Organizational Cybersecurity Post The Pandemic: An Exploration of Remote Working Risks and Mitigation Strategies

Dr. Stephen Treacy, Anoop Sabu, Thomas Bond, Joseph O'Sullivan, Jack Sullivan, Peter Sylvester
Department of Business Information Systems
Cork University Business School, Ireland

Stephen.treacy@ucc.ie

Abstract: The Covid-19 pandemic has forced organisations to embrace the largest remote workforce in history, yet this upheaval also brought an increasing number of cyber vulnerabilities to the fore. Organisations must remain committed to not leaving business processes, personal data, or vital infrastructure at risk, which has proved challenging for most. As remote working establishes itself as the new normal, criminals are seeking to capitalize on the widespread cybersecurity uncertainty, and succeeding. Private organisations and cybersecurity professionals must come together to establish robust solutions for home working cybersecurity.
This investigation explores several prevalent cyber risks (private networks, public hotspots, remote desktop protocol, authentication policies, virtual private network configuration and phishing attacks) across three key threat classifications of management, technical and human factors when remote working from the perspective of twenty industry experts. These findings offer key insights to emerging vulnerabilities, while also revealing defined strategies for organisations to help mitigate these challenges.

Keywords: Cybersecurity, Remote Working, Covid-19, Threat Classification, Phishing.

1. Introduction

As the Covid-19 pandemic struck Wuhan, China in 2019 before subsequently spreading across the world in January 2020, businesses had to quickly adapt, abruptly shifting their employees to remote working. As this new way of doing business suddenly became the norm, organisations quickly realized they were being unprecedently challenged to protect valuable data from employee behaviours being targeted by hackers and social engineers. While safe in the comfort of an organizational setting when it comes to cybersecurity, working from home employees tend to develop security amnesia, often abandoning routine security practices, for example establishing authentication procedures, or forwarding suspicious emails, links or attachments to their IT Department. Though employees might initially plan to report these occurrences, including phone calls from social engineers designed to extract valuable information under the guise of pretending to be clients, customers or employees from other offices, they often do not, continuing instead to absentmindedly open links and attachments, and/or engaging in these phone calls without asking for proper verification (Borkovich and Skovira, 2020). Researchers generally agree that unfortunately it is the well-intentioned yet careless worker, vendor, consultant, or other stakeholder that represents as much of a danger to an organisation's cybersecurity as faceless actors on the outside. As a result, valuable lessons that have been learned by organizations in the wake of remote working have often been due to employees abandoning routine security practices when working from home. As more people continue to join and engage with these digital platforms as part of their daily life, so too does the number of cyberattacks that are increasing in many countries, opening new playing fields for cybercriminals to target and exploit. Organisations need to take immediate action to mitigate new cybersecurity risks created by this sudden shift to remote working, because otherwise similar gaps in the organisational and employee protection may be exploited.

2. Literature Review

The Covid-19 pandemic has demonstrated organisations' dependence on information technology, especially the need for adequate cybersecurity to protect the remote workforce and the technologies we are using (Furnell et al., 2021). Cybersecurity can be defined as being the "*collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*" (ITU, 2008). Modern cybersecurity thus involves detecting behavioural anomalies to prioritise the most severe threats, reducing investigation and threat detection times. According to Shi (2020), it is evident that Covid-19 has impacted cybersecurity spending by firms and organisations, outlining that spending has decreased even though 46% of organisations reported an increased amount of cybersecurity threats related to remote working, with 49% expecting an incident or data breach within a month of the report. Similarly, according to the Federal Bureau

of Investigation, the number of successful attacks exploded across the United States by 600%, and across the globe by 300% since the Covid-19 pandemic hit (Borkovich and Skovira, 2020). This represents a massive increase from the average cost of a data breach in 2019 when it was $3.92 million, or $152 per lost or stolen record and has been directly attributed to the amount of employees now working from remotely due to the invisible threat of Covid-19, a further 1.6% increase from 2018 according to IBM (2019).

