https://doi.org/10.48009/4_iis_2020_234-246

Issues in Information Systems
Volume 21, Issue 4, pp. 234-246, 2020

WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19

Debra J. Borkovich, Middle GA State University, debra.borkovich@mga.edu
Robert J. Skovira, Robert Morris University, skovira@mga.edu

ABSTRACT

Technology and industry experts are warning businesses and individuals against the increasing threat of worldwide cyber-attacks. According to the FBI, the number of successful attacks skyrocketed across the U.S. by 600% (Inglet, 2020) and across the *globe by 300% (FBI IC3 Report, April 2020) since the COVID-19 pandemic hit. This great increase in successful attacks is directly attributed to the number of people working remotely or telecommuting due to the invisible threat of COVID-19. Once again, people are exposed as the weakest link in organizations by opening attachments; having greater data access or more administrator rights than required; downloading sensitive information onto thumb drives; forwarding work emails to personal accounts; or sharing documents they should not. Our research focuses on the cybersecurity issues of employees working-from-home and the constant struggle to secure confidential business and personally identifiable information outside of a proper office environment. Therefore, this paper explores the cyber risks and rewards to businesses and individuals when employees work from home and further offers recommendations to curb and mitigate these nefarious cyber influences upon teleworkers and their organizations.*

Keywords: COVID-19, Coronavirus, Corporate Culture, Cybersecurity, Teleworking, Working-from-Home

INTRODUCTION

Due to the COVID-19 pandemic, otherwise known as the Coronavirus, an upper-respiratory disease that struck Wuhan, China in 2019 and spread throughout the world in January of 2020, businesses adapted quickly by abruptly shifting employees to remote working. Social distancing practices were put into place to maintain physical distance of 6 feet or 2 arms' lengths between people to slow the spread of this highly contagious disease; and groups, crowds, and mass-gatherings were highly discouraged (www.cdc.gov). Government and self-mandated quarantines prevailed, and employees of all ranks were either laid off or told to work from home (WFH) for safety. As WFH or teleworking became the norm, the challenge organizations now face is protecting valuable data from risky employee behaviors targeted by hackers and social engineers.

This novel Coronavirus (or SARS-2) is causing a sweeping new WFH culture around the globe with far-reaching global technology implications, including a stepped-up demand for solutions like virtual desktop infrastructure and Desktop as a Service (DaaS) (Burke, 2020). Although two-step password authentication and Virtual Private Networks (VPN) are frequently implemented by organizations, WFH employees tend to develop security amnesia, abandoning routine office security practices, such as forwarding suspicious Emails, SPAM, Vlogs, Texts, Invitations, links, and attachments to the IT Department. In their defense, teleworkers generally plan to send (or report) these suspicious hacker events, including random phone calls from social engineers soliciting information while pretexting as customers, clients, or employees from other offices, *but often do not*, while absentmindedly opening links and attachments and/or participating in phone calls without proper verification of the sources.

Human error is attributed as the primary threat to companies' data security, and most IT teams lack true visibility of this employee vulnerability exacerbated by the remoteness of employees and lack of adequate cybersecurity planning for teleworkers. Many business leaders were lax to address security cultures and adopt advanced solutions to prevent employees from making the costly mistakes that result in data breaches and non-compliance. It is critical these solutions do not impede employees' productivity, since reports have shown that people will find workarounds if security gets in the way of them performing their jobs. Subject matter experts generally agree, well-intentioned but careless employees, consultants, vendors, and other stakeholders pose as much danger to an organization's cybersecurity as faceless hackers on the outside. In fact, 90% of successful hack attacks or incidents are ascribed to human error or behavior (Kelly, 2017). Therefore, valuable lessons-learned, are often attributed to employees abandoning routine security practices when working from home. People are the weak link in any organization, opening attachments, downloading sensitive information onto thumb drives, forwarding work emails to their personal computers, or sharing documents that they should not. In most cases, employees receive some information security training when they join a company, but typically this training is not repeated on a routine basis, and to date most corporations have not developed and memorialized a policy and procedure for teleworkers (Burke, 2020). Regardless, the human factor is consistently blamed as security's weakest link due to behavioral, social, and cultural vulnerabilities (Angwin, 2014; Garrett & Danziger, 2008).

Teleworkers are also subject to social engineering via random phone calls soliciting information or working remotely in public spaces where hacking, shoulder-surfing, and dumpster-diving are prevalent. Popularized into common parlance by Mitnick and Simon (2002), social engineering is an attack vector that relies heavily on human interaction that involves manipulating people into breaking normal security protocols, procedures, and best practices in order to gain access to computer systems, networks or physical locations for financial or other gain. These techniques are designed and deployed to lure unsuspecting users into providing business confidential and personally identifiable information (PII). Once the data are obtained, cybercriminals then attempt to infect computer systems and networks with malware by opening links to infected sites, sending e-mail or texting scams and attachments containing computer viruses and network worms, phishing and pharming hooks, and encouraging the overall use of public networks, mobile device apps, and infected external drives (Borkovich & Skovira, 2019).

Public and private organizations alike are often blamed for cybersecurity breaches due to managements' inability or reticence to recognize, plan, and fund adequate teleworker measures, consistently analyze, test, scan, update, maintain, and backup networks, hardware, software, communication equipment, and storage devices, and to adequately train employees to recognize and report pretexting overtures and cyberattacks, both real or perceived (Bloom, 2014). The sudden onset of the COVID-19 pandemic exacerbated and disrupted the development and training of WFH policies and procedures for many organizations. Traditional cybersecurity strategies are often vulnerable to insider threats due to a long-established practice focused on perimeter security, lacking the vital technology necessary to detect and stop attackers already within a system or network (Sobers, 2017). An expert hacker's approach typically focuses on the data, not the infrastructure that permits its access. And employees already have access to this valuable organizational data, generally more access than needed, just by logging into their work computers. A hacker can infiltrate a single vulnerable user account by encrypting thousands of files without being noticed, many of which the user probably neither used nor required (Reilly, 2012).

