

AN EXPLORATORY STUDY OF CYBERSECURITY IN WORKING FROM HOME: PROBLEM OR ENABLER?

*Mary Bispham, Sadie Creese, William H. Dutton, Patricia
Esteve-González, and Michael Goldsmith*

ABSTRACT

This article explores the implications of a shift to working from home (WFH) in the context of the COVID-19 pandemic. The literature and news coverage of this topic focuses on rising concerns over cybersecurity. Based on in-depth exploratory interviews with cybersecurity experts, it is apparent that cybersecurity problems do arise, but the advances in cybersecurity have enabled this shift and the scaling up of WFH. This qualitative research suggests the need for survey research and selected case studies to gain a more empirically anchored perspective on the degree that cybersecurity has raised problems but also enabled WFH.

Keywords: working from home, cybersecurity, COVID-19 pandemic, Internet, remote work

Mary Bispham: Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School and Department of Computer Science, University of Oxford, Oxford, United Kingdom

Sadie Creese: Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School and Department of Computer Science, University of Oxford, Oxford, United Kingdom

William H. Dutton: Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School and Department of Computer Science, University of Oxford, Oxford, United Kingdom

Patricia Esteve-González: Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School and Department of Computer Science, University of Oxford, Oxford, United Kingdom

Michael Goldsmith: Global Cyber Security Capacity Centre (GCSCC), Oxford Martin School and Department of Computer Science, University of Oxford, Oxford, United Kingdom

<https://doi.org/10.5325/jinfopoli.12.2022.0010>



JOURNAL OF INFORMATION POLICY, Volume 12, 2022

This work is licensed under Creative Commons Attribution CC-BY-NC-ND

The potential for working from home (WFH), remotely, or on the move—telework—is not new.¹ However, while research on this topic waned, the phenomenon of remote working has been rising in prominence, particularly in the wake of the COVID-19 pandemic. Especially in the more developed economies, the pandemic accelerated WFH as social distancing and lockdowns prevented normal travel to offices and away from home.

This shift led us to focus on the potential of new or elevated cybersecurity problems being driven by WFH. We consider this question primarily from the perspective of the cybersecurity of employer organizations. WFH may exacerbate organizational cybersecurity problems in various respects, such as through increased risk to the confidentiality of organizational data accessed or stored outside the organization's internal network, or through a reduction of employees' access to IT support.

This article provides an overview of the cybersecurity issues tied to shifts to working remotely and particularly from households. We then describe the exploratory approach of this study, which is based on qualitative in-depth interviews. This is followed by a brief review of the literature. Our review covers literature on both the technical and human factors that have been related to cybersecurity in WFH. Thereafter, we discuss interviews with experts in cybersecurity who have experience in managing issues tied to WFH. The findings from our interviews suggest that while many organizations did experience an increase in particular types of cybersecurity threats because of the move to large-scale WFH during the pandemic, the relationship between cybersecurity and WFH is complex and inconsistent across different sectors. The interviews supported the potential for WFH to have exacerbated organizational vulnerability to various cybersecurity challenges, including phishing, ransomware, and unauthorized access to confidential data. Interviews identified a complex set of possible drivers for this increased vulnerability, including the use of personal devices for organizational purposes, insecure home infrastructures, insecure implementation of remote access technologies, as well as social isolation and lack of IT support for employees WFH. However, those interviewed also identified cybersecurity measures that were designed to support remote working and WFH well before the pandemic. These measures were possible to scale up

We thank Alistair Fenemore, Graham Ingram, Richard Starnes, and our anonymous expert interviewees for their input to this study. An earlier version of this article was presented at the Policy Research Conference on Communications, Information, and the Internet (TPRC49), September 22–24, 2021. We thank Carolin Weisser Harris and several anonymous TPRC reviewers for their comments on earlier drafts.

1. Nilles et al.; Short et al.

to enable a smoother transition to WFH for more individuals during the pandemic than might otherwise have been possible. The conclusion of this article discusses the case for further research on the issues identified in this study.

Cybersecurity and the Rise of WFH

Cybersecurity has addressed remote and distributed systems since before the inception of shared and Cloud computing. However, recent COVID-19 experiences have focused on the risks of distributed computing for the security of institutions—from business to healthcare and educational institutions. Rapid moves toward increased working and learning from home across many organizations have dramatically changed the scale and pace of this phenomenon. Examples abound, such as with central business districts having emptied in many major cities, such as London, as commuters have stayed at home to work. Also, the campuses of many universities have been repurposed to support remote learning with teachers and students working from dormitories or their homes.

Despite variations across nations, Figure 1 shows how the percentage of employed people WFH increased since 2019 in the 27 European Union (EU) member states, relative to 8 non-EU nations in the European region. This comparative difference might reflect a difference in capacity for those in different occupations to work from home depends on the education and skills of workers in a country, the type of jobs drawn by its economic activity, the possibility of performing all the tasks of such jobs at home, and, if any of such tasks require an Internet connection, the availability of access to the Internet at home.² In fact, the feasibility of WFH is likely to be heavily dependent on Internet access.³ While shifts in WFH are associated with the erosion of boundaries of private and public institutional networks in households, the use of remote work centers, and work on mobile devices, the question remains: Are those moving into WFH facing more cybersecurity issues?⁴

2. Garrote Sanchez et al.; Dingel and Neiman.

3. Garrote Sanchez et al.

4. There is data on the percentage of individuals who experienced cybersecurity-related incidents in 2019 for the same countries as the ones mentioned in Figure 1 except Romania (Eurostat, "ICT Usage in Households and by Individuals"). However, the same data for 2020 are not available yet, and we do not know whether the recent explosion in WFH was mirrored in proportionate increases of cybersecurity-related incidents in those countries.

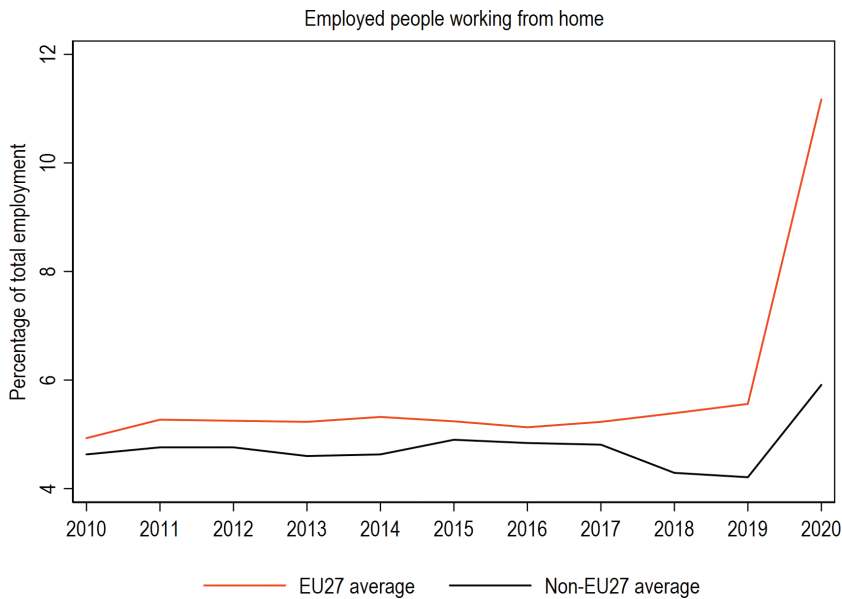


FIGURE 1 Employed people WFH as a percentage of total employment.⁵

Cybersecurity experts focus on the changing nature of threats and vulnerability when considering whether institutions have the right risk controls in place for the security of their assets and business operations. For example, changing the use of technology, the Internet, and other approaches to distributed computing can increase the number of vulnerabilities that malicious actors may exploit—what security experts have called an expansion of the attack surface.

But external factors (as well as technological infrastructures) can cause circumstances to quickly change the way individuals use networks, as in the case of the pandemic shifting more work into households and mobile access. In such circumstances, attack surfaces can change in nonincremental ways, not only by providing new ways to attack but also by making new assets reachable and thereby increasing the interest of threat actors. This shift could make the likelihood of attacks increase, as well as the potential losses or harm. Is the increasing dependence on technology that occurred

5. Eurostat, "Employment LFS Series." This sample has 27 EU member states (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden) and 8 additional neighbor countries (Iceland, Montenegro, North Macedonia, Norway, Serbia, Switzerland, Turkey, and the United Kingdom).

during the COVID-19 pandemic an example of this? Is there growing evidence of a rise in malicious attacks during this period?

