© Universiti Tun Hussein Onn Malaysia Publisher's Office

JTS

Journal of Techno Social

http://penerbit.uthm.edu.my/ojs/index.php/jts
ISSN : 2229-8940 e-ISSN : 2600-7940

Cybersecurity Threats and Best Practices of Working from Home

Syarifah Hanan Syed Faisal[1], Fadillah Ismail[1]*

[1]Faculty of Technology and Business Management,
Universiti Tun Hussein Onn Malaysia, 86400 MALAYSIA

*Corresponding Author

DOI: https://doi.org/10.30880/jts.2022.13.02.001
Received 01 January 2021; Accepted 09 August 2021; Available online 10 January 2022

Abstract: The concept of working from home due to the transmission of COVID-19 is not a new culture. In this era of pandemic, this has become a new norm in almost all sectors of employment. The concept of working from home demands the use of digital equipment and internet services. This situation however, has exposed the employees to cybersecurity risks as well as the employers. According to Cyber Security Malaysia (CSM), a total of 4,596 reports were made on cybercrime cases, earlier this year until April. Therefore, this paper will examine the effects of working from home and the threats of cybercrime. Also, this paper will provide the possible solutions to overcome this problem.

Keywords: Cybersecurity, working from home, cybersecurity threats

1. Introduction

The COVID-19 pandemic has urged people worldwide to stay at home, as the number of infection cases increases. The government has decided to command 'lockdown' to the country to flatten the curve of COVID-19 transmission. This current command has led to a change of working manner; people need to work from home using digital network communications and devices for their safety and health. To go through these changes, the employees need to have awareness and knowledge of cybersecurity and cybercrime. Cybercriminals are taking this into an advantage by being sneaky and spreading panic messages and warnings to digital users.

Working from home is a new working environment nowadays. It is also known as telecommunicating or working remotely. It is a concept where people can do their work from home. Through this concept, flexible working hours are given for employees to finish their tasks as assigned by their employers. It contributes significantly to delivering work-life balance to both employee and company by accomplishing the work. It is an approach which the internet and mobility are activated, regardless of the job's physical location. It can be concluded that employees work remotely from home or irrespective of any places (MBA Skool, 2020).

According to Seemma, Nandhini, and Sowmiya (2018), cybersecurity is defined as protecting an interconnection system where hardware, software, and database are included in cyberattacking. Enterprises and organisations usually use cybersecurity and physical security for their database information centre and other computerised systems to be safe from unauthorised access. It is designed for cybersecurity for maintaining confidential data information. According to De Groot (2020), cybersecurity is related to technologies, processes, and practices designed to protect digital networks, devices, and database information. Other than that, it is also designed to preserve computerised programs such as firmware, operating systems, mobile applications, and cloud services from unauthorised access and damage due to cyber threats. It also refers to information technology security. By referring to these two definitions above, it can conclude that cybersecurity is an essential role in the cyber world network.

A cybersecurity threat of cyberattack is a possible malicious action directed at data destruction, data theft, or in general, digital life alteration. Cyberattacks include malicious software, privacy violations, attacks on Denial of Service

Corresponding author: fadillah@uthm.edu.my

(DoS), and other network attacks. Cyber threats often relate to the likelihood of a successful cyberattack, which would obtain unauthorised access, destroy, interrupt or rob an IT asset, a computer network, intellectual property (IP), or some other sensitive data type. Cyberattacks may be generated from remote locations by trusted users in the enterprise or by unauthorised parties (Tunggal, 2020).

2. Best Practices of Working from Home (WFH) To Maintain Productivity among Employees

On March 18, 2020, the Government of Malaysia officially ordered Movement Control Order (MCO) to flatten the COVID-19 transmission curve that has led the organisations to work from home. Working from home has become a new norm that many organisations shifted from traditional operating methods to full or partial WFH. The transmission has been smoother for some companies, especially if their employees are already knowledgeable in working remotely with the needs of technology available before the MCO (New Straits Times, 2020). However, despite being at home while working, there will be at-home distractions. There is a need to acknowledge how to balance our commitment to chores at home and work tasks. Further discussion will be about the practices of working from home.