Corporations have embraced or at least toyed with telecommuting since experimenting with it in 1973 (Nilles, 1976; 1998). The years that followed increased this practice successfully in concert with the invention of the mobile phone (1980s), the World Wide Web (1989), the ubiquitous go-anywhere laptop (1990s), and mainstream broadband, wireless networking, smart phones, robotics, and everything digital in the 2000s (Borkovich & Noah, 2014). The Global COVID-19 2020 Work From Home Experience Survey reported that, over 56% of corporate U.S. employees are working from home and nearly 80% reported they want to (Lister, 2020). *So why is our business confidential data and personally identifiable information (PII) so insecure when we WFH? T*here will always be reasons for people to bend the rules and leak data outside of their organization, either maliciously or negligently. But the consequences for doing so, could be devastating for any company, including huge fines, loss of competitive advantage, and a damaged reputation (Sadler, 2020). For individuals, the loss of PII may result in devastating personal identity theft. So as more businesses adopt remote working practices, it is important that advanced technologies, training, and compliance are in place to ensure company sensitive data are secure and not at risk.

Our research sets-forth a critical 21st century literature review and an exploratory case study narrative, albeit limited to the salient and material events of the cyber risks and rewards to businesses and individuals when employees WFH. We discuss the influence of cybersecurity upon digital teleworkers, what it is and how it began, its present underpinnings and vulnerabilities, and its future influence on the betterment of securing workplace computer systems, networks, and its valuable data. Furthermore, we include the results of unstructured interviews with professional and managerial employees of both large and small business concerns who are currently experiencing telework in the Age of COVID-19. Our purpose is to show how and why organizational planning and data loss prevention needs to be aggressive and flexible if it is going to be effective. We conclude with recommendations to curb and mitigate these nefarious cyber influences upon unsuspecting teleworkers and their organizations.

LITERATURE REVIEW

The global shift to remote working has posed new security challenges for businesses, and traditional security solutions are failing to curb the problem of the insider threat and accidental data loss. And working from home (WFH) has compounded both internal (employees) and external threats (hackers and social engineers). According to Hewlitt-Packard and the FBI, the number of cyber and hacking attempts have skyrocketed across the U.S. by 600% (Inglet, 2020) and across the globe by 300% (FBI IC3 Report, April 2020) since the COVID-19 pandemic hit. This increase in attacks is directly attributed to the number of people working remotely due to the invisible threat of COVID-19. This section describes the results of several Work From Home (WFH) Surveys conducted by information technologists, cybersecurity experts, and academics prior to and during the onset of the virus pandemic.

"Computers don't create crimes. It is the people that use computers that commit the crimes. And people in the organizations can be, and often are, complicit" (Viljoen, 2018, para. 10). Prior to its own 2017 email platform breach, Deloitte published this client warning: "A hacker compromised a firm's global email server through a stolen administrator account that provided privileged, unrestricted access to all areas. The account, stored in a Microsoft Azure cloud service platform required only a single password and did not have two-step authentification" (The Guardian, 2017). This example illustrated that any and all organizations are vulnerable to social engineering hackers, even those that purport to be cybersecurity experts, and especially those that espoused WFH practices and extensive employee global travel. Deloitte ultimately followed its own cyber advice, and a year later was ranked as a cybersecurity global leader in the ALM Best Cybersecurity Consulting Report (Becker, 2018).

2015 Premiere Global Services Inc. (PGI) Global Telework Survey

The notion of working in an office from 9 to 5 was quickly being replaced by the new digital workplace in the 21st century, where everything employees needed to successfully do their jobs was available online due to technology advances and the rapid consumer adoption of mobile devices. The PGI Survey reported that 60% of Atlanta, GA remote workers said that they would leave their current job for a full-time remote position at the same pay rate; 79% of respondents would telecommute at least one day a week; 60% of teleworking respondents would resign their current positions for a similar job with similar pay if they could WFH full-time; 55% of non-teleworking respondents wished they had the ability to telecommute; 50% of teleworking respondents would telecommute more often if offered, with 2-3 days being the most popular frequency; and the most common response given by 54% of non-teleworkers when asked why they do not telecommute was: "Not an option in my role" (O'Brien, 2020).

2018 CyberArk Report

Prior to the onset of COVID-19, the frequency and severity of cybersecurity incidents increased and statistics reported that threat response and mitigation were not keeping pace with unabated risks. According to the CyberArk Report (Bourne, 2018), global security professionals reported that some of the top cyber security threats faced were: targeted phishing attacks (56%); insider threats (51%); ransomware/malware (48%); unsecured privileged accounts (42%); and unsecured data stored in the cloud (41%). Even though the nature of the perceived threats had not significantly changed in recent years, many organizations were not proactively adapting their cyber defenses to stay ahead of attackers and protect their sensitive information and systems. And 46% stated their security strategy rarely changed substantially after cyberattacks and despite known risks, many organizations did not adequately manage or secure their privileged user accounts. Unmanaged teleworkers, unsecured third-party and remote consultant and vendor access remained a significant security risk to corporations, as 51% of all CyberArk Survey respondents reported they gave third-parties remote access to their internal networks but rarely monitored their activity.