Cybersecurity needs to evolve rapidly to cope with new needs brought about by such change. These challenges are already being faced by businesses seeking to enable WFH, and by universities enabling faculty to teach and meet students remotely, as just two of many examples. However, lessons learned from experiences like “zoom-bombing” show that, despite advances in cybersecurity technologies, it is not necessarily the case that institutions are sufficiently prepared or that Internet users have developed an effective “cybersecurity mindset” that would ensure they are able to know how to anticipate and avoid risks in such situations.⁶ Most early research suggested that cybersecurity problems tied to WFH are growing.⁷

We, therefore, sought to explore what cybersecurity problems are emerging and what capacities are critical to support this rapid move to more distributed mobile, remote, and work-at-home options in the face of COVID-19. This research should help inform more representative surveys across multiple stakeholders, from individuals WFH to public and private organizations who employ them to be resilient when faced with future events, which may result in equally fast-paced changes in how we use technology and the Internet.

Approach and Methods

In line with the uncertainties surrounding cybersecurity in WFH, our initial focus was on a meta-analysis of the research literature (published articles, academic studies, security specialist reports, etc.) reporting on the issues and responses. Our initial efforts focused on summarizing the key cybersecurity problems and capacities identified to determine whether there are any capacity needs that are not being met.

However, while we found many speculative forecasts of the problems likely to arise, we concluded that there was not yet a significant body of systematic empirical research on this topic. While the Internet and computing have supported some level of WHF and distance education for decades, there has been surprisingly little research on cybersecurity issues in these areas. Moreover, much of the early research has been undertaken

6. Dutton.

7. Ponemon; Tanium.

by the cybersecurity industry, which does not openly share the full detail of much of its data and findings. We concluded that there was a need for more independent research on the actual experiences of users and organizations during and in the aftermath of the pandemic.

Given that the existing literature is dominated by forecasts versus actual empirical studies, we undertook in-depth interviews to provide an exploratory qualitative understanding of the problems, before collecting more systematic survey-based evidence. These in-depth interviews were focused on those in the cybersecurity industry and those staff in organizations supporting individuals WFH. We asked them about their role and responsibilities and any cybersecurity issues arising from individuals WFH (Appendix). The interviews probed for the kinds of attacks and vulnerabilities addressed. The questions enabled us to gain a sense of respondents' views on trends in cybersecurity in WFH.

Six in-depth interviews with cybersecurity professionals were conducted in February and March 2021. All the interviewees were in senior positions and had years of experience working in the cybersecurity industry. Throughout this article, we reference the interviewees by their respective numbers [1–6] to maintain the confidentiality of their contributions. Also, the interviewees were asked to review an earlier draft of this article and provide their feedback. Two of the interviewees [2, 3] were overseeing information security in universities, whereas the other four interviewees were working in industry: one was in a consulting firm [1], one in a communications company [6], and two in threat intelligence [4, 5]. All of the interviewees were male and based in the United States or the United Kingdom.

Review of the Literature

Given that the changing context shaped by the COVID-19 pandemic was a primary motivation for this work, literature was reviewed on distributed cybersecurity in the context of both the COVID-19 context and prior to the pandemic. To identify academic literature on distributed cybersecurity in the context of the COVID-19 pandemic, a Google Scholar search for the keywords “cybersecurity, remote working, and COVID-19” was conducted. A second search for the same keywords and adding the keyword “resilience” was also conducted. The searches were limited to resources published in 2020. The first 100 of over 15,000 Google Scholar search results were reviewed. In addition to the search of the academic literature,

the review also included some prominent technical blog articles, consultancy firm reports, and government briefings.

To identify academic literature on distributed cybersecurity from the prepandemic era, a Google Scholar search for the keywords “cybersecurity remote working” was conducted that covered the years 1980–2019. The first 30 of nearly 1,000 search results were reviewed. In addition to the search for academic literature, some technical articles on Google’s “BeyondCorp” system for distributed cybersecurity were reviewed. Table 1 summarizes the academic literature reviewed in this section.

One of the most general observations from this literature search was the dramatic rise in the number of academic works published since 2019—orders of magnitude more research and analysis of cybersecurity in the context of remote working. This underscored the developing wisdom that the shift to WFH in response to the pandemic would be associated with greater problems with cybersecurity. Nevertheless, the limits of research in this area before 2020 are surprising since increased levels of remote working have been anticipated for decades.⁸

Cybersecurity in WFH Predating the Pandemic

Despite the uptake in studies of cybersecurity during the pandemic, the literature reviewed indicated that the kinds of attacks being reported during the pandemic were not new or limited to the COVID-19 pandemic (Table 1). Based on the samples reviewed, many of the cybersecurity issues were a focus before the pandemic. These included work on phishing attacks, the security of networks, remote access technologies, externally hosted software, and the vulnerabilities associated with Bring Your Own Devices (BYOD) and insider threats.⁹ Increases in phishing attacks have been regularly observed in relation to other types of disasters and notable events before COVID-19.¹⁰ Attacks linked to remote working, such as attacks on the Remote Desktop Services (RDP) protocol, were also prevalent before the pandemic, albeit on a smaller scale.¹¹

8. Nilles et al.; Venkatesh and Vitalari.

9. For example, Williams et al. identified a link between BYOD practices and increased risk of insider threats.

10. Lallie et al.

11. Faulds and Raju report data indicating that only 10% of workers were working remotely on a full-time basis before the pandemic, with a further 20% WFH on a part-time or occasional basis.

TABLE I Cybersecurity Issues Identified on WFH or Remotely in the Literature Reviewed

Cybersecurity Issues	Predating the Pandemic	During the Pandemic
Phishing attacks	Lallie et al. (2021)	Ahmad (2020) Lallie et al. (2021) Nicol (2020)
DDoS attack		Nicol (2020)
Ransomware attacks		Ahmad (2020)
Security of networks	Awan et al. (2016) Baker (2020) Peck et al. (2017) Dowling (2012) Osborn et al. (2016) Ward and Beyer (2014)	Ahmad (2020) Nicol (2020) Weil and Murugesan (2020)
Remote access technology	Lallie et al. (2021)	Lallie et al. (2021)
Externally hosted software	Awan et al. (2016)	
Open Wi-Fi		Weil and Murugesan (2020)
Vulnerabilities associated with BYOD	Williams et al. (2019)	Weil and Murugesan (2020)
Insider threat	Chapman (2020) Williams et al. (2019)	Chapman (2020)
Workers circumventing security controls		Nicol (2020)
Security management	Blythe (2013)	Dwivedi et al. (2020)
Vulnerabilities in videoconferencing platforms		Hakak et al. (2020) Okerefor and Manny (2020) Weil and Murugesan (2020)
Exposure of login credentials and confidential information		Ahmad (2020)
Sudden shift to work from home or remotely in a large scale		Nicol (2020)
Vulnerabilities in drone operations		Chamola et al. (2020)

A few areas relevant to the cybersecurity of WFH received more attention before the pandemic, such as the security of networks, which has been a major question since the early days of the Internet, though less so

as the Internet became more trusted for business and commerce (Table 1). Externally hosted software was a focus for research in earlier years when this represented a shift from in-house software. For example, more research identified the opening of Internet-facing ports and externally hosted software, such as Sharepoint, on personal devices as “hotspots” of cyber risk in the context of a university network.¹² More recent developments, such as Cloud computing have eased concerns over externally hosted software. Insider threat associated with remote working was also a known issue before the pandemic. One article, though focusing primarily on insider threats as a consequence of remote working during the COVID-19 era, cited an earlier survey from 2018 claiming that 32% of organizations “had experienced a cyber-attack as a direct result of an employee working outside of the business’ security perimeter.”¹³

In a review of cybersecurity in the workplace, Blythe refers tangentially to issues associated with remote working, stating that they “provide challenging issues for workplaces to manage security.” One effort focusing on the security of remote working in the prepandemic era is the BeyondCorp architecture—updated to BeyondProd—that eschews perimeter-based approaches to security to enable Google employees to work securely from external networks, without requiring the use of a Virtual Private Network (VPN).¹⁴ Such initiatives have contributed to a decline of research since 2019 focused on managing security within the organization’s security perimeter.

Analogous to COVID-19, incidents forcing work from home and remotely have been occasions for more research on cybersecurity risks. For instance, Dowling reflected on the security of networks in the context of a temporary shift to remote working by London-based workers during the London 2012 Olympics but does not consider the issue more broadly.

