Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
CHAPTER 3

Working from home users at risk of COVID-19 ransomware attacks

Anthony An Duong\textsuperscript{a}, Abubakar Bello\textsuperscript{b}, and Alana Maurushat\textsuperscript{a}

\textsuperscript{a}School of Social Sciences, Western Sydney University, Sydney, NSW, Australia, \textsuperscript{b}Cyber Security and Behaviour, School of Social Sciences, Western Sydney University, Sydney, NSW, Australia

1 Introduction

The year 2020 has seen an increase in online usage as many would find themselves working and studying from home. This was due to the COVID-19 pandemic where it has forced many people to stay at home. It became a situation where accessing the internet has become a necessary requirement as working from home user must be able to continue their organizational duties as well as to be up to date with their prescribed news about the COVID-19 pandemic.

First accounts on the coronavirus were reported on December 2019 and has gradually spread to multiple countries around the world (Nebehay, 2020). In extreme circumstances, the coronavirus is very dangerous as it can cause respiratory infection which may lead to death (World Health Organisation, 2020). As of March 2020, the COVID-19 cases have risen to 7,50,000 and death toll was around 36,000 (The Guardian, 2020). Due to the alarming cases and death tolls, it has led many organizations to move their employees to work from home to reduce the spread of the virus and to adhere to quarantine rules as well. However, sadly, on October 15, 2020, the global death toll has reached more than one million (Worldometer, 2020). The year 2020 was indeed a difficult year for many people. Many working from home users would have to face the new reality to work online.
Many working from home users are required to use an electronic device of their own choice so that they can continue their studies or organizational duties. Furthermore, maintaining communication with others during the COVID-19 pandemic has become a necessary mission as well. For working from home user to be able to continue their studies, work, and communication with others, it does require them to be able to connect to the internet which has led to cyber-security concerns. As such, the concerns are mainly around the fact that many working from home user may not have a strong understanding that they may have weak security control measures (KPMG, 2020). Having a weak security home environment could lead to cyber-criminals exploiting those vulnerabilities. The COVID-19 pandemic has pushed many people to work from home. However, it is believed that the COVID-19 pandemic would open more doors for cyber-criminals (Coker, 2020) as there are many people working online who may not be fully aware that they can be vulnerable to potential cyber-attacks.

One of the cyber-attacks that cyber-criminals would most likely launch during the COVID-19 pandemic is ransomware. Ransomware is one of many dangerous malicious software that can infect a working from home user’s electronic device. As such, it has the capabilities to prevent the user from having access to their respective data. Access to their data would be provided if the user is able to pay the demanded ransom to the cyber-criminals (Richardson & North, 2017). The year 2020 has seen an increase in ransomware usage by cyber-criminals (Skybox Security, 2020). The increase in ransomware usage is an indicator that cyber-criminal is using this opportunity to exploit working from home users during the COVID-19 pandemic. As such, many working from home users could be susceptible to the ransomware attack which can produce many challenges ahead.

Many of the challenges against ransomware may also include that victims and organization may not be able to identify genuine sources, mobile phone mitigation challenges against ransomware, ransomware has strong encryption algorithm, increase in digital extortion, targeting more organization than individuals, and most concerning that many victims are willing to pay the ransom to the cyber-criminals. Ransomware is the most dangerous malware that can be used by cyber-criminals during the COVID-19 pandemic. However, cyber-criminals must use an attack vector to deliver the ransomware to working from home user.

The attack vectors that cyber-criminals can use to deliver ransomware are social engineering, phishing, trojan, remote desktop protocol, drive-by download, and malvertising. Social engineering requires the cyber-criminals to interact with the target to build trust for the purpose of gaining information (Krombholz et al., 2015). Social engineers may also send phishing emails in the hope that victims would interact with the malicious contents where the possibilities of installing a trojan can happen. Trojan is
normally considered a legitimate software (Grace, 2020) although it could potentially be ransomware itself. Cyber-criminals may wish to use a remote desktop protocol to remotely access (Arntz, 2018) a working from home user’s electronic device to install ransomware. Drive-by download and malvertising are other ways for cyber-criminals to distribute ransomware. During the COVID-19 pandemic, working from home users may face the possibility of ransomware attacks via the six attack vectors. Furthermore, this had led to the need to understand how it is important to implement strong security measures against any ransomware attacks during the COVID-19 pandemic.

Normally mitigation against ransomware attacks would normally work if the individual and organization have strong comprehension that their data is extremely important, and action must be taken to protect their assets. There are existing defense mechanisms that working from home user can implement in their own home environment. Web content filtering, black and white listing, seeking professional consultation, intrusion detection system, and firewall are examples of existing defense mechanism against ransomware attacks although they have control gaps within them. Thus, a mitigation model against ransomware is developed to assist working from home user to understand the security measures that are required to mitigate against potential ransomware. This paper starts with an overview of ransomware followed by issues and challenges with ransomware, ransomware attack vectors, existing defense mechanisms and control gaps, and mitigation model against ransomware.

## 2 Overview of ransomware

### 2.1 What is ransomware

Ransomware is a dangerous malware that has the capabilities to prevent users from accessing their data (refer to Fig. 1). Normally, if a user wishes to have access to their data again, they are required to pay the ransom so that the cyber-criminal can provide them with a private key to decrypt their data (Richardson & North, 2017). Normally, cyber-criminals

![FIG. 1 Stages in ransomware.](image-url)
would prefer the victim to pay the ransom in a form of Bitcoin as these are usually encrypted and it would make it harder to trace the transaction (Newby & Razmazma, 2016). Ransomware has a dangerous encryption algorithm that can prevent the user from accessing their data, although it is also capable to disrupt other electronic devices.

Normally, ransomware is used to target personal computer devices as they do generally attract cyber-criminals. However, ransomware can have the abilities to also attack mobile phone devices. As such, it works by altering the PIN on the personal mobile devices forcing the victim to pay the ransom so that they can receive the new PIN to unlock it (Zetter, 2015). Due to the malware abilities to target personal computers and mobile phone devices, ransomware may be a preferable choice for cyber-criminals to use to launch an attack onto their victims who are working from home. Not only the malware can encrypt victim’s data, but it does also tend to force their victims to pay the ransom as well. As such, symantec have estimated that ransomware annually extorted millions of their victims and has noted that forwarding the ransom to cyber-criminals would not guarantee that their data will be released back to them (Zetter, 2015). Over the years, cyber-criminals have used ransomware to cause a lot of disruption to their targets. Ransomware has become more sophisticated as well as more modernized for cyber-criminals. To understand how ransomware grew to be the most dangerous and atrocious malware, it is important to discuss it origins as well as how it grew over the years. The first ransomware was first utilized in 1989 which was called the AIDS Trojan ransomware.

2.2 Ransomware evolution

In 1989, AIDS Trojan ransomware was the first-known ransomware that was organized to be deployed through 20,000 infected floppy disks (Johansen, 2019). The intention was to maliciously target the staff members at the AIDS research project and World Health Organization (WHO) (Trautman & Ormerod, 2018). From the infect computer, the AIDS ransomware would encrypt data files as well as hide the directory folders that was in the C drive. AIDS silently stay dormant in the computer systems and after the system undergoes 90 restarts, the ransomware would get activated. Due to the technology at the time, the AIDS ransomware could not propagate on a large scale as there were less computer connectivity (Yaqoob et al., 2017). The introduction of ransomware was indeed terrifying at the time. AIDS ransomware has set an example where a malicious software is capable to lock people out from accessing their files. As technology continues to advance, so would ransomware.
The AIDS ransomware was the beginning of the making of many more potential ransomwares. Among many of the ransomware programs that were later introduced, cyber-criminals had attempted to find ways to improve it from its predecessor. But at the same time would implement different ways to deliver the malware to its victims. In 2005, Trojan.Gpcoder was introduced and spread via phishing emails (Sjouwerman, 2015). Luckily at the time, Trojan.Gpcoder has very weak encryption and it was very easy to overcome its challenges (Richardson & North, 2017). Trojan. Gpcoder was not the most sophisticated ransomware but nevertheless has open more door for new ransomware to be introduced.

In the following year, Trojan.Cryzip was introduced in early 2006 which had the capabilities to copy files from the victims and deleting the original version from the user electronic device (Richardson & North, 2017) which may be the first kind of ransomware to do so. Locker ransomware had begun to surface in 2007 where the attack had begun to spread towards the United States and Europe (Zetter, 2015). Ransomware started to become a major issue around 2011 as 30,000 new strain was introduced in the first quarter, another 30,000 introduced in the second quarter, and third quarter saw another 60,000 new strains (Sjouwerman, 2015). Citadel is a toolkit that was introduced in 2012 which can dispense and produce ransomware (Segura, 2016). Up until 2012, ransomware was growing at a rapid pace and has become the most used malware by cyber-criminals and has grown to be more atrocious over the following years.