2020 Tessian Report

Tessian's 2020 State of Data Loss Prevention Report (Sadler, 2020) explored accidental and intentional data loss occurring in business networks. Additionally, the report revealed how the necessary shift to WFH created security challenges for businesses, also covering why traditional security solutions fail to curb accidental data loss. Tessian, an email security firm for organizations implementing its automatic Human Layer Security platform, protects employees on email from risks including data exfiltration, data loss, and phishing attacks. Vulnerable humans are not only the backdoor to cyber mischief, they represent the obvious front-door to intrusions, as well. The human factor in every organization is often ignored, unmanaged, and untrained, yet it is a critical element in building a strong cyber defense. While 91% of IT leaders trust their staff to follow best security practices when working remotely; 52% of employees believe they can get away with riskier behavior when working from home; 48% cite not being watched by IT as a reason for not following safe data practices; closely followed by being distracted (47%). Additionally, staff members report that security policies are a hindrance: 84% of IT leaders stated that data loss prevention is more challenging when employees WFH; 51% say such policies impede productivity; 58% of employees think information is less secure when working remotely; and 54% of employees find workarounds if security policies stop them from performing their jobs. Consequently, 30% of breaches involve internal actors exposing company information, as a result of negligent or malicious acts. Insider threats and data loss over email is particularly challenging for IT leaders to control, due to lack of visibility of the threat. Other revelations evidenced that: U.S. employees are twice as likely to send company data to their personal email accounts than their UK counterparts (82% vs. 35%); and IT leaders in U.S. organizations with over 1,000 employees estimate that just 720 emails are sent to unauthorized accounts a year. However, actual Tessian platform data reports that at least 27,500 unauthorized emails are sent a year or 38X more than IT leaders estimated; and one-third (34%) of U.S. employees take company documents with them when they leave a job (Sadler, 2020).

2020 Help Net Security Statistics Report

According to 2020 employee statistics from Help Net Security, the number of remote working jobs in the U.S. has more than doubled in the last four years, as employers acknowledged the need to change traditional working practices, further blurring the lines between home and the office (Baiati, 2020). This shift has huge benefits by improving people’s work-life balance, increasing employee productivity, and boosting employee retention rates. But data security is at a greater risk as staff are more likely to send important and, even, confidential company information to personal email accounts, with the usual intention of working on documents at home; however, many companies are completely unaware of how prevalent and risky these actions are. According to tech firm Probrand, nearly two-thirds of U.S. and U.K. employees have forwarded customer emails to their personal email accounts and 84% of them did not feel they were doing anything wrong (Biaiti, 2020).

2020 Harris Poll for Glassdoor Employers

Glassdoor Employers sponsored an online Harris Poll (April 2020) to explore how the COVID-19 pandemic transformed the way we live and work. The Poll results of 1,188 employed U.S. adults aged 18 or older cited their employers’ response to COVID-19 and the employees’ personal WFH sentiments. 472 respondents exclusively worked from home due to COVID-19 and were surveyed on their expectations for re-entering the workplace amid virus concerns; the remainder worked from home on a part-time basis. The Poll showed that 45% of employees expected to return to their company’s office during the summer, and nearly 3 in 4 employees were eager to return (Fluker, 2020). However, the Survey revealed that WFH amid the pandemic proved more difficult than both the employers and employees anticipated, as employees embraced teleworking; but employers were divided in their responses. Survey participants cited that their major WFH concerns were social media and TV distractions; lack of human interaction; at-home childcare; and social interaction as a parent. Table 1 summarizes selected Harris Poll results directly related to the pros and cons of teleworking during the COVID-19 pandemic (Fluker, 2020). *Note: Not one WFH respondent cited cybersecurity, technology, data confidentiality, or privacy issues as concerns.*

Table 1. Harris Poll Results for Glassdoor Employers – Teleworkers' Sentiments during COVID-19
Pros: Teleworker Benefits
• ***Mandatory Remote Work***: 67% of employees support the decision to mandate employees to work from home indefinitely due to COVID-19.
• ***Confidence in Remote Work Capability***: 3 in 5 U.S. employees (60%) are confident they can efficiently WFH if required indefinitely.
• ***Maintain Productivity***: 50% of employees believe they are equally or more productive working from home as their normal work location.
• ***Confidence by Age***: 68% of employees aged 18-34 v. 44% of employees aged 55-64 reported confidence in efficiently working remotely.
• ***Confidence by Gender***: 25% of female employees reported it is not possible to do their job remotely, compared to 14% of male employees.
• ***Confidence Among Parents***: 71% of employed parents with children under age 18 said they are confident to work remotely if they have to.
• ***Eagerness to Return:*** 72% say they are eager to return to their company's office, and among those: o 79% of men are more likely than women (61%) to say they are eager to return to their company's office. o 45% expect to return to working in their company's office in some capacity in Summer 2020. o **Top Factors:** Socializing with coworkers (52%) and in-person work collaboration (46%) are top reasons to return to the office.
• **More Flexible Work Options:** 65% would work from home full-time after COVID-19 restrictions are lifted if given the option.
• **Consider Remote Openings:** 60% would be more likely to apply to a position that is entirely remote if they were looking for a new job.
Cons: Remote Work Distractions
• ***Top Distraction***: The top distraction cited by teleworkers is watching TV and social media participation (32%).
• ***Lack of Human Interaction:*** 22% of employees are concerned about going 'stir crazy' when being mandated to work from home.
• ***At-Home Childcare:*** 27% of parents with children under 18 are concerned about the difficulty of managing children while WFH.
• ***Social Interaction as a Parent:*** 25% of parents with children under age 18 cited lack of social interaction when WFH; 18% of employees without children under age 18 disagreed.

2020 Wrike Remote Work Security Survey

Wrike, a collaboration software company, conducted a Remote Work Security Survey (Pham, 2020) of 1,002 workers at companies greater than 200 employees and found that nearly 1 in 5 indicated that they had not received any company guidelines for data security while working remotely. Approximately 41% of workers said they still use personal applications to transmit confidential files on at least a weekly basis. Clearly, individual homes are uncontrolled, unsecure environments; therefore, permitting employees to work outside a controlled environment can expose the organization to significant long-term risks. Figure 1 illustrates the frequencies that employees transmit and share business confidential data on unsecured platforms, generally for a perceived convenience or efficiency.