12. Awan et al.

13. Chapman discusses insider threats linked to remote working from an industry perspective.

14. A Virtual Private Network (VPN) enables users to connect more securely over the public Internet. Instead of connecting to a destination directly, a VPN allows users to connect indirectly via an encrypted connection to a VPN server, which makes users’ personal devices less externally visible. A VPN may be used to connect to public websites, via a commercial VPN provider, as well as to private company intranets, via a custom corporate VPN; Peck et al.; Osborn et al.; Ward and Beyer; Baker.

Cybersecurity in WFH during the Pandemic

As noted earlier, there has been a rapid increase in the proportionality of research on cybersecurity related to shifts toward remote WFH. This has been attributed in part to vulnerabilities created by increased levels of remote working.¹⁵ A survey of 1,002 respondents conducted in March and April 2020 estimated that 91% of executives believed that cyberattacks on their organization increased because of remote working during the pandemic.¹⁶ Eighty-five percent believed that their own organization was not adequately prepared to deal with a sudden shift to WFH.¹⁷

In addition, some areas of security risks have been more directly attributed to the context created by COVID-19. For example, cyberattacks reported during the COVID-19 pandemic were mainly about phishing attacks seeking to exploit uncertainty surrounding responses to the pandemic.¹⁸ Lallie et al. cite reports of a 600% increase in phishing as a consequence of the pandemic in March 2020. In their UK-specific case study, they show links between the timing of specific attacks and government announcements concerning the pandemic. Phishing attacks and attacks linked to vulnerabilities associated with remote working are on the face of it separate issues; however, it is possible that vulnerability to phishing attacks may be even higher in the context of remote working, due to the additional factors of social isolation and more limited access to IT support. Likewise, reports in the United States about phishing attacks on hospitals in the midst of the pandemic have raised alarms about this as a rapidly growing and serious problem.¹⁹

Regarding vulnerabilities linked to remote working, attacks targeting remote access technology, such as Microsoft's RDP protocol,²⁰ are also reported to have increased dramatically as a consequence of the shift to remote working during the pandemic.²¹ Successful attacks on remote access

15. See Dwivedi et al.

16. VMware Carbon Black.

17. See Bannister; VMware Carbon Black.

18. Lallie et al.

19. CISA.

20. Remote Desktop Services (RDP) is a protocol for Internet users to remotely log onto Windows boxes. This is a feature of the Windows operating system for computers that gives a user remote desktop access to the Windows software on a computer. Given their purpose in providing easier remote access to a computer's software, it is not surprising that these services have had a history of introducing security risks.

21. See, for example, Leyden.

technology can be used, for example, to launch ransomware attacks in which a victimized organization's data are encrypted by attackers demanding payment for its decryption.

There are also areas of security research that seem to have developed since 2019—new problems. The general shift to WFH has been identified as a risk (Table 1), as well as vulnerabilities of videoconferencing platforms, such as “Zoom-bombing.”²² Zoom-bombing is not always treated as a cybersecurity issue, but a sizeable number of publications have, as these platforms allow those attending a meeting to share their screens, so a malicious user could “bomb” a meeting, such as by sharing vulgar images or listening in on a private meeting.²³ That said, the dramatic rise in videoconferencing and teaching led to clear examples of Zoom-bombing and a wave of press coverage that might have exaggerated the security issues, despite the real problems that users needed to address.²⁴ However, it was an easily managed threat addressed by more control over screen-sharing rights by the moderator of the meeting.

There are also some areas of cybersecurity and WFH that reflect the diffusion of new technologies more than the shift in working places or the COVID-19 pandemic. For instance, risks have been identified with the increased use of drone delivery services, triggered by new technology and the pandemic, and the associated risk of exploitation of vulnerabilities in drone operations, such as GPS jamming.²⁵

Notwithstanding the research noted earlier, it is likely that the harms and responses resulting from increases in attacks and vulnerabilities have yet to be fully realized and reported. The review demonstrated that publications on distributed cybersecurity during the pandemic consisted primarily of speculative academic work,²⁶ some research by the security

22. Hakak et al.

23. Okereafor and Manny discuss further cybersecurity issues associated with videoconferencing, such as man-in-the-middle attacks to listen in on a private meeting.

24. Issues surrounding Zoom-bombing were discussed here: <https://www.ox.ac.uk/news/science-blog/fbi-follows-oxford-academics-guide-beat-zoom-bombers>.

25. Chamola et al.

26. For example, Ahmad speculated, based on third-party sources, that cybercrime damage could double during the pandemic due to increases in phishing attacks as well as ransomware attacks, insecure remote access to corporate networks, remote workers exposing login credentials, and exposure of confidential information to other people in the home of remote workers.

industry, which is often linked to their products or services, and practical recommendations from industry and government.²⁷

One speculative academic contribution claims, based on industry observations, that information services across the world have coped well with the challenge of the COVID-19 crisis, despite identifying a number of vulnerabilities connected to remote working necessitated by the COVID-19 pandemic, including Zoom-bombing, vulnerabilities associated with BYOD, unpatched routers, and open Wi-Fi not protected by strong passwords.²⁸ Nevertheless, as the exploratory interviews described in the next section suggest, the best approaches to security are unsettled and evolving.

Exploratory Interviews

The open-ended, semistructured interviews with experts and practitioners supporting the cybersecurity of Internet users WFH reinforced some issues raised in the literature but also led to a more fundamental reframing of the issue—focusing more attention on how cybersecurity capacities in the household have actually enabled more WFH.

Cybersecurity Problems Tied to WFH

Interviews suggested that it is difficult to confidently discern the degree that WFH can be seen separately from other trends shaping cybersecurity. One interviewee emphasized another complexity that success rates of attacks were more difficult to track than the criminal activity itself. This is “modern crime” [5]. The proportion of bank robberies has decreased, but

27. Nicol also speculates on the cybersecurity consequences of the COVID-19 pandemic, based on the perspective of a university staff member in the United States. The article states that the sudden shift to remote working as a consequence of the pandemic will test the scalability of computing at the “edge.” The article cites interesting but anecdotal evidence that parts of the cybersecurity architecture, such as commercial VPNs are failing to deal adequately with the increased load. The article further speculates on a likely increase in vulnerability to phishing and DDoS attacks as a consequence of the shift to remote working, as well as an increased vulnerability due to the propensity of remote workers circumventing security controls if these are impeding the efficiency of their work. A DDoS attack is one in which malicious actors seek to undermine the availability of a system by flooding it with large volumes of nonlegitimate traffic from multiple sources.

28. Weil and Murugesan.

the prevalence of cyberattacks has increased [5]. The interviewee said that the current challenge in cybersecurity was “no longer ‘the guy with the hoodie’ but from organized crime and nation states. These are the challenges we face—the world we are living in” [5].

Increasing the Number of Cyber-Attacks?

One interviewee, a university information security officer, described a “concerted campaign” of cyberattacks against his university, which began before the COVID-19 pandemic reached the United Kingdom [2]. While these attacks were contained, they increased over time with many attacks appearing to take advantage of the COVID-19 theme and increased levels of remote working. However, given that attacks began to rise before the pandemic hit, the interviewee noted that the cause could not be attributed solely to the pandemic. In addition to WFH trends and the pandemic, the media notoriety of many faculty appeared to contribute by making some individuals more prominent and also facing higher workloads during the pandemic [2]. However, over time, the attacks became more “explicitly COVID-19 themed” [2].

A threat researcher in the industry [5] made a convincing case that users were more susceptible to cyberattacks in the combined context of WFH and the pandemic, illustrated by a proliferation of mobile apps purporting to provide COVID-19 information that were in fact stealing data from users. The interviewee said that users’ susceptibility was not necessarily linked to WFH as such, but that it was an ingredient “in that pot of” general disorientation during the pandemic. But a wide range of attacks has been seen during the pandemic, from hacking into corporate networks via RDP ports to consumer fraud and fraud targeting hospitals. It has been “for want of a better word, a s**t-show.” This has been “the best time to be a cybercriminal” [5].

However, a communications security expert at a large communications company had not seen a large increase in attacks [6]. He said that his company had already been “sort of enabled” for WFH before the pandemic, in terms of processes for remote working and the availability of company-owned devices. While his company had experienced some capacity issues with respect to the transition to WFH during the pandemic, they had not seen an increase in cyber incidents. There seemed to be significantly higher levels of attempted phishing attacks aimed at company employees using the COVID-19 theme, but he observed no increased susceptibility to phishing attacks [6].