2.1 Remote Working Security Risks

Given the significant costs of a data breach to multiple parties, it is critical to implement relevant protection mechanisms in response to general and specific threats. Unfortunately, connecting any system to the internet brings with it inherent security risks as accessing any internet resource opens a communication path that crosses a suite of network equipment from where the connection begins to the destination system, with each communication node representing a potential security vulnerability. For the purpose of this study, the security risks affecting employees engaging in remote working can be divided into three threat classifications: management factors, technical factors, and human factors, as outlined by Wang and Ruan (2020).

Private and public organisations alike are often blamed for cybersecurity breaches due to management's inability to recognize, plan, and fund adequate remote working measures, continuously analyse, scan, test, update and maintain networks and to adequately train employees to recognize and report pretexting cyberattacks, both real and perceived (Bloom, 2014). The difficulty increases therein as employees are now relying on their private networks to gain access to their office network which are not as secure (Ramadan et al., 2021). Improper system configuration has thus become a concern for organisations as wireless networks are more vulnerable than wired networks since intruders can pick up signals from outside the host building allowing the opportunity to breach the network for malicious purposes (Zafft and Agu, 2012). Organisations need to be aware of hackers exploiting weak and unsecured private networks from their employees locations to gain access to their data, as research highlights that many of these networks are not even secured using basic encryption standards (Goldsborough, 2015).

From a technical perspective to counter these issues, mechanisms that reduce network security risks, and use network vulnerability scanning, firewalls, network access controls, and network intrusion detection systems should be implemented (Wang and Ruan, 2020). Unfortunately, an area of concern that has emerged as a network hardware defect has been identified from extant literature as Remote Desktop Protocol (RDP), used to successfully authenticate an unauthorized host that leaves footprints in both the host and network logs. While this service is primarily used by legitimate network administrators, it has also become a primary tool used by attackers since discriminating between legitimate and malicious use of this tool is challenging resulting in the rise of cybercriminals targeting RDP networks (Blanch, 2018). Authentication is similarly vital to maintain the integrity of the system at large, encompassing policies that employees must go through to gain access to confidential and sensitive data. Recent literature has explored how static passwords can increase a user's vulnerability to attack due to their reuse and repeatability making them easier to steal (Channabasava and Kanthimathi, 2019). Most employees choose simple passwords which might lead to a privacy breach or system vulnerability, with Stobert and Biddle (2014) outlining the demands of having multiple accounts on multiple platforms as the reason for password reusability.

Lastly, the human factor represents an additional threat classification as we play an important role in the design, installation, production and maintenance of any infrastructure, with human error leading to the potential disruption or damage of operations (Dhillon and Liu, 2006). This is particularly relevant when the security, stability and reliable operation of the system is critical, with vulnerable virtual private network (VPN) configuration and malicious phishing attacks established as inherent risks. Malicious cyber actors are leveraging existing VPN vulnerabilities to hijack online meetings, teleconferences and online courses which have been established without security controls (Ramadan et al., 2021). Similarly, these same actors have long exploited the human point of failure to gain access to systems, and the number of phishing and cybercrime risks have increased dramatically during the Covid-19 pandemic (Tran, 2020). Phishing attacks target individuals and organisations by collecting personal information and data through different mediums, with these hackers identifying targets and techniques to launch their attacks such as clickjacking, spear phishing, cross-site scripting, man in the middle and malvertising (Alabdan, 2020, Gupta et al., 2018). These schemes are intended to make the person respond without thought, and can be quite difficult to spot, resulting in the human factor being consistently blamed as security's weakest link due to behavioural, social and cultural vulnerabilities (Angwin, 2014).