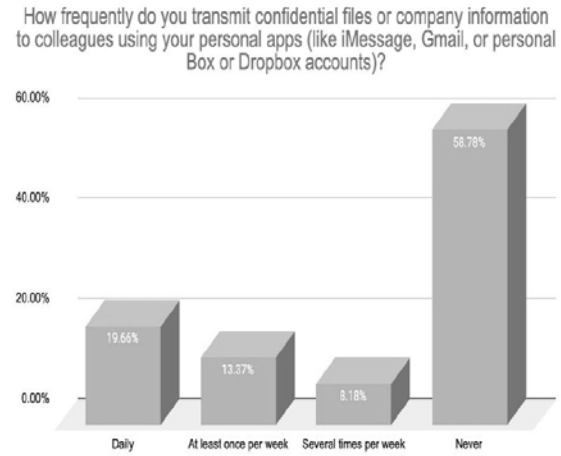

Figure 1. Wrike's 2020 survey shows that 41% of employees surveyed transmitted company data via unsecured platforms. *Copied with permission from Wrike Website (Public Domain).*

Figure 2. Social Media Companies considering WFH on a permanent or conditional basis for January 2021. *Copied with permission from Google Images (Public Domain).*

2020 Announcements from Twitter & Square

Due to COVID-19, several companies like Twitter and Square recently made the decision to transition their workforces to telework permanently, adapting the WFH model and sending shock waves through the business community grappling with the issue of whether or not or when to re-open. Nevertheless, Google and Facebook have announced plans to permit employees to WFH through the end of 2020 (Brandon, 2020; Brownlee, 2020). Figure 2 illustrates the primary WFH companies in this sector. Considering benefits like reduced commute times and operational costs, lower pollution levels, and increased morale and productivity, a permanent WFH business model may work well for fully digitized tech firms, but not all. On the heels of surprisingly successful WFH experiences, survey data clearly suggested a momentum toward expanded telework policies going forward. Corporate leaders have revealed short-term success of forced virtual working while also instantly reducing operational expenses. While teleworking can be part of an effective, contemporary organizational design, moving to widespread, long term remote working may result in a grave and risky mistake for many. Our research continues by discussing the pros and cons of teleworking by conversing with actual remote employees mandated to WFH.

RESEARCH METHODOLOGY

Our research focused on the overarching topic of cybersecurity threats to employees mandated to WFH due to the COVID-19 pandemic, by posing two specific questions: *1). Why is telework considered to be a data security risk for organizations?* - and - *2). How does working from home in the Digital Age contribute to this data security risk?* To pursue answers to our questions, we selected the qualitative two-step methodology of literature review in the narrative form of historical academic and subject matter expert research (Lundy, 2008; Berg & Lune, 2012; Tan, 2015), coupled with a case study of unstructured interviews (Creswell, 2013) solicited from professional and managerial teleworkers.

Step one commenced with an historical literature research of six telework studies and reports. This qualitative methodology for studying past events, phenomena, or occurrences provided investigators with possible, instead of probable, understandings and influences that shape the present and may lead to future outcomes (Monaghan & Hartman, 2000). Also viewed as an advantage due to the unobtrusive nature of historical research, this method itself cannot directly affect its subject matter (Deflem & Dove, 2013). Explicit documented historical research can be validated and triangulated as the contemporary witnesses are available for corroboration. Step two involved sourcing a population of professional and managerial employees working for technology firms in the U.S. Mid-Atlantic region. This sourcing resulted in conducting unstructured interviews from a sample size of twelve (12) adults (aged 24-62) who volunteered to participate anonymously from 2 large engineering and 2 small technology firms in Southwest Pennsylvania. Due to the bounded time constraints of access with each participant via a single 30 minute Zoom meeting, we developed and posed a short list of open-ended questions for each subject in order to ease the interviewee into the process and to help jump-start a conversation. Routinely, only a few suggestive remarks were needed as each participant eagerly led the conversation among different topics that she/he believed would be of interest to the WFH theme of our research. Our primary queries to start each interview were: *1). What do you like and dislike about WFH?* - and - *2). Do you have any concerns about cybersecurity, data or document management, technology, or personal privacy when you WFH?* Each participant was encouraged to take the conversation in any WFH direction that she/he felt would interest the researcher.

We then evaluated, analyzed, and triangulated our findings, matching and comparing after-action surveys, technical reports, and historical literature with transcripts from the unstructured interviews to interpret the results, develop mitigation strategies, recommendations, and conclusions.

RESULTS

The Results section provides findings from the unstructured interview transcripts of conversations with professional and managerial employees regarding their teleworking experiences during the COVID-19 pandemic of 2020. It is important to note that these interviews were recorded during May of 2020, while the mandatory stay-at-home orders in the U.S. for non-essential workers (promulgated by various State Governments) were still in full force and effect. The intent of the interviews was to delve deeper into the meanings behind the statistics reported by the 2020 Work From Home Surveys that we studied (see Literature Review), so our next phase was to speak with teleworkers about their WFH experiences. The COVID-19 pandemic has altered the way we work and interact with each other in and outside of the workplace, so we felt it was critical to find out if real employees mirrored some or all of the Survey results. Many organizations have shifted to WFH for safety reasons as we shelter-in-place, and as a result many employees and employers are wondering when, and if, it makes sense to return to the physical workplace.

Our conversations with professionals and management are consolidated into summary responses to our queries. The following Key describes each participant: (Pseudonym; Age; Job Title; Business Size (Large (L) or Small (S)).