Enabling Phishing Attacks?

One interviewee, working in threat research, said that from mid-March 2020, the situation had been “absolute bedlam,” with the widespread use of the COVID-19 theme as a phishing lure and in malicious content. He said that since mid-March his team had been tracking thousands of criminal campaigns and fraud scams, all leveraging COVID-19 and WFH in one way or another. The interviewee said that his team was the busiest it has ever been, citing the fact that they had been at the “high incident event” level defined by his company for major events and vulnerabilities, a level that would usually last only for a week or two, but continued since the early stages of lockdown. They had “never had so many problems” [5].

Multiple other interviews noted an increase in phishing attacks [1,4]. One interview within the security community cited a 600% increase in phishing attacks during the pandemic [1]. The interviewee attributed this spike—one of the “biggest” he has seen—to malicious users, primarily “cyber-criminals,” taking advantage of so many people being “exposed,” working “outside their corporate network” during the pandemic [1]. It also made phishing attacks easier to scale to more users since the world was facing the same problem with the pandemic and with similar concerns over their health and safety. In addition, technical advances, such as in AI, might allow malicious users to create more personalized phishing emails by gathering information on individuals. This would allow them to perform so-called “spear-phishing” attacks aimed at specific individuals but on a much larger scale.

Still another information security manager at another university saw no appreciable increase. He saw no evidence of increased susceptibility to phishing or vulnerability to other types of cyberattack as a consequence of remote working. The interviewee qualified this by stating that the IT security team would not necessarily have visibility of all the cyber incidents that may have occurred, but he had no sense that there was less reporting of incidents during the WFH period.

More Compromised Accounts?

Organizations have faced problems with email and accounts being compromised since the inception of the Internet. This was behind a long-term campaign to introduce stronger passwords and systems for regularly updating old passwords. However, weaknesses in existing processes have pushed organizations to multifactor authentication (MFA).

One university interviewee noted that his university experienced nearly a four-fold increase in the number of compromised accounts recorded, most of which occurred in the first six months of 2020. However, the increase started before the lockdown necessitated by the pandemic.

However, the information security manager of another major university noted that "... while a massive increase in account compromises was anticipated due to the move to remote working in the pandemic, this had not actually been seen in practice, yet" [3]. However, he noted that an increase in account compromises was anticipated, saying: "People click on links—that's what they do" [3]. Nevertheless, the number of problems were at about the same level with no uptick on any specific type of issue.

This interviewee was asked whether the apparent lack of an increase in compromised accounts might be due to incidents not being reported. The interviewee stated that this was possible in theory, but there was "enough coming through to give reasonable confidence" that users were still reporting incidents but at about the same level as they were before the pandemic [3]. The interviewee speculated that users may be more likely to report incidents affecting their personal devices than corporate ones, so he did not expect WFH to depress the propensity to report problems.

One compromised account at a major university had its alias changed to that of a top university officer and was then used to send an email out in the name of this official with a COVID-19 theme. It was identified as fake only because it referred to an incident "on campus," when the university was not a "campus-based" university. An industry security executive also discussed such issues as "CEO impersonation" attacks in the context of WFH—attacks involving, for example, a fake email to a head of accountancy in their CEO's name requesting a bank transfer. The link to the security effects of WFH is that in-person verification of email requests was no longer possible or was more difficult. Employees may be trained to verify email requests over the phone, but this is not a full or viable solution if it required sharing the home numbers of employees and managers.

Enabling More Ransomware Attacks?

Ransomware refers to software that can be maliciously installed on a computer or a network, such as by opening a link, that is designed to block access to critical data, such as by encrypting files, until a ransom is paid. Ransomware attacks have been increasing, based on our interviews with security industry executives [1, 4], and several notorious attacks

have brought this risk to the attention of a wider public.²⁹ In the United Kingdom, for example, serious ransomware attacks on two universities during 2020 alerted the sector to this potential.

At these two universities, ransomware attacks were executed via an open RDP port and subsequent privilege escalation. At one interviewee's university, this incident was used to emphasize the importance of minimizing the use of RDP and implementing VPN gateways. The message was: "That could have been us" [3].

An industry threat researcher focused on the use of the RDP, saying that major ransomware groups have leveraged the RDP protocol as an entry point. While in January 2020 there were around 1.5 million systems online that were publicly accessible by RDP, by March the volume had increased significantly to around 3–3.5 million, arguably due to a rush to maintain access during WFH in the pandemic. As he put it, this led to the back door—or even the front door—being left wide open. The interviewee said that unpatched VPN servers and unpatched Citrix systems had been a major entry point for cybercriminals, along with RDP servers with very easily guessable passwords.

Instead of simply increasing the frequency of ransomware attacks, the pandemic may have reshaped the bait used by the attackers. As one information security expert suggested, it was not so much that the number of phishing attacks had increased, but that their tone had changed to take advantage of the pandemic situation with COVID-19-themed "click bait."

There was a discussion regarding financial loss because of cyber incidents and possible accountability of budget holders. A key interviewee at a major university was not aware of any instances where the university had reimbursed individuals for financial loss because of phishing attacks. The issue of payment of ransom to attackers in ransomware attacks for recovery of data had been much debated, but the university had not yet had to face this issue in practice. The interviewee's own view was that ransom should not be paid to cybercriminals under any circumstances. If you did, you might as well put a "target on your back" [3].

29. <https://www.varonis.com/blog/ransomware-statistics-2021/>.

Drivers of Problems in WFH

Problems are driven by a multiple sets of institutions and stakeholders, not only the employee who is WFH. As this section illustrates, there are many incentives and problems that could exacerbate cybersecurity in WFH.

Incentivization and Tools of Malicious Actors

Supporting the Business Model Behind Cybercrime. There is a powerful economic incentive behind many cyberattacks, such as phishing attacks. In ways analogous to telemarketing, a malicious user only needs to be successful a few times to realize the significant financial gain. The financial success of organizations behind cyberattacks and phishing attacks, in particular, has contributed to cybercriminals putting more time, money, and thought into malicious email, while victims are likely to have put little or no thought into the possibility. The information security officer we interviewed noted, “there are better and better fakes, making it harder to spot fakes” [2].

A threat intelligence executive interviewed discussed a phone hijacking attack, adding that the risk of criminals involved in these types of attacks being investigated and caught is negligible and that the situation is similar with respect to ransomware and phishing attacks. Large numbers of phishing emails can be sent out at very low cost to the attacker. “10,000 phishing messages might yield 5 wins, which would be a success” [4]. This means that only a small percentage of these need to be successful to yield a return—creating “the perfect business model” [4].

Modularization of Cybercrime as a Commodity. In discussing susceptibility to deep fake attacks, a threat intelligence manager said that—like phishing attacks—these may have increased in WFH during the pandemic because of disruption and isolation. But also, he said that deep fakes had previously required a high level of technical competence, such as in audio engineering, but many of these techniques had now been commoditized. For example, there are tools available that enable attackers to easily create deep fakes without advanced technical knowledge. This is part of the general trend of “modularization” of cybercrime in the current era, with structures for sharing expertise and specializations in the cybercrime world. Tasks, such as malware development and deep fake creation can be “outsourced” by attackers, they do not need to be capable of making them themselves. This

has accelerated the rate of change in criminal activities—“the ecosystem is in place now” [4].

With respect to deep fakes, the interviewee said that video deep fakes, such as capable of impersonating individuals in videoconferencing calls, are likely to be possible within five years [4]. But another interviewee [5], whose company had a deep fake lab for developing methods for detecting deep fakes, said that while the threat from adversarial machine learning was going to increase over time, “why does an adversary need that when the password for a company is ‘welcome’.” Solutions to most security issues may be far more basic than the detection of deep fakes. “Imagine the film *Mission Impossible*...you don’t need Ethan Hawke when the front door is open, the alarm code is 1234—and everybody’s out” [5].

Limitations on the Knowledge and Awareness of Internet Users

A Lack of Awareness? Those who work from home often lack adequate awareness of cybersecurity risks. In part this is due to a lack of interest or priority placed on cybersecurity by users, but as one interviewee put it: “the level of user education required to ensure reliable phishing detection is currently unrealistic” [2]. The information security officer interviewee underscored this lack of basic understanding of security issues, providing an example of a user with a system “three versions old, which did not have up-dated security patches.” He said it worked fine. Many users don’t appreciate the risk unless they “experience them” [2].