In 2013, CryptoLocker was introduced where it used a private and public cryptography to encrypt victim’s data (Richardson & North, 2017). Initially, CryptoLocker was delivered via Gameover ZeuS banking Trojan botnet but later cyber-criminals used emails to distribute the malware where they claimed to be FedEx or UPS (Zetter, 2015). Victim would normally have up to 72h to pay the ransom (Sjouwerman, 2015). Between September 2013 and May 2014, approximately 5,00,000 victims had the CryptoLocker ransomware infection (Cannell, 2016). The end of 2015 was devastating as the FBI reported that all victims of ransomware had paid approximately 27 million dollars to their extortionist (Cannell, 2016) and this would no doubt continue to rise over the next coming years as ransomware becomes more advanced in terms of encryption as well as extortion. It was clear at this point that ransomware was indeed becoming more weaponized by cyber-criminals and has continued to extort more victims. This would have had a negative financial and emotional impact on the victims. The COVID-19 pandemic presents several opportunities for cyber-criminals as many people are working from home and are connected to the cyberspace.

The COVID-19 pandemic has forced many organizations and their respective employees to work from home. Due to the unexpected adaptation to work from home, it is possible that working from home user are not
prepared for a new transition but at the same time may lack understand-
ing of the cyber-risk during the COVID-19 pandemic. As such, cyber-
criminals would see this as a great opportunity to exploit working from home users during the COVID-19 pandemic. The first half of 2020 saw an alarming 72% increase in ransomware attack growth (Skybox Security, 2020). The possibility of such an enormous growth may have been due to the weak security controls as well as the possibility of users being lured into phishing emails during the COVID-19 pandemic (KPMG, 2020).

The introduction of ransomware has indeed disrupted many busi-
tnesses, organizations, and victims. The malware itself has grown to become the most popular tool to be used by cyber-criminals. However, cyber-criminals would normally decide to use either a crypto or locker ransomware as these are the two common types used by extortionists.

2.3 Ransomware types

2.3.1 Crypto-ransomware

If the user were infected with crypto-ransomware and chooses to remove it from their media storage device, this would still leave their data encrypted (Richardson & North, 2017). However, crypto-ransomware would leave the critical system files untouched which still allows the users to have some access to their device as the cyber-criminals would need the victim to pay the ransom via their infect electronic device (Savage, Coogan, & Lau, 2015). By using crypto ransomware, the victim would have to pay the ransom in bitcoins (Richardson & North, 2017) as this type of payment is untraceable (Rosenberg, 2015). This type of ransomware would be the first choice for cyber-criminal as the aim is to prevent the user from accessing their data as well as become unable to trace the cyber-criminal’s whereabouts.

2.3.2 Locker-ransomware

The second type is locker-ransomware where it prevents the user from accessing their electronic devices (Savage et al., 2015). The data itself that is on the user’s electronic device would remain untouched. In this case, the user may choose to easily remove their media storage from their electronic device, making the likelihood that their data is not damage or encrypted. Usually the payment would be present in payment vouchers where the victim is required to send the payment codes (Savage et al., 2015). Therefore, this type of ransomware is usually not the best choice for cyber-criminals as it is not the most effective way to extort their victims to pay the ransom.
Crypto-ransomware and locker-ransomware are the two types that can be used by cyber-criminals to extort their victims. It has been discussed that has grown to become a popular tool to be used by cyber-criminals which would produce many challenges ahead. These challenges against ransomware attacks would most likely be related to weak security controls measures within a person’s home environment as well as not realizing how easy it is for cyber-criminals to exploit those vulnerabilities.

3 Challenges and issues with ransomware

3.1 Internet of thing challenges against ransomware

In the digital age, individuals have started to embrace the benefits of using the Internet of Things (IoT). IoT has become an important aspect in people’s lives as it provides many ways to assist with their daily tasks or needs. As such, IoT has given individuals the ability to connect to their smart cars (Al-Fuqaha et al., 2015), homes (Ahmed et al., 2016), parking (Perera et al., 2013), utility meters (Sanduleac et al., 2016), healthy monitors (Ghosh et al., 2016), and other potential electronic applications. However, this may provide a several opportunities for cyber-criminals to exploit as IoT devices are programmed to store sensitive and personal information. Basically, IoT devices are data collectors and stores information like age, name, location, health details, and much more where the possibility of cyber-criminals stealing one’s identity is quite high (NortonLifeLock Employee, 2019). The concerns are mainly on not having strong defensive control for IoT or for users’ respective electronics devices. Developing security as well as designing preventative measures against ransomware attacks was perhaps considered challenging as well as quite alarming (Jing et al., 2014). The COVID-19 pandemic has forced most people to work from home but at the same time provided users with little protection against ransomware attacks.

Working from home users would utilize electronic or IoT devices to continue to perform their personal or organization duties. IoT does contain sensitive information which is why it has provided a high level of uncertainty as cyber-criminals may choose to launch a ransomware attack onto any desirable targets. Ransomware is much different from other traditional malware attacks as it has the capabilities to affect large working environments leading financial losses as well suffering from an information breach (Bertino & Islam, 2017). Once the breach is successful, the ransomware would hold the victim’s data hostage, may only allow restrict access to their electronic devices, demanding the ransom, and once the ransom is paid cyber-criminals may choose to decrypt the victim’s data (Yaqoob et al., 2017). If the user has failed to pay the ransom, the cyber-
criminals may wish to extend the payment deadline or permanently remove all data from the victim’s electronic device (Nassi et al., 2017).

3.2 Victims or organization may not know how to identify genuine sources

Considering that working from home has pushed people to move onto the internet, it could be quite difficult for them to identify genuine sources as cyber-criminals do have ways to lure working from user into their malicious deceptions. These malicious deceptions may lead the victim to install and execute a ransomware. As such, the challenges that arises with ransomware is that they can surreptitiously infiltrate computers using various unauthentic, malicious, and fraudulent applications (Bugeja et al., 2017). There are cases where the software would falsely generate an alarm that would make the user believe that their systems has been compromised and require them to pay the money for data recovery (Yaqoob et al., 2017).

3.3 Mobile phone mitigation challenges

Across the globe, ransomware has been identified as a threat to network and computer security (Gazet, 2010). Due to its covert nature, it has spread to hand-held mobile phone devices. Mobile detection approaches have not been effective to detect ransomware (Andronio et al., 2015) leaving billions of phone users to be vulnerable to ransomware attacks (Popoola, Ojewande, Sweetwilliams, John, & Atayero, 2017).

3.4 Ransomware has strong encryption algorithm

For cyber-criminals to extort their targets, they would usually launch a ransomware attack that can encrypt the files on the electronic device of the victim. Encrypting victims’ files has indeed become one of the many threats of ransomware as they are not usually easy to decrypt. By encrypting the victim’s files, the cyber-criminals would demand a high ransom so that they can decrypt the user’s files. The ransomware would encrypt the full hard drive or Computer’s Master File Table (MFT). Cyber-criminals would normally use trojans to deliver ransomware to their victims as it helps disguise the files as authentic. Within any computer security environment, advanced encryption can in fact be helpful to effectively protect sensitive information. But has been integrated into ransomware which has become a malicious tool for cyber-criminals to use and became a serious cyber-threat as ransomware are equipped with enhance algorithms to lock victim’s data (Popoola et al., 2017)
3.5 An increase in digital extortion

The number of online users and services would indeed continue to grow over many years to come. Due to the number of online users and services on the internet growing exponentially, it would indeed increase digital extortion (Bhardwaj, 2017). Over the years, ransomware has been rated as the highest cyber-threat because it has caused lots of disruption to many businesses (Brewer, 2016). Approximately 80% of ransomware attacks can discover vulnerabilities in flash application that are found in many businesses which can destructively propagate itself across the network holding many users or businesses hostages (Popoola et al., 2017). There are many working from home users and online services during the COVID-19 pandemic. Many would not realize that the cyber-criminals would also occupy the cyber-space who can exploit this opportunity to digitally further extort and to have a powerful financial gain from online businesses and working from home users.

3.6 Ransomware attacks are targeting more organizations than individuals

Nowadays, many cyber-criminals would choose to focus to target large organization than individuals. The shift from individual to large organization is that organization tends to hold enormous form of information and may have a large attack surface. For instance, in 2016, the Hollywood Presbyterian Medical Centre was attacked, and had to shut down due to being bit by a Crypto-ransomware. It had encrypted all information and files in their computer systems and had denied access to medical staff from retrieving patients’ sensitive and personal health archives (Everett, 2016). The Methodist Hospital is another example where Kentucky was lucky enough to retrieve and recover patient archives. The cyber-criminals had used stolen administrative credentials and had infect the Methodist Hospital network servers with SamSam ransomware (Popoola et al., 2017).