2.2 Research Gap

Organisations have traditionally spent considerable resources to promote a secure working environment in their offices, however, the Covid-19 pandemic has disrupted this paradigm and forced employees to work remotely. While the workforce can remain just as, if not more productive, organisations need to ensure that these remote working conditions keeps company data as secure as it was in the corporate office (Wallace et al., 2021). Attackers now have multiple entry points and employers must take into consideration the heightened security risks of having a remote and dispersed workforce. Organisations need to be better protected, more secure and should not ignore the vital part their employees play in keeping their data safe (Malecki, 2020). While employees in most cases receive some security training upon joining an organisation, unfortunately this training is rarely delivered on a routine basis, and to date, most organisations have not developed nor circulated a policy and procedure for remote workers (Burke, 2020). We therefore want to take the aforementioned security risks into account from the perspective of industry experts, and state our research questions as: (i) *How are organisations mitigating their management security risks (private network and public hotspot usage) in response to the remote working paradigm?*; (ii) *How are organisations mitigating their technical security risks (RDP and authentication policies) in response to the remote working paradigm*?; and (iii) *How are organisations mitigating their human security risks (VPN configuration and phishing attacks) in response to the remote working paradigm*?

3. Methodology

The purpose of this study is to investigate remote working cybersecurity threats across three key areas from the perspective of security experts, tackling the emerging trends and vulnerabilities organisations are continuing to face while their employees are remote working. To facilitate this investigation, expert judgement can be used to formally bound problems when no data are available through the use of semi-structured interviews (Wilson, 2017). This allowed the researcher to explore emergent topics within the interview setting as they arose, while also empowering the researcher to pursue additional lines of questioning towards cybersecurity threats that the experts had evident experience of. A predominant reason for developing theory from this approach is that it facilitates rich, qualitative evidence, along with testable propositions (Gregor, 2006, Sutton and Straw, 1995). Given how this approach is deeply embedded in rich, empirical data, building theory from evidence gathered produces theory that is accurate, honest, interesting and testable (Eisenhardt and Graebner, 2007). This study uses the definition provided by Garthwaite et al. (2005), who describe experts as being "*persons to whom society and/or peers attribute special knowledge about matters being elicited*" (p. 681). More importantly, it is also the ability to use this knowledge that defines a good expert (O'Hagan et al., 2006). Experts were identified through appropriate case selection methodologies in accordance with Yin (2008) and Seawright and Gerring (2008), ensuring several objectives: (i) a representative sample of expert roles was obtained where similar results were predicted and used as literal replications; (ii) useful variations on the security risks of interest were obtained; and (iii) experts occupied senior roles that made them knowledgeable about the risks being researched. It is from these characteristics, and being consistent with Marshall et al. (2013), that twenty security experts were identified, with titles including directors, founders and managers.

This protocol was aimed to be flexible, and to allow for adjustments based on insights offered through the interviews which was subsequently analysed through the Gioia methodology. This approach facilitates the processing and interpretation of data by establishing concepts and themes, providing an academically rigorous structure with which the data can be interpreted, following five key steps (Gioia et al., 2013): (i) transcript analysis where the researchers searched for similarities and differences among the emerging categories being coded; (ii) first order concepts where the researchers identified if the themes and ideas suggest in the interviews could become conceptual understandings that serve to explain answers to the research questions; (iii) second order concepts where the previous concepts were further broken down to create research findings; (iv) aggregate dimensions where direct quotes are translated through first-order concepts to theoretical and academic understandings of the second order concepts, and are finally reduced to structurally supported and rigorously achieved dimensions that represent findings; and (v) data structures were then created to act as visual aids outlining the steps involved from inception of the theme to the themes created in the aggregate dimensions.