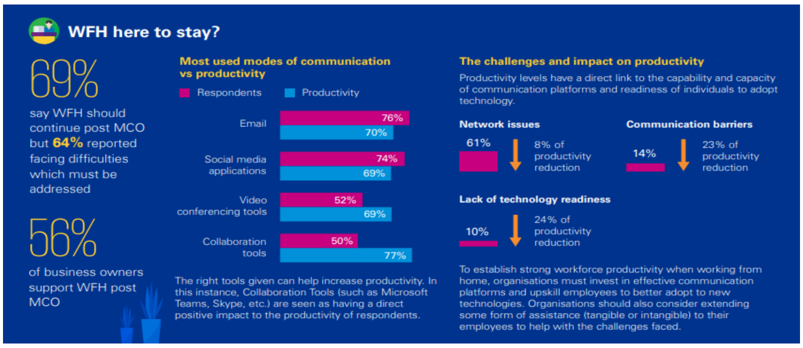
Firstly, maintain healthy and consistent connections with supervisors by communicating openly and sometimes with project managers and, where it is possible to allow for flexibility. Replace casual conversations at the office with e-mails and texts, better managing up by being clear about due dates, priorities, and expectations based on what is needed from the managers or what they need from the employees. Prioritise what's more important, urgent, and neither then explore how to manage those items together (Lane, Mullen, & Costa, 2020).

Next, make use of the user-friendly time-management app or external monitoring aid. These can be helpful to keep us organised and on track with deadlines for our job tasks. Setting timers on our phones or watches can be one of the right choices to balance our work tasks and chores at home. Moreover, we have to be flexible with ourselves by respecting that we need leisure time despite the efforts we had given to our work. Thirdly, differentiate work hours and personal time because it is crucial to set boundaries on our work hours. It can prevent a compulsion to work around the clock because working can be difficult for one's family.

Furthermore, different workspaces and living spaces can be crucial while working from home. It can be done by leaving the living space when it is time to work by entering a productive and new space to tour job tasks and have meetings with other colleagues. It can help set up a new workspace into an office space to have a sense of normalcy. Other than that, it is crucial to maintain a healthy and acceptable level of productivity at work by keeping a de-cluttered workspace. A messy workspace can be challenging for us to stay organised emotionally and mentally (Lane et al., 2020). These practices of working from home can influence the productivity of the employees when working from home.

3. Impact of Working from Home during COVID-19

Over 3,000 respondents in Malaysia expected working from home (WFH) to be a long-lasting procedure in this new norm reality. COVID-19 pandemic has pushed the worldwide workforce to unintentionally into a large working remotely experiment. Globally, the companies adopted rapidly working from home measures to continue their operations. Between April 7 to May 19, 2020, a public survey has conducted by Klynveld Peat Marwick Goerdeler (KPMG) Malaysia. It is an effort to have an understanding of the social well-being of working from home. This effort can be used as a result of the COVID-19 pandemic (KPMG Malaysia, 2020). The survey results have comprehensive insights into the impact and challenges towards productivity while working from home.



The right tools given can help increase productivity. In this instance, Collaboration Tools (such as Microsoft Teams, Skype, etc.) are seen as having a direct positive impact to the productivity of respondents.

Productivity levels have a direct link to the capability and capacity of communication platforms and readiness of individuals to adopt technology.

To establish strong workforce productivity when working from home, organisations must invest in effective communication platforms and upskill employees to better adopt to new technologies. Organisations should also consider extending some form of assistance (tangible or intangible) to their employees to help with the challenges faced.

Fig. 1 - The most used modes of communication vs productivity and the challenges and impact on productivity

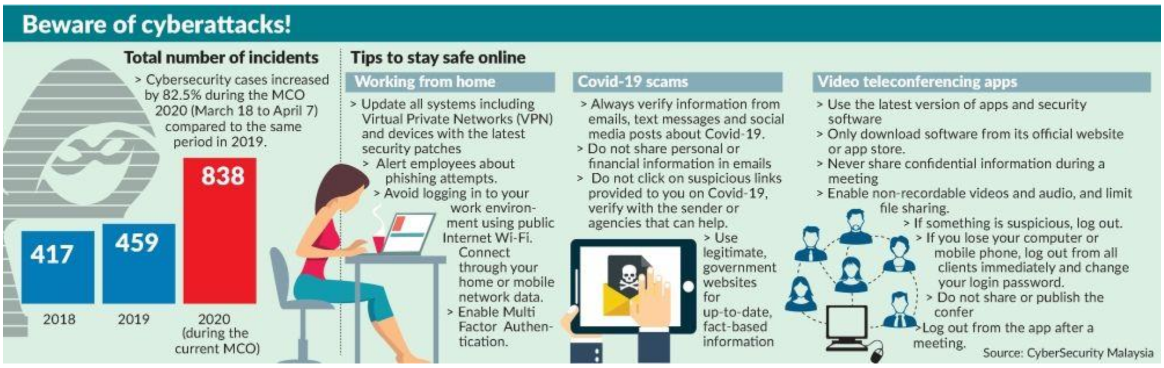
Based on Figure 1 above, 69% say that working from home should continue post Movement Control Order (MCO) and 56% of business owners support working from home post Movement Control Order (MCO). However, 64% reported facing difficulties: network issues, communications barriers, and lack of technology readiness. These difficulties have influenced productivity among workers while working from home. The statistics data showed that 61% of respondents have network issues that have led to 8% productivity reduction. Then, 14% of respondents have communication barriers that have led to 23% of productivity reduction, and 10% of respondents have a lack of technology readiness that has led to 24% of productivity reduction. So the organisations have to provide effective communication platforms and train employees better in adopting the use of new technologies to create firm workforce productivity when working from home (KPMG Malaysia, 2020).