Another interviewer noted that some rise in attendance in cybersecurity awareness programs had been observed with the shift to remote working, although levels of attendance were still not high. Awareness training had been moved from face-to-face to online. Levels have increased from two or three people in a training session to 20–25 [3].

However, another information security interviewee explained that a key problem with awareness raising is that it tends to be seen as overly reliant on fear, saying it tends to be “purely negative and fear-based” [2]. As he said, it is “a challenge to present cybersecurity as a benefit” [2] and provides easy steps to take.

Knowledge, Communication, and Training Deficits. One interviewee emphasized that ordinary employees who are WFH often have “insufficient knowledge to secure themselves” [1]. He argued that domestic IT infrastructures are not designed for WFH and that ordinary Internet users often do not have sufficient knowledge to secure their home environment [1].

As a security executive noted, in discussing the risks of poor firmware in many home routers, most users do not even know what firmware is, let alone how to flash the ROM (install a new read-only memory) on a home router.

Communication is another issue within organizations. Put simply, it is often difficult to reach everyone in an organization, even when they are in the office. Quickly reaching everyone when there is a cybersecurity risk or campaign is a problem for intraorganizational communication and is exacerbated when most are WFH [2]. An example was communicating with users when their account has been compromised, such as while WFH. They would need an alternative email address so they could be notified of the problem [2].

Unpredictable User Reactions to Security Interventions. Some security interventions for WFH could be counterproductive. One interviewee recounted the early attempts to identify and counter the so-called 419 advance fee routines or scams.³⁰ If a possible 419 scam was detected, it would be labeled as potentially dangerous communication. Unexpectedly, this labeling seemed to lead to an increase rather than a decrease in the success of these attacks!

The (Non)Use of Particular Technologies and Practices

Using Personal Devices for Institution-Based Communication and Information. As the literature also noted, several interviewees focused on a reliance on personal devices as one element of increased vulnerability linked to the increase in WFH [1, 2]. Personal devices represent another virtual move

30. Attempts to steal money by mail, fax, or any media, but is an increasingly online scam via email to Internet users. The letter or email convinces the receiver that they will realize a major financial benefit if they only give a small advance payment to help a person in need. The victim of the scam pays the advance to someone they've been led to trust in the expectation that they will in turn receive something of greater monetary value, but in the end, they receive little or nothing. It is called a 419 scam after a Nigerian legal code 419, which is infringed by such a scam. Early forms of this scam were so prominently tied to Nigeria that they came to be known as a "Nigerian scam" and then a 419 scam. It is also called an "advance fee fraud." While it may have originated in Nigeria, it has diffused worldwide. Analogous scams include the "Spanish Prisoner" scam, and the "black money" scam.

out of the normal office setting. Also, using the same device for work and home purposes presents a “risk of attacks, such as cross-site scripting” [2].³¹

At one major university, the pandemic spurred them to manage cybersecurity in early 2020, just when they had also begun a cloud migration project. They relied on cloud services, VPN access, and RDP, as noted by one interviewee: “When the pandemic struck, there were high levels of [a] perceived requirement for use of the RDP, due to access to some services being linked to a specific desktop machine. Some attempts to bypass VPN gateways for this purpose were seen” [3]. He noted that many staff still were “using their own devices at home, with software updates on these devices not managed by the university” [3].

Bring Your Own Devices. At one university, an interviewee noted that the institution provides laptop devices to administrative and academic staff if required for their work. Academic staff have the option of centrally managed, locally managed, or self-managed devices. Central management is possible for Windows and Mac devices only, Linux devices are either locally managed or self-managed [3].

At this same university, students are encouraged to use their own devices. In the current situation, some university devices have been purchased for use by students who do not have their own devices. Also, around 2,000 laptops were purchased for use by staff who had been using an office-based desktop before the pandemic if they were required to work from home and could not use their own device, for example, because they were sharing a device with a spouse also WFH.

New Security Protocols. Many organizations, including universities, have introduced new authentication procedures to reduce the number of accounts compromised such as by inadequate passwords. MFA has been one that was triggered in part by more WFH but also by industry-wide pressures, such as from auditing firms to strength authentication mechanisms. But MFA cannot protect users from many attacks, such as phishing. Moreover, the transition to MFA was not seen as a remedy for all. An interviewee stated that their university had not implemented MFA to

31. Cross-Site Scripting (XSS) is an attack in which the attacker can inject malicious code (usually JavaScript) into a legitimate website (see <https://portswigger.net/web-security/cross-site-scripting>). If a user clicks on a link to the compromised website, the malicious code will execute on the user's local system. XSS can be used, for example, to exfiltrate authentication tokens from a victim.

improve the security of user accounts due to the complexity of implementing this, such as with faculty traveling internationally, and an IT culture within their university that has been very resistant to change.

Another new possible technical fix is developing around what is called Domain Mark Authentication Reporting and Conformance (DMARC).³² This entails techniques analogous to the digital signing of internal emails [2]. If an external email presents itself as an internal email, it will be marked, helping the user to identify fake emails. Another approach was noted by a university information security manager, who noted the introduction of a banner indicating if an email came from an external email address [3]. However, since this is based on its claimed and not necessarily its actual origin, it is not a foolproof defense against phishing.

Another security expert but in a communications company confirmed that his company flags external email as an anti-phishing measure [6]. He said that identification of an email as external was based not only on the sender's purported address but that a variety of common practices were used before an email "lands in an inbox," such as inspecting attachments and checking the legitimacy of links.

Cloud Computing. The shift to Cloud computing was a focus of most interviews. At one university, the implementation of Microsoft365 cloud services was a focus in addressing WFH [3]. However, this university faced resistance to change in this move, as they did with a switch to MFA. At universities, much of the complexity of the implementation of cloud services is due to many edge cases. One example of an edge case was a department using an open-source legacy email client, and therefore being reluctant to change to Outlook365, to access Outlook on the Web (OWA), the browser interface to Exchange365.

The Introduction of New Applications and Services Those WFH have been introduced to some technologies that they have never used before [1], such as videoconferencing and meetings through such applications as

32. DMARC is a system for authenticating email to provide greater confidence in the identity of the sender. Work on these standards began in 2010 and it came into use around 2012. The rise of deceptive emails has contributed to their rising use. Its use is limited in that it requires senders and receivers to collaborate to ensure proper authentication, and many users will continue to work with unauthenticated emails rather than miss important messages. Organizations with regular internal and external email contacts are well-positioned to set this system up to assure recipients that the message is genuine. The use of DMARC is promoted by DMARC.org.

Zoom, Microsoft's Teams, Google Meet, Collaborate, Cisco's WebEx, LiveWebinar, and Skype. One university interviewee noted that in the early days of remote working, Zoom rapidly became a de facto communications tool, causing some security and privacy concerns [3]. The introduction of Zoom during the pandemic was a major innovation across many WFH in business and education, leading to some early teething problems, such as around Zoom-bombing.³³ As such innovations are new to most users they can pose problems until individuals learn how to use them safely, such as how to mute their audio or video when they wish, or not to allow others to share their screens during a meeting, unless specifically enabled by the meeting's chair.

Interviewees at two different UK universities noted the issue around Zoom-bombing, during the early days of the pandemic, which led the organization to promote Microsoft Teams, largely due to security as Teams was within the university's tenancy with Microsoft with cloud application security around it and aligned with their use of other Microsoft services [2, 3]. One threat intelligence manager noted the speed of this transition, saying that security personnel at Zoom had to suddenly "scramble" to improve the security of the tool itself, as well as of users' interactions with it, with users needing to realize their own responsibility to use the technology securely [4].

Altering Social Contexts, Resources, and Interactions

Isolation and Lack of Support Staff and Interpersonal Feedback. The shift to WFH undermined the normal routines and processes people were comfortable within the workplace. Their sense of the normal was "destabilized" with this move, which made them more vulnerable to phishing attacks, such as attacks "crafted to credibly appear as though they originated in the university" [2]. For example, "fake login pages" that might have appeared abnormal in the office, may not at home, such as if the user is on their own laptop at home rather than on the system they used in the office [2].

Many individuals working at home are isolated—alone and distanced from IT support staff available at the workplace. A military colloquialism of "distance from the flag" was used to underscore the greater vulnerability of those WFH as being similar to a soldier being stranded at an outpost distant from the protection of a major military base [1]. Even the presence of other people, not simply technical experts, can help avoid problems,

33. <https://billdutton.me/2020/03/26/zoom-bombing-the-future-of-education/>.

such as by enabling a person who receives a suspicious email to “compare notes” with a colleague “on an email they might suspect of being a phishing attack” [2]. You “cannot walk down the hall to speak with an IT support staff member,” or even “have someone to talk to, to put a hand on your shoulder” [2].