4. Findings

4.1 Research Question 1

The issue of insecure public and private Wi-Fi networks was highlighted as being a problem area for the experts in this investigation. Employees were advised to use secured and private Wi-Fi when working remotely, and on occasion when an employee needs to connect over a public hotspot, they were advised to utilise a virtual private network (VPN). The practice of using public hotspots is one that should be discouraged: "*Organisations can't use public or Wi-Fi, or hotspots*" (E-11). IT security governance teams were encouraged to "*explicitly outline an organisation's stance on the use of public and private Wi-Fi to prevent ambiguity*" (E-3). Organisations should grant network access to an employee's home IP address, and no access should be given to an IP address deemed potentially unsafe. Even with tools and policies organisations may have in place, the experts advised to whitelist and blacklist IP addresses to minimize the security risk level. In addition, since the use of public hotspots by employees "*can further expose an organisation's network and make it even more susceptible to attack or infiltration*" (E-8), strict policies such as IP filtering have become even more vital for organisations. The majority of experts agreed that effective training is necessary to promote awareness of network vulnerabilities when working from home: "*Employees need to be regularly trained on the differences between public and private Wi-Fi, especially on the associated risks*" (E-14), at least annually. Some experts, however, were conflicted, arguing that "*training does not generally work*" (E-7), and that for some organisations there is a need to focus on employee behaviour rather than policy. This lack of confidence in employees results in a zero-trust approach where "*the underlying network should not be trusted… (as it) exposes organisations to other security threats*" (E-8). Private Wi-Fi should also be encrypted, with authentication protocols being enforced for organisations to have "*Wi-Fi enabled entrusted devices*" (E-14), with all devices and technologies being updated and patched regularly: "*IT teams are able to push security patches and updates remotely*" (E-19), often with "*proprietary software*" (E-1). The experts also stressed to maintain zero-trust policies "*irrespective of remote work or non-remote work*" (E-3).

Experts highlighted the need for comprehensive governance strategies in the event of a breach through these networks, including the use of response teams, data security, and backups, along with the need for "*a full governance model from notification of a breach to first responder… (and) an escalation strategy from our IT team, governance and security team, through to our response team*" (E-3). Organisations were also advised to have both internal and external communication plans to issue in the event of an attack. These can be communicated appropriately to both team members and customers should the system need to go offline for any period while a solution is applied. The experts described how some large organisations also have dedicated security operation centers who review all possible breaches and "*if there is a breach of any kind, we immediately reach out to the relevant stakeholders*" (E-13). The team then revokes all access to the network that other employees might have. Furthermore, organisations should have data security policies that cover the event of breaches, where employees will immediately report "*the instance of a breach*" (E-4) and be well educated on what steps should be pursued thereafter. Organisations were advised to have cloud backups or replicas of the main systems to prevent data loss, with the ideal response strategy being able "*to have an exact replica of their systems that is totally isolated and decoupled from the production systems*" (E-8), as the attackers may still be operating within the network, infiltrating more data and infecting other machines resulting in everything needed to be shut down. This strategy aids the organization in shutting down existing machines which are running, allowing the response teams to perform analytics and investigate the nature of the attack: "*if its ransomware, it will spread and make the data breach worse*" (E-8).

4.2 Research Question 2

Similarly, the pandemic forced organisations to rely on RDP for business continuity, with the experts arguing that RDP can only be utilized by organisations if it is managed properly with certain controls. For instance, one expert advised organisations to "*limit RDP software solely to within the local area network (LAN)*" (E-14). Other experts described how they prevent employees downloading RDP software, and how organisations have RDP sites blocked from being accessible: "*we're able to block standard RDP ports from being used on the network*" (E-6). Any other use of RDP should not be permitted. Unfortunately, the consensus among experts was that RDP is suspect to unsecure and outdated technology: "*RDP is very, very weak for security. We don't do it, we can't do it, its forbidden*." (E-9), with one expert even going so far as to describe RDP as being "*a honeypot for attackers*" (E-8). The security risks were highlighted as being too great as the technology was described as easily penetrable and largely outdated. Experts stressed that organisations should not invest on securing RDP, but to