- "Don't tell my IT guy, but I have discovered interesting workarounds to get my job done more efficiently. Yes, I send personal emails from my work account and vice versa. I may be side-stepping data security, but I now have a lot more time to spend doing other things while I WFH." *(Jake; 24; Engineer; SB)*
- "I am succeeding with my own work – actually I am more productive and efficient than ever by WFH. But I need the team collaboration to get large projects completed, like Customer Proposals. I am also scheduling Face Time or Zoom meetings because I need input or data from others, but more often than not people can't make the meetings I set up. Then I just have to wait for the information I need. I don't want to complain because I like WFH. But collaboration is hard and I hate to wait. If I was in the office, I would track people down!" *(Seth; 40; Proposal Manager; LB)*
- "I discovered that a great deal of functionality I use on my work laptop, I can use as Apps on my smartphone. It's easy, convenient, and I don't have to stay home. I can jog or buy groceries and I am still always on. I have to remember that the next time I jog and join a meeting or call, I need to set my device on mute or everyone knows I'm not home!" *(Sam; 49; Staff Attorney; LB)*
- "Yeah, I do forward work emails with attachments to my home email address. But that's because my own laptop is easier to use and I don't have to VPN into the system to get my work done. It's just more convenient. And if I need to work all day without turning off my laptop, sometimes the VPN connection is lost and then I have a real mess. I submit lots of Help Desk Tickets!" (*Julie; 42; Payroll Supervisor; LB)*
- "No, I don't work from Starbucks, but that's because my local shop is closed. Yes, I used to use the WI-FI in Starbucks and at the airport and other places, but our most recent IT training sternly forbid it – and I don't want to lose my job. We were sent email warnings about using public WI-FI from the IT Department and once the hacking was explained, I requested a hot spot and my boss approved the purchase. So I never had to use public WI-FI again!" *(Sarah; 37; Business Developer; SB)*
- "I am worried about bandwidth when I WFH all day non-stop. My kids and husband watch TV, stream movies, use apps and social media, and both kids have school online. How long can we keep this up without a crash?" *(Maya; 56; Accounting Manager; SB)*
- "No, I have never been worried about cybersecurity. Isn't that the job of the company? After all, they told me to WFH! I love the flexibility of WFH. I can boot up my laptop at midnight after my children are sound asleep and work all night if I want to. This way I can participate in Zoom meetings or conference calls during the day and still be available for my children." *(Angela; 26; Purchasing Assistant/Data Entry; SB)*
- "I am worried about returning to work and how it will upset my 2 kids and my dog. They are all so used to me being home and available 24/7, that I am expecting tears and tantrums from all of them. How are parents going to cope with the guilt?" *(Rose; 29; Purchasing Agent; SB)*
- "Funny you should ask about security and privacy. Just last week I received 3 random emails to my personal computer telling me I had to pay a bit coin ransom because the person knew my password. It was strange because each email was from a different person, but everyone had the same few letters in the middle of my password. So I changed most of my passwords, but I have so many that I doubt I caught them all. I didn't report it to IT because the emails came to my personal email address, but I was worried for a couple days. Now you made me think about it again!" *(Rich; 43; Logistics Manager; SB)*
- "Sometimes I forget that I am on the clock even though I am working at home, and I surf the web for long periods of time. I don't feel guilty, because I work more than 8 hours a day, but I don't want to get caught. I've been wondering if our IT guys are following us on the company computers. So I open my personal laptop next to my work laptop and use them both all day!" *(Mary; 54; HR Generalist; LB)*
- "I'm a Sales Rep and I'm very concerned about how our clients are perceiving us. I can't travel so I communicate with my Government Customers by mobile phone, Zoom, and Face Time. But is it enough? Will our contracts be renewed or will some other company step-in? I am great in a face-to-face situation and I can read body-language well, but I have no real idea how I'm perceived now. Selling is my livelihood and I'm not doing it! Recently my company banned the use of Zoom for security reasons, so we have to use

the Go-2-Meeting product that was purchased off the shelf and then customized by our IT Department. It works OK but it's really not user-friendly, like Zoom!" *(Hal; 50; Sales Director; LB)*

- "I'm more concerned with re-opening our office that I am with cybersecurity. We need to communicate that the workplace is going to look very different with new rules for social distancing and guidelines for sanitizing, and we have to keep employees informed. I have no idea how we are going to keep people from congregating at coffee stations, restrooms, hallways, etc. We may have to shut down all those areas and that will ruin our informal collaborations. Maybe we should consider WFH the norm, downsize the office space, and only come in for major events. We'd save costs, but would we succeed?" *(Bob; 62; COO; LB)*

The interviews evidenced that the majority of participants preferred the freedoms of WFH in an unrestricted environment, to working in a restrictive office facility with others. These results were also generally consistent with the Literature Review survey statistics of employees' assertions that they can get away with riskier behavior when working from home. The majority of our interviewees openly stated that they were also willing to take substantial risks (termination, probation, poor performance reviews, demotion of responsibilities, loss of income, and humiliation) with cybersecurity, document and data management, and personal identity threats in exchange for the benefits of teleworking. We now continue with the Discussion section that compares and interprets the findings of the Literature Review statistics with the transcripts of the unstructured employee interviews regarding their 2020 telework experiences during the COVID-19 pandemic.