Another interviewee was not sure whether isolation and lack of in-person IT support in WFH had increased the susceptibility to phishing, but he said it was clear that the pandemic situation had generally increased susceptibility to fake information—“the ability to have your values questioned and—your position normalized has been impacted” [5]. However, the interviewee also noted that not all cyberattacks in the pandemic situation are human enabled. For instance, access via unsecured RDP ports and subsequent lateral movement using tools that are not flagged does not necessarily involve the manipulation of humans [5].

Realities of the Household. In most cases, the household has not been designed for WFH. It is the case that more households are moving toward designs that enable WFH, such as additions of a garden office or other home office space, and faster Internet connections, but the design of most households did not anticipate a massive shift to WFH or more hybrid working patterns.

Individuals WFH face many issues tied to the nature of households. One of our interviewees [5] noted as an aside that he is himself building a bespoke office on his own property for home working, due to too many distractions from family and home life in WFH. Those living in households with multiple family members including children can face security issues related to multiple users of some of the same infrastructures, such as routers and laptops. Steps taken to enhance the cybersecurity capacity of the household by one member can be undone by another, such as by distributing the password for a router.

One of our interviewees, a threat intelligence manager, thought that WFH during the pandemic had often forced employees to act insecurely, such as by connecting their work laptop to a home network also used by other family members, including teenagers [4]. He argued that some of the most insidious attacks he saw in recent years were attacks on home routers, which often have poor firmware [4]. He explained that malware infection on a home router renders even quality endpoint protection, such as antivirus software, useless.

Information Infrastructures of the Home

Limited or Poor Internet Access. Many reside in households within areas with remote or slow access to the Internet, which can lead to individuals creating “work arounds” [1], such as greater use of their mobile phones for office work. As one interviewee put it: “Too many people are stuck doing their job from an iPhone or using some insecure workarounds that compromise integrity and availability” [1]. At one of the large universities, staff experienced bandwidth issues in remote working, with someone led to using their neighbor’s Wi-Fi for obtaining better service [3]. But a business threat intelligence manager security also emphasized a big problem with the capacity of home connections in the move to WFH during the pandemic, especially if the same network is being used simultaneously by other family members, such as for homeschooling [4]. Another security executive argued that the lack of access can be viewed as a security issue, such as in the context of the Cybersecurity Triad model (CIA) of security covering the confidentiality, integrity, and availability of information systems and data [1], since a system would be insecure if its information resources were not confidential, genuine, or accessible.³⁴

Moving to Zero Trust Environments, Equipment, and Services. In pre-WFH, most members of organizations were used to working in a trusted information and communication environment. With increased WFH, everyone needed to get used to working in a “world of zero trust” [2].³⁵ In the normal office environment, for example, university staff would be working and emailing on the organization’s domain name system (DNS) network domain, in which IT could set up a “response policy zone” (RPZ) that could block known purveyors of malware at the DNS level. Or using

34. Cyber security experts refer to a cyber triad of Confidentiality, Integrity, and Availability (CIA) to define the functions of an organization’s information security systems. This triad is all about ensuring: Confidentiality, that authorized users able to access this data and malevolent cyber actors are not; Integrity, that the system and data are accurate and correct, such that there are no damaged system files and no one has undermined the integrity of financial or other information; and Availability: that systems, data, and information are available, such as not subject to a denial of service attack or denied access via ransomware (see <https://www.bmc.com/blogs/cia-security-triad/>).

35. The “zero trust” concept is that users and devices need to be subject to the same level of security whether they are on an external untrusted network or on an internal trusted network (see <https://cloud.google.com/beyondcorp/>). In a “zero trust” environment, trust focuses on endpoint-level security, ideally with enhanced authentication processes for users and devices replacing blind trust in the presence of an internal network.

“DNS poisoning,” the university could prevent a user from accessing a link within the email via the university’s DNS if it had been seen before and blocked. Even “if the user was fooled by a convincing phishing email, they would be prevented from accessing any link in the email” [2].

Zero trust solutions seemed promising to interviewees. One noted the future of remote working will require it. As he said, “VPNs aiming to bring users logically ‘on-prem’ are now outdated technology” [2]. This points to new technical solutions, like Google’s BeyondCorp, an early zero trust system, which shifts control from the perimeter to individual devices and users.³⁶

Political–Administrative Structures and Practices

Organizations Not Prepared for the Rapid Shift to WFH. The suddenness with which the transition to WFH occurred, the lack of preparation in most organizations for the WFH transition, and the pressure to ensure business continuity were major contributory factors in the increase in security issues during the pandemic [1]. The rapid rise of the COVID-19 pandemic and subsequent variants took most of the world and most companies by surprise.

The threat intelligence manager interviewed was concerned that people did not appreciate the loss of a protective perimeter. Speaking in terms of the traditional “rings of security,” he said “the outer shell of security—it just went away, around the March 1 last year” [2020], and that it had taken a couple of weeks for the realization of what had happened to sink in with companies [4].

Many may have had contingency plans for working remotely or from home, but most did not anticipate the rapid scaling up of WFH in the wake of the pandemic. This left many staff who shifted to WFH with less awareness, training, and equipment for WFH than they might otherwise have had in place. One interviewee stated that many companies did not have a business continuity and disaster recovery (BCDR) plan in place before the pandemic. Another interviewee said that while there were some companies that had a significant WFH capacity before the pandemic, such as with good VPNs, most really didn’t. Going from 20% to 100% of people WFH had been “an absolute nightmare” for many organizations [4].

36. This approach aims to both improve the security of remote connections from an external network and to protect against threats from malicious infiltration of an internal network.

The Cultures of Organizations: Prescriptive versus Proscriptive Security. Security is often perceived to conflict with other objectives. A threat intelligence manager noted that, in industry, business continuity is often the main priority, leading to the use of nonapproved systems for business purposes. If it helps with productivity, the “psychology is—I just want to get stuff done” [4]. Another emphasized the priorities of organizations.

The interviews revealed some distinct differences across organizations in how they value security relative to other values within the organization, such as personal creativity and productivity. Some universities were cited as having a relatively prescriptive approach to security. An interviewee said that imposing a security solution that would not be universally feasible would not work, citing the example of using personal mobiles for MFA. He noted that while there is no intention to compromise cybersecurity on the part of academic staff, there is a “reluctance to be constrained.” “People won’t use their personal mobile phones for university business.” In some instances, at his university, people will complain about whatever solution is suggested. There are valid security concerns. However, there are so few instances of real problems that the IT security team often just deals with it. They try to support their academic staff.

More generally, across the economy, a threat intelligence manager said that there has been an “explosion” in MFA during the pandemic. However, he warned that while everyone should be doing MFA on their phone, the way in which SMS authentication measures have been implemented in response to WFH, such as using only two-factor SMS authentication (2FA), during the pandemic has unintentionally built up a “ticking time-bomb” where people think they are protected but they are not [4]. Their 2FA systems are open to “swapping attacks.”³⁷

Unknown Time Horizons and Short-Term Stop Gaps. Not only were organizations not prepared for a dramatic shift to WFH, but also many did not expect the pandemic situation would last as long as it did. The feeling that the situation was temporary led, according to the threat intelligence manager, to the implementation of some “stop-gap” solutions that were

37. Swapping attacks, SIM swapping, or SIM Jacking happens when a malicious user exploits the limits of two-factor authentication by fraudulently tricking a mobile phone carrier to transfer a mobile user’s phone number to the SIM card of the fraudulent user. They can then use their SIM card to access accounts linked to a victim’s mobile. A well-publicized account of such an attack is at: <https://www.nbcnews.com/business/consumer/how-hackers-are-hijacking-your-cell-phone-account-n859986>

“insane, in retrospect” [4]. He said that if users had realized that WFH due to the pandemic would last longer, they would have done things differently. An example of an insecure stop-gap solution was an employee who was unable to send a document above a certain size as an attachment through their work email, so they might send it via a less secure route, such as Facebook messenger instead.