spend money replacing it with more modern solutions: "*The only discussion around RDP should be how to we replace the existing service so that we don't use RDP anymore*?" (E-8). For organisations that continue to use RDP however, several recommendations were presented by the experts, including the adoption of monitorization tools, VPNs, and encryption protocols. Additionally, organisations have also used VPN connections as a solution to mitigate RDPs vulnerabilities, although "*not for any work deemed valuable or confidential*" (E-12). While RDP has been widely documented by the experts as being a vulnerable technology and advocating against its use, organisations continue to use it internally necessitating response strategies due to high risk of attack. The experts described how secure cloud computing, employee use of RDP and quarantining of servers could play an important role in responding to threats of this nature. Experts recommended organisations to ensure adequate measures and response strategies are in place for after any attack, as "*RDP is a huge headache in terms of online security, and the vulnerabilities and issues that come with it*" (E-6). Many organisations the experts worked with either had RDP banned, or only allowed their IT teams to use the technology. Experts described this justification as the more technically qualified the employee, the quicker a data breach or infiltration over RDP can be discovered. The average employee will not be able to identify a breach, meaning infiltration goes unnoticed for longer, causing increasing levels of fallout: "*If you are getting an attack on RDP, that means the hackers are already in your network. To get to the RDP, you have to first breach the cloud network, but if that's secure enough, its prevented*" (E-1). An effective response strategy should also detail when a server should be "*quarantined*" (E-16) to provide extra protection when a server is infiltrated.

Authentication was also discussed as an important process to allow employees gain access to confidential and sensitive data, while dissuading malicious actors from breaching their networks. As organisations initially struggled with remote working protocols, the topic of IT security and governance policies were outlined by experts as having a huge influence on how authentication password policies were implemented across all devices. There are several layers of authentication that organisations need to follow, ranging from an employee's own workstation, to VPN and single sign on, with experts arguing that improvement is needed across all areas, including: "*devices should not be jailbroken, or rooted, devices should have a passcode, copy/paste is disabled, screenshot is disabled, devices should contact mobile device management every seven days, no VPN can be configured on personal devices...*" (E-17). Experts also advised organisations to adopt multi-level authentication, that should initially seek to "*authenticate the workstation via a certificate exchange between computer and VPN server. Next phase is your traditional username and password, followed by multifactor hardware or software tokens*" (E-12) which should consist of a "*password of alphanumeric values and authentication code from authenticator app*" (E-20). Experts recommended that all passwords should be changed every three months to add an extra layer of rigor. These steps can help provide a rigorous authentication policy to mitigate the possibility of cyber-attack or infiltration. Unfortunately, experts revealed that many organisations are using the same level of authentication policies they were using pre-pandemic. In those cases where infiltration does occur, a proactive response is required across several key areas with experts providing several examples of strategies: "*Firstly, disable the user account immediately. Secondly, close all user sessions. Thirdly, create a script so that service desk engineers can run it with a click of a button to perform all activities including password changes, then notify the organisation's security team*." (E-17). The experts argued that communicating updates to authentication software should be the last critical step to take: "*You don't have to go to Microsoft to download the latest updates for example, it is being pushed by corporate*" (E-9). This results in all technology being up to date with the latest security updates and patches, with organisation's information security officers communicating these protocols and response strategies with employees. Red team tests were also described as another way where organisations can test portals of systems, identifying what threats devices are exposed to: "*You can look at what devices are exposed to authenticate which have a certificate with the company name… You have to keep doing that scan at least two or three times a day on your public facing infrastructure to contain any inadvertent exposures*" (E-5). Experts outlined the necessity of being extremely aggressive in finding exposures before attackers do, because attackers are always looking.

4.3 Research Question 3

The experts agreed VPNs helped organisations during the initial seismic shift to remote working, scaling up their infrastructures to handle the large amounts of traffic passing through their system from employees working virtually, specifically through increasing VPN encryption and authentication. VPN connectivity must also be managed on a layered basis, which provides added security across three factors of authentication: "*We authenticate the machine, the user, and then we use a form of multi-factor as well on top of that. It would be incredibly difficult for someone to connect who does not have authorization*" (E-12). Every expert stressed how critical employee cybersecurity training is to their organization, with the use of VPN being a prominent factor in