Other than the challenges towards employees' productivity, a survey of 104 participants has been conducted related to the psychological impact on individuals working from home during COVID-19 in Malaysia (Marimuthu & Vasudevan, 2020). Of the 104 participants surveyed, 81 were scored 3 out of 5 for stress and pressure while working from home during COVID-19. Furthermore, 81 participants recorded that they were depressed, irritated, and sleep disturbed during COVID-19. It indicates that the pandemic has mentally influenced workers who work from home during the COVID-19 Movement Control Order (MCO). However, despite the insights given, these data can also lead to some issues related to cybersecurity threats that could happen in Malaysia.

4. Issues Related to Cybersecurity Threats during COVID-19 Pandemic Period

During this pandemic COVID-19, cybersecurity cases have risen by 82.5%. This current situation has led to the use of technologies increases that make cybersecurity cases occur. Cybersecurity Malaysia received 838 incident reports regarding cybersecurity threats since the beginning of the MCO period. Then, 18% of these total incidents involved local businesses, while other home consumers and others were involved. These reported cases are fraud, intrusion such as hacking or data breach attempts, and cyber harassment such as cyberstalking. Internet fraud cases like scams, phishing, or social engineering have been deceived victims into receiving their confidential information. Chief Executive Officer of Cybersecurity Malaysia, Datuk Dr Amirudin Abdul Wahab, said these incidents happened due to many people using the internet. He also highlighted that the environment is suitable for cybercriminals to strike, so cybersecurity is crucial during these times. It is because hackers want to ultimately profit from this pandemic by using virus-themed efforts at social modification, the selling of falsified surgical masks, and disseminating disinformation. (Meikeng, 2020).

Cybercriminals have been using COVID-19 as an excuse to trap the people by using malware attacks. Besides, established organisations are usually a good target for cybercriminals to make a larger-scale attack by a distributed denial of service (DDOS) to use the resources or make services to their intended buyers (Meikeng, 2020).



> Cybersecurity cases increased by 82.5% during the MCO 2020 (March 18 to April 7) compared to the same period in 2019.

> Update all systems including Virtual Private Networks (VPN) and devices with the latest security patches
> Alert employees about phishing attempts.
> Avoid logging in to your work environment using public Internet Wi-Fi. Connect through your home or mobile network data.
> Enable Multi Factor Authentication.

> Always verify information from emails, text messages and social media posts about Covid-19.
> Do not share personal or financial information in emails
> Do not click on suspicious links provided to you on Covid-19, verify with the sender or agencies that can help.
> Use legitimate, government websites for up-to-date, fact-based information

> Use the latest version of apps and security software
> Only download software from its official website or app store.
> Never share confidential information during a meeting
> Enable non-recordable videos and audio, and limit file sharing.
> If something is suspicious, log out.
> If you lose your computer or mobile phone, log out from all clients immediately and change your login password.
> Do not share or publish the confer
>Log out from the app after a meeting.