3.7 Many are willing to pay the ransom

If an organization was attacked by ransomware and has no form of backup, they may have little choice but to pay the ransom to the cyber-criminals to avoid the data being lost. As such, it was found that approximately 46% of organization had encountered a form of ransomware attack, and about 57% of those were medium-size organization and 53% were large organization. Many of these organizations were more than willing to pay the ransom (Popoola et al., 2017). Without a data recovery in place, organization would have little choice but to obey the cyber-criminal’s order and pay the ransom in exchange for their data.
In 2016, it was reported by Federal Bureau of Investigation (FBI) that one billion US dollar was loss from ransomware attacks (Popoola et al., 2017). The losses have demonstrated that many victims would be more than happy to pay the ransom so that they can have access to their data again. Approximately 40% of victims would indeed pay the ransom. In addition, it was found that 3 out of 4 ransomware attacks, cyber-criminals were more than happy to negotiate the ransom with the victim but usually would give on average a 28% reduction from the original demanded ransom (Popoola et al., 2017). Due to the alarming number of victims and organizations paying the ransom to cyber-criminals, it may demonstrate there are very little security controls measures against ransomware attacks. It is important for working from home user to be prepare and anticipate any ransomware attack, especially during the COVID-19 pandemic. For ransomware to be delivered and executed correctly, it does require the victim to either interact with the cyber-criminals directly, indirectly or may accidentally download and execute an unknown program or software. To spread and distribute ransomware, cyber-criminals may either use one or a combination of attack vectors to lure their victims.

4 Ransomware attack vectors

Ransomware is normally spread and distribute via social engineering, phishing, trojans, remote desktop protocol, drive-by downloads, and malvertising. Social engineering is to develop a relationship with their victim to extract personal and sensitive information from them. Other attacks vectors such as phishing, Trojan, Remote Desktop Protocol, Drive-by Downloads, and Malvertising can cause the same level of disruption but is reliant to be delivered via social engineering tactics. Due to the nature of social engineering, the victim may not be able to know whether they are communicating to a trustworthy source. Due to the COVID-19 pandemic, it is possible for cyber-criminals to distribute ransomware to working from home user by using the either of the six attack vectors.

4.1 Social engineering

The purpose of social engineering is to build trust but at the same time access and obtain information from potential victims and organization. Normally, social engineers would manipulate, influence, and deceive their targets to give away sensitive information (Krombholz et al., 2015). Employees may fall into social engineer’s trap if they believe that they were communicating with a trustworthy source or the user has failed to detect the deception from the cyber-criminals (Qin & Burgoon, 2007).
Usually, email is a common medium that social engineers would use to communicate to their targets (Krombholz et al., 2015). It is known to be the most convenient way to deceive their targets to visit a suspicious source where the victim may unintentionally install ransomware. In the digital era, it has given social engineers the ability to deceive and trick their victims. However, all cyber-criminals would have different intentions and would choose to adopt many different types of approaches to trick their targets. These approaches are typically either physical, social, reverse, technical, and socio-technical.

4.1.1 Types of social engineering

1. Physical approaches

The physical approaches would require the social engineer to physically obtain information by hand normally in a form of a piece of paper. There are some circumstances where employee would be required to dispose piles of paper into a recycling bin. In this case, it would no doubt make it more convenient for social engineers to find personal and sensitive information. This is commonly known as dumpster diving as it requires the social engineer to physically search through the recycling bin for information (Granger, 2001). Other physical approaches would involve theft and extortion (Krombholz et al., 2015). However, due to the COVID-19 pandemic, social engineers may be reluctant to use this approach. But nevertheless, there is a possibility that working from home user may decide to throw out documents. The electronic device specifications could be found within a recycling bin. After the social engineers have found the exact specification from the target’s electronic device, they may wish to practice how to install ransomware onto the model device before initiating the real attack.

2. Social approaches

This approach would require heavy reliance on socio-psychological methods like Cialdini’s principles of persuasion so that social engineers can trick their victims (Krombholz et al., 2015). To increase the success of the attack, social engineer would develop a relationship with the victim. An electronic device such as a phone is commonly used with this type of social engineering (Granger, 2001). As such, it is possible for working from home user to encounter this type of approach from social engineers.

3. Reverse social engineering

Reverse social engineering has three distinctive steps. The first step is to disrupt, destroy, and damage the target’s computer system which may involve disconnecting an employee from the organization’s network. The second step requires the social engineers to advertise themselves
making the victim believe that they are capable to resolve the problem. The final step is to convince the victim to give their password or install a software so that they can fix the issue (Krombholz et al., 2015). The software that could be install may very well be ransomware and working from home users may face this possibility.

4. Technical approaches

This method would normally be initiated over the internet. The goal is to gather information that they can find on the internet. Normally, search engines and social network platform are valuable information and tools for social engineers to use. If it was found that a user who uses the same password across multiple platforms or accounts, a social engineer may unlawfully access those accounts (Granger, 2001). Considering that many working from home user are online during the COVID-19 pandemic and are exchanging information with each other, it would create a pool of opportunities for cyber-criminals to harvest that information.

5. Socio-technical approaches

Social-technical approaches involve combining several approaches of social engineering. An attacker may wish to create a malware-infected media storage and place it in a location where the victim would most likely use it (Krombholz et al., 2015). A device like a USB stick may contain a malware like trojan (Stasiukonis, 2006) leading to the possibility of ransomware to be installed. Social engineers may wish to add labels such as “confidential” to lure victim to use the media storage (Krombholz et al., 2015).

4.2 Phishing

Phishing is an attack vector that can deceive the victim to install a ransomware. This attack vector requires the use of impersonation to gather usernames, passwords, and other credentials from their victims (Aburrous et al., 2010). Since there are many people working from home, cyber-criminals may choice to use phishing attacks to trick the victim to install ransomware. Depending on the circumstance and intention, the cyber-criminal may wish to use either email, spear, whaling, and smishing and vishing.

4.2.1 Types of phishing
1. Email phishing

Normally in a form of a spam message that claims to be from a legitimate organization. The spam email would most high likely have an
embedded link, which requires user to interact with the link, to redirect them to an unauthentic webpage (Almomani et al., 2013). Approximately, 80% of ransomware attacks are normally distributed via email phishing attacks (Solomon, 2019). Maze ransomware is an example of a ransomware that was deliver via phishing emails (Gendre, 2020).

2. Spear-phishing

Spear-phishing is very similar to email-phishing. However, this method is all about targeting a specific individual or organization (Amro, 2018). Ryuk ransomware is an example that was delivered via spear-phishing where it had targeted a single organization and had demanded a high ransom for data retrieval (Checkpoint, 2020).

3. Whaling-phishing

Whaling-phishing is designed to target high profile individuals. This method requires a large amount of time to gather information about target and may need to develop trust with them (Amro, 2018). Zeppelin ransomware is an example that was delivered via whaling-phishing (BlackBerry, 2019).

4. Smishing and vishing

Smishing and vishing does not use any form of emails phishing. But is heavily reliant on the user mobile phones devices. As such, smishing requires the cyber-criminals to forward a short messaging service (SMS) or text messages via phone to their victim. While vishing uses a phone call or voice mail to lure the victim into giving the attackers their personal information. Filecoder ransomware is an example where users interact with the link which install a malicious app that would be presented to the victim as an adult game simulator (Osborne, 2019).

4.3 Trojan

Trojan is a type of malware that can disguise itself as a legitimate software (Grace, 2020). The malware itself does require a medium so that it can infect the user’s computer. It can be accomplished when a user receives a phishing email believing that it is legitimate without realizing that they have accidentally downloaded the attachment. If the user decides to execute the file, the trojan malware can spread itself, affecting files and damaging one’s electronic device (Alison, 2020). As previously discussed in ransomware overview, AIDS trojan ransomware is an example as well as Trojan.Gpcoder and Trojan.Cryzip.

I. Social engineering, security, and cyber attacks
4.4 Remote desktop protocol

Remote Desktop Protocol is being able to remotely access an electronic device for the purpose of accessing the desktop, files, and other applications (Arntz, 2018). For working purposes, working from home user may require to remotely access another colleague’s electronic device to resume and commerce organizational duties. Due to the COVID-19 pandemic, cyber-criminals may disguise themselves as authentic IT support to have remote access to an individual electronic device. It is possible for cyber-criminals to use RDP to deliver Ryuk ransomware to the target electronic device (Checkpoint, 2020).