With respect to the possible effects of “short-term” thinking contributing to security issues, particularly in WFH at the start of the pandemic, the same interviewee said it was also necessary to consider the perspective of cybercriminals. They also did not know how long the pandemic situation was likely to last. Had the cybercriminals realized the long-term opportunity that the pandemic represented, from their point of view, they would probably have changed their “revenue model.” The interviewee suggested that this may be changing with the realization on the part of cybercriminals that the shift to WFH, because of the pandemic, may be likely to be for the long term—the effects of this are yet to be seen.

Cybersecurity as an Enabler

As the interviews progressed, it became increasingly clear that cybersecurity could be an enabler, not just a new set of problems emerging from work at home. A number of themes developed that supported this alternative framing of WFH.

Advantages of Larger Firms and Institutions: Scaling Up. Interviews touched on the advantages of larger companies and institutions in being more likely to have had established processes for working remotely, such as from home. In many large institutions, some percentage of employees would have been working remotely or from home. This has led organizations to create the services and provide the equipment and training valuable for those employees. So, for that set of firms and institutions, the pandemic primarily presented the problem of scaling up the numbers of employees WFH, not creating capabilities from scratch.

A security expert in a communications company stated that his company had been well-prepared for remote working, but mainly had to scale up [6]. He said that the use of videoconferencing had already been common across the company before the pandemic hit, and many company staff had been issued with company laptops for WFH, although in some countries a BYOD model was in place instead for a variety of reasons. Strong policies were in place for use of devices in WFH, such as about the

upgrading of machines and guidance prohibiting sharing of passwords. He thought that the company's widespread use of Citrix remote desktop or cloud solutions such as Office 365 had enabled company data to remain resident, avoiding the need for employees to download data to their local machines in WFH, and that this stood the company in good stead for the move to WFH during the pandemic.

However, scaling was dramatic. The interviewee said that while before the pandemic, the WFH rate for company staff had been an estimated 20% (one day a week at home), and often involving hybrid home-office working by individuals; during the pandemic, this rate had increased to as much as 95%. He said that some network operations center staff and field engineers still needed to be on-premises [6].

Technological Support. Technical advances are increasingly capable of detecting potential problems [1], such as through pattern recognition. For example, advances in SPAM detection have enabled most users of up-to-date software to filter most SPAM, which often identifies legitimate messages. A related possibility is using artificial intelligence (AI) with threat intelligence to detect malicious email, such as phishing scams. However, some interviewees warned that a focus should remain on user education and technical controls as AI is not yet at a point to address these problems.

Integrated Cloud Services are another technical support mechanism for facilitating WFH and reducing security divides between larger and smaller companies [1]. Integrated cloud solutions such as Microsoft 365 have in-built security.

VPNs have been important for remote and WFH, but there have been weaknesses. One university interviewee [2] noted that they had no centrally managed VPN, as departments and institutes often had their own VPN. On some occasions, such as during lockdowns with exceptionally high traffic, VPNs have undermined effective working, leading some to find work arounds.

Changing Perceptions of Security. Training of employees could be reviewed to ensure that they gain a stronger sense of the personal benefits to themselves of cybersecurity. It is not just a corporate or institutional requirement but a positive gain for them. One interviewee referred to this as the "Grandma's Cookie Jar" concept [1]. It is important to protect that jar because those cookies are for you. By protecting their cybersecurity, it is beneficial to themselves—not only the organization. But as the threat intelligence manager put it: A key problem

is that often individuals themselves are not actually at risk from cyber-crime, but they are targeted as a route into a corporate network [4]. He argued that “people cut corners to get stuff done” [4]. They probably learn more from trying to protect their children online, than themselves or their company.

Nothing New. In many respects, WFH did not represent a brand-new arrangement, but a scaling up of what was already being done. For example, with respect to the IT staff at one university, an interviewee noted that before the pandemic, the information security team had been partly co-located, although one team member had joined during 2020 and has never been in the office. Remote working has not had too much effect on the IT security team in terms of loss of face-to-face contact—as the University campus was spread out, much of the contact with users had been conducted online, often by email anyway, and it has been easy to replicate intrateam face-to-face contact with video calls [3].

Likewise, as noted earlier, many in most organizations had been WFH and remotely for years. The pandemic rapidly increased the proportionality of this activity and created more of a problem of scaling existing approaches than facing a new problem.

We Haven't Seen Anything Yet. The future could be worse. As our threat intelligence manager noted, criminals have yet to take advantage of some of the cybersecurity issues created by the pandemic [4]. He said that this was one of the most worrying aspects of the situation—20 years of information security best practice has been abandoned overnight, and cybercriminals have yet to catch up with the opportunities that this presents for them—its “like shooting fish in a barrel.” However, as the interviewee said, as the prevailing view in the information security community is that there won't be a return to prepandemic patterns of working, they are starting to see more investments in more secure systems for remote working, such as VPNs [4].

Conclusions and Discussion

Reframing the Issue of Cybersecurity in WFH

The literature reviewed for this study, particularly those publications focused on forecasting impacts, together with news coverage on this topic, suggest that WFH is raising new and more challenging issues for cybersecurity. In

addition, a number of interviewees in this study suggested that there are areas in which cybersecurity problems have risen, such as around phishing attacks. However, a less-anticipated but striking theme from our expert interviews was about the successful management of cybersecurity despite the WFH shift. For example, many approaches to safely WFH have been used for years by some portions of the workforce for some portions of the workweek. This incremental WFH pattern created technical and other cybersecurity strategies that enabled more people to work more exclusively from home without dramatic problems with cybersecurity. This led us to reframe the problem for research in this area to define a new focus for cybersecurity research.

Cybersecurity Is Not Undermining Effective Working at Home

The potential for WFH has been greatly enhanced by the level of cybersecurity enjoyed by many Internet users, albeit this has been taken for granted. Many employees, teachers, and students have experience in WFH and remotely. As one interviewee observed, employees who had done a lot of business travel in prepandemic times were generally more attuned to the intricacies of WFH.

To this point, one information security officer [2] noted that although his university was considering much more of a return to on-premises working but that:

... the mixture of home and office working is here to stay. Whatever the new ways of working they come up with, many organizations will avoid going back to the old ways of always in, in favor of always on (but from anywhere).

He argued that our questions had even more significance, as with a shift from WFH to a more routine hybrid model, there would be a “risk of a cognitive over-load if the cybersecurity practices are different from in the office to in the home. Too much to learn for busy people, too much reliance on spotting different threats depending on their environment.” To him, this meant an even greater focus on a Zero Trust approach.

The Need for Further Research

The pandemic has diminished in many nations and is likely to be better managed in due course, but WFH is likely to continue in many

institutions, even if better balanced with work in the office. Asked about the future of remote working after the pandemic, one of our interviewees said that one of his university's recovery work streams was around hybrid remote working, as they viewed this as likely to be "the new normal." Some obvious exceptions exist, such as around lab work. But he saw this as a major cultural change, with people wanting to continue working full- or part-time from home. He noted that these preferences need to be balanced with student expectations, such as in the frequency of seeing their instructors in person.

The literature review and exploratory interviews suggest the need to focus more research on whether cybersecurity has been a major enabler of WFH—and not simply a problem created by moving away from the central sites of business, governmental, and educational institutions. However, our limited number of interviews were focused on the United Kingdom and the United States. A male perspective might be prevalent in the security community, but future interviews should take in other perspectives, which might, for example, take privacy into greater account. While we do not profess to have anywhere near an adequate sample of cybersecurity experts in the United States and the United Kingdom, we have no interviews that might tap the perspectives of non-European and non-American stakeholders or from a wider range of sectors, including the experiences of journalists, media organizations, and nongovernmental organizations (NGOs). The relative lack of strong research on the problems associated with WFH also leaves many questions about their prominence and impact on the potential for the new patterns of work that might follow from the pandemic, such as with increases in remote, mobile, and home working. Key questions include: What are the cybersecurity issues arising from WFH? Are they new? Has WFH been enabled or undermined by weaknesses in cybersecurity?

Further research should include meta-analyses of cybersecurity incident reports, which we will develop into data points for a meta-analysis that helps identify the severity, number, and targets of major types of attacks on individuals WFH. This could inform the development of a typology of capacities and problems faced in WFH. Building such typologies of capacities and issues will be valuable to the development of survey research, which might be essential to gaining a more generalizable sense of the scale and severity of different problems and infrastructures, particularly if we can conduct a variety of population surveys in multiple nations across regions for the world. Survey work could also be complemented by two or

more in-depth case studies of each kind of risk or problem to illuminate the social and technical dynamics of building cybersecurity capacity.

