q. 31, 105–136. https://doi.org/10.2307/25148783.

Pedrozo-Pupo, J.C., Pedrozo-Cortés, M.J., and Campo-Arias, A. (2020). Perceived stress associated with COVID-19 epidemic in Colombia: an online survey. Cad. Saúde Pública 36. https://doi.org/10.1590/0102-311X00090520.

Pfleeger, S.L., Predd, J.B., Hunker, J., and Bulford, C. (2010). Insiders Behaving Badly: Addressing Bad Actors and Their Actions. IEEE Trans. Inf. Forensics Secur. 5, 169–179. https://doi.org/10.1109/TIFS.2009.2039591.

Piquero, N.L., and Sealock, M.D. (2000). Generalizing general strain theory: An examination of an offending population. Justice Q. 17, 449–484. https://doi.org/10.1080/07418820000094631.

Piquero, N.L., and Sealock, M.D. (2004). Gender and general strain theory: A preliminary test of Broidy and Agnew's gender/GST hypotheses. Justice Q. 21, 125–158. https://doi.org/10.1080/07418820400095761.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.-Y., and Podsakoff, N.P. (2003). Common Method Biases in Behavioral Research: a Critical Review of the Literature and Recommended Remedies. J. Appl. Psychol. 88, 879. .

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Inf. Secur. Tech. Rep. 15, 112–133. https://doi.org/10.1016/j.istr.2010.11.002.

Ruiz, J.M., Matthews, K.A., Scheier, M.F., and Schulz, R. (2006). Does who you marry matter for your health? Influence of patients' and spouses' personality on their partners'

psychological well-being following coronary artery bypass surgery. J. Pers. Soc. Psychol. 91, 255–267. https://doi.org/10.1037/0022-3514.91.2.255.

Ryan, R.M., and Deci, E.L. (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. Contemp. Educ. Psychol. 25, 54–67. https://doi.org/10.1006/ceps.1999.1020.

Shaikh, A. (2018). Shadow-IT System and Insider Threat: An Assessment of an Opportunity Dimension for the Identity Theft. In HCI International 2018 – Posters' Extended Abstracts, C. Stephanidis, ed. (Cham: Springer International Publishing), pp. 314–317.

Shropshire, J., Warkentin, M., and Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Comput. Secur. *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002.

Silic, M., and Back, A. (2014a). Shadow IT – A view from behind the curtain. Comput. Secur. 45, 274–283. https://doi.org/10.1016/j.cose.2014.06.007.

Silic, M., and Back, A. (2014b). Shadow IT – A view from behind the curtain. Comput. Secur. 45, 274–283. https://doi.org/10.1016/j.cose.2014.06.007.

Silic, M., Barlow, J.B., and Back, A. (2017a). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Inf. Manage. 54, 1023–1037. https://doi.org/10.1016/j.im.2017.02.007.

Silic, M., Barlow, J.B., and Back, A. (2017b). A new perspective on neutralization and deterrence: Predicting shadow IT usage. Inf. Manage. 54, 1023–1037. https://doi.org/10.1016/j.im.2017.02.007.

Singh, A., and Chatterjee, K. (2017). Cloud security issues and challenges: A survey. J. Netw. Comput. Appl. 79, 88–115. https://doi.org/10.1016/j.jnca.2016.11.027.

Siponen, M., and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Q. 34, 487–502. https://doi.org/10.2307/25750688.

Stanton, J.M., Stam, K.R., Mastrangelo, P., and Jolton, J. (2005). Analysis of end user security behaviors. Comput. Secur. 24, 124–133. https://doi.org/10.1016/j.cose.2004.07.001.

Stojmenovic, I., and Wen, S. (2014). The Fog computing paradigm: Scenarios and security issues. In 2014 Federated Conference on Computer Science and Information Systems, pp. 1–8.

Tabachnick, B.G., and Fidell, L.S. (2007). Using multivariate statistics, 5th ed (Boston, MA: Allyn & Bacon/Pearson Education).