4.5 Drive-by download

Drive-by download is where the user’s unintentionally visits a perfectly disguise website that downloads a file or software on their electronic device without their consent (Cassetto, 2019). If a user were to interact with a phishing email link, it may redirect them to a malicious drive-by download webpage where they may unintentionally download ransomware. Bad rabbit ransomware was introduced in 2017 and spread via drive-by download where users had visited a genuine website without knowing that it was already compromised (Mamedov et al., 2017).

4.6 Malvertising

Malvertising disguises themselves as unauthentic online advertisement. It distributes malware and other forms of threat to user by installing a malicious code on the electronic device, then sends information to cyber-criminal command and control (C&C) servers (Lastline, 2018). Cyber-criminals may wish to install ransomware install onto the user’s electronic device. Sodinokibi Ransomware is an example that was deliver via malvertising (Trend Micro, 2019).

5 Existing defense mechanism and control gaps

Normally, defense mechanism is normally designed to mitigate against any cyber-risk. A control gap may occur only when there are very little to zero control measures that are in place. Without having proper controls in place or outlined, it may not be effective to prevent a risk from occurring (Knowledge Leader, 2019). There are mitigation techniques that can be effective against ransomware attacks. But mitigation against ransomware can only be effective if only the individuals and organization realize how precious their assets are and how protecting it is the first necessary step for
the organization. As such, there are times where an individual or organization information is compromised and this can be due to many reasons. But it is mainly due to not frequently practising cyber-security defense measures, understanding that the cyber-world is always changing, and to act accordingly to those changes.

Most of our information is stored digitally and it is quite easy to access them. For cyber-criminals to gain access to an organization information and infrastructure, they would usually interact or trick employees to give them information. It is important to realize that human do make errors as they are the weakest link within any organization (Bhayani, 2019). Especially, if they do not understand the consequences of cyber-attacks, how it can negatively impact their lives, and affect the reputation of the organization. Web content filtering, black and white listing, third-party consultation, intrusion detection system, and firewall are some examples of existing defense mechanism that can help detect and evade ransomware but may have controls gaps that can be challenging for working from home users.

5.1 Web content filtering (WCF)

WCF can be used to mitigate against ransomware attacks as it is designed to be embedded into a web-browsing application that is capable to screen active contents from webpages that user visited. The purpose is to see if the contents have codes that could potentially install and run a malicious payload onto the user’s electronic device. As such, suspicious webpages that runs and execute Java codes can possibly harm users’ electronic devices (Australian Cyber Security Centre, 2017) are filtered and blocked. However, WCF may block a website that is non-malicious which may irritate working from home users. They may need to apply the necessary changes to the filtering system so that they can access the exact website to resume working from home duties. In addition, there are approximately three to five million brand new websites that are introduced onto the internet each week which can be difficult to filter out the malicious and non-malicious contents. WCF can help working from home users to be safe from malicious websites but may prohibit the use of some websites which may be important for some to resume working from home duties.

5.2 Black and white listing

There are many ways for ransomware to be installed and executed onto the victim electronic device and organization may wish to obtain a black and white list. Blacklisting is a list of known suspicious but potentially
malicious Uniform Resource Locator (URL) (Sheng et al., 2009). Visiting a suspicious website may result ransomware being installed onto the victim or organization electronic devices. That is why it is helpful for organization to obtain a blacklist as they can identify which URL that can harm, damage, or access their information without their permission. However, this approach may not be effective to identify and detect vishing, and smishing attacks (Shahriar et al., 2015). In addition, the AV-TEST Institute have reported that over 3,50,000 malicious contents were introduced every day and may be difficult to track and black-list those contents (Bisawa, 2020).

Whitelisting is the reverse of blacklisting as it is about providing users websites that are trustworthy for them to access (Shahriar et al., 2015). It can be quite effective to detect potential smishing attacks (Mahmoud & Mahfouz, 2012). Due to new number of websites being introduced each week, keeping the white list up to date can be challenging, and may affect the operation for the organization (Bisawa, 2020). Black and white listing does present similar control gaps to WCF.

5.3 Third-party mitigation

Seeking professional consultation can be essential as the victim or organization may not know any mitigation or recovery technique that has occur from ransomware attacks (Shinde et al., 2016). This type of assistant can be important especially if the victim or organization does not know what type of ransomware that they had encountered. In addition, third-party consultation does provide a deep analysis of the current situation that the victim and organization are currently facing, such as the damage that was done by the ransomware. They may also provide to their victim and/or organization appropriate mitigation procedures that can control and prevent the situation from escalating or occurring again. However, as previously mentioned in ransomware attack vectors, social engineers may attempt to use reverse social engineering. As such, there is a possibility that the third-party entity may could be a social engineer themselves, leading them to have access to the organization network as well exploit other vulnerabilities (Infosec Resources, 2018).

5.4 Intrusion detection system

An intrusion detection system (IDS) is another existing defense mechanism that can detect potential ransomware attacks. It is a hardware appliance or software application that has the capabilities to screen the traffic that is moving through the individuals or organizations network.
Furthermore, IDS can also alert users when it has detected a suspicious action and other potential threats within the network that could harm the individual (Pratt, 2018). However, IDS would usually require experienced personnel to understand how to resolve the issue as the software application or hardware appliance is not designed to prevent the incident from happening on its own. Furthermore, it cannot process any encrypted packets which is a concern as cyber-criminals may surreptitiously pass the encrypted packets through the individuals or organizations network (Rapid7, 2017).

5.5 Firewall

Working from home users may wish to use firewall as a layer to prevent any potential ransomware attacks. It is a firmware or software that is designed to prevent any illegal access to an individual’s or organization’s network, inspect outgoing or incoming traffic, and identify and block potential threats (Rouse, 2020). However, firewall cannot protect users from opening or interacting with potential phishing emails (Cockerham, 2018) which may lead them to intentionally install ransomware.

The five existing defense mechanisms can be used in a working from home environment. However, it does have potential control gaps that can be challenging for working from home users as they may lack the understanding that each existing defense mechanism may have its own limitation. Therefore, it is extremely practical to have a cyber-awareness training model for employees to practice and to be aware that frequent practices would strengthen the weakest link that are presented in within the organization.

6 Mitigation model against ransomware

To avoid the possibilities of cyber-criminals installing ransomware onto the victim’s electronic devices, this section would discuss how to mitigate against the six attack vectors. To have a successful outcome, it is important for the IT department to explain and demonstrate to working from home users the concept of each attack vector, how to appropriately respond to each of them, and how to implement the mitigation model against each of the attack vectors. Refer to Fig. 1 for the general flowchart for how to implement the model to teach Working from Home (WFH) users to mitigate against the six attacks.
6.1 Recommended mitigation against social engineering

To avoid being a victim of social engineering attacks, one must realize that their information is the most valuable assets. Protecting the physical and digital security are the steps that employees must take to avoid being a victim of social engineering. It is important for all members within an organization to know that the likelihood of being a victim of a social engineer attack is possible. As such, implementing a strong physical security will build a strong physical structure that would prevent social engineer from obtaining personal and sensitive information from the victim.

1. Do not touch anything suspicious or unknown

As such, working from home users must understand that they should not touch or use anything that does not belong to them as it may contain malware. Saleem and Hammoudeh (2018) explains that one must not plug-in any unknown or suspicious USB or other electronic devices. They must forward the unknown electronic device to their respective IT department so that they can analyze it.

2. Shredding documents

If there was a decision where the employee was instructed to throw away the physical copies into a recycling bin, the chance of a dumpster diver obtaining that information could happen. If it is necessary to throw away the physical copies, employee must use a paper shredder. The purpose of shredding one’s documents is to protect against identify theft, produce high confidence from customer, and prevent any possible privacy losses (Data Safe, 2019) such as user’s device specification.

3. Other required physical protection

Other ways to strengthen the physical security is to report any suspicious activities as well as to install a CCTV surveillance for the purpose of monitoring one’s working environment (Saleem & Hammoudeh, 2018). In the case for physical approach of social engineering, the aspects of having physical security will reduce the likelihood of being a potential victim of social engineering. However, it is evenly as important for organization to strengthen the digital security aspect as well.

4. Digital protection

Most of the information that are stored in an organization would be stored digitally. This can provide employees the capability and convenience to work remotely (Rivera, 2019). However, despite the convenience of having information ready to be access remotely, working from home user must implement a strong digital security to protect one’s information. Saleem and Hammoudeh (2018) suggest that having antimalware, spam
protection guard, and firewall are examples of digital security which can be effective against social engineering which can be implemented within a home environment. Also, employees are encouraged to use passphrase instead of passwords so that it is complex for cyber-criminals to hack but at the same time easy for the user to remember (Australian Cyber Security Centre, 2020b).

### 6.1.1 How to implement “Recommended mitigation against social engineering”

Referencing the stages from Fig. 2, Table 1 provides a snapshot of how the IT department can implement the “Recommended mitigation against social engineering” as well as how to help and educate WFH user how to mitigate against social engineering attacks.