that training: "*During the Covid-19 pandemic, we strengthened our VPN and were more vocal about when you should use it, and when you should not*" (E-15). Some organisations tested their employees four times a year on the evolving risks as part of a "*quarterly certification*" (E-3) ensuring that their employees knew how to use VPNs effectively. Company policies have been forced to make wholesale changes and are now being reviewed and updated annually. For example, organisations now have factored in "*audit requirements*" (E-12) as part of their annual training and policy reviews, with other organisations introducing a "*split tunnelling*" (E-17) VPN system that enables only office traffic to pass through a VPN and the public connection going through a user's internet connection. These controls help mitigate evolving cybersecurity issues and demonstrate how important it is for companies to regularly review their policies. While devices that use VPN connectivity can be breached, they are more secure than a network accessed without a VPN, with experts outlining several mechanisms with which to monitor VPN use, for example, monitoring any "*land-speed violations*" (E-5). This mechanism involves the monitoring of logins, identifying the geographical location on where access points are coming from, and if the user is coming from various countries in a manner of minutes. All "*anomalous activity*" is immediately investigated by the security team to ensure there are no compromises on the network. Layering the infrastructure allows for more concise response strategies after identifying a breach, depending on what environment may have been accessed by external actors, for example whether access was gained to "*the development environment, or the operations environment etc…*" (E-10). Once the breach is isolated, forensic diagnostics can be subsequently implemented to measure the impact. These response strategies center around continuous monitoring and investigating to counter the risks associated with data breaches.

Experts also described phishing attacks as being the most prevalent form of cyberattack since the pandemic began and after organisations transitioned to remote working. Given their constantly evolving nature, experts highlighted the importance of training, monitoring, management, and decoy methods to combat this issue. Some organisations aimed to provide this training on a quarterly basis, but at the outset of the pandemic they "*were doing it nearly weekly, as phishing is the most prevalent type of attack to the employee base*" (E-14), with other experts claiming that "*You can never do enough education in this space*" (E-15). Several experts described how these organisations manage the risk of phishing by performing regular tests on their employees: "*We do phishing campaigns at least once a quarter*" (E-15), whereby they send out fake phishing emails to their employees, and receive a report on who clicked into the mail: "*Our team sends everyone a link, and tell them* "You all need new computers, please go on this link and choose which one you want." *A lot of people click through because they think it's from someone they know, which it is, but the link is often dangerous*" (E-7). The employees that accessed the content would then receive links to more education on phishing. Organisations are also increasing their reliance on anti-phishing software to survey all inbound emails, with some software packages with built-in functionality to identify phishing attempts, capable of catching "*millions of phishing items every day*" (E-15), however, the more sophisticated the attack, the more likely it might slip through the filtering technology. Larger organisations were described as having the ability to dedicate entire teams during the Covid-19 pandemic to make monitoring and management of phishing their full-time job due to the surge of attacks. Communication was identified as a vital component to any occurrence of phishing, identifying possible and real issues and making their stakeholders aware of any phishing campaigns. Reporting any suspicious activity by employees also aids organisations: "*We have a phishing button on our email clients that enables people to report back into security and say something isn't right, can we investigate*" (E-14). This type of reporting means that phishing emails that successfully slip through email-filters can be quickly dealt with. If a phishing email is clicked on by an employee, the experts described how organisations have protocols in place to track back and identify the impact path. While some operating procedures can vary, it is critical at minimum to contact the employee immediately, assess what was clicked on and if anything was shared, reset passwords, and shut down all active sessions of the user.

5. Discussion and Conclusions

Our study distinguishes itself from prior cybersecurity research in terms of literature selection criteria, research focus, and research output. This study identifies several approaches on how to mitigate cyber-attacks in these areas to maintain an optimal remote working environment. Firstly, from a management perspective, these findings reveal several regulatory and training recommendations that should be implemented within the technical architecture of an organization, for example, effective use of data policies and encryption methods should be developed to ensure cyber safety of employees working on their private networks. Additionally, security protocols should be enforced on users such as setting up router passwords, hiding Service Set Identifiers (SSID), keeping the system firewall updated, using efficient antivirus software and other protective tools like IP address filtering along with whitelisting of IPs to prevent involuntary/voluntary access to malicious websites.

