Keep Calm and Carry on with Cybersecurity @Home: A Framework for Securing Homeworking IT Environment

Max Hashem Eiza[1], Romanus Izuchukwu Okeke[2], John Dempsey[1], Vinh-Thong Ta[1]

[1]School of Psychology and Computer Science, University of Central Lancashire (UCLan), Preston UK
[2]Lancashire School of Business and Enterprise, University of Central Lancashire (UCLan), Preston UK

ABSTRACT

For the first time in modern history, businesses had to suddenly facilitate homeworking for a large proportion, if not all, of their workforce because of COVID-19 pandemic. The fact that employees access sensitive corporate data from non-corporate networks opens the door wide for many cybersecurity risks that could result in data loss, breaches and consequently huge financial loss. Since the move was sudden, most businesses, especially small ones, did not have the time to assess their homeworking cybersecurity requirements. This paper aims to bridge this gap and propose a multi-layered framework that is focused on businesses' requirements to guide cybersecurity @home activities. The framework can be also beneficial for businesses that currently have homeworking cybersecurity policies to assess their compliance with the framework and enrich it.

Keywords: Cybersecurity; COVID-19 pandemic; Cyber risk awareness; Homeworking; IT Environment.

1 INTRODUCTION

Homeworking has become the new norm during COVID-19 outbreak where over 45% of the workforce, an increase from 5% in 2019, are now working from home in the UK (Bela, Wilkinson, & Monahan, 2020). With less than 15% of businesses provide IT training for non-technology specialist

employees (Bela, Wilkinson, & Monahan, 2020), there are many gaps in knowledge and skills this sudden shift has amplified. Homeworking (aka working from home) means that employees are accessing sensitive corporate data using their personal devices and networks that might be outdated and/or shared with other people in their household. According to recent surveys by Morning Consult + IBM Security (Morning Consult + IBM Security, 2020) and Morphisec (Sheva, 2020), on average, 54.5% of employees use their personal devices as their work devices with no new tools to secure them. In another survey (Christian, 2020), which was conducted on 900 participants, only 52.7% of employees working from home said they have a corporate device assigned for work. These numbers are not a surprise as Bring Your Own Device (BYOD) trend has led to 67% of employees using their personal devices for work even before COVID-19 pandemic (Deyan, 2020). BYOD has been encouraged and adopted by organisations because it generates on average an extra $350 of value each year per employee! (Deyan, 2020)

To adjust to homeworking, employees need to setup new communications tools such as Zoom and Microsoft Teams. However, setting up these new tools with little or no expertise creates new security threats if employees get any settings wrong. Furthermore, these tools suffered from many security breaches (e.g., during COVID-19 lockdown, Zoom was hacked several times during video conference meetings (Marotti, 2020) and remote class lessons (BBC, 2020)). This has created a new wave of cyberattacks that exploit these unprecedented work conditions (e.g., nearly third of Britons were targeted by scammers since the start of COVID-19 pandemic (Kundaliya, 2020)).

This paper aims to address this challenge by devising a multi-layered framework for a cybersecure homeworking IT environment. While businesses can get the government-backed Cyber Essentials for protection against cyberattacks (HM Government, Department for Digital, Culture, Media & Sport, 2018), there is no standard nor a framework for businesses with a homeworking workforce. Hence, this paper proposes a similar approach: Cybersecurity Essentials @Home for employees to help businesses ensuring 1) their workforce has a cybersecure homeworking IT environment and 2) compliance with data protection and relevant policies is upheld while working from home. The primary goals of this paper are 1) raising cyber awareness for businesses and their employees; 2) helping businesses to get their workforce cybersecurity ready @home to build an agile workforce during/beyond COVID-19 pandemic; and 3) providing a background for further research development.

It is worth noting that the proposed framework is not expected to provide a one-fit-all solution because a) it is not feasible to model the specific IT systems and requirements of every business; and b) businesses will continue to have unique threats based on their capabilities, resources, risk tolerance, compliance obligations and IT environment. However, the framework is expected to enable every business to assess their current position and benefit from the provided tools and practices to better manage their homeworking cybersecurity. Admittedly, some industrial sectors (e.g., information and communication, financial services, and real estate activities) will benefit more from this framework. The reason behind that is they provide far more homeworking opportunities compared to other sectors such as transportation and storage, food services, wholesale and retail, and repair, which provide relatively fewer opportunities for people to work from home.

BACKGROUND

This work is motivated by the following questions: How has homeworking changed cybersecurity culture, compliance and risk? and what can improve homeworking cybersecurity? The sudden shift to homeworking, COVID-19 has imposed, creates and aggravates gaps in cybersecurity and presents new cybersecurity risks to businesses. Currently, there is no standard for securing homeworking IT environment considering businesses' requirements. There are, however, few attempts by some security centres to create guidance and tips to keep remote workers cybersecure @home such as UK National Cyber Security Centre (NCSC) guidance (National Cyber Security Centre (NCSC), 2020), SANS Working from Home Kit (SANS Institute, 2020) and HIPPA @Home (Woodside, 2020).

In the same context, many organisations, such as NHS Trusts (Cornwall, 2020) and London Councils (London Councils, 2020), have devised their own homeworking policies to help their employees work effectively from home while meeting the business needs. These policies and guidelines focus on homeworking as a new mean of achieving business's goals. For instance, they address the legal obligations of both employees and employers while setting the outline for a homeworking agreement. Homeworking environment in general, not just IT, is considered from health, safety and wellbeing perspective. Therefore, these policies lack an in-depth evaluation of the cybersecurity processes and operations in the homeworking environment. Nonetheless, they provide a step in the right direction to achieve safe, healthy and cybersecure homeworking environment.

In general, these attempts fall short of recognising the variety of businesses' cybersecurity requirements, their business operations, risk tolerance and

compliance obligations. They are basically a set of tips and recommendations that do not come close to cover the myriad of technologies businesses use and therefore, need to secure while homeworking. For instance, all these attempts, mentioned above, assume experienced know-how homeworking workforce. This is not always the case. Besides that, businesses might be using different technologies to those recommended (e.g., NCSC guidance gives advice about the use of Virtual Private Network (VPN) for remote access). However, not all businesses use VPN (e.g., some businesses might still be using the outdated Remote Desktop Protocol (RDP) and TeamViewer for remote access!) Even VPN access can be compromised if setup improperly.

From businesses' perspective, reports on rising number of cyberattacks attributed to COVID-19 pandemic (Tidy, 2020) (e.g., phishing and business email scams) mean that a data breach is now more likely than ever. Any data breach would violate data protection laws such as the General Data Protection Regulation (GDPR) (Information Commissioner's Office (ICO), 2018), and leave businesses facing financial and reputational damages. These risks are further amplified by the impact of homeworking. Therefore, in this paper, we will focus on this unique situation businesses face to develop a framework that meet their requirements in terms of cybersecurity, compliance and risk, while having homeworking workforce. Given these unprecedented times, building an agile cybersecure @home workforce is now more important than ever.

It is worth mentioning that, in this paper, we assume that employees are happy to share and utilise their home IT environment to carry out their jobs. This means sharing some data with their employers about their home environment (e.g., number of people living there, existing devices, Internet connection, etc.) There are situations where employees do not feel comfortable doing so especially if homeworking is enforced by their employer rather than being caused by unavoidable circumstances like the current pandemic. Exploring and discussing these cases is outside the scope of this paper and left for future work.

2 Related Works

Since the start of COVID-19 pandemic, many organisations have put some guidelines to help businesses move to remote working safely. As mentioned before, examples of these guidelines are the UK NCSC's "*Home working: preparing your organisation and staff*" (National Cyber Security Centre (NCSC), 2020), SANS' *Security Awareness Work-from-Home Deployment Kit* (SANS Institute, 2020) and *HIPAA @Home: How to Keep Your Remote*

Workers Cybersecure Out of the Office (Woodside, 2020). These guidelines do not provide a systematic framework that could be applied for a large range of businesses nor cover the myriad of technologies businesses use. Another example of these efforts are best practice advices written by security professionals in different blogs such as Bruce Schneier's Work-from-Home security advice (Schneier, 2020) and 7 Best Practices for Securely Enabling Remote Work from CyberArk (Silberman, 2020). These best practices, tips and guidelines can be summarised in four points:

1. **Create new accounts and access for staff working from home**. Some guidelines (e.g., (Silberman, 2020)) recommend using multi-factor authentication (MFA) and single sign-on (SSO) to access corporate resources. Using MFA is essential to prevent the use of compromised/stolen credentials while SSO makes it easier for staff to sign once and use their credentials everywhere.

2. **Control access to corporate network and resources remotely**. UK NCSC recommends using VPN to allow homeworking staff access corporate network (National Cyber Security Centre (NCSC), 2020). It states that VPN software should be setup correctly and fully patched since attackers have long targeted VPN services. It is a tricky matter, with the sudden move and inexperienced staff, to ensure that VPN is setup correctly. Moreover, VPN is not designed to provide granular access to critical resources. Therefore, it is advised to reduce the reliance on VPNs (Silberman, 2020).

3. **Take ownership/control of staff's working devices if possible**. This advice is important because owning/controlling staff's work devices will allow the business to encrypt data at rest and have full control over these devices (e.g., delete all data if the device is stolen, disable the use of removable media, etc.) In principle, businesses can remotely configure these devices and enforce strict access policies like prohibiting access to social media, personal emails and software installation. However, to do so, the business should have the resources and a dedicated IT team who has the experience to configure, enforce and monitor these remote devices. It requires a considerable amount of investment that many businesses might not be able to commit to especially with the current situation (i.e., COVID-19 financial impact on businesses.) Therefore, more emphasis is put on educating staff and encouraging them to look after their devices. Still, there is a high risk given that most staff are not tech-savvies and many of them use weak passwords, do not patch/update their systems, share the same device with other family and/or household member, etc.

4. **Setup policies to provide the least privileged and/or just-in-time access to resources**. This is very useful advice to give access only when needed for those who need it (Silberman, 2020). However, this requires huge amount of IT management overhead, access review to users' permissions and migrating some services to other platforms that can facilitate these features. All this will produce new challenges and financial liabilities where businesses are struggling to keep their business going during these challenging times.

Collectively, these points of best practices are very generic and most of them do not consider businesses requirements, different capabilities, different tools, the nature of the business's operations and the size of its workforce.

In addition to these guidelines, there are risk assessment standards that businesses can follow such as ISO/IEC 27005 (ISO, 2018) and NIST 800-30R1 (NIST, 2012). However, they include a generic approach of risk assessment for all kinds of scenarios. In most cases, while carrying out a risk assessment using one of these standards, it is assumed that staff's devices at home are out of scope, which means, to save cost, businesses do not invest in protecting their employees' home IT environment. However, during COVID-19 lockdown, homeworking IT environment must be included in the scope of the risk assessment, which complicates the whole process.

To rectify these issues, this paper proposes a multi-layered framework that is primarily designed for homeworking scenario and could be used alongside the above-mentioned risk assessment standards. The framework aims to embed different businesses cybersecurity needs and identify the benefits, limitations and suitability of different tools that are traditionally used to access work remotely. To do that, we first review the security risks for businesses when employees are working from home. Secondly, we propose a systematic framework specifically devised for the homeworking scenario.

As mentioned before, the proposed solution is not a "catch-all" framework. However, it is expected to provide businesses with the right tools to assess their current cybersecurity posture, devise secure homeworking policies and improve their overall cybersecurity.

3 Cybersecurity @Home Framework

To achieve this paper's aim, we start by explaining the problem recently facing businesses and present the developed framework thereafter.

3.1 Problem Formulation

Recent survey of 3000 remote office workers and IT professionals in the US, UK, France and Germany showed that 77% of remote employees are using unmanaged, insecure BYOD devices to access corporate networks and data (CyberArk, 2020). Considering the challenging conditions COVID-19 have created, especially for working parents, the survey indicated that cybersecurity best practices are not one of their top priorities. It also noted that 93% have reused passwords across applications and devices with 37% insecurely save passwords in browsers on their corporate machines. In terms of video conferencing, 66% of staff have adopted communication/collaboration tools such as Zoom and Microsoft Teams, which have recently reported security vulnerabilities. Moreover, 29% of the surveyed staff said they allowed other members of their household to use their corporate machines for activities such as schoolwork, gaming and shopping.

These statistics clearly show how homeworking has changed the landscape of cybersecurity for businesses and generated new risks that should be considered. This is especially dangerous when it comes to organisations that are responsible for managing critical systems and resources such as critical infrastructure, banks and health services. If privileged credentials of remote workers are compromised, this could cause serious damage to the organisation's most critical systems and resources.

3.2 An Overview of Cybersecurity Risks for Businesses during COVID-19 Pandemic

Cybersecurity risk is defined as the exposure to harm or loss resulting from breaches of or attacks on IT systems. However, Schlarman argued that this definition must be broadened to encompass "*the potential of loss or harm related to technical infrastructure or the use of technology within an organisation*." (Schlarman, 2016) Majority of businesses fear that massive migration to homeworking would lead to spike of cyberattacks and data related breaches.

While homeworking, during COVID-19 pandemic, led to huge economic benefits to IT industry and serving public goods, there are huge cybersecurity risks/threats which have massive impact on individuals and business productivity. The authors in (Lallie, et al., 2020) suggest that cybersecurity risks and concerns associated with homeworking have reached an unprecedented level ever experienced by businesses and individuals. The concerns have motivated researchers to ask key questions: 1) What are cybersecurity risks during COVID-19 pandemic? 2) What is the impact of

the pandemic on increasing cybersecurity risks? 3) What are the common cybersecurity risks during the pandemic and how are the risks contrasted across business sectors? and 4) How are businesses and government agencies responding to these questions? Answering these questions would help in prioritising cybersecurity essentials to design an appropriate framework for securing homeworking IT environment. Thus, providing vital knowledge for improving cybersecurity activities of businesses that would enhance risk tolerance and compliance obligations while securing their employees' homeworking IT environment.

Although the extent and impact of the cybersecurity risks influenced by COVID-19 pandemic vary across studies, most of the researchers agreed that the impact is huge and unprecedented. Weil and Murugesan (Weil & Murugesan, 2020) suggest that the pandemic 'stress test' IT systems including security and IT governance measures in both home and corporate environments.

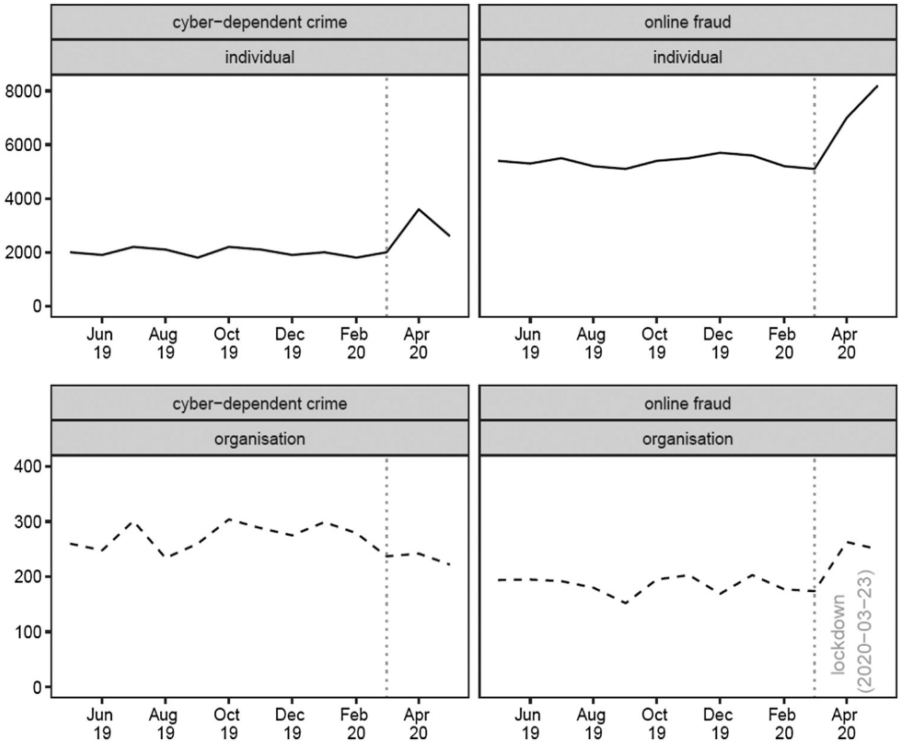

Figure 1. Cyber-dependent crimes and online frauds known to police by victim (Buil-Gil, Miró-Llinares, Moneva, Kemp, & Díaz-Castaño, 2020)

The authors in (Buil-Gil, Miró-Llinares, Moneva, Kemp, & Díaz-Castaño, 2020) conducted a preliminary analysis of short-term impact of COVID-19 and lockdown measures on cyber-dependent crime and online fraud in the UK. Using time series analyses of police crime data from May 2019 to May 2020, they indicated that reports of cybercrime have increased during the COVID-19 outbreak, and these were remarkably large during the two months with the strictest lockdown policies and measures. The analysis shows that the number of frauds associated with online shopping and auctions, and hacking of social media and email accounts, have seen the largest increase in the number of incidents. Although these crimes are most common cybercrime categories in the UK, the authors concluded, as shown in Figure 1, that the striking increase in cyber-dependent crimes has mainly been experienced by individual victims rather than organisations. This shows that the responsibility of protecting the cyberspace has shifted from corporate business organisations to individuals due to homeworking.

Other studies such as (Ofcom, 2020), (Rodger, 2020), (Chadwick, 2020) (Clymo, 2020) and (McCorkell, 2020) have reported various forms of cyberattacks impersonating business organisations including government agencies (e.g., WHO), supermarkets (e.g., Tesco) and airlines. Lallie *et al.* (Lallie, et al., 2020) use the UK as a case study to analyse the extent of the COVID-19 cybersecurity related risks. Although their findings show a loose correlation between COVID-19 policy/news announcements of homeworking and associated incidents of cyber-crime attacks/breaches, they noted that '*the extent of the cybersecurity related problems faced in the UK was quite exceptional*' with comparatively high level of suspect emails and fraud reported. Table 1 depicts some COVID-19 related cyberattacks reported in the UK between March 2020 and May 2020.

TABLE 1 Descriptions of COVID-19 Related Cyberattacks in the UK
Key: P: Phishing (or Smishing); Ph: Pharming; E: Extortion; M: Malware; F: Financial Fraud.

Source	Attack Type	Description	Report Date	Attack Date
(Ofcom, 2020)	P, M	SMS informs recipient to stay at home with a link for more information. Link directs recipient to a malware ridden website	24/03/20	-
(Rodger, 2020)	P, Ph, F	Free school meal SMS directs recipient to website which steals payment credentials	25/03/20	24/03/20
(Chadwick, 2020)	M	Fake NHS website gathers user credentials	28/04/20	-
(Clymo, 2020)	P, M	Email purports to offer job retention payment as per the UK governmental announcement	30/04/20	19/04/20
(McCorkell, 2020)	P, M	Recipients are directed to a fake track and trace website which collects user credentials	13/05/20	-

The UK NCSC has, by early May 2020, reported more than 160,000 suspicious emails leading to removal of over 300 fake websites (National Cyber Security Centre (NCSC), 2020). In a similar report, (Ofcom, 2020) indicated that, in May 2020, fraud victims have lost more than £4.6 million to coronavirus-related scams during the lockdown, with 11,206 people claim to have been victims of email (Phishing) and text (Smishing) attempts to trick them into giving out personal details, as well as more than 2,000 victims lost cash through fake online goods sales, bogus cold-calls, non-existent pension plans and other frauds. Action Fraud, the UK crime reporting agency, estimated that about £2.4 million has been lost in cyber-enabled scams linked to COVID-19. Up to June 2020, the UK NCSC had 5,000 reports about suspicious emails in just one day which led to taking down of more than 80 websites and 471 fake online shops while HM's Revenue and Customs took down 292 fake websites. These reports accounted for only some of the selected cases, not considering the unreported cases due to privacy and branding related reasons for individuals and businesses, respectively.

Recent studies by (Burgess, 2020), (Khan, Brohi, & Zaman, 2020), (Stein & Jacobs, 2020) and (Cook, 2020) have highlighted four business sectors that are prime targets of cyberattacks: healthcare, financial services, medical suppliers and manufacturing, government agencies and media outlets. These sectors have played massive role in supporting livelihood and survival of people that are working from home. People are on the lookout of developing news of COVID-19 from government agencies and media and have increased online financial transactions due to lockdown of commercial activities. Most of healthcare systems are heavily dependent on the ICT applications during the peak of the pandemic which makes the healthcare a prime target by cyber attackers (Khan, Brohi, & Zaman, 2020).

Various cybersecurity bodies and government agencies have responded to address those impending cyber risks. However, the response has not been coordinated with concrete effort that is underpinned by empirical-driven framework. For instance, UK NCSC and the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA) provided an advisory report on exploitation by cybercriminal and advanced persistent threat groups of the current COVID-19 global pandemic (UK NCSC and the US DHS CISA, 2020). The report showed an increasing number of malicious cyber actors exploiting the current COVID-19 pandemic for their own objectives. The UK NCSC has detected more UK government branded scams relating to COVID-19 than any other subject. The report indicated that from the data seen to date, the overall levels of

cybercrime have not increased, although there is recorded number of a growing use of COVID-19 related themes by malicious cyber actors.

Furthermore, UK NCSC and US DHS CISA indicated that, at the same time, the surge in homeworking has increased the use of potentially vulnerable services such as VPNs amplifying the threat to individuals and organisations. The report, however, indicates that the information is a non-exhaustive list of indicators of compromise for detection as well as mitigation advice suggesting that more comprehensive research and analysis are needed to understand the full picture of cybersecurity risks associated with COVID-19 pandemic. The UK NCSC and US DHS CISA report further noted that cybersecurity risks in the current pandemic is a fast-moving situation and that the advisory report does not seek to catalogue all COVID-19 related malicious cyber activity, suggesting that individuals and businesses should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves and their organisations.

At the moment, the biggest challenge remains is how to secure the new homeworking IT environment while ensuring critical business functions are operating without interruption. Additionally, how to keep individuals and businesses protected from cyber attackers exploiting the uncertainty of COVID-19 situation. These questions would not be appropriately addressed without investment in rigorous empirically driven interdisciplinary research that would involve concerted efforts of businesses, research institutions, cybersecurity practitioners and government agencies. Hence, this framework is developed to be the first step towards full research development of addressing cybersecurity risks of homeworking IT environment.

3.3 The Developed Cybersecurity @Home Framework

Based on the cybersecurity risks businesses are now facing, according to the overview above, we develop a multi-layered framework that can help organisations focus their efforts to meet these requirements and achieve cybersecurity @home for their homeworking employees. The framework offers multiple cycles to reflect the ongoing process of evaluating current practices to achieve the desired state. It compiles several approaches, recent standards, practices, tools and strategies that are suitable to improve homeworking cybersecurity. In addition, it provides a common language for expressing, managing and communicating cybersecurity risks to homeworking staff. Figure 2 shows an illustration of the developed framework.

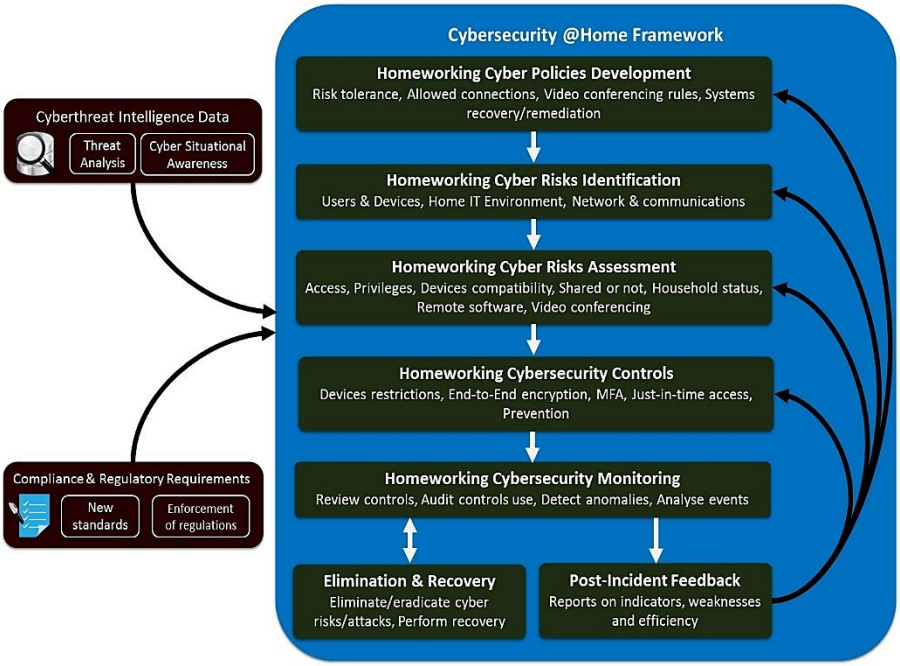

Figure 2. Cybersecurity @Home Framework.

3.3.1 Homeworking Cyber Policies Development

At the beginning, organisations start by defining their default high-level information security policy. They need to decide which areas they want to protect and which they do not (i.e., within scope, out of scope). Since we are designing this framework for homeworking IT environment, it is within scope and should be added to the current policies organisations already have. It is vital to integrate the new risks created by homeworking IT environment with those organisations are used to deal with on daily basis. For instance, risk tolerance, aka risk appetite, by the business will determine the rules that need to be in place for both office and homeworking environments. The following areas should be addressed in this step:

- Video conferencing policy – this might be one of the newest areas the business needs to look at thoroughly given that employees are now conducting online business meetings at home using non-corporate devices and connections. Organisation should determine conditions that should be met before starting, during and after a business-related video conference session (e.g., no one should hear the exchanges during the online meeting, cameras and microphones should be controlled by the

host organisation, when not in use, cameras and microphones must be off, all the sessions must be controlled via a dedicated business-based server, windows should be closed to avoid being seen by anyone, etc.). Moreover, does the house have adequate physical security in place against burglaries? Does home insurance cover the loss of business equipment or should the business extend their insurance policies? Does the home environment have smart devices such as Alexa or any other smart home devices that is monitoring, and potentially recording, the contents of video conference discussions that could lead to a data breach? Same goes to mobile phones (e.g., Google and Siri). Even though these devices might also be present in the workplace, especially mobile phones, meetings and video conferences usually take place in a dedicated room where employees can be asked to switch off their mobile phones (e.g., as part of the workplace policy to guard the secrecy and confidentiality of these meetings). This however is more difficult to enforce while employees are working from home. All these questions are novel due to the shift to homeworking and businesses urgently need to address them.

- Allowed connections – this is essential to determine what connections are allowed while homeworking staff are accessing corporate data: should the connection be encrypted? If yes, should the organisation provide the encryption keys and set the related algorithms? Is the use of VPN allowed? Are there any restrictions that should be in place to access specific data such as customers personal data on a secure server (e.g., this might require access through a specific portal with different set of keys)?
- Systems recovery/remediation – based on the sensitivity and risk tolerance, the business needs to identify the procedures needed to recover from any potential incident. How critical it is to recover systems to normal operations (e.g., health services vs. online shopping)? The nature of the business's operations will determine the timelines that should be adhered to in these situations.

3.3.2 Homeworking Cyber Risks Identification

In this step, the organisation starts to gather information about the current cybersecurity posture while facilitating homeworking for staff. Traditionally, risk identification applies to corporate network perimeter, devices, employees, third-party users, etc. It is usually conducted by the business's IT security team. In this new setting, employees will need to collaborate with the IT security team to carry out this risk identification

since the perimeter is no longer the organisation's premises. This collaboration may include filling in risk identification questionnaire for the IT security team to identify any risks at the homeworking IT environment. This leads to a shared responsibility between employees and the organisation whereas previously it was solely the IT team responsibility. This new collaboration is essential so businesses can understand their employees' homeworking IT environment. It is worth pointing out that the data collected about employees' home conditions must be treated as confidential personal data. Hence, this data should go under the relevant data protection regulations (e.g., GDPR) to avoid any privacy implications for employees.

To identify cyber risk at the homeworking environment, the following points and questions should be considered:

- Devices – How many devices are used to access the corporate network? Do they belong to the business or personal devices or a mix of both? Are they shared with other household members? What type of devices are used (e.g., PC, laptop, tablet, mobile phone)? Which operating systems these devices use (e.g., Windows, Linux, Mac, Android, iOS)? And which versions of these operating systems are installed?

- Users – Is your homeworking staff using a shared device with someone else? What level of access do they need to do their job? how many users are sharing the same device if any? Can their role be delegated to someone else if their remote access is not secure?

- Home IT Environment – Which technology is used to access the Internet (e.g., WiFi, 4G/5G, both)? Are these devices secure and use the latest encryption standards (e.g., WiFi is using WPA2 with strong non-default password)? Is there a private space available for your staff to participate in sensitive/confidential online meetings? If there is not, how can these staff participate to avoid being left out? It is the business's responsibility to ensure no discrimination occurs against employees where their homeworking environment is inadequate. Do staff need to save any corporate data on their homeworking devices? Can this data be encrypted fully or partially?

- Network & Communications – How does business facilitate remote access to their corporate network and resources? Do staff need to configure any remote access software? Do they have the training necessary to do so or can this be done automatically? Are staff allowed to access corporate resources over public networks (e.g., public open WiFi)? Does the business have the tools to detect such access and

impose conditions (e.g., deny, conditional allow)? Are there any regulatory requirements to ensure that personal data is handled correctly and is transmitted securely?

It is worth noting that these questions are by no means an exhaustive list of all the possibilities. These are examples of different scenarios.

3.3.3 Homeworking Cyber Risks Assessment

Based on the data gathered in the previous stage, businesses should be in position to assess the cyber risks with their homeworking staff. Input from cyber threat intelligence received from other businesses in the sector or other sectors can be very helpful as well. This includes but not limited to:

- Access and privileges – What assets homeworking staff have access to? How critical are these assets to the business? Can users' access and privileges downgraded/revoked (i.e., access review based on their last access)?
- Homeworking devices compatibility – Are staff's devices compatible with the business access policy (e.g., only Windows machines are allowed access to the corporate network)? Is there a compatible version of the remote access software the business uses for the homeworking device? Does it have any known vulnerability?
- Household status – Can shared devices be allowed to access corporate resources? How can access be verified to authenticate and authorise the member of staff? How sensitive and confidential the data that can be access by the homeworking device? What are the risks of exposing personal data? Can this risk be tolerated?
- Remote access tools – What are the available tools for the business to use (e.g., VPN, RDP, Web-based access, TeamViewer, etc.)? Are these tools secure to use based on the latest vulnerabilities known? How easy it is to setup/configure any of these tools? Can this be done remotely by the business IT team?
- Video conferencing – What are the available tools for the business to use (e.g., Microsoft Teams, Zoom, Cisco Webex Teams, etc.)? What are the factors the business can control is these tools (e.g., Zoom and Webex allows hosts to mute/unmute participants and stop participants' videos)? However, features such as control participants' microphones and cameras are not yet available. Therefore, the business will be bound by these limitations unless they want to develop a bespoke solution. What is the nature of these meetings (confidential, general, or a mix of

both)? Is end-to-end encryption required? Is collaboration required (e.g., exchange of files, white boards, tasks, etc.) or just video chatting? Can personal devices be used for video conferencing? Can the business tolerate someone else in the household listening to the conversation?

3.3.4 Homeworking Cybersecurity Controls

Once the organisation understands their homeworking cyber risks and security requirements, they can select the appropriate controls to mitigate/eliminate the identified risks and comply with their developed policies earlier. There is a variety of tools that can be used. In the following, we will focus on controls that can help achieving cybersecure homeworking IT environment:

- Devices restrictions – this control is popular if the organisation wants to restrict access to their corporate resources from specific devices and/or operating systems. For instance, a business can deny any access coming from a mobile device (e.g., a mobile phone or a tablet). This can be done on the operating system (OS) level where devices that have out-dates OS will not be allowed access (e.g., Windows 7 or older, out-dated Android, etc.)

- End-to-End Encryption – this option allows the business to ensure all communication and access is protected. They can set this option for video conferencing and collaboration apps to ensure everything is end-to-end encrypted (e.g., the latest update from Zoom provides end-to-end encryption for paying customers, Cisco Webex Teams offers end-to-end encryption and locking messaging rooms (Cisco, 2020)). Furthermore, access to any corporate resource must be over an encrypted channel. This control can be extended to fully or partially encrypt data at home where homeworking staff might need to store data temporarily on their devices.

- MFA – as mentioned before, it is essential to ensure only those who are authorised to access resources can do that. MFA can help in avoiding situations where stolen credentials might be used. Common options for this control can be text messages, secret token that expires after a certain time, fingerprint, voice recognition, etc.

- Just-in-time Access – this control is one of the many benefits of migrating to cloud-based services because it can be easily managed. The idea is to give employees access to the resource they need when they need it and for a limited time. It should be noted that implementing this control might not be straightforward for many organisations especially

if they are operating a traditional on-premises network. However, it is worth investigating because it allows a granular time-restricted control that can be automated to make life easier for both homeworking staff and businesses.

3.3.5 Homeworking Cybersecurity Monitoring

This stage is part of the cyber risk management process where the business can check whether the implemented controls are working effectively or not. If there are any incidents and/or new reports received via cyberthreat intelligence data, notifications will be generated to change/remove the weak control. This step is not as simple as 'replace and keep going', it must involve checks to ensure the new control maintains at least the same risk level or lower risk level in accordance to the homeworking cyber policies. In addition to that, any change in the homeworking IT environment (e.g., change of ISP, new installed OS, new software updates, etc.) should be analysed to ensure it does not pose a new risk.

Arguably, this stage is the most important one in the proposed framework because it ensures a continuous monitoring of the current situation and feedback to other stages should any incident occurs and/or a change is required whatever the change might be (e.g., a control must be changed, software tool must be removed because it becomes vulnerable, etc.). It can be seen in Figure 2 that this stage works very closely with the next sub-stages: elimination & recovery and post-incident feedback. Therefore, it can be considered as part of the incident response cycle businesses should already have (note the loop between monitoring and elimination & recovery). If they do not have it, this framework offers the opportunity to integrate cyber risk assessment for homeworking IT environment and incident response planning.

3.3.6 Elimination & Recovery and Post-Incident Feedback

Finally, these two sub-stages serve the purpose of continuous assessment and learning from the fast-changing events. Procedures such as disconnecting a device, denying access, revoking credentials, isolating resources, remotely installing/removing software, etc. are valuable to eliminate/eradicate cyber-attacks. It is trickier in a homeworking IT environment because businesses might not have full control of their employees' devices. Therefore, these procedures should be considered to operate mostly from the business's side, which can be difficult to achieve if the previous steps were not followed correctly. For instance, some homeworking staff might not feel comfortable allowing someone from work

to change their personal devices security controls because they are worried about their privacy. Hence, it is essential to define ringfences and manage permissions correctly before setting up and allowing staff to work from home.

As it is always the case where 100% cybersecurity cannot be achieved, post-incident feedback is extremely important to learn lessons about what worked and what did not. Does the business have the right indicators? Were they accurate and reported on time? How long did it take to eliminate the risk element and recover systems if necessary? Answers to these questions will provide data for previous stages in the framework to learn and adapt to the new status.

3.4 Using the Developed Cybersecurity @Home Framework

It is widely agreed that cyber risk assessment is time consuming and costly process. Usually, organisations do not have to conduct a full practice more than once a year depending on the nature of their operations. However, with a pandemic like COVID-19, it is important to follow a continuous incremental approach to avoid sudden shifts and address new cyber threats. This will also address issues like outdated cybersecurity controls. Therefore, the developed framework in Figure 2 can be applied depending on the budget of the business and their policy. For instance, large businesses would follow an agile approach applying and using this framework while smaller businesses might not be able to repeat the full cycle more than once a year. Either way, the framework offers a great flexibility and added value to businesses who will have their own cyber risk procedures to follow. It is envisaged that organisations will use the framework described above to:

1. Describe their current cybersecurity status for their homeworking policies, if any, including any risk assessment they have in place, previous experience with cyberattacks, any incident response plans, etc. This step will setup the scene for the next stages.
2. Describe their goal state for cybersecurity @home based on their business's requirements, operations, compliance, etc.
3. Identify gaps and areas for improvement within their employees' homeworking IT environment. The framework provides variety of tools and advice to fill these gaps.
4. Continuously assess progress toward the goal state and measure the success of applying and/or using any measures. This step will feedback to step 1 to review the current status.

By repeating these steps over time, organisations should be able to improve their cybersecurity posture for their homeworking staff and help them make the right decisions in terms of implementing cybersecurity measures and future investments. Furthermore, this process will produce an effective document to communicate cybersecurity risks, procedures and measures in place for staff regardless of their IT experience.

Finally, since the framework is not technology-specific, this offers flexibility for a business to implement the suite of suggested solutions that are suitable for their needs.

3.5 Socioeconomic Benefits of the Developed Framework

Besides cybersecurity, the proposed framework can lead to benefits related to the economic and social impacts of COVID-19 outbreak. As previously stated, COVID-19 has contributed to a huge rise in cyberattacks. From an economic point of view, a successful cyberattack against any business will result in financial and reputational damage including but not limited to 1) data breach fines in compliance with the GDPR (Information Commissioner's Office (ICO), 2018); 2) disruption to the business's operations leading to loss of revenue; 3) costs associated with recovering from a cyberattack; 4) loss of customers (e.g., in 2019, 33% of UK organisations said they lost customers after a data breach (Swinhoe, 2020)); and 5) loss of valuable business information such as intellectual properties, which may lead to more financial losses. Therefore, it is more important than ever for businesses to ensure their homeworking workforce will not be the weakest link in their organisation.

On the other hand, this emerging risk and the new working conditions have put employees under an enormous amount of pressure leading to anxiety, worries and fear of losing their jobs as a result of a successful cyberattack against their employer. According to (Bada & Nurse, 2020), when users are asked to make security-related decisions such as not opening emails from unknown senders, not opening unknown attachments and using security software such as a firewall, it causes them feelings of anxiety due to their lack of knowledge about the implications of taking the wrong decision. This anxiety, coupled with the social disruption to daily lives caused by COVID-19 restrictions, has a negative impact on the social and mental health of homeworking workforce. Having this framework to help businesses implementing the suite of the right cybersecurity solutions for their homeworking employees, and automate the process where possible, will contribute to alleviating these feelings of worry and fear.

4 FUTURE RESEARCH DIRECTIONS

As stated before, this is the first attempt to devise a specific framework for cybersecurity @home. To ensure it achieves its goals, testing and evaluating the developed framework through collaborating with businesses will be essential. Therefore, in the future, we plan to establish an online focus group where participants from different UK businesses across different sectors will assess the developed framework against their cybersecurity requirements and expectations of their homeworking employees. The participants in this activity will be recruited from the pool of IT managers, heads of cybersecurity, and system administrators of the participating businesses. They will assess the developed framework against their organisation's homeworking cybersecurity needs and give feedback to the researchers.

Besides the framework document, we plan to implement a prototype of the developed framework for testing with homeworking users. This will be also essential to establish the benefits of this framework and its applicability in real-world business environments.

This plan reflects that this framework will not be set in stone but dynamic and evolving as technologies, threats, risks and businesses' requirements change. Therefore, the framework will be a living document where revisions can be made to improve it to contribute to the goal of building businesses cyber resilience via a strong cybersecure homeworking IT environment.

5 CONCLUSION

The sudden change, from office-based working to homeworking COVID-19 pandemic imposed on businesses, changed the cyberthreats landscape and introduced new cyber risks. Employees are now accessing corporate resources from non-corporate machines and/or networks (i.e., from home). This issue needs to be addressed to mitigate any cyber risks generated by this new norm. Many efforts from governmental agencies, cybersecurity firms and practitioners to write guidelines and tips to achieve cybersecurity @home have been done. However, they all fell short of addressing the problem systemically considering different businesses' cybersecurity requirements and expectations of their homeworking staff. In this paper, we developed a novel cybersecurity @home framework to help both businesses and employees to address cyber risks that are introduced to the new working environment. The framework provides simple yet comprehensive steps to address this issue considering the homeworking scenario specifically. It is the first step towards building an agile cybersecure @home working force during and beyond COVID-19 pandemic.

6 REFERENCES

Bada, M., & Nurse, J. (2020). The Social and Psychological Impact of Cyber-Attacks. In V. Benson, & J. Mcalaney, *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 73-92). Academic Press.

BBC. (2020, April 10). *Coronavirus: Teachers in Singapore stop using Zoom after 'lewd' incidents*. Retrieved from BBC : https://www.bbc.co.uk/news/world-asia-52240251

Bela, A., Wilkinson, D., & Monahan, E. (2020). *Technology intensity and homeworking in the UK.* Office for National Statistics. Retrieved 05 20, 2020, from https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/technologyintensityandhomeworkingintheuk/2020-05-01

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, 1-13.

Burgess, M. (2020, Mar 22). *Hackers are targeting hospitals crippled by coronavirus*. Retrieved from Wired: https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing

Chadwick, J. (2020, April 28). *Cyber criminals create a spoof copy of the NHS website in the midst of the coronavirus pandemic to trick users into downloading dangerous malware that can steal their passwords and credit card data*. Retrieved from Daily Mail: https://www.dailymail.co.uk/sciencetech/article-8250737/Kaspersky-detects-fake-NHS-site-steals-credit-card-data.html

Christian, P. (2020, October 08). *Risky business: survey shows majority of people use work devices for personal use*. Retrieved from Malwarebytes: https://blog.malwarebytes.com/malwarebytes-news/2020/10/work-devices-for-personal-use/

Cisco. (2020, June 16). *free Webex Teams client - overview*. Retrieved from Cisco community: https://community.cisco.com/t5/collaboration-voice-and-video/free-webex-teams-client-overview/

Clymo, R. (2020, April 20). *Hackers exploit HMRC Coronavirus Job Retention Scheme with phishing email scam*. Retrieved from TechRadar: https://www.techradar.com/uk/news/hackers-exploit-hmrc-coronavirus-job-retention-scheme-with-phishing-email-scam

Cook, A. (2020, Mar 16). *COVID-19: Companies and Verticals at Risk for Cyber Attacks*. Retrieved from Digital Shadows: https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/

Cornwall, C. (2020, July 17). *Final Framework Homeworking Policy v1.6 17th July 2020*. Retrieved from NHS East and North Hertfordshire CCG: https://www.enhertsccg.nhs.uk/sites/default/files/documents/Aug2020/FIN

AL%20Framework%20Homeworking%20Policy%20v1.6%20%2017th%20July%202020.pdf

CyberArk. (2020, June 03). *CyberArk - Remote Work Study: How Cyber Habits at Home Threaten Corporate Network Security*. Retrieved from CyberArk: https://investors.cyberark.com/press-releases/press-release-details/2020/Remote-Work-Study-How-Cyber-Habits-at-Home-Threaten-Corporate-Network-Security/default.aspx

Deyan, G. (2020, September 13). *41 Stunning BYOD Stats and Facts to Know in 2020*. Retrieved from Techjury: https://techjury.net/blog/byod/

HM Government, Department for Digital, Culture, Media & Sport. (2018, Jan 16). *Cyber Essentials Scheme: overview*. Retrieved from https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Information Commissioner's Office (ICO). (2018, May 25). *Guide to the General Data Protection Regulation (GDPR)*. Retrieved from Information Commissioner's Office (ICO): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

ISO. (2018, July 01). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. Retrieved from ISO: https://www.iso.org/standard/75281.html

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.* TechRxiv.

Kundaliya, D. (2020, June 15). *One in three Britons targeted by scammers since the start of coronavirus crisis, Citizens Advice reveals*. Retrieved from Compting: https://www.computing.co.uk/news/4016501/britons-targeted-scammers-start-coronavirus-crisis-citizens-advice-reveals

Lallie, H., Shepherd, L., Nurse, J., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. *arXiv:2006.11929*.

London Councils. (2020, August 06). *Merton - Home working Policy* . Retrieved from London Councils: https://www.londoncouncils.gov.uk/node/3265

Marotti, A. (2020, Apr 02). *Zoom video meetings are being interrupted by hackers spewing hate speech and showing porn. It's called 'Zoombombing.' Here's how to prevent it.* Retrieved from ChicagoTribune: https://www.chicagotribune.com/coronavirus/ct-coronavirus-zoombombing-20200401-wf2pvzqhbngitankuokvinvk2m-story.html

McCorkell, A. (2020, June 01). *Industry experts warn of new Covid-19 scams including NHS Test & Trace scheme exploit*. Retrieved from SC Magazine UK: https://www.scmagazineuk.com/industry-experts-warn-new-covid-19-scams-including-nhs-test-trace-scheme-exploit/article/1684834

Morning Consult + IBM Security. (2020). *Work From Home Study - Survey Results.* IBM.

National Cyber Security Centre (NCSC). (2020, April 02). *Home working: preparing your organisation and staff*. Retrieved from National Cyber

Security Centre (NCSC): https://www.ncsc.gov.uk/guidance/home-working

National Cyber Security Centre (NCSC). (2020, May 07). *NCSC shines light on scams being foiled via pioneering new reporting service*. Retrieved from National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/news/cyber-experts-shine-light-on-online-scams

NCSC and US' Department of Homeland Security Cybersecurity and Infrastructure Security Agency. (n.d.).

NIST. (2012, Sept 01). *Guide for Conducting Risk Assessments.* Retrieved from National Institute of Standards and Technology (NIST): https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Ofcom. (2020, April 09). *Advice for consumers: coronavirus scam calls and texts: We have received reports of scam calls and texts relating to the coronavirus, or Covid-19.* Retrieved from Ofcom: https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/coronavirus-scam-calls-and-texts

Rodger, J. (2020, Mar 25). *The school meals coronavirus text scam which could trick parents out of thousands*. Retrieved from Birmingham Mail: https://www.birminghammail.co.uk/news/midlands-news/school-meals-coronavirus-text-scam-17975311

SANS Institute. (2020, Mar 19). *SANS Security Awareness Work-from-Home Deployment Kit*. Retrieved from SANS Security Awareness: https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

Schlarman, S. (2016, June 08). *CYBER RISK APPETITE: Defining and Understanding Risk in the Modern Enterprise.* Retrieved from RSA: https://www.rsa.com/en-us/blog/2016-06/cyber-risk-appetite-defining-understanding-risk-modern-enterprise

Schneier, B. (2020, Mar 19). *Work-from-Home Security Advice*. Retrieved from Schneier on Security : https://www.schneier.com/blog/archives/2020/03/work-from-home_.html

Sheva, B. (2020, June 09). *Morphisec Releases Work-From-Home Employee Cybersecurity Threat Index*. Retrieved from Morphisec: https://blog.morphisec.com/newsroom/morphisec-releases-work-from-home-employee-cybersecurity-threat-index

Silberman, A. (2020, July 30). *7 Best Practices for Securely Enabling Remote Work*. Retrieved from CyberArk: https://www.cyberark.com/resources/blog/7-best-practices-for-securely-enabling-remote-work

Stein, S., & Jacobs, J. (2020, Mar 20). *Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

Swinhoe, D. (2020, May 06). *UK cybersecurity statistics you need to know*. Retrieved from CSO Online:

https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html

Tidy, J. (2020, Mar 13). *Coronavirus: How hackers are preying on fears of Covid-19*. Retrieved from BBC: https://www.bbc.co.uk/news/technology-51838468

UK NCSC and the US DHS CISA. (2020, April 08). *Advisory: COVID-19 Exploited by Malicious Cyber Actors*. Retrieved from National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience—Cybersecurity Response to COVID-19. *IT Professional*, 4-10.

Woodside, S. (2020, Mar 19). *HIPAA @ Home: How to Keep Your Remote Workers Cybersecure Out of the Office*. Retrieved from MedStack: https://medstack.co/blog/hipaa-home-how-to-keep-your-remote-workers-cybersecure-out-of-the-office/

BIOGRAPHICAL NOTES

Max Hashem Eiza received his MSc and PhD from Brunel University London, UK in 2010 and 2015 respectively. After that, he joined Liverpool John Moores University (LJMU), UK as a research assistant in cybersecurity. Since 2016, he is working as a lecturer in cybersecurity at the University of Central Lancashire (UCLan), UK. Max's research is centred on cybersecurity and data privacy with the aim of developing novel schemes/protocols for various applications. Specifically, his research interests encompass the emerging security, privacy, trust, and identity management issues in the following areas: Vehicular Networks, Internet of Things, Big Data, Cloud Computing, Smart Grid, and Smart City.

Romanus I. Okeke is a Lecturer in Operations & Project Management at the University of Central Lancashire, UK where he received MSc in Computing and PhD in Information Systems & Operations Management in 2010 and 2015 respectively. From 2011 to date he has successfully led multidisciplinary research projects in identity theft prevention, intelligence operations, data analytics and decision modelling as a Postdoc Research Associate at Lancashire Constabulary Hutton and Office for Students UK and Postdoc Research Fellow at Institute of Security & Information Systems at the LSBE. His research interests span across Cybersecurity, Data Science & Cloud Computing. He is an Associate Fellow of UK Higher Education Academy, a member of The Society of Research Software Engineering, UK, The Royal Statistical Society and The Institute of Operations Management, UK.

John Dempsey joined UCLan as a Lecturer in 2000 where he has held several responsibilities; he is currently the course leader for the Forensic Computing and Security course and the University Digital Safety Advocate. John achieved his MRes in Child Computer Interaction in 2016 and is currently completing his PhD. His main research focus is around helping children take mindful decisions when

disclosing potentially private information in an online setting. John's teaching interests include Digital Forensics and Cyber Security. He is a member of the British Computer Society and Fellow of the Higher Education Academy (FHEA).

Vinh-Thong Ta: Vinh Thong Ta received the MSc degree in 2008 in computer science/IT security from the Budapest University of Technology and Economics (BUTE). He earned the PhD degree in 2014 in IT security from the Budapest University of Technology and Economics (BUTE), in the Laboratory of Cryptography and System Security (CrySyS Lab). He worked as a researcher at Institut National de Recherche en Informatique et en Automatique (INRIA), in the group PRIVATICS, where he worked on privacy by design and accountability areas. He joined UCLan in 2015 where he currently holds a senior lecturer position in the School of Psychology and Computer Science. His teaching and research interests include Network Security, Cryptography, IT Security Management, Malware Analysis, Penetration Testing, Computer Forensic, Game Theory and Machine Learning in Security. He is member of the British Computer Society (BCS) and Fellow of Higher Education Academy (FHEA).

REFERENCE

Reference to this paper should be made as follows: Eiza, M.H., Okeke, R.I., Dempsey, J. & Ta, V.T. (2020). Keep Calm and Carry on with Cybersecurity @Home: A Framework for Securing Homeworking IT Environment. *International Journal on Cyber Situational Awareness*, Vol. 5, No. 1, ppxx-yy