DISCUSSION

Clearly the literature review of statistical surveys concurred with our case study interviews of WFH employees affirming that prior to and during the onset of COVID-19, C-Suite Officers, Company Presidents, and leadership staff rarely prepared and published Work From Home (WFH) business continuity and cybersecurity plans for its remote employees. With no end to the Coronavirus in sight, Government and commercial customers alike will start to demand documented WFH plans in their bids and proposals before new work or contracts are awarded. Business Continuity Plans will also need to include Disaster Recovery (DR) plans, cybersecurity policies and procedures, training, and audits that cover WFH practices. These are all costly endeavors but necessary safeguards for company and client data, and employee personally identifiable information (PII), *if only to limit a corporation's liability.*

Other challenges associated with a corporate WFH policy are development of revised budgets as substantial funding will be needed to upgrade or replace antiquated architecture, inadequate infrastructure, network bandwidth, cloud access, and raw computer power to service teleworkers in multiple locations, as well as office facilities. Enterprise Resource Management Systems, sophisticated software, and online learning platforms are also required for constant collaboration and routine training. Antiquated VPN technology is rarely replaced with WFH solutions, such as Microsoft OneDrive, Teams, Citrix ShareFile, and others to access files (Burke, 2020). This paradigm shift can present challenges for a company, such as choosing the right technologies to help get the work done, managing remote employees, and finding the right work-life-balance in an always-on culture.

However, we also learned that the WFH benefits are substantial and hard to relinquish once they are experienced. For instance, some of the key benefits of teleworking are: improved employee productivity and satisfaction; reduction of unscheduled absences; less wasted time in non-essential meetings and side-bar chats; and a better work-life-balance that improves physical and mental health. Employers can benefit by saving overhead costs, eliminating facilities and time zones; reducing travel costs; and increasing the talent pool with WFH employees.

Consistent with the 2020 Tessian Report (Sadler, 2020), our interviewees concurred that IT Departments are generally unaware of, or too busy, to monitor and track employee email activity when work emails are forwarded to personal accounts. There can be no denying that monitoring all employee email behavior is an arduous task for IT and compliance teams to undertake. With the average employee sending and receiving 124 emails a day, and with daily email traffic increasing 5% year on year, deciphering data exfiltration within email logs is like finding a needle in a haystack. An organization may opt to simply blacklist all freemail domains. However, this can impede productivity and is usually ineffective given that many clients, small firms, contractors, and job seekers use freemail accounts. A more intelligent approach to data exfiltration may be machine learning, if it can evolve to understand the differences between authorized and unauthorized freemail accounts and analyze email content to determine whether it is sensitive or non-sensitive (Westfall, 2020).

Additionally, the corporate culture must adapt to include WFH employees. Open communication and collaboration are generally lacking regardless of an employee's location. An environment of open and transparent communications with constant feedback must be strongly encouraged and enforced for remote employees. Although meetings tools such as Zoom, Skype, Google Hangouts, Go-to-Meeting, etc. are essential, opening instant messaging channels (IMs) are crucial engagement for remote employees offering an informal means of communication (the proverbial water-cooler effect) without waiting for information from a Zoom meeting or an email reply. Therefore, to ensure success, laptops, printers, smartphones, collaborative tools, software platforms, and apps for sharing and meetings must be readily available. And remote employees must be adequately trained on all devices, as well as, critical cybersecurity initiatives, data security, and reporting protocols.

Consequently, we determined that *Research Question #1. Why is telework considered to be a data security risk for organizations?* was directly resolved by the Literature Review and 2020 WFH Statistical Surveys that clearly elicited questionnaire replies that confirmed the cybersecurity and data management risks of teleworkers. However, *Research Question #2. How does working from home in the Digital Age contribute to this data security risk?* was indirectly resolved through the employee interviews by the obliviousness of employee responses to risky data management and email practices and total unawareness of cybersecurity threats they were routinely taking with company and personal technology at their daily disposal when WFH.

Initiatives for teleworking must become part of internal company culture if there's hope for widespread success and adoption. Most organizations today have access to the tools and solutions necessary to make remote work feasible and productive, but if policies, procedures, training programs, and audits aren't adopted and welcomed fully by WFH employees and corporate leadership, then remote work will not succeed. Companies are expanding their workforce to include talented employees globally and in the last decade, the number of remote and WFH employees has grown 115% (Garamendi, 2017). Clearly, there is a pressing need for improved corporate cybersecurity practices and planning for teleworkers. More definitive and enforceable regulations will drive better security protocols, and more rigorous compliance requirements will force more effective privacy practices (Keizer, 2012). Per the CyberArk Report (Bourne, 2018), 83% of IT security professionals say new privacy requirements and security recommendations such as the EU General Data Protection Regulation (GDPR) implemented in 2018 and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework released in 2019 (promulgated in the U.S. Cybersecurity Enhancement Act of 2014) are enhancing our overall security and privacy posture. Reforming the organizational security culture remains a top priority but is often overlooked or neglected, misperceived as a cost factor or necessary evil rather than a differentiating factor or competitive advantage. Rather than viewing security simply as a cost, digital business champions should recognize it as a key aspect of every project and activity, then use it to differentiate themselves from their less-secure competitors (Elgar, 2019).

Therefore, based upon our study of Working from Home (WFH) during the Age of COVID-19, we recommend establishing or adapting an inclusive WFH corporate culture that includes teleworkers. To this end, we developed Table 2. detailing the critical elements required to maintain a workable corporate culture as the: "6 Essential WFH Culture (C) Factors: Control; Collaboration; Communication; Cost; Cloud; & Culture."

Table 2. "6 Essential WFH Culture (C) Factors" Strategies to Develop an Inclusive WFH Corporate Culture

• **Control**	Control & monitoring solutions must be measured & appropriate. Micromanaging keystrokes & web surfing is not efficient. Set goals & metrics, measure output, & reward performance.
• **Collaboration**	Use Zoom, Skype, Google Hangouts, IMs, etc. routinely; Share documents & insights; Join teams.
• **Communication**	Clarify roles & responsibilities; Document everything digitally and make it accessible to all employees; Share information transparently & solicit feedback; Use Email; IM; etc.
• **Cost**	Accrued savings per remote worker are between $11K & and $20K annually; lowered expenses in real estate; overhead; & equipment are plusses for employers (Westfall, 2020).
• **Cloud*****	Enterprise is responsible for securing cloud workloads; vendors offer improved efficiency & reliability; access to on-demand computing; flexible pricing; increased services; accessible from any device.
• **Culture**	Cultural paradigm shift requires more corporate trust & greater employee responsibility; higher workforce retention & loyalty; higher productivity & output; WFH results in empowerment.