By implementing the above recommendation from Table 1, it would greatly benefit working from home users and organizations. As such, this implementation is there to help them to understand the dangers as well as prepared them to mitigate against social engineering attacks.

**FIG. 2** Implementation flow chart to teach working from home (WFH) users.
Social engineers may wish to use other tactics to gain personal/sensitive information from their victims. The most common method that social engineer would use is to send out many emails to potential victims to obtain their private information. In this case, it is known as phishing where its purpose is to obtain the victims usernames, passwords, and other credentials (Aburrous et al., 2010). As such, it is important that

### TABLE 1  Implementing “Recommended mitigation against social engineering” to WFH users.

| Stages | Description |
|--------|-------------|
| Stage 1 | The IT department are required to organize a short online module with quizzes and answers to teach working from home users about social engineering attacks and its potential to spread ransomware |
| Stage 2 | All working from home users are required to complete the short modules with quizzes and answers before moving to stage 3 |
| Stage 3 | Using any online face-to-face medium, the IT department are required to personally teach working from home users about the concept of social engineering. Repeat if working from home users have not yet understand the concept of social engineering |
| Stage 4 | Using any online face-to-face medium, the IT department must demonstrate how to respond appropriately to potential social engineering attacks. For instance, the IT may say that if you are asked to give your username and password to suspicious sources, one must be able to deny it request. Repeat if working from home users have not understood how to respond appropriately to social engineering attacks |
| Stage 5 | Using any online face-to-face medium, the IT department are required to go through all the “Best practices against social engineering” with working from home users. For instance, IT may show to working from home user how to correctly install a prescribe antimalware and how to update it regularly. Repeat if working from home user have not understood how to appropriately apply the security control measures from “Best practices against social engineering” |
| Stage 6 | At this stage, working from home user would now have a strong comprehension about the concept of social engineering, how to appropriately respond to it, and how to appropriately apply the security controls measures from “Best practices against social engineering” |
| Stage 7 | Every 6 months, the IT department must go through stage 2 with working from home users to ensure that they are up to date with their skills. Stage 3, 4 and 5 are other optional stages working from home user may wish to go through again to help rejuvenate their training |
| Stage 8 | In the future, an organization may recruit new working from home users. The IT department are required to go through stage 2–7 with the new working from home users |

### 6.2 Phishing drill simulation

Social engineers may wish to use other tactics to gain personal/sensitive information from their victims. The most common method that social engineer would use is to send out many emails to potential victims to obtain their private information. In this case, it is known as phishing where its purpose is to obtain the victims usernames, passwords, and other credentials (Aburrous et al., 2010). As such, it is important that
individuals who are working from home understand the consequences of phishing emails and how it can potentially affect their personal lives and the reputation of the organization as well. To prevent such event from happening, it is advisable that the organization IT department organize a phishing drill simulation to mitigate against phishing attacks.

The phishing drill simulation should be created and run by the IT departments of the organization. The purpose of this phishing mitigation drill is to educate everyone in the organization about the dangers of phishing attacks and to help prepare them against ransomware attacks via phishing. This would require working from home user to be exposed to examples of phishing emails, that are not intended to be maliciously dangerous but rather asking them to identify the real and phishing emails (Scarfone et al., 2008). Hence, the phishing mitigation drills should be implemented into the awareness and training program to help enhance working from home user to react and recognize malicious email addresses, links, and attachments (Sittig & Singh, 2016).

6.2.1 How to implement “Phishing Drill Simulation”

Referencing the stages from Fig. 2, Table 2 provides a snapshot of how the IT department can implement the “Phishing Drill Simulation” as well as help and educate WFH user how to mitigate against phishing attacks.

The above-recommended implementation from Table 2 would greatly benefit working from home users and organizations. It is to help them to understand the dangers as well as prepared them to mitigate against phishing attacks.

6.3 Secure remote desktop protocol

It is important to configure an individual’s remote desktop protocol to prevent cyber-criminals having the opportunity to access one’s electronic device. In doing so, would also avoid the possibilities of ransomware being installed (Whitney, 2019). In order to prevent one’s remote desktop protocol being exposed to cyber-criminals, users must follow the recommend outline plan.

1. Change RDP Port

Change port 3389 to another port is a necessary step (Cobb, 2020). This would provide the reassurance that users would not appear on a list of possible attacks (Arntz, 2018).

2. Restrict and limit access

To prevent any of the consequences from remote desktop attacks, it is important to only allow remote desktop port to be access by trusted parties
only and by doing so would prevent any unnecessary malicious attempts (Cobb, 2020). For windows 10 platform, to create a user group for the purpose of remote access, the user may wish to proceed to do the following:

1. Navigate to the “setting” application
2. Go to “system” and select “Remote Desktop”
3. Select “Select users that can remotely access this PC”
4. Then the user will see a “Remote Desktop Users” dialog window box
5. Click the “add” button, then click onto “Advanced” button

### TABLE 2
Implementing “Phishing Drill Simulation” to WFH users.

| Stages | Description |
| --- | --- |
| Stage 1 | The IT department are required to organize a short online module with quizzes and answers to teach working from home users about phishing attacks and its potential to spread ransomware |
| Stage 2 | All working from home users are required to complete the short modules with quizzes and answers before moving to stage 3 |
| Stage 3 | Using any online face-to-face medium, the IT department are required to personally teach working from home users about the concept of phishing. Repeat if working from home users have not yet understand the concept of phishing |
| Stage 4 | Using any online face-to-face medium, the IT department must now demonstrate how to respond appropriately to potential phishing emails. For instance, the IT may say if there is anyone who were to encounter a phishing email, one must not interact with the contents within the email. Repeat if working from home users have not understood how to respond appropriately to phishing emails |
| Stage 5 | Using any online face-to-face medium, the IT department are required to go through the “phishing drill simulation” with working from home users. For instance, IT must show at least 10 real emails and 10 fake phishing emails to working from home users. All working from home users are required to identify and explain with reason which email is real and phishing. Repeat if working from home user were not able to correctly identify a real and phishing email from the “phishing drills simulation” |
| Stage 6 | At this stage, working from home user would now have a strong comprehension about the concept of phishing attacks, how to appropriately respond to it, and how to identify real and phishing emails from the “phishing drill simulation” |
| Stage 7 | Every 6 months, the IT department must go through stage 2 with working from home users to ensure that they are up to date with their skills. Stage 3, 4 and 5 are other optional stages working from home user may wish to go through again to help retrain themselves |
| Stage 8 | In the future, an organization may recruit new working from home users. The IT department are required to go through stage 2–7 with the new working from home users |

3. Working from home users at risk of the COVID-19 ransomware
6. Click “Find now” and select the user you wish to have access to the “Remote Desktop Users” group. After that click “Ok”

7. Then click “OK” (Admin, 2019)

3. Use VPN and principle of least privilege

   Due to the number of employees working from home, using Remote Desktop may be necessary. An organization must highly consider using a VPN to not only enable remote access but would not expose the organization electronic device to the internet. In addition, it is very important to only ensure those employees can have access to Remote Desktop but at the same time only grant certain permission that are required for them to complete their work (Cobb, 2020).

4. Up to date software and patches

   Cyber-criminals tend to exploit vulnerabilities from outdated software. Working from home users must have the latest updates so that they can have an up-to-date version for both server and client software (Cobb, 2020).

5. Strong passphrase

   It is recommended to implement two-factor authentication and strong password when using RDP (Cobb, 2020). In addition, passphrase is normally a lot better than passwords as they are unique, complex, and longer phrases, and quite easy to remember (Australian Cyber Security Centre, 2020b). Diceware was created by Arnold Reinhold, IT guru, which was developed to generate a passphrase for users from a list of 7776 words where each corresponding phrase would have a 5-digit number next to it (Lemonnier & Latto, 2020). The user would have to:

1. Install Diceware: can be open in a text editor application.
2. Users must roll a die at least 5 times or roll 5 dice all at once and placed the number in order that it was generated.
3. Search for the 5-digit number in the list that match the number you have rolled.
4. Repeat the process again at least 9 times to generate 9 unique word paraphrase.
5. Memorize the new paraphrase (Reinhold, 2020).

   Users should be advised that they must also include capitals, symbols, and numbers into the paraphrase so that it would increase security. But it is not recommended to use the same paraphrase across different service as if one account get compromised than other account that the user is using would also get compromised (Lemonnier & Latto, 2020).
6.3.1 How to implement “Secure Remote Desktop Protocol”

Referencing the stages from Fig. 2, Table 3 provides a snapshot of how the IT department can implement the “Secure Remote Desktop Protocol” as well as help and educate WFH user how to mitigate against remote desktop protocol attacks.