In summary, there has been a surprisingly limited range of independent empirical research on cybersecurity issues in distributed settings, such as around WFH. However, many forecasts and early research suggest that this will be a significant and rapidly growing area of research. Our qualitative research raised a number of themes and open up this area of further research, such as in tracking developments and trends that will inform a set of recommendations on building the cybersecurity capacity of individuals and organizations WFH and reducing associated harms. However, considering our in-depth interviews, cybersecurity should be examined as an enabler of WFH and not only as opening up a set of cybersecurity problems.

APPENDIX

Semistructured Interview Questions and Prompts

Have you received reports of cybersecurity incidents in your organization that have occurred as a consequence of the move toward greater levels of remote working during the COVID-19 pandemic? What steps have you taken to mitigate the risk of cybersecurity incidents in connection with WFH?

Have you received reports from employees/individuals of concern regarding intrusion into their private life by employers as a consequence of remote working during the pandemic? What steps have you taken to address such concerns?

Finally, we have identified a number of problems related to cybersecurity and privacy in WFH—some of which you have mentioned—and wondered if any of these issues have been an issue in your work with users in your organization. Let me note these and get your quick view on whether each of these has not been a problem, a problem but relatively insignificant, or a major problem for you and your organization? PROMPTS ON: any increase in problems related to phishing emails, in connection with the use of personal devices or use of personal email by employees WFH, with remote access technology used for WFH, such as remote desktop sharing or VPNs, with the use of videoconferencing software—such as Zoom or Microsoft Teams—for remote collaboration

during the pandemic, or problems as a consequence of insufficient security in the household, such as insecure Wi-Fi, or sharing of information with or by other members in the household.

BIBLIOGRAPHY

- Ahmad, Tabrez. "Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity." 2020. SSRN 3568830.
- Awan, Malik Shahzad Kaleem, Pete Burnap, and Omer Rana. "Identifying Cyber Risk Hotspots: A Framework for Measuring Temporal Variance in Computer Network Risk." *Computers & Security* 57 (2016): 31–46.
- Baker, Brandon. "BeyondProd: The Origin of Cloud-Native Security at Google." 2020. <https://www.usenix.org/conference/enigma2020/presentation/baker>.
- Bannister, Adam. "Remote Working during Coronavirus Pandemic Leads to Rise in Cyber-attacks, Say Security Professionals." *The Daily Swig*, July 14, 2020. <https://portswigger.net/daily-swig/remote-working-during-coronavirus-pandemic-leads-to-rise-in-cyber-attacks-say-security-professionals>.
- Blythe, John. "Cybersecurity in the Workplace: Understanding and Promoting Behaviour Change." *Proceedings of CHIItaly 2013 Doctoral Consortium* 1065 (2013): 92–101.
- Chamola, Vinay, Vikas Hassija, Vatsal Gupta, and Mohsen Guizani. "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact." *IEEE Access* 8 (2020): 90225–65.
- Chapman, Phil. "Are Your IT Staff Ready for the Pandemic-Driven Insider Threat?" *Network Security* 2020, no. 4 (2020): 8–11.
- CISA. "Ransomware Activity Targeting the Healthcare and Public Health Sector." *Cybersecurity & Infrastructure Security Agency*, October 28, 2020. <https://us-cert.cisa.gov/ncas/current-activity/2020/10/28/ransomware-activity-targeting-healthcare-and-public-health-sector>.
- Dingel, Jonathan I, and Neiman Brent. "How Many Jobs Can Be Done at Home?" 2020. https://bfi.uchicago.edu/wp-content/uploads/BFI_White-Paper_Dingel_Neiman_3.2020.pdf.
- Dowling, Mike. "Enabling Remote Working: Protecting the Network." *Network Security* 2012, no. 3 (2012): 18–20.
- Dutton, William H. "Fostering a Cybersecurity Mindset." *Internet Policy Review*. 6, no. 1 (2017). doi:10.14763/2017.1.443, <https://policyreview.info/node/443/pdf>.
- Dutton, William H., and Brian D Loader. eds. *Digital Academe: New Media and Institutions in Higher Education and Learning*. London: Taylor & Francis/Routledge, 2002.
- Dwivedi, Yogesh K., D. Laurie Hughes, Crispin Coombs, Ioanna Constantiou, Yanqing Duan, John S. Edwards, Babita Gupta et al. "Impact of COVID-19 Pandemic on Information Management Research and Practice: Transforming Education, Work and Life." *International Journal of Information Management* (2020): 102–211.
- Eurostat. "Employment LFS Series." 2021a. Accessed July 30, 2021. https://ec.europa.eu/eurostat/databrowser/view/LFSA_EHOMP__custom_899843/bookmark/table?lang=en&bookmarkId=1a955ba3-e7ff-42b5-9449-69a6db8750ff.
- Eurostat. "ICT usage in Households and by Individuals." 2021b. Accessed July 30, 2021. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_pb/default/table?lang=en.
- Faulds, David J., and P. S. Raju. "The Work-from-Home Trend: An Interview with Brian Kropp." *Business Horizons* 64, no. 1 (2021): 29.

- Garrote Sanchez, Daniel, Nicolas Gomez Parra, Caglar Ozden, Bob Rijkers, Mariana Viollaz, and Hernan Winkler. "Who on Earth Can Work from Home?" World Bank Group Policy Research Working Paper 9347, 2020.
- Hakak, Saqib, Wazir Zada Khan, Muhammad Imran, Kim-Kwang Raymond Choo, and Muhammad Shoib. "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies." *IEEE Access* 8(2020): 124134–44.
- Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. "Cybersecurity in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic." *Computers & Security* 105, no. 102248(2020): 1–20.
- Leyden, John. "RDP Attacks Skyrocket Amid COVID-19 Lockdown." *The Daily Swig*, May 11, 2020. <https://portswigger.net/daily-swig/rdp-attacks-skyrocket-amid-covid-19-lockdown>.
- Nicol, David M. "In the Petri Dish: Cybersecurity Pushed to the Edge." *IEEE Computer Architecture Letters* 18, no. 3 (2020): 4–5.
- Nilles, Jack M., F. Roy Carlson, and Paul Gray. *Telecommunications-Transportation Tradeoff: Options for Tomorrow*. New York: John Wiley & Sons, 1976.
- Okerefor, Kenneth, and Phil Manny. "Understanding Cybersecurity Challenges of Telecommuting and Video Conferencing Applications in the COVID-19 Pandemic." *International Journal in IT & Engineering* 8, no. 6(2020): 13–23.
- Osborn, Barclay, Justin McWilliams, Betsy Beyer, and Max Saltonstall. "BeyondCorp: Design to Deployment at Google." *Google Research* 41 (2016): 28–34. <https://research.google/pubs/pub44860/>.
- Peck, Jeff, Betsy Beyer, Colin Beske, and Max Saltonstall. "Migrating to BeyondCorp: Maintaining Productivity While Improving Security." 2017. <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/f29b3e764b1122d508b7b53544a3bbadd6cd101.pdf>.
- Ponemon, Ponemon Institute. "Cybersecurity in the Remote Work Era: A Global Risk Report." 2020 *Research Report*. Michigan, USA: Ponemon Institute, 2020. <https://www.keeper.io/hubs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf>.
- Short, John, Ederyn Williams, and Bruce Christie. *The Social Psychology of Telecommunications*. John Wiley and Sons, 1976.
- Tanium. "When the World Stayed at Home." *Research Report*. Emeryville, CA: Tanium, 2020. <https://staging.tanium.com/resources/when-the-world-stayed-at-home/>.
- Venkatesh, Alladi, and Nicholas P. Vitalari. "An Emerging Distributed Work Arrangement: An Investigation of Computer-Based Supplemental Work at Home." *Management Science* 38, no. 12 (1992): 1687–1706.
- VMware Carbon Black. "Global Threat Report. Extended Enterprise under Threat." 2020. <https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-grt-extended-enterprise-under-threat-global.pdf>.
- Ward, Rory, and Betsy Beyer. "BeyondCorp: A New Approach to Enterprise Security." 2014. <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf>.
- Weil, Tim, and San Murugesan. "IT Risk and Resilience—Cybersecurity Response to COVID-19." *IEEE Computer Architecture Letters* 22, no. 3 (2020): 4–10.
- Williams, Matthew L., Michael Levi, Pete Burnap, and R. V. Gundur. "Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory." *Deviant Behavior* 40, no. 9 (2019): 1119–31.