Tan, G.W.-H., Ooi, K.-B., Leong, L.-Y., and Lin, B. (2014). Predicting the drivers of behavioral intention to use mobile learning: A hybrid SEM-Neural Networks approach. Comput. Hum. Behav. 36, 198–213. https://doi.org/10.1016/j.chb.2014.03.052.

Taylor, M., Haggerty, J., Gresty, D., and Lamb, D. (2011). Forensic investigation of cloud computing systems. Netw. Secur. 2011, 4–10. https://doi.org/10.1016/S1353-4858(11)70024-1.

The CERT Insider Threat Center (2014). Unintentional Insider Threats: Social Engineering (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University).

Vance, A., Lowry, P.B., and Eggett, D. (2015). Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations. MIS Q. 39, 345–366. .

Venkatesh, V., Brown, S.A., Maruping, L.M., and Bala, H. (2008). Predicting Different Conceptualizations of System Use: The Competing Roles of Behavioral Intention,

Facilitating Conditions, and Behavioral Expectation. MIS Q. 32, 483–502. https://doi.org/10.2307/25148853.

Walterbusch, M., Fietz, A., and Teuteberg, F. (2017). Missing cloud security awareness: investigating risk exposure in shadow IT. J. Enterp. Inf. Manag. 30, 644–665. https://doi.org/10.1108/JEIM-07-2015-0066.

Warkentin, M., and Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. Eur. J. Inf. Syst. 18, 101–105. https://doi.org/10.1057/ejis.2009.12.

White, K.M., Smith, J.R., Terry, D.J., Greenslade, J.H., and McKimmie, B.M. (2009). Social influence in the theory of planned behaviour: The role of descriptive, injunctive, and in-group norms. Br. J. Soc. Psychol. 48, 135–158. https://doi.org/10.1348/014466608X295207.

Willison, R., and Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Q. 37, 1–20. .

Willison, R., Warkentin, M., and Johnston, A.C. (2016). Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives: Examining the Influence of Disgruntlement on Computer Abuse Intentions. Inf. Syst. J.

Wu, I.-L., and Chen, J.-L. (2005). An extension of Trust and TAM model with TPB in the initial adoption of on-line tax: An empirical study. Int. J. Hum.-Comput. Stud. 62, 784–808. https://doi.org/10.1016/j.ijhcs.2005.03.003.

Zhang, S., Zhao, J., and Tan, W. (2008). Extending TAM for online learning systems: An intrinsic motivation perspective. Tsinghua Sci. Technol. 13, 312–317. https://doi.org/10.1016/S1007-0214(08)70050-6.

Zimmermann, S., and Rentrop, C. (2014). ON THE EMERGENCE OF SHADOW IT - A TRANSACTION COST-BASED APPROACH. ECIS 2014 Proc.

Zimmermann, S., Rentrop, C., and Felden, C. (2016). A Multiple Case Study on the Nature and Management of Shadow Information Technology. J. Inf. Syst. 31, 79–101. https://doi.org/10.2308/isys-51579.

VITA

As a graduate student in the department of Information Systems and Cyber Security (ISCS), Patricia Akello began her studies at UTSA in the fall of 2015. Her educational background includes a BS in Computer Science from Makerere University in Uganda, East Africa, a M.Sc. in Information Technology from UTSA, and a Graduate Certificate in Technology Commercialization from UTSA. Her previous work experience includes serving as a faculty co-lead to both Italy and Israel for UTSA's College of Business international immersion programs, as well as serving as a teaching assistant in the ISCS and Marketing departments. Her experience outside of UTSA and academia includes advocacy and fundraising for humanitarian causes at Invisible Children, UNHCR, Friends of Refugees and Amani Women Center. She also worked briefly in regulatory compliance in the consumer banking sector. As a multidisciplinary researcher, her research interests include cloud security and privacy compliance, insider threats, machine learning, social media & text analytics, blockchain, and misinformation. Her work has been presented at various conferences and journals, including Americas Conference on Information Systems (AMCIS), Emerging Researchers National (ERN) Conference in STEM and the International Journal of Information Management (IJIM)