The above-recommended implementation from Table 3 would greatly benefit working from home users and organizations as it helps them understand the dangers as well as how to mitigate against remote desktop protocol attacks.

| Stages | Description |
|--------|-------------|
| Stage 1 | The IT department is required to organize a short online module with quizzes and answers to teach working from home users about remote desktop protocol attacks and its potential to spread ransomware |
| Stage 2 | All working from home users are required to complete the short modules with quizzes and answers before moving to stage 3 |
| Stage 3 | Using any online face-to-face medium, the IT department are required to personally teach working from home users about the concept of remote desktop protocol. Repeat if working from home users have not yet understand the concept of Remote Desktop Protocol |
| Stage 4 | Using any online face-to-face medium, the IT department must now demonstrate how to respond appropriately to potential remote desktop protocol attacks. For instance, the IT may say that if a suspicious source asks the working from home user to change their port number to 3389 where one should not comply with the demand. Repeat if working from home users have not understood how to respond appropriately to potential remote desktop protocol attacks |
| Stage 5 | Using any online face-to-face medium, the IT department are required to go through all the “Secure Remote Desktop Protocol” with working from home users. For instance, IT may show to working from home user how to correctly use Diceware to generate their new passphrase. Repeat if working from home user have not understood how to appropriately apply the security measures from “Secure Remote Desktop Protocol” |
| Stage 6 | At this stage, working from home user would now have a strong comprehension about the concept of remote desktop protocol, how to appropriately respond to it, and how to appropriately apply the security measures from “Secure Remote Desktop Protocol” |
| Stage 7 | Every 6 months, the IT department must go through stage 2 with working from home users to ensure that they are up to date with their skills. Stage 3, 4 and 5 are other optional stages working from home user may wish to go through again to help retrain themselves |
| Stage 8 | In the future, an organization may recruit new working from home users. The IT department is required to go through stage 2–7 with the new working from home users |
6.4 Closed gate approach to Trojan

Trojan is a type of malware that can disguised themselves as legitimate software (Grace, 2020). Once they are in the user's electronic device, they may not know its existents. This type of malware has the capabilities to record things on the victim electronic device and send back information to the cyber-criminals (Anderson, 2019). In this case, trojan can act as an installer for ransomware. To avoid this, users are encouraged to follow the recommendation below.

1. Up to date software and patches

To avoid cyber-criminals exploiting vulnerabilities that are found from outdate patches, it is recommended that users have the latest update for their operating systems, software, and browser (Anderson, 2019).

2. Firewall

It is recommended to have configure one’s firewall to control incoming malicious internet traffic and prevent the possibility of Trojans being installed onto the user’s electronic device (Anderson, 2019). It was discussed that firewall would have its own unique control gaps. However, the IT department would be responsible to teach working from home users to understand function of a firewall and how to manually detect a possible trojan.

3. Antimalware

Antimalware is to ensure that one has not installed Trojan onto one’s electronic device and to scan other programs and files to see if they are safe to execute. It is important to have the latest patches for antimalware (Anderson, 2019).

4. Never open suspicious attachments, or install and execute them

It is recommended to never interact with suspicious emails and their attachments as the user may unintentionally download Trojan (Anderson, 2019). This also applies for installing and running programs that comes from vague and suspicious sources. Always double check the sources before interacting with them.

6.4.1 How to implement “Closed Gate approach to Trojan”

Referencing the stages from Fig. 2, Table 4 provides a snapshot of how the IT department can implement the “Closed Gate Approach to Trojan” as well as help and educate WFH user how to mitigate against trojan attacks.
TABLE 4 Implementing “Closed Gate approach to Trojan” to WFH users.

| Stages  | Description                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Stage 1 | The IT department is required to organize a short online module with quizzes and answers to teach working from home users about trojan attacks and its potential to spread ransomware |
| Stage 2 | All working from home users are required to complete the short modules with quizzes and answers before moving to stage 3                             |
| Stage 3 | Using any online face-to-face medium, the IT department are required to personal teach working from home users about the concept of trojan. Repeat if working from home users have not yet understand the concept of trojan |
| Stage 4 | Using any online face-to-face medium, the IT department must now demonstrate how to respond appropriately to potential trojan attacks. For instance, IT may say that if a suspicious source asks the working from home user to open and install the program from the email, one must not comply with the demand. Repeat if working from home users have not understood how to respond appropriately to potential trojan attacks |
| Stage 5 | Using any online face-to-face medium, the IT department are required to go through all the “Never Open the Gate for Trojan” with working from home users. For instance, IT may show to working from home user how to correctly configurate one’s firewall to prevent the possibility of trojans being installed onto the electronic device. Repeat if working from home user have not understood how to appropriately apply the security measures from “Never Open the Gate for Trojan” |
| Stage 6 | At this stage, working from home user would now have a strong comprehension about the concept of trojan, how to appropriately respond to it, and how to use and appropriately apply the security measures from “Never Open the Gate for Trojan” |
| Stage 7 | Every 6 months, the IT department must go through stage 2 with working from home users to ensure that they are up to date with their skills. Stage 3, 4 and 5 are other optional stages working from home user may wish to go through again to help retrain themselves |
| Stage 8 | In the future, an organization may recruit new working from home users. The IT department are required to go through stage 2-7 with the new working from home users |

The above-recommended implementation from Table 4 would greatly benefit working from home users and organizations as it helps them to understand the dangers as well as how to mitigate against trojan attacks.

6.5 Drive-by downloads controls

It is important for users must be aware that ransomware that can be spread via drive-by downloads. There are times where it can be quite difficult to pick up as its purpose is to surreptitiously download itself onto
the user’s electronic device. To avoid any unnecessary frustration and consequences of being victimize by ransomware, it is recommended to do the following:

1. **Up to date software and patches**
   
   Is important to have an up-to-date software to avoid cyber-criminals exploiting vulnerabilities from users (Levinson, 2012) as well as keeping other application regularly updated.

2. **Web-filtering**
   
   Web filtering software can prevent users from going into compromised websites as they have built-in mechanism that can detect and determine if a user has come across an unsafe website (Levinson, 2012). Web filtering does have its own unique limitation. It is important for the IT department to teach working from home users to understand function as well as how to manually detect a potential drive-by download page.

3. **Disable java**
   
   Within the user’s PDF reader preference list, it is important that users disable JavaScript and for IT departments to remove any Java that are in their systems (Levinson, 2012).

4. **BLADE—Block all drive-by download exploits**
   
   BLADE, developed by SRI International and Georgia Tech, is a windows immunization system that can block drive-by download from occurring and infecting the user’s systems (Levinson, 2012).

**6.5.1 How to implement “Drive-by Downloads Controls”**

As seen in the stages in Fig. 2, Table 5 provides a snapshot of how the IT department can implement the “Drive-by Downloads Controls” as well as help and educate WFH user how to mitigate against drive-by download attacks.

The above recommended implementation from Table 5 would greatly benefit working from home users and organizations as it helps them to understand the dangers as well as how to mitigate against drive-by download attacks.

**6.6 Malvertising interaction controls**

Malvertising disguises themselves as legitimate advertisement on a website. This attack vector is like drive-by download but requires the user to interact with the malicious advertisement. Once a user interacts with a
malicious advertisement, it can surreptitiously install a ransomware into victim’s electronic device. To prevent this from happening, users must follow the below recommendation:

1. **Up to date software and patches**

It is important that users realize that they should remove vulnerabilities that are in their electronic devices. This can be as simple as updating one’s application, operating systems, and web browser. In addition, users must

| Stages | Description |
|--------|-------------|
| Stage 1 | The IT department is required to organize a short online module with quizzes and answers to teach working from home users about drive-by download attacks and its potential to spread ransomware |
| Stage 2 | All working from home users are required to complete the short modules with quizzes and answers before moving to stage 3 |
| Stage 3 | Using any online face-to-face medium, the IT department are required to personal teach working from home users about the concept of drive-by download. Repeat if working from home users have not yet understand the concept of drive-by download |
| Stage 4 | Using any online face-to-face medium, the IT department must now demonstrate how to respond appropriately to potential drive-by download attacks. For instance, IT may say that a phishing email may have an embedded suspicious link which could lead them to a drive-by download page and one must not press on. Repeat if working from home users have not understood how to respond appropriately to potential drive-by download attacks |
| Stage 5 | Using any online face-to-face medium, the IT department is required to go through all the “Do not Drive-by download” with working from home users. For instance, IT may show to working from home user how to correctly use and install Web filtering software. Repeat if working from home user have not understood how to appropriately apply the security measures from “Do not Drive-by download” |
| Stage 6 | At this stage, working from home user would now have a strong comprehension about the concept of drive-by download, how to appropriately respond to it, and how to use and appropriately apply the security measures from “Do not Drive-by download” |
| Stage 7 | Every 6 months, the IT department must go through stage 2 with working from home users to ensure that they are up to date with their skills. Stage 3, 4 and 5 are other optional stages working from home user may wish to go through again to help retrain themselves |
| Stage 8 | In the future, an organization may recruit new working from home users. The IT department are required to go through stage 2–7 with the new working from home users |

TABLE 5 Implementing “Drive-by downloads controls” to WFH users.
also remove any flash or java software that they do not usually to prevent being exploited by malvertising (Lake, 2020).