Source: CyberSecurity Malaysia

Fig. 2 - The total number of cyberattack incidents

Recently, fraud topping the list at 5,697 cases among the total of 7,765 incidents in the Cybersecurity Malaysia reports during the first eight months of this year. Besides fraud, hacking, which includes intrusion incidences, ranked second with 993 cases, followed by cyber harassment with 409 instances and malicious cases with 351 cases during COVID-19. According to Datuk Dr Amirudin Abdul Wahab, expected cases to rise between 11,000 and 12,000 based on the current trend because cybercriminals will try to get profits from the most people who are online these days through scams or fraudulent schemes. He said that the regulatory body expects the number to surpass last year's record of 10.772 by year-end. "Through our Cyber999 Help Centre, we found that the highest number of cases were recorded in April, which was during the Movement Control Order period. At that time, many people had to work from home and did their shopping online," said the CEO of Cybersecurity Malaysia. He added that the problem they have to deal with is exposure to cybersecurity as they embrace the new norm post-COVID19 (Bernama, 2020)

4. What to Do about Cybersecurity Risks

Current security solutions in network-based cyberspace give an open the door to the attacker by communicating first before authentication thereby leaving a black hole for an attacker to enter the system before authentication (Deepak Puthal, Saraju P. Mohanty, Priyadarsi Nanda, & Uma Choppali, 2017). It is to ensure cybersecurity in employees working from home, and there are several things that organisations can do.

Information Technology services enhance business activities and provide business information on our doorstep. Information Technology infrastructure and services are an integral part of any business and are unavoidable in today's competitive business scenario (Veerasamy, Senthil, 2015). Information technology infrastructure such as laptops and internet access should be provided by employers considering information security policies, security software such as antivirus software, and updated firewalls and communication systems through encryption processes. Perimeter elements are devices or software that connect a corporate network to the outside world or interact with connection requests from the outside world first. For this hardware or software to be used and managed correctly, what needs to be protected, what threats are, and the organisation's needs should be determined (Goksel, Ibrahim, Mustafa, Murat, 2019). The provision of security perimeter by employers in accessing an organisation's data, network, and information systems such as virtual private networks (VPNs), the condition of passwords, and robust authentication systems, security mechanisms are necessary for dealing with suspicious network access.

If both are implemented, the risk of cybersecurity threats will be at a low level. With this, the information technology department or cybersecurity management unit can address cybersecurity threats more specifically. The parties involved can anticipate more specific types of attacks or cybersecurity threats that can create a high surge in its presence or threaten the organisation's digital environment. It can also focus more on critical cybersecurity points for an organisation such as financial and accounting systems, digital storage of shared file storage, user and corporate databases, organisational e-mail service systems, information systems, and server computers. It can also provide technical solutions and measurements in dealing with certain digital activities to employees, such as efficient and secure password management. It can also look at the cybersecurity of each organisational structure as a whole and identify groups of high-risk employees contributing to cybersecurity threats. The management team needs to plan a sound, efficient, and effective strategy in dealing with cybersecurity threats to enable working from home as a new norm.

5. Conclusion

In conclusion, employers and employees need to cooperate to avoid these issues from deteriorating their performance and profits. A licensed counsellor Surenthiran Pillai Venayagam Pillai suggested that employers could alleviate their workers' emotional stress by offering physical, psychological, and political assistance. Employers should help workers build a proper home workspace by supplying ergonomic seats, appropriate internet quota, or other items to operate smoothly for physical service. For therapeutic help, employers should include or build platforms to ensure workers have access to health interventions, such as professional sharing or therapy. Employers must also develop specific uniform protocols for workers to follow to eliminate performance issues (Krishnan, 2020).

Moreover, to separate these machines, companies can enforce a quarantine network. The workplace network's guest Wi-Fi feature makes it simple to run and guarantees efficiency that can proceed with the additional protection of quickly blocking or disconnecting insecure gadgets. Because employees who work in a less organised setting from home might be more likely to let their security guards on the security front and press on the links, they would not usually be in the workplace. Just one incorrect click by an employee will have drastic consequences and losses for the organisation such as records, credibility, and assets. Furthermore, several company-issued computers will not be able to deploy or execute software upgrades, which would increase the volatility of unpatched network devices, exposing companies to cybersecurity risks (Hoong, 2020).

Many workers who work remotely have been using their own devices, but not those issued by companies, which creates another safety blackboard for companies that could open doors for cybercriminals to enter the corporate network unprotected or easily entered. To detect and neutralise evasion risks, companies must improve their internal cyber defence infrastructures. With a live discovery or response mechanism, an endpoint detection or response approach enables companies to rapidly respond to and address possible cyber problems with a single panel (Hoong, 2020).