The findings also highlight the emphasis that should be placed on utilising VPN, whether on private or public networks to have an additional layer of security. For public networks specifically, training must be provided on safe usage and to develop a zero-trust approach. Secondly, from a technical perspective, RDP was unanimously identified as a technology that needs to be replaced due to the inherent security vulnerabilities, and to ensure multi-factor authentication is adopted as a basic requirement. While RDP is still in use in many organisations, companies are now migrating to more reliable technologies like VPN and Citrix to deliver secure remote working environments. The findings also highlight how MFA security strengthens the encryption architecture irrespective of what the primary layer of encryption is, which could differ across companies. The primary form of encryption however should not be stagnant, as expressed by experts and proven methods that passwords/access policies need constant updating to stay ahead of potentially malicious actors. Thirdly, from the human perspective, this can be viewed as one of the most prominent causes of breaches irrespective of the security measures implemented. Blindly trusting that employees will do the right thing can lead to catastrophic consequences. To that end, technology and employee training needs to be coupled together to maximize security efficiency. With the surge of VPN usage due to the sudden shift to remote working, organisations have had to significantly increase their infrastructure capacities to ensure a smooth and secure transition, however, this should not come at the expense of security, as there has to be extensive work put into the VPN client in the first place before it is distributed to the employees. Similarly, phishing emerged as a significant human threat level event, that could bypass all security measures in place and cause havoc to an organisation. The findings recommend developing a combination of phishing filtering technology and employee awareness training to avoid successful phishing attacks, in addition to frequent tests and monitoring systems. The findings presented herein should be considered as a roadmap with which the organisation can use to develop efficient mitigation strategies for remote working threats. Indeed, even providing visibility over these areas allows organisations to critically analyse their needs and capabilities to further refine existing security policies. These findings reveal key insights to develop new mitigation strategies, technologies and flexible solutions for remote working, and methods to facilitate optimal stakeholder engagement in their delivery that aligns with business needs. While we endeavoured to achieve the highest levels of rigour and accuracy, as is true of any research this study has several limitations, which can be addressed by future research. One limitation is the fact that only six technologies were included in the risk categorisation, based on relevance and priority, from the wide array of technologies that are an aspect of the remote working environment. Topics that have not been studied may become more of a priority later on as the current environment evolves; leaving a gap to build on our current findings. In addition to advancing our understanding of cybersecurity practices within organisations, this investigation can also inform policy makers of the possible determinants and outcomes of these specific cybersecurity incidents. In doing so, it may also have important implications for improving the discussion of cybersecurity activities in financial disclosures, and effective communication of such information with relevant stakeholders. We are still at an early stage of this transformation however, which presents future investigations with an exciting research area.

References

ALABDAN, R. 2020. Phishing attacks survey: types, vectors, and technical approaches. *Future Internet,* 12**,** 168.

ANGWIN, J. 2014. Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance: Chapter 1: Hacked. *Colo. Tech. LJ,* 12**,** 291.

BLANCH. 2018. *Five issues facing secure remote access to IIoT machines* [Online]. Machine Design. Available: https://www.machinedesign.com/automation-iiot/article/21836802/five-issues-facing-secure-remote-access-to-iiot-machines [Accessed 21/10/2021].

BLOOM, N. 2014. To raise productivity, let more employees work from home. *Harvard Business Review, January–February*.

BORKOVICH, D. J. & SKOVIRA, R. J. 2020. Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems,* 21..

BURKE, S. 2020. *Coronavirus Is Creating A Global 'Work-At-Home' Culture* [Online]. CRN. Available: https://www.crn.com/news/cloud/coronavirus-is-creating-a-global-work-at-home-culture [Accessed 15/11/21].

CHANNABASAVA, H. & KANTHIMATHI, S. Dynamic Password Protocol for User Authentication. Intelligent Computing-Proceedings of the Computing Conference, 2019. Springer, 597-611.

DHILLON, B. & LIU, Y. 2006. Human error in maintenance: a review. *Journal of quality in maintenance engineering*.