2. Safe practice—Think and look before clicking

In general, users must be cautions when interacting and clicking onto anything on the internet. As such, it is recommended that users should never interact with pop-up advertisement, vague notices, or any suspicious advertisement. In doing so would lower one’s chance of being victimize by ransomware (Panda Security, 2019).

3. Ad blockers

Ad blockers are design to filter any malicious advertisement that the user may encounter. Its main function is to protect individuals from clicking and viewing malicious advertisement. Furthermore, ad blocker can reduce cookies number being saved onto the electronic device, protect individual’s privacy, and load webpages faster (Panda Security, 2019).

4. Antimalware

It is still recommended for users to have antimalware install onto their electronic device so that the security software can scan one’s systems for potential malware or to perform regular check-ups (Panda Security, 2019).

6.6.1 How to implement “Malvertising Interaction Controls”

Based on stages shown in Fig. 2, Table 6 provides a snapshot of how the IT department can implement the “Malvertising Interaction Controls” as well as help and educate WFH user how to mitigate against malvertising attacks.

The above-recommended implementation from Table 6 would greatly benefit working from home users and organizations as it helps them to understand the dangers as well as how to mitigate against malicious advertisement attacks.

The mitigation model against ransomware attacks would provide working from home user and organization the necessary training and understanding to avoid a devastating ransomware attack. However, it is important to always frequently backup their data. Not only it can help assist with the restoration process but can help avoid business disruption and for the organization to continue working uninterrupted (Australian Cyber Security Centre, 2020a). In addition, this would also prevent the possibility that the target paying the demanded ransom as well. There are different types of data backup methods that working from home users and organizations can choose to implement. Full, differential, and incremental are examples of data backup strategies that can be used within any working environment.
TABLE 6  Implementing “Malvertising Interaction Controls” to WFH users.

| Stages | Description |
|--------|-------------|
| Stage 1 | The IT department is required to organize a short online module with quizzes and answers to teach working from home users about malvertising attacks and its potential to spread ransomware |
| Stage 2 | All working from home users are required to complete the short modules with quizzes and answers before moving to stage 3 |
| Stage 3 | Using any online face-to-face medium, the IT department are required to personal teach working from home users about the concept of malvertising. Repeat if working from home users have not yet understand the concept of drive-by download |
| Stage 4 | Using any online face-to-face medium, the IT department must now demonstrate how to respond appropriately to potential drive-by download attacks. For instance, IT may say that one should never interact with pop-up advertisement, vague notices, or any suspicious advertisement. Repeat if working from home users have not understood how to respond appropriately to potential malvertising attacks |
| Stage 5 | Using any online face-to-face medium, the IT department are required to go through all the “Never interact with any Malvertising” with working from home users. For instance, IT may show to working from home user how to correctly use and install Ad blockers. Repeat if working from home user have not understood how to appropriately apply the security measures from “Never interact with any Malvertising” |
| Stage 6 | At this stage, working from home user would now have a strong comprehension about the concept of malvertising, how to appropriately respond to it, and how to use and appropriate apply the security measures from “Never interact with any Malvertising” |
| Stage 7 | Every 6 months, the IT department must go through stage 2 with working from home users to ensure that they are up to date with their skills. Stage 3, 4 and 5 are other optional stages working from home user may wish to go through again to help retrain themselves |
| Stage 8 | In the future, an organization may recruit new working from home users. The IT department are required to go through stage 2–7 with the new working from home users |

7 Regular and consistent data backup

7.1 Full back up

The first type that working from home user or organization may wish to implement is a full back up plan. This type would usually resolve around backing up all data that is on the system and this includes all hard copies data. Implementing full backup does allow the user to easily find files but can consume a lot of time to perform this type of backup (HP Invent, 2017).
An organization may have terabytes worth of data to backup which can devour a lot of drive to backup as well as being very time consuming. On the other hand, full back up can be used by working from home users as they do not usually have huge amount of data to backup.

7.2 Differential back up

The second type is a differential back up where it only stores data that have undergone changes since its previous full back up. Compare to performing a full back up, it does not consume a lot of time. It can be performed daily which would produce the most up to date data sets that can be restore for future use. Differential back up can take a lot of capacity to be stored but as long as it can be managed onto one media device, it should not impose any problems for the users (HP Invent, 2017).

7.3 Incremental back up

The incremental backup would require storing all files which has undergone certain changes since its previous backup. This would take up less storage space in the media device as it stores files that have change or been created since its prior backup. However, the restoration process is complex as it requires multiple drives to restore the data (HP Invent, 2017) which may cause the process to be slow.

It is important for working from home users and organizations to develop a habit to secure and back up their data. The three back up methods can be use in any circumstances. However, it is encouraged for working from home user and organization to use a full back up method as it ensures that all files have at least a one back up for the restoration process. The process to restore the full back up can be time consuming. However, in the event of a ransomware attack, a full back up ensures working from home users and organizations data is safe and can resume studying and working duties.

8 Conclusion

During the COVID-19 pandemic, the cyberspace has become a necessary dimension for users to communicate and connect with others. However, it is a period where many would find themselves to be in a position of hardship as many would be working and interacting with others from the comfort of their own home via their unique electronic devices. The electronic devices that working from home user are using would have sensitive and personal information on it. During the COVID-19 pandemic,
connecting to the internet is a requirement but due to the influx of online users, there is will many cyber-criminals who would choose to exploit other during the COVID-19 pandemic. As such, many working from home user would enter the cyberspace without realizing that there may be vulnerabilities within their own home environment which can be a cybersecurity concern. Due to the sudden change to work from home, many would not have realized that strengthen their security measures is the key to prevent cyber-criminals from exploiting their vulnerabilities.

By strengthen one’s home environment, it would have prevented many cyber-criminals from launching malicious attack during the COVID-19 pandemic. Ransomware has become a lucrative choice for cyber-criminal to use as it is malicious software that can infect and prevent a working from home user’s from accessing their data. Furthermore, there are working from home users that are susceptible to the ransomware attack because their electronic devices do have sensitive information can be used against them. Using powerful encryption, cyber-criminals would hold onto working from home user’s data until they pay them the demand ransom. Ransomware was a popular choice for cyber-criminals to use as there are many online users that can be extorted during the COVID-19 pandemic. This in turn would produce many challenges for working from home users.

Working from home would produce many challenges against ransomware. Some of these challenges may include that many were not able to identify genuine sources which may have led to the installation of a ransomware. Mobile phone users may be target for ransomware attacks as there are very little mitigation measures for hand-held devices. Ransomware has evolved to a point where it has strong encryption to prevent the user from accessing their data. Malwares have evolved over the years which has led to more digital extortion where organization has come a desirable choice to be targeted by cyber-criminals. Many individuals working from home users may have to face the difficult decision to pay the ransom to regain access to their data. For ransomware to be installed correctly, cyber-criminals must use an attack vectors to deliver it to the target.

The dangerous malware is reliant upon the delivery of the six attack vectors which are social engineering, phishing, trojan, remote desktop protocol, drive-by download, and malvertising. Without having a strong security measures against ransomware, many working from home user would face the possibility of digital extortion from cyber-criminals. There are existing defense mechanisms that can mitigate ransomware attacks but has its own control gaps. However, organization’s IT department would be responsible to cyber-train their employees to protect their assets and reputation. The mitigation model against ransomware is developed to assist working from home user to mitigate against potential ransomware

I. Social engineering, security, and cyber attacks
attacks. In addition, individuals and organization must continue to back up their data to ease disruption. However, future work must focus on education around danger of ransomware and how to mitigate it.

Since ransomware attacks have increased over the years it has led to more victims being extorted by cyber-criminals. As such, it is recommended that future work must start to focus more on teaching and educating working from home users about the dangers of ransomware attacks and how to mitigate such an event from occurring. Future work may also implement a ransomware mitigation program into secondary school and tertiary education which would also further cyber-enhance future generation to be prepared for potential ransomware attacks. In doing so, it would encourage more people to actively protect their data as well as produce an outcome where many cyber-users understand the concept of ransomware and would hopefully strengthen future generation from any potential cyber-attacks, especially during the COVID-19 pandemic.