***Due to the limited understanding of the challenges of securing cloud workloads in certain environments while managing thousands of remote machines and configurations deploying the Internet of Things (IoT) devices, in concert with Global Positioning Systems (GPS) without security checks, represents another vulnerability for organizations, their customers, and other stakeholders (Evans, 2019).

To successfully enforce the new inclusive WFH culture, cybersecurity training and monitoring has to be a major plank of the new platform. Adequate technology must be assessed and acquired, routinely patched, and the organization's leaders must re-assess the business continuity and infrastructure plans to operationalize WFH as a normal (not a-typical) practice. We recommend that employees are consistently motivated with innovative training programs, communication media, and incentives. Furthermore, organizations may opt to develop and perform a WFH Cybersecurity Knowledge Management Program, starting with an audit to learn both the explicit and tacit information already established for remote employees. It is imperative to learn what is known and not known, prior to commencing the development of an important new WFH enterprise-wide initiative.

We recommend that future research of professional and managerial teleworkers employed by high tech companies be conducted in other regions of the U.S., specifically comparisons of employees from urban versus rural locations. Additionally, we plan longitudinal ethnographic studies of teleworkers as they transition from the novel Coronavirus scenario to teleworking permanently for high tech companies. Furthermore, to advance generalizations of results, researchers should consider quantitative statistical survey studies to target responses from other teleworking populations, domestic and globally, by increasing the sample sizes.

CONCLUSION

By addressing our research questions through a substantive and material literature review of subject matter experts and a limited case study of teleworkers, we confirmed that Working from Home (WFH) presents a serious vulnerability to cybersecurity threats, such as malicious hackers and social engineers. Once again, the human factor is identified as the weakest link to information security (corporate and personal). From our study we learned that moving from inertia to action is not an easy process, regardless of the type or size of the organization or the rank and role of an individual. We further grasped that building awareness is just the first step to develop a modern cyber defense in the remote workplace and that a strong technical infrastructure and business continuity plan are essential to success. Organizations must turn knowledge into action to defend against multiple cyber threats by mitigating risk. This WFH initiative demands support, buy-in, and funding from the most senior levels of the organization and must be extended to all stakeholders. Cybersecurity protection for teleworkers starts with robust ethics training and security education programs. Users must be trained to never click on suspicious links and always guard their log-in credentials, regardless of the workplace location. In the event that cyber intrusions are successful, it is critical to employ a high-quality cybersecurity solution that can both eliminate infections and track their source (Pankov, 2019). Protecting the organization from being victimized by hackers and social engineers must be the responsibility of each and every employee, regardless of location. Anyone can be exploited from executive and line management, through professionals, technicians, vendors and consultants, to receptionists, and anyone with a keyboard; however, teleworkers may be the most isolated and vulnerable. We argue that the challenge to defend against human-based cyber and social engineering vulnerabilities is substantial and can no longer be ignored. As the U.S. begins to rebound after the COVID-19 pandemic, businesses will continue to WFH for the foreseeable future. With masked phishing threats, malware, and ransomware on the rise, we must all be vigilant to protect against the scourge of encrypted malicious traffic from hackers and social engineers, *regardless of where we telework*.

REFERENCES

Angwin, J. (2014). *Dragnet nation: A quest for privacy, security, & freedom.* New York: Times Books.

Apgar, M. (1998, May-June). The alt workplace: Changing where & how people work. *Harvard Business Review*. Retrieved from: https://hbr.org/1998/05/the-alternative-workplace-changing-where-and-how-people-work

Baiati, N. (2020, May 29). Employees abandoning security when working remotely. Help Net Security. Retrieved from: https://www.helpnetsecurity.com/2020/05/29/abandoning-security-when-working-remotely/?utm_source=360Works%20CloudMail&utm_medium=email&utm_campaign=NewsWatch

Becker, L. (2018). Best Cybersecurity Consulting Report for 2018. *The ALM Vanguard. Retrieved from:* www.alm.com/intelligence/consulting-industry

Berg, B., & Lune, H. (2012). *Qualitative research methods for the social sciences*. Upper Saddle River, NJ: Pearson.

Berners-Lee, T., & Fischetti, M. (1999). *Weaving the web: The original design and ultimate destiny of the World Wide Web by its inventor.* San Francisco, CA: Harper.

Bloom, N. (2014). To raise productivity, let more employees work from home. *Harvard Business Review* (Extracted from the Jan.-Feb. 2014 Issue). Retrieved from: Retrieved from: https://hbr.org/2014/01/to-raise-productivity-let-more-employees-work-from-home

Borkovich, D. J., & Noah, P. D. (2014). Big data in the Information Age: Exploring the intellectual foundation of communication theory. *Information Systems Education Journal, 12*(1), 15-26.

Borkovich, D. J., & Skovira, R. J. (2019). Cybersecurity inertia and social engineering: Who's worse, employees or hackers? *Issues in Information Systems*, *20*(3), 139-150.