EISENHARDT, K. M. & GRAEBNER, M. E. 2007. Theory building from cases: opportunities and challenges. *Academy of Management Review,* 50**,** 25-32.

FURNELL, S., HANEY, J. & THEOFANOS, M. 2021. Pandemic Parallels: What Can Cybersecurity Learn From COVID-19? *Computer,* 54**,** 68-72.

GARTHWAITE, P. H., KADANE, J. B. & O'HAGAN, A. 2005. Statistical methods for eliciting probability distributions. *Journal of the American Statistical Association,* 100**,** 680-701.

GIOIA, D. A., CORLEY, K. G. & HAMILTON, A. L. 2013. Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods,* 16**,** 15-31.

GOLDSBOROUGH, R. 2015. Staying Safe When Using Wi-Fi. *Teacher Librarian,* 42**,** 65.

GREGOR, S. 2006. The Nature of Theory in Information Systems. *MIS Quarterly,* 30**,** 611 - 642

GUPTA, B. B., ARACHCHILAGE, N. A. & PSANNIS, K. E. 2018. Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems,* 67**,** 247-267.

IBM. 2019. *Cost of a data breach study: Global overview* [Online]. Available: https://www.ibm.com/downloads/cas/ZBZLY7KL [Accessed].

ITU. 2008. *Definition of cybersecurity referring to ITU-T X.1205, overview of cybersecurity* [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed 13/10/2021].

MALECKI, F. 2020. Overcoming the security risks of remote working. *Computer Fraud & Security,* 2020**,** 10-12.

MARSHALL, B., CARDON, P., PODDAR, A. & FONTENOT, R. 2013. Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. *Journal of computer information systems,* 54**,** 11-22.

O'HAGAN, A., BUCK, C. E., DANESHKHAH, A., EISER, J. R., GARTHWAITE, P. H., JENKINSON, D. J., OAKLEY, J. E. & RAKOW, T. 2006. *Uncertain judgements: eliciting experts' probabilities*, John Wiley & Sons.

RAMADAN, R. A., ABOSHOSHA, B. W., ALSHUDUKHI, J. S., ALZAHRANI, A. J., EL-SAYED, A. & DESSOUKY, M. M. 2021. Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation,* 2021.

SEAWRIGHT, J. & GERRING, J. 2008. Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly,* 61**,** 294-308.

SECURITY. 2020. *Half of organisations experienced security incidents while working remotely* [Online]. Security Magazine. Available: https://www.securitymagazine.com/articles/93505-half-of-organizations-experienced-security-incidents-while-working-remotely [Accessed 15/11/2021].

SHI, F. 2020. Surge in security concerns due to remote working during COVID-19 crisis. Barracuda.

STOBERT, E. & BIDDLE, R. The password life cycle: user behaviour in managing passwords. 10th Symposium On Usable Privacy and Security ({SOUPS} 2014), 2014. 243-255.

SUTTON, R. I. & STRAW, B. M. 1995. What theory is not. *Administrative Science Quarterly,* 40**,** 371-384.

TRAN, C. 2020. Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. *arXiv: 2006.11929 v1*.

WALLACE, S., GREEN, K., JOHNSON, C., COOPER, J. & GILSTRAP, C. 2021. An Extended TOE Framework for Cybersecurity Adoption Decisions. *Communications of the Association for Information Systems,* 47**,** 51.

WANG, Z. & RUAN, Q. 2020. Research on network security subsystem based on digital signal. *Journal of Intelligent & Fuzzy Systems,* 38**,** 97-103.

WILSON, K. J. 2017. An investigation of dependence in expert judgement studies with multiple experts. *International Journal of Forecasting,* 33**,** 325-336.

YIN, R. 2008. *Case Study Research: Design and Methods 4th Edition*, London: Sage Publisher.

ZAFFT, A. & AGU, E. Malicious Wi-Fi networks: A first look. 37th Annual IEEE Conference on Local Computer Networks-Workshops, 2012. IEEE, 1038-1043.