The COVID-19 pandemic has opened more doors for online user to enter the cyberspace. But will contain a haven of cyber-criminals who would see this as an opportunity to hurt others. During the COVID-19 pandemic or other similar circumstance, one must be able to strengthen their security control measures as well as to prepare themselves that they could be a possible victim of any ransomware attacks.

References

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Predicting phishing websites using classification mining techniques with experimental case studies. In 2010 seventh international conference on information technology: New generations (pp. 176–181). IEEE.

Admin. (2019). Add user to remote desktop users group in windows 10. Top Password Software. Retrieved October 9, 2020, from https://www.top-password.com/blog/add-user-to-remote-desktop-users-group-in-windows-10/.

Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5), 10–16.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376.

Alison, G. (2020). What is a Trojan? Is it a virus or is it malware?. Norton. Retrieved October 9, 2020 https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html.

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. IEEE Communication Surveys and Tutorials, 15(4), 2070–2090.

Amro, B. (2018). Phishing techniques in mobile devices. arXiv. preprint arXiv:1802.04501.

Anderson, S. (2019). How to defend your PC and devices against a Trojan Horse virus. Safety Detectives. Retrieved October 20, 2020 from https://www.safetydetectives.com/blog/what-is-a-trojan-horse-and-how-to-protect-against-it/.

I. Social engineering, security, and cyber attacks
I. Social engineering, security, and cyber attacks
Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in Computer Virology, 6*(1), 77–90.

Gendre, A. (2020). Ransomware examples: Recent attacks and distribution methods. Vade Secure. Retrieved October 9, 2020, from https://www.vadesecure.com/en/ransomware-examples-recent-attacks-and-distribution-methods/.

Ghosh, A. M., Halder, D., & Hossain, S. A. (2016). Remote health monitoring system through IoT. In *2016 5th international conference on informatics, electronics and vision (ICIEV)* (pp. 921–926). IEEE.

Grace, A. (2020). *What is a Trojan? Is it a virus or is it malware?*. Norton. Retrieved October 20, 2020 from https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html.

Granger, S. (2001). *Social engineering fundamentals, part I: Hacker tactics*. SecurityFocus.

HP Invent. (2017). *The importance of protecting your data*. Retrieved October 2020, 20 from https://myconsole.com.au/wp-content/uploads/2017/04/hp_why_backup.pdf.

Infosec Resources. (2018). *The advantages & disadvantages of outsourcing incident response*. Retrieved on October 22, 2020, from https://resources.infosecinstitute.com/advantages-disadvantages-outsourcing-incident-response/#gref.

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501.

Johansen, A. G. (2019). *What is ransomware and how to help prevent ransomware attacks*. Norton. Retrieved October 9, 2020, from https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html.

Knowledge Leader. (2019). *Control gap remediation methodology training guide*. Retrieved October 9, 2020, from https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/gucontrolgapremediationmethodologytrainingpresentation.

KPMG. (2020). *The rise of ransomware during COVID-19*. Retrieved October 9, 2020, from https://home.kpmg/au/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122.

Lake, J. (2020). *What is malvertising and how can you defend against it?*. Comparitech. Retrieved October 20, 2020 from https://www.comparitech.com/blog/information-security/malvertising/.

Lastline. (2018). *Malvertising: What you need to know*. Retrieved October 20, 2020 from https://www.lastline.com/blog/how-malvertising-works-what-you-need-to-know/.

Lemonnier, J., & Latto, N. (2020). *Oops!.. I think I scanned a malware*. arXiv preprint arXiv:1703.07751.

Levinson, M. (2012). *6 ways to defend against drive-by downloads*. CIO. Retrieved October 9, 2020, from https://www.cio.com/article/2448967/6-ways-to-defend-against-drive-by-downloads.html.

Mahmoud, T. M., & Mahfouz, A. M. (2012). SMS spam filtering technique based on artificial immune system. *International Journal of Computer Science Issues (IJCSI), 9*(2), 589.

Mamedov, O., Sinitsyn, F., & Ivanov, A. (2017). *Bad Rabbit ransomware*. SecureList. Retrieved October 20, 2020 from https://securelist.com/bad-rabbit-ransomware/82851/.

Nassi, B., Shamir, A., & Elovici, Y. (2017). *Oops!. I think I scanned a malware*. arXiv preprint arXiv:1703.07751.

Nebehay, S. (2020). *WHO says it no longer uses `pandemic` category, but virus still emergency*. Reuters. Retrieved October 9, 2020, from https://www.reuters.com/article/uk-china-health-who-idUKKCN20I0PD.

Newby, T. G., & Razmazma, A. (2016). *An untraceable currency? Bitcoin Privacy Concerns*. Fintech Weekly. https://www.fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns.

I. Social engineering, security, and cyber attacks
NortonLifeLock Employee. (2019). *Internet of Things (IoT) security: 9 ways you can help protect yourself*. Norton. Retrieved October 9, 2020 from https://us.norton.com/internetsecurity-IOTsecuring-the-internet-of-things.html.

Osborne, C. (2019). *This new Android ransomware infects you through SMS messages*. ZDNet. Retrieved October 9, 2020, from https://www.zdnet.com/article/this-new-android-ransomware-infects-you-through-sms-messages/.

Panda Security. (2019). *Malvertising: What it is and how to protect yourself*. Retrieved October 20, 2020 from https://www.pandasecurity.com/en/mediacentre/malware/malvertising/.

Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2013). Context aware computing for the internet of things: A survey. *IEEE Communication Surveys and Tutorials, 16*(1), 414–454.

Popoola, S. I., Ojewande, S. O., Sweetwilliams, F. O., John, S. N., & Atayero, A. A. (2017). *Ransomware: Current trend, challenges, and research directions*. San Francisco, USA: World Congress on Engineering and Computer Science.

Pratt, M. K. (2018). *What is an intrusion detection system? How an IDS spots threats*. CSO. Retrieved October 22, 2020 from https://www.csoonline.com/article/3255632/what-is-an-intrusion-detection-system-how-an-ids-spots-threats.html.

Qin, T., & Burgoon, J. (2007). An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *Intelligence and security informatics, 2007* (pp. 152–159). IEEE.

Rapid7. (2017). *The pros & cons of intrusion detection systems*. Retrieved October 22, 2020 from https://blog.rapid7.com/2017/01/11/the-pros-cons-of-intrusion-detection-systems/.

Rosenberg, J. M. (2015). *A Q&A about the malicious software known as ransomware*. Retrieved October 10, 2020, from https://phys.org/pdf347719229.pdf.

Rouse, M. (2020). *Firewall*. Search Security. Retrieved October 22, 2020 from https://searchsecurity.techtarget.com/definition/firewall.

Saleem, J., & Hammoudeh, M. (2018). Defense methods against social engineering attacks. In *Computer and network security essentials* (pp. 603–618). Cham: Springer.

Sanduleac, M., Chimirel, C. L., Eremia, M., Toma, L., Cristian, C., & Stanescu, D. (2016). Unleashing Smart Cities efficient and sustainable energy policies with IoT based unbundled smart meters. In *2016 IEEE international conference on emerging technologies and innovative business practices for the transformation of societies (EmergiTech)* (pp. 112–117). IEEE.

Savage, K., Coogan, P., & Lau, H. (2015). The evolution of ransomware. Mountain View CA: Symantec Corporation.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. *NIST Special Publication, 800*(115), 2–25.

Segura, J. (2016). *Citadel: A cyber-criminal’s ultimate weapon?*. Malwarebytes. Retrieved October 9, 2020, from https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/.

Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security, 6*(3), 206.

Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J., & Zhang, C. (2009). *An empirical analysis of phishing blacklists*. CEAS.

---

I. Social engineering, security, and cyber attacks
Shinde, R., Van der Veeken, P., Van Schooten, S., & van den Berg, J. (2016). Ransomware: Studying transfer and mitigation. In 2016 international conference on computing, analytics and security trends (CAST) (pp. 90–95). IEEE.

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied Clinical Informatics, 7(2), 624.

Sjouwerman, S. (2015). A short history & evolution of Ransomware. Retrieved October 9, 2020, from https://www.knowbe4.com/ransomware#ransomwretimeline.

Skybox Security. (2020). COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%. Retrieved October 9, 2020, from https://www.skyboxsecurity.com/news/covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50/.

Solomon, H. (2019). Ransomware now stealing data, warns Ontario cybercop. IT World Canada. Retrieved October 9, 2020, from https://www.itworldcanada.com/article/ransomware-now-stealing-data-warns-ontario-cybercop/423168.

Sjouwerman, S. (2015). A short history & evolution of Ransomware. Retrieved October 9, 2020, from https://www.knowbe4.com/ransomware#ransomwretimeline.

I. Social engineering, security, and cyber attacks

Zetter, K. (2015). Hacker lexicon: A guide to Ransomware, the scary hack that’s on the rise. Wired. https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/.