Bourne, V. (2018). *CyberArk Global Advanced Threat Landscape Report 2018*. Retrieved from: https://www.cyberark.com/resource/cyberark-global-advanced-threat-landscape-report-2018-security/

Brandon, J. (2020, May 12). This is huge: Twitter CEO says employees can work from home forever. *Forbes Online Journal*. Retrieved from: https://www.forbes.com/sites/johnbbrandon/2020/05/12/this-is-huge-twitter-ceo-says-employees-can-work-from-home-forever/#4f2d1ff54382

Brownlee, D. (2020, May 18). Twitter, Square announce work from home forever option: *Forbes Online*. Retrieved from: https://www.forbes.com/sites/danabrownlee/2020/05/18/twitter-square-announce-work-from-home-forever-optionwhat-are-the-risks/#19c53fe82565

Burke, S. (2020, April 2). Coronavirus Is Creating A Global 'Work-At-Home' Culture. CRN Online. Retrieved from: https://www.crn.com/news/cloud/coronavirus-is-creating-a-global-work-at-home-culture

Creswell, J. W. (2013). *Review of the Literature: Research Design, Qualitative, Quantitative, & Mixed Methods Approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications.

Deflem, M., & Dove, A. L. (2013). Historical Research and Social Movements. In D. Snow, D. Porta, B. Klandermans, & D. McAdam (Eds.), *The Wiley-Blackwell Encyclopedia of Social and Political Movements* (pp. 560-563). Malden, MA: Wiley-Blackwell.

Elgar, E. (2019). *Telework in the 21st century*. Northampton, MA: International Labor Organization.

Evans, L. (2019). Cybersecurity: *What you need to know about computer and cybersecurity, social engineering, and The Internet of Things.* No city, state: Self-published by Lester Evans.

Fluker, D. (2020, March 23). *Harris Poll for Glassdoor: COVID-10 Sentiments on Working-From-Home.* Retrieved from: https://www.glassdoor.com/employers/blog/new-survey-covid-19/

Garamendi, J. (2017). GPS vulnerable, but there is a solution. *National Defense of NDIA, CI*(758), 15-16.

Garrett, R. K., & Danziger, J. N. (2008). On cyberslacking: Workplace status and personal Internet use at work. *Cyberpsychology & Behavior, 11*(3), 287-292.

Inglet, M. (2020, June 1). It's just ballooning up: Technology experts warn against increasing cybersecurity threats. *KTVB Crime Online*. Retrieved from: https://www.ktvb.com/article/news/crime/its-just-ballooning-up-technology-experts-warn-against-increasing-cyber-security-threats-covid-19-pandemic/newswatch

Keizer, G. (2012). *Privacy*. New York: Picador USA.

Kelly, R. (2017, March). 90% Cyberattacks are caused by human error or behavior. *Chief Executive Online*. Retrieved from: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Lister, K. (2020). Work-from-Home Experience Survey. Retrieved from: https://globalworkplaceanalytics.com/telecommuting-statistics

Lundy, K. S. (2008). Historical Research. In L. M. Given (Ed.), *The SAGE Encyclopedia of Qualitative Research Methods: Volumes 1 & 2* (pp. 395-399). Thousand Oaks, CA: SAGE Publications.

Mitnick, K., & Simon, W. (2002). *Art of deception: Controlling the human element of security*. Indianapolis: Wiley.

Mitnick, K., & Simon, W. (2006). *Art of intrusion: The real stories behind the exploits of hackers, intruders & deceivers*. Indianapolis: Wiley Publishing, Inc.

Monaghan, E., & Hartman, D. (2000). Undertaking Historical Research in Literacy. In M. Kamil, & P. Mosenthal, (Eds.), *Handbook of Reading Research: Vol. III* (pp. 109-122). New Jersey: Lawrence Erlbaum Associates.

Nilles, J. (1976). *The Telecommunications-Transportation Tradeoff*. New York: Wiley Interscience.

Nilles, J. (1973). *Managing Telework: Strategies for Managing the Virtual Workforce*. New York: Wiley & Sons.

No author. *FBI IC3 Cyber Report*. (2020, April). Retrieved from: https://www.fbi.gov/investigate/cyber/ic3.

O'Brien, S. (2020, June 23). *Premiere Global Services, Inc. Global Telework Survey*. Retrieved from: https://www.pgi.com/blog/2015/06/pgi-global-telework-survey/

Pankov, N. (2019, May). Solo: A Cybersecurity Story. Retrieved from: https://usa.kaspersky.com/blog/solo-starwars-cybersecurity/17651/

Pham, M. (2020, May 14). *Remote work security survey results: Is remote work really secure?* Retrieved from: https://www.wrike.com/blog/remote-work-security-survey/

Reilly, R. (2014, June). 95% Successful security attacks are the result of human error. Retrieved from: https://venturebeat.com/2014/06/19/95-of-successful-security-attacks-are-the-result-of-human-error/

Sadler, T. (2020). *State of Data Loss Prevention: 2020 Tessian Report*. Retrieved from: https://www.tessian.com/resources/#report/

Sobers, R. (2017). Why the OPM breach report is a call to action to embrace data centric security. *Contract Management*, *57*(2), 28-33.

Tan, J. (2015). Historical research: A qualitative research method. *Academia (21 April 2015)*. Retrieved from: file:///C:/Users/Downloads/HISTORICAL_RESEARCH_A_QUALITATIVE_RESEAR.pdf

The Guardian. (2017, September 25). Deloitte hit by cyberattack revealing clients' emails. Retrieved from: https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-emails

Viljoen, T. (2018). Cybercrime is not just a tech problem. Deloitte Online. Retrieved from: https://www2.deloitte.com/au/en/pages/risk/articles/cybercrime-tech-problem.html

Westfall, C. (2020, May 21). How organizations can create a working from home culture. *Forbes Online.* Retrieved from: https://www.forbes.com/sites/chriswestfall/2020/05/21/how-organizations-can-create-a-work-from-home-culture-and-embrace-the-remote-workforce/#743a85df41a1