Other than that, the correct technology is just one aspect of the cybersecurity equation, whether workers are at home or beginning to go back to work. Employees play an essential role in deterring cyber threats like whether they operate on their laptop or a company-owned one. IT agencies must reiterate to their staff the value of keeping stringent metrics on cyber protection, which are easily ignored when they work from home or when they come to work. In addition to training cybersecurity staff and raising awareness about phishing and suspicious connexions, IT managers can provide workers with a simple way to monitor cybersecurity concerns, such as an easy to recall e-mail address (Hoong, 2020).

Whilst, luckily, the potential danger to health posed by the COVID-19 pandemic in Malaysia is easing, the cybersecurity problems affecting companies attributable to workers continuing to operate from home or beginning the return to the workplace, taking equipment with them, must remain a top priority for IT agencies. A mixture of the next decade's security technologies, system management, and the development of cyber-conscious personnel are necessary for any company to keep ahead of the cyber threats that continue to bomb us at this period (Hoong, 2020).

Acknowledgement

The authors would like to acknowledge the Faculty of Technology and Business Management, Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, Johor.

References

Bernama. (2020). Spike in cyber threats; fraud tops list. Retrieved October 30, 2020, from New Straits Times Online website: https://www.nst.com.my/news/nation/2020/09/622861/spike-cyber-threats-fraud-tops-list

De Groot, J. (2020). What is Cyber Security? Definition, Best Practices & More | Digital Guardian. Retrieved October 27, 2020, from Digital Guardian's Blog website: https://digitalguardian.com/blog/what-cyber-security

Deepak Puthal, Saraju P. Mohanty, Priyadarsi Nanda, and Uma Choppali, 2017. Building Security Perimeters to Protect Network Systems against Cyber Threats. A novel way to avoid cyber threats. IEEE Consumer Electronics Magazine 6(4):24-27 · October 2017 DOI: 10.1109/MCE.2017.2714744.

Goksel Uctu, Mustafa Alkan, Ibrahim Alper Dogru, Murat (2019). Perimeter Network Security Solutions: A Survey. DOI: 10.1109/ISMSIT.2019.893282. Conference: 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). https://www.researchgate.net/publication/337978630

Hoong, W. J. (2020). BERNAMA - Cybersecurity in a flexible working culture. Retrieved November 3, 2020, from BERNAMA Online website: https://www.bernama.com/en/thoughts/news.php?id=1860524

KPMG Malaysia. (2020, July 7). The Work-From-Home Revolution - KPMG Malaysia. Retrieved October 30, 2020, from KPMG Malaysia Online website: https://home.kpmg/my/en/home/insights/2020/03/the-business-implications-of-coronavirus/the-work-from-home-revolution.html

Krishnan, D. B. (2020). WFH: Experts speak about issues to be addressed. Retrieved November 3, 2020, from New Straits Times Online website: https://www.nst.com.my/news/nation/2020/10/634557/wfh-experts-speak-about-issues-be-addressed

Lane, I. A., Mullen, M.G., & Costa, A. (2020). Working from Home During the COVID-19 Pandemic: Tips and Strategies to Maintain Productivity & Connectedness. *Worcester, MA: University of Massachusetts Medical School, Department of Psychiatry, Implementation Science and Practice Advances Research Center (ISPARC), Transitions to Adulthood Center for Research.*, *17*(5), 1–9. Retrieved from https://f.hubspotusercontent20.net/hubfs/2914128/Upbeat Memo_Teaching_From_Home_Survey_June_24_2020.pdf

Marimuthu, P., & Vasudevan, H. (2020). *the Psychological Impact of Working From Home During*. (June).

MBA Skool. (2020). Work From Home Definition & Importance | Human Resources (HR) Dictionary | MBA Skool-Study.Learn.Share. Retrieved October 29, 2020, from mBa sKOOL.com website: https://www.mbaskool.com/business-concepts/human-resources-hr-terms/16870-work-from-home.html

Meikeng, Y. (2020). Cybersecurity cases rise by 82.5% | The Star. Retrieved October 29, 2020, from The Star Online website: https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825

New Straits Times. (2020). The work from home revolution. Retrieved October 31, 2020, from New Straits Times Online website: https://www.nst.com.my/news/nation/2020/04/584802/work-home-revolution

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(11), 125-128.

Tunggal, A. T. (2020). What is a Cyber Threat? | UpGuard. Retrieved November 2, 2020, from UpGuard website: https://www.upguard.com/blog/cyber-threat

Veerasamy, Senthil, 2015, Information Technology Services Issues and challenges with a case study in small medium enterprises. International Journal of system and software engineering. DOI 10.21863/ijsse/2012